Amendement 2
Cristian-Silviu Buşoi
au nom de la commission de l'industrie, de la recherche et de l'énergie

Rapport **A9-0307/2023**
Josianne Cutajar
Services de sécurité gérés
(COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

Proposition de règlement
–

AMENDEMENTS DU PARLEMENT EUROPÉEN*

à la proposition de la Commission

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

du ...

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,

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

vu l'avis du Comité économique et social européen[1],

après consultation du Comité des régions,

statuant conformément à la procédure législative ordinaire[2],

[1] ***JO C 349 du 29.9.2023, p. 167.***

[2] ***Position du Parlement européen du … [(JO …)/(non encore parue au Journal officiel)] et décision du Conseil du …. .***

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)***, 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) Afin de garantir la résilience de l'Union face aux cyberattaques et de prévenir toute vulnérabilité sur le marché de l'Union, le présent règlement vise à compléter le cadre réglementaire horizontal établissant des exigences complètes en matière de cybersécurité pour tous les produits comportant des éléments numériques conformément au règlement (UE).../... du Parlement européen et du Conseil[4] (2022/0272(COD)), en fixant des exigences essentielles pour les services de cybersécurité gérés, leur application et leur fiabilité.

---

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) .../... du Parlement européen et du Conseil du ... sur ... (JO L …, …, ELI: …).***

(3) Les services de sécurité gérés ***sont des services fournis par les fournisseurs de services de sécurité gérés conformément 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 de la directive (UE) 2022/2555. Ces 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 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 ▌. 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 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.

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 de certification, tels que le traitement des incidents, les tests d'intrusion, les audits de sécurité et les conseils 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 de cybersécurité, 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 peut 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.

(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 immédiat en cas d'incidents de cybersécurité importants et 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 des risques de l'Union***. ***La certification des services de sécurité gérés peut jouer un rôle dans la sélection des*** fournisseurs de confiance ▌.

(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, 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.

(7) Les schémas européens de certification pour les services de sécurité gérés devraient conduire à l'adoption de ces services et à une concurrence accrue entre les fournisseurs proposant des 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, les 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 microentreprises ou les petites et moyennes entreprises (PME), 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 de certification devraient contribuer à leur accessibilité, en particulier pour les petits acteurs, tels que les microentreprises et les PME, 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 petites et moyennes entreprises (PME) 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 conformes aux exigences définies dans le présent règlement. Le programme pour une Europe numérique et d'autres programmes pertinents de l'Union prévoient que la Commission devrait mettre en place un soutien financier et technique permettant à ces entreprises de contribuer à la croissance de l'économie européenne et au renforcement du niveau commun de cybersécurité européenne dans le paysage de 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 microentreprises et les PME.***

(9) ***Le schéma de certification de l'Union 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, en particulier en ce qui concerne l'objectif consistant à ce que 75 % des entreprises de l'Union commencent à utiliser l'informatique en nuage, l'IA ou les mégadonnées, à ce que plus de 90 % des microentreprises et des PME atteignent au moins un niveau élémentaire d'intensité numérique et à ce que les services publics essentiels soient proposés 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 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 ***des services de sécurité gérés*** puissent être couverts par un schéma de certification ***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 de l'Union fiable, tout en créant des partenariats avec des pays tiers partageant les mêmes valeurs, le processus de certification établi dans le cadre fixé par le présent règlement devrait être rationalisé de manière à faciliter 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 sur 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, à la fois formelles, par exemple par le biais de l'université ou de cours, et informelles, 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 essentiels et 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'ENISA et les parties prenantes, y compris le secteur privé et le 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 ces mesures visent à attirer davantage de femmes et de filles dans ce domaine et contribuent 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 microentreprises et les PME. Il est aussi important que les fournisseurs de ces services 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 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 d'ajouter la possibilité de créer des schémas de certification de cybersécurité pour les fournisseurs de services de sécurité gérés. Ce faisant, il précise et clarifie également certaines dispositions 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 des articles 49 et 49 bis, ne devraient en aucune manière préjuger de l'évaluation et du réexamen plus larges dudit règlement requis en vertu de son article 67, y compris, en particulier, de l'évaluation de l'impact, de l'efficacité et de l'efficience du titre dudit règlement relatif aux schémas de certification de cybersécurité. Cette évaluation et ce réexamen concernant le titre relatif aux schémas de certification de cybersécurité 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 l'adoption 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 tel qu'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[6] et a rendu un avis le 10 janvier 2024[7],

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

---

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

7 ***JO C .../...***

Article premier

Modifications du 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 ***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 ***en matière de sécurité, 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;

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 ▌ niveau ***suffisant et approprié*** 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;

c bis) les évolutions technologiques ainsi que la disponibilité et le développement de schémas internationaux de certification de cybersécurité et de normes internationales et industrielles;

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) ▌L'article 49 est ***modifié comme suit***:

a) les paragraphes 1, 2, 3 et 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, conformément à l'article 49, paragraphe 6, l'ENISA fournit des informations sur la manière dont elle s'est conformée à cette obligation.

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. Les groupes de travail ad hoc créés à cette fin comprennent, le cas échéant et sans préjudice des procédures et de la marge d'appréciation établies 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, 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, ***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 conformément à l'article 48.

2 Au cours de la préparation d'un schéma candidat par l'ENISA, conformément à l'article 49, le Parlement européen et le Conseil peuvent demander à la Commission, en sa qualité de président du groupe européen de certification de cybersécurité (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 et le Conseil 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 le Conseil sur les questions visées au paragraphe 3 du présent article lors de l'évaluation du présent règlement conformément à 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) 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) ▌ 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) 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) ▌ que les produits TIC, services TIC et processus TIC ▌ déployés dans le cadre de la fourniture des services de sécurité gérés soient sécurisés par défaut et dès la conception, ***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 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.»;

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 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.»;

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 et services de sécurité gérés couverts;»;

a bis) 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;»;

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:

«1) 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;»;

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 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:

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 ***intérêts et les besoins spécifiques des microentreprises et des*** 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.»

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 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.»;

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 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 de l'Union.»;

19) L'annexe est remplacée par le texte figurant 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 ..., le

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

ANNEXE

EXIGENCES AUXQUELLES DOIVENT SATISFAIRE LES ORGANISMES D'ÉVALUATION DE LA CONFORMITÉ

Les organismes d'évaluation de la conformité qui souhaitent être accrédités satisfont aux exigences suivantes:

1. ***Un organisme d'évaluation de la conformité est constitué en vertu du droit national et possède la personnalité juridique.***
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 n'interviennent pas directement 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, ou ne représentent pas les parties engagées dans ces activités. 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.

6. Si un organisme d'évaluation de la conformité appartient à une entité ou à une institution publique, ou est géré par une telle entité ou institution, l'indépendance de l'autorité nationale de certification de cybersécurité et de l'organisme d'évaluation de la conformité et l'absence de conflit d'intérêts entre ces deux instances sont garanties et documentées.

7. Les organismes d'évaluation de la conformité veillent à ce que les activités de leurs filiales et sous-traitants n'aient pas d'incidence sur la confidentialité, l'objectivité ou l'impartialité de leurs activités d'évaluation de la conformité.

8. Les organismes d'évaluation de la conformité et leur personnel accomplissent les activités d'évaluation de la conformité avec la plus haute intégrité professionnelle et la compétence technique requise dans le domaine spécifique et sont à l'abri de toute pression ou incitation susceptible d'influencer leur jugement ou les résultats de leurs travaux d'évaluation de la conformité, notamment des pressions ou incitations d'ordre financier, en particulier de la part de personnes ou de groupes de personnes intéressés par les résultats de ces activités.

9. Un organisme d'évaluation de la conformité est capable d'exécuter toutes les tâches d'évaluation de la conformité qui lui ont été assignées au titre du présent règlement, que ces tâches soient exécutées par l'organisme d'évaluation de la conformité lui-même ou en son nom et sous sa responsabilité. Toute sous-traitance ou consultation de personnel externe est documentée de manière appropriée, ne fait intervenir aucun intermédiaire et fait l'objet d'un accord écrit couvrant, entre autres, la confidentialité et les conflits d'intérêts. L'organisme d'évaluation de la conformité en question assume la responsabilité des tâches accomplies.

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:

a) du personnel requis ayant les connaissances techniques et l'expérience suffisante et appropriée pour exécuter les tâches d'évaluation de la conformité;

b) de descriptions des procédures à suivre pour effectuer l'évaluation de la conformité, afin de garantir la transparence et la reproductibilité de ces procédures. Il se dote de politiques et de procédures appropriées faisant la distinction entre les tâches qu'il exécute en tant qu'organisme notifié en vertu de l'article 61 et ses autres activités;

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.

11. Un organisme d'évaluation de la conformité se dote des moyens nécessaires à la bonne exécution des tâches techniques et administratives liées aux activités d'évaluation de la conformité et a accès à tous les équipements et installations nécessaires.

12. Les personnes chargées d'effectuer des activités d'évaluation de la conformité possèdent:

a) une solide formation technique et professionnelle couvrant toutes les activités d'évaluation de la conformité;

b) une connaissance satisfaisante des exigences applicables aux évaluations de conformité auxquelles elles procèdent et l'autorité nécessaire pour effectuer ces évaluations;

c) une connaissance et une compréhension adéquates des exigences et des normes d'essai applicables;

d) l'aptitude à rédiger les attestations, procès-verbaux et rapports qui

constituent la matérialisation des évaluations de la conformité effectuées.

13. L'impartialité des organismes d'évaluation de la conformité, de leurs cadres supérieurs, des personnes chargées de l'exécution des activités d'évaluation de la conformité et de tout sous-traitant est garantie.

14. La rémunération des cadres supérieurs et des personnes chargées de l'exécution des activités d'évaluation de la conformité ne dépend pas du nombre d'évaluations de la conformité effectuées ni de leurs résultats.

15. Les organismes d'évaluation de la conformité souscrivent une assurance couvrant leur responsabilité civile, à moins que cette responsabilité ne soit assumée par l'État membre conformément à son droit national ou que l'évaluation de la conformité ne soit effectuée sous la responsabilité directe de l'État membre.

16. L'organisme d'évaluation de la conformité et son personnel, ses comités, ses filiales, ses sous-traitants et tout organisme associé ainsi que le personnel des organes externes d'un organisme d'évaluation de la conformité assurent le respect de la confidentialité et sont liés par le secret professionnel pour toutes les informations obtenues dans l'exercice de leurs tâches d'évaluation de la conformité au titre du présent règlement ou de toute disposition de droit national donnant effet au présent règlement, sauf dans les cas où la communication d'informations est requise par le droit de l'Union ou de l'État membre auquel ces personnes sont soumises, et sauf à l'égard des autorités compétentes de l'État membre où il exerce ses activités. Les droits de propriété intellectuelle sont protégés. L'organisme d'évaluation de la conformité possède des procédures documentées concernant les exigences du présent point.

17. À l'exception du point 16, les exigences de la présente annexe n'empêchent en rien les échanges d'informations techniques et d'orientations réglementaires entre un organisme d'évaluation de la conformité et une personne qui introduit une demande de certification ou envisage de le faire.

18. Les organismes d'évaluation de la conformité agissent conformément à un ensemble de conditions cohérentes, justes et raisonnables, en tenant compte des intérêts des PME pour ce qui est des redevances.

19. Les organismes d'évaluation de la conformité respectent les exigences de la norme

pertinente qui est harmonisée au titre 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 pertinente qui est harmonisée au titre du règlement (CE) nº 765/2008 en ce qui concerne l'accréditation de laboratoires qui réalisent des essais.

Or. en