COM(2023) 208 final

ASSEMBLÉE NATIONALE **SÉNAT**

Reçu à la Présidence de l'Assemblée nationale
le 26 mai 2023

Enregistré à la Présidence du Sénat
le 26 mai 2023

TEXTE SOUMIS EN APPLICATION DE L'ARTICLE 88-4 DE LA CONSTITUTION

PAR LE GOUVERNEMENT,

À L'ASSEMBLÉE NATIONALE ET AU SÉNAT.

Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2019/881 en ce qui concerne les services de sécurité gérés

E17789

Conseil de
l'Union européenne

Bruxelles, le 21 avril 2023
(OR. en)

8511/23

Dossier interinstitutionnel:
2023/0108(COD)

CYBER 91
JAI 469
TELECOM 107
DATAPROTECT 109
MI 312
IND 180
CODEC 661

PROPOSITION

Origine:	Pour la secrétaire générale de la Commission européenne, Madame Martine DEPREZ, directrice
Date de réception:	19 avril 2023
Destinataire:	Madame Thérèse BLANCHET, secrétaire générale du Conseil de l'Union européenne
N° doc. Cion:	COM(2023) 208 final
Objet:	Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL modifiant le règlement (UE) 2019/881 en ce qui concerne les services de sécurité gérés

Les délégations trouveront ci-joint le document COM(2023) 208 final.

p.j.: COM(2023) 208 final

COMMISSION
EUROPÉENNE

Strasbourg, le 18.4.2023
COM(2023) 208 final

2023/0108 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

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

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

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

Justification et objectifs de la proposition

Le présent exposé des motifs accompagne la proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2019/881[1] en ce qui concerne les services de sécurité gérés.

La modification ciblée qui est proposée vise à permettre, au moyen d'actes d'exécution de la Commission, l'adoption de schémas européens de certification de cybersécurité pour les «services de sécurité gérés», en plus de ceux concernant les produits TIC (technologies de l'information et de la communication), services TIC et processus TIC, qui sont déjà couverts par le règlement sur la cybersécurité. Les services de sécurité gérés jouent un rôle de plus en plus important dans la prévention et la limitation des incidents de cybersécurité.

Dans ses conclusions du 23 mai 2022[2] sur la mise en place d'une posture cyber de l'Union européenne, le Conseil a invité l'UE et ses États membres à redoubler d'efforts pour relever le niveau global de cybersécurité, par exemple en facilitant l'émergence de fournisseurs de services de cybersécurité fiables, et a souligné qu'encourager le développement de ces fournisseurs devrait constituer une priorité de la politique industrielle de l'UE dans le domaine de la cybersécurité. Il a également invité la Commission à proposer des pistes pour encourager l'émergence d'un secteur des services de cybersécurité fiable. La certification des services de sécurité gérés est un moyen efficace de renforcer la confiance dans la qualité de ces services et de faciliter ainsi l'émergence d'un secteur européen des services de cybersécurité fiable.

Dans la communication conjointe intitulée «La politique de cyberdéfense de l'UE», adoptée par la Commission et le Haut Représentant le 10 novembre 2022[3], il a été annoncé que la Commission étudierait la possibilité d'élaborer, au niveau de l'UE, des schémas de certification de cybersécurité pour le secteur de la cybersécurité et les entreprises privées. Les fournisseurs de services de sécurité gérés joueront également un rôle important dans la réserve de cybersécurité au niveau de l'UE, dont la mise en place progressive est soutenue par le règlement sur la cybersolidarité, proposé parallèlement au présent règlement. La réserve de cybersécurité au niveau de l'UE doit être utilisée pour soutenir les mesures de réaction et de rétablissement immédiat en cas d'incidents de cybersécurité importants et de grande ampleur. Les services de cybersécurité pertinents fournis par des «fournisseurs de confiance» visés dans le règlement sur la cybersolidarité correspondent aux «services de sécurité gérés» dans la présente proposition.

Certains États membres ont déjà commencé à adopter des schémas de certification pour les services de sécurité gérés. Il existe donc, en raison des incohérences relatives aux schémas de certification de cybersécurité dans les différents pays de l'Union, un risque croissant de fragmentation du marché intérieur concernant les services de sécurité gérés. La présente proposition permet la création de schémas européens de certification de cybersécurité pour ces services afin d'éviter une telle fragmentation.

---

1 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).

2 Document 9364/22.

3 JOIN(2022) 49 final.

- **Cohérence avec les dispositions existantes dans le domaine d'action**

La présente proposition est cohérente avec le règlement sur la cybersécurité, qu'elle modifie. Elle s'appuie sur les dispositions dudit règlement et les adapte pour y inclure également les services de sécurité gérés. Les modifications proposées se limitent à ce qui est strictement nécessaire et ne modifient pas les caractéristiques ou le fonctionnement du règlement sur la cybersécurité.

La présente proposition est également cohérente avec la 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)[4]. Les fournisseurs de services de sécurité gérés sont considérés comme des entités essentielles ou importantes appartenant à un secteur hautement critique au titre de la directive (UE) 2022/2555. Le considérant 86 de ladite directive énonce que 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. Les entités essentielles et importantes au sens de la directive (UE) 2022/2555 doivent donc faire preuve d'une diligence renforcée lorsqu'elles sélectionnent leurs fournisseurs de services de sécurité gérés.

La présente proposition vise à améliorer la qualité des services de sécurité gérés et à accroître leur comparabilité. Elle permet ainsi aux entités essentielles et importantes de faire preuve d'une diligence renforcée lorsqu'elles sélectionnent leurs fournisseurs de services de sécurité gérés, ainsi que l'exige la directive (UE) 2022/2555. En outre, la définition du terme «services de sécurité gérés» figurant dans la présente proposition découle de la définition du terme «fournisseur de services de sécurité gérés» de la directive (UE) 2022/2555 et y est très similaire. Pour ces raisons, la proposition présente un haut degré de complémentarité avec la directive SRI 2.

Enfin, la présente proposition est complémentaire de la proposition de règlement sur la cybersolidarité. La proposition de règlement sur la cybersolidarité met en place un processus de sélection des fournisseurs en vue de constituer une réserve de cybersécurité au niveau de l'UE, qui devrait notamment tenir compte du fait que ces fournisseurs ont obtenu une certification européenne ou nationale en matière de cybersécurité. Les futurs systèmes de certification pour les services de sécurité gérés joueront donc un rôle important dans la mise en œuvre du règlement sur la cybersolidarité.

- **Cohérence avec les autres politiques de l'Union**

La présente proposition n'affecte pas la cohérence du règlement sur la cybersécurité par rapport au règlement (UE) 2016/679 (règlement général sur la protection des données, ci-après le «RGPD»)[5] et à ses dispositions relatives à la mise en place de mécanismes de certification ainsi que de labels et de marques en matière de protection des données aux fins de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent ledit règlement. Le règlement sur la cybersécurité est sans

[4] JO L 333 du 27.12.2022, p. 80.
[5] JO L 119 du 4.5.2016, p. 1.

préjudice de la certification des opérations de traitement de données, y compris lorsque ces opérations sont intégrées dans des produits et services, en vertu du RGPD.

En outre, la présente proposition n'affecte pas la compatibilité du règlement sur la cybersécurité avec le règlement (CE) nº 765/2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché[6], en particulier en ce qui concerne le cadre relatif aux organismes nationaux d'accréditation et aux organismes d'évaluation de la conformité ainsi qu'aux autorités nationales de contrôle de la certification.

2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

• Base juridique

La présente proposition modifie le règlement sur la cybersécurité, qui est fondé sur l'article 114 du traité sur le fonctionnement de l'Union européenne (TFUE). Comme dans le cas du règlement sur la cybersécurité, la présente proposition vise à éviter la fragmentation du marché intérieur, notamment en permettant l'adoption de schémas européens de certification de cybersécurité pour les services de sécurité gérés. Les États membres ont commencé à adopter des schémas de certification pour les services de sécurité gérés. Il existe donc un risque concret de fragmentation du marché intérieur pour ces services, auquel la présente proposition vise à remédier. Par conséquent, l'article 114 du TFUE constitue la base juridique pertinente pour la présente initiative.

• Subsidiarité (en cas de compétence non exclusive)

L'objectif consistant à permettre l'adoption de schémas européens de certification de cybersécurité pour les services de sécurité gérés et à éviter la fragmentation du marché intérieur ne peut être atteint au niveau national, mais uniquement au niveau de l'Union. En outre, les services de sécurité gérés, sur lesquels porte la modification proposée, sont offerts par des fournisseurs actifs dans toute l'Union, tout comme leurs principaux clients potentiels. Une action au niveau de l'Union est donc à la fois nécessaire et plus efficace qu'une action au niveau national.

• Proportionnalité

La proposition est une modification ciblée du règlement sur la cybersécurité. Elle se limite à ce qui est strictement nécessaire pour atteindre son objectif, à savoir permettre l'adoption de schémas européens de certification de cybersécurité pour les services de sécurité gérés, en plus de ceux concernant les produits TIC, services TIC et processus TIC Les modifications proposées adaptent, en particulier, le champ d'application du cadre européen de certification de cybersécurité pour y inclure les «services de sécurité gérés», introduisent une définition de ces services conforme à la directive SRI 2 et modifient les objectifs de sécurité de la certification de cybersécurité européenne afin de l'adapter aux «services de sécurité gérés». Les autres modifications sont de nature technique et visent à garantir que les articles concernés s'appliquent également aux «services de sécurité gérés». L'initiative proposée est donc proportionnée à l'objectif poursuivi.

• Choix de l'instrument

Étant donné que la proposition modifie le règlement (UE) 2019/881, l'instrument juridique approprié est un règlement.

---

6 JO L 218 du 13.8.2008, p. 30.

3. RÉSULTATS DES ÉVALUATIONS EX POST, DES CONSULTATIONS DES PARTIES INTÉRESSÉES ET DES ANALYSES D'IMPACT

- **Évaluations ex post/bilans de qualité de la législation existante**

Sans objet.

Consultation des parties intéressées

Des consultations ciblées ont été menées avec les États membres et l'ENISA. Lors de ces consultations, les États membres ont décrit leurs activités et positions actuelles en ce qui concerne la certification des services de sécurité gérés. L'ENISA a exposé son point de vue et ses conclusions à l'issue des discussions avec les États membres et les parties prenantes. Les observations et informations reçues des États membres et de l'ENISA ont alimenté la présente proposition.

- **Obtention et utilisation d'expertise**

Sans objet.

- **Analyse d'impact**

Une dérogation à l'exigence de procéder à une analyse d'impact a été demandée car la proposition constitue une modification très limitée et ciblée du règlement sur la cybersécurité. La proposition habiliterait la Commission à adopter, au moyen d'actes d'exécution, des schémas européens de certification de cybersécurité pour les «services de sécurité gérés», en plus de ceux concernant les produits TIC, services TIC et processus TIC, qui sont déjà couverts par ledit règlement. Toutefois, la modification proposée n'aurait d'effet qu'une fois que ces schémas de certification auront été adoptés à un stade ultérieur. En outre, la modification n'affecterait pas le caractère volontaire des schémas de certification.

- **Réglementation affûtée et simplification**

Sans objet.

- **Droits fondamentaux**

La proposition n'a pas de conséquences prévisibles pour la protection des droits fondamentaux.

4. INCIDENCE BUDGÉTAIRE

Néant.

5. AUTRES ÉLÉMENTS

- **Plans de mise en œuvre et modalités de suivi, d'évaluation et d'information**

Les dispositions devant être modifiées par la présente proposition seront appréciées dans le cadre de l'évaluation périodique du règlement sur la cybersécurité qui doit être effectuée par la Commission conformément à l'article 67 dudit règlement. Ladite évaluation porte notamment sur les effets, l'efficacité et l'efficience des dispositions relatives au cadre de certification de cybersécurité au regard des objectifs consistant à garantir un niveau adéquat de cybersécurité des produits TIC, services TIC et processus TIC dans l'Union et à améliorer le fonctionnement du marché intérieur. La proposition contient une modification qui fait en sorte que l'évaluation porte également sur les services de sécurité gérés. La Commission est également tenue de transmettre le rapport d'évaluation, accompagné de ses conclusions, au

Parlement européen, au Conseil et au conseil d'administration de l'ENISA; les conclusions du rapport doivent être rendues publiques.

- **Explication détaillée de certaines dispositions de la proposition**

La proposition comporte deux articles. Alors que l'article 1er contient les modifications apportées au règlement (UE) 2019/881, l'article 2 concerne l'entrée en vigueur. L'article 1er contient des modifications ciblées visant à modifier le champ d'application du cadre européen de certification de cybersécurité dans le règlement sur la cybersécurité afin d'y inclure les «services de sécurité gérés» (voir articles 1er et 46 du règlement sur la cybersécurité). Il introduit une définition de ces services, qui est très proche de la définition du terme «fournisseur de services de sécurité gérés» figurant dans la directive SRI 2 (voir article 2 du règlement sur la cybersécurité). Il ajoute également un nouvel article 51 bis relatif aux objectifs de sécurité de la certification européenne de cybersécurité, adaptés aux «services de sécurité gérés». Enfin, la proposition contient un certain nombre de modifications techniques visant à garantir que les articles concernés s'appliquent également aux «services de sécurité gérés».

2023/0108 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

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,

vu l'avis du Comité des régions,

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(1) Le règlement (UE) 2019/881 du Parlement européen et du Conseil[7] 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 TIC, services TIC et 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) Les services de sécurité gérés, qui 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, ont gagné en importance en ce qui concerne la prévention et de la limitation des incidents de cybersécurité. En conséquence, les fournisseurs de tels services sont considérés comme des entités essentielles ou importantes appartenant à un secteur hautement critique au titre de la directive (UE) 2022/2555 du Parlement européen et du Conseil[8]. Au titre du 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

[7] 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).

[8] 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).

cyberattaques et, du fait de leur grande intégration dans les activités des opérateurs, ils représentent un risque particulier. Les entités essentielles et importantes au sens de la directive (UE) 2022/2555 doivent donc faire preuve d'une diligence renforcée lorsqu'elles sélectionnent leurs fournisseurs de services de sécurité gérés.

(3) Les fournisseurs de services de sécurité gérés jouent également un rôle important concernant la réserve de cybersécurité de l'UE, dont la mise en place progressive est soutenue par le règlement (UE).../.... [établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir]. La réserve de cybersécurité de l'UE doit être utilisée pour soutenir les mesures de réaction et de rétablissement immédiat en cas d'incidents de cybersécurité importants et de grande ampleur. Le règlement (UE).../... [établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir] met en place un processus de sélection des fournisseurs constituant la réserve de cybersécurité de l'UE, qui devrait, entre autres, tenir compte du fait que le fournisseur concerné a obtenu une certification européenne ou nationale en matière de cybersécurité. Les services pertinents fournis par des «fournisseurs de confiance» au titre du règlement (UE).../... [établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir] correspondent aux «services de sécurité gérés» conformément au présent règlement.

(4) La certification des services de sécurité gérés est non seulement pertinente dans le processus de sélection de la réserve de cybersécurité de l'UE, 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 qu'ils traitent, 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 pour les services de sécurité gérés contribuent à éviter la fragmentation du marché unique. Le présent règlement vise donc à améliorer le fonctionnement du marché intérieur.

(5) 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 de leur personnel. 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 d'un service de sécurité géré puissent être couverts par un schéma de certification, il est par conséquent nécessaire de modifier le règlement (UE) 2019/881.

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

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Modifications apportées au règlement (UE) 2019/881

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

(1) À l'article 1er, 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 et 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 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, y compris la réaction aux incidents, les tests d'intrusion, les audits de sécurité et le conseil»;

(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;

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 remplacé 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:

a) en surveillant, en permanence, les évolutions dans les domaines connexes de la normalisation et en recommandant des spécifications techniques d'utilisation appropriées dans le développement des schémas européens de certification de cybersécurité en application de l'article 54, paragraphe 1, point c), dans les cas où il n'existe aucune norme;

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;

c) en évaluant les schémas européens de certification de cybersécurité, conformément à l'article 49, paragraphe 8;

d) en participant aux examens par les pairs, conformément à l'article 59, paragraphe 4;

e) en aidant la Commission à assurer le secrétariat du GECC, conformément à l'article 62, paragraphe 5.»;

(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) À l'article 46, les paragraphes 1 et 2 sont remplacés par le texte suivant:

«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. Il atteste 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 très haut niveau de connaissances techniques pertinentes et d'intégrité professionnelle.»;

(6) À l'article 47, les paragraphes 2 et 3 sont remplacés par le texte suivant:

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

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

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;

b) le droit ou la politique applicable de l'Union ou d'un État membre;

c) la demande du marché;

d) l'évolution de la situation en ce qui concerne les cybermenaces;

e) une demande de préparation d'un schéma candidat spécifique par le GECC.»;

(7) À l'article 49, le paragraphe 7 est remplacé par le texte suivant:

«7. La Commission, se fondant sur le schéma candidat préparé par l'ENISA, peut 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 des articles 51, 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 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:»

(9) 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) faire en sorte 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 très haut niveau de compétence et de connaissances techniques dans le domaine spécifique, une expérience suffisante et appropriée et la plus haute intégrité professionnelle;

b) faire en sorte 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 très élevé;

c) protéger les données consultées, stockées, transmises ou traitées de toute autre façon dans le cadre de la fourniture de services de sécurité gérés 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) faire en sorte 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) faire en sorte 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) garder une trace 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) faire en sorte que les produits TIC, services TIC et processus TIC [et le matériel] déployés dans le cadre de la fourniture des services de sécurité gérés soient sécurisés par défaut et dès la conception, ne contiennent pas de vulnérabilités connues et comprennent les dernières mises à jour de sécurité;»;

(10) 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 et 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 et 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 et 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.»;

(11) 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 et 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 visée à 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.»;

(12) 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 et services de sécurité gérés couverts;»;

(b) 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 et 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;»;

(c) le point l) est remplacé par le texte suivant:

«l) les règles relatives aux conséquences pour les produits TIC, services TIC, processus TIC et 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;»;

(d) 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 et services de sécurité gérés, d'exigences de sécurité, de critères et méthodes d'évaluation et de niveaux d'assurance;»;

(e) 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;»;

(13) 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 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 et 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:

(aa) 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;

(bb) 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 PME;»;

(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 visée à 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.»

(14) 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.»;

(15) 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 et 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.»;

(16) 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);»;

(17) 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 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 de l'Union.»;

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 Strasbourg, le

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