Conseil de
l'Union européenne

Bruxelles, le 29 mai 2018
(OR. en)

9350/18

Dossier interinstitutionnel:
2017/0225 (COD)

CYBER 115
TELECOM 152
CODEC 860
COPEN 163
COPS 175
COSI 129
CSC 170
CSCI 80
IND 143
JAI 514
JAIEX 55
POLMIL 61
RELEX 463

NOTE

Origine:	la présidence
Destinataire:	Conseil
Nº doc. préc.:	8834/18
N° doc. Cion:	12183/17
Objet:	Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) n° 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité) - Orientation générale

I. INTRODUCTION

1. Le 13 septembre 2017, dans le contexte de sa stratégie pour un marché unique numérique, la Commission a adopté et transmis au Conseil et au Parlement européen la proposition mentionnée en objet[1], dont la base juridique est l'article 114 du TFUE. Cette proposition, qui fait partie du "train de mesures sur la cybersécurité", vise à assurer un niveau élevé de cybersécurité, de cyberrésilience et de confiance au sein de l'Union, en vue d'assurer le bon fonctionnement du marché intérieur.

2. Le règlement proposé fixe les objectifs, les tâches et les aspects organisationnels de l'ENISA, Agence de l'Union européenne pour la cybersécurité, et crée un cadre pour l'établissement de systèmes européens de certification de cybersécurité, afin de garantir un niveau adéquat de cybersécurité pour les produits et services TIC dans l'Union. La proposition de la Commission est accompagnée d'une analyse d'impact qui porte sur un ensemble spécifique de huit options stratégiques, couvrant le réexamen de l'ENISA et la certification de cybersécurité en matière de TIC.

3. La proposition de règlement comprend deux grands volets:

   - un mandat permanent pour l'Agence, d'une portée délimitée compte tenu des besoins dans le cadre des nouvelles priorités et des nouveaux instruments politiques, ainsi qu'un ensemble renouvelé de tâches et de fonctions pour l'Agence, afin qu'un soutien effectif et efficace puisse être apporté aux efforts déployés par les États membres, les institutions de l'UE et les autres parties prenantes pour assurer la sécurité du cyberespace;

   - un cadre européen de certification de cybersécurité pour les produits et services TIC, ainsi que des règles régissant les systèmes européens de certification de cybersécurité, permettant que les certificats délivrés dans le cadre de ces systèmes soient valides et reconnus dans tous les États membres et remédiant à l'actuelle fragmentation du marché.

[1] Doc. 12183/17; 12183/1/17 REV 1; 12183/2/17 REV 2.

4. En octobre 2017, le Conseil européen[2] a demandé que les propositions de la Commission concernant la cybersécurité soient élaborées de manière globale, présentées en temps utile et examinées sans retard, sur la base d'un plan d'action devant être établi par le Conseil.

5. Le 12 décembre 2017, le Conseil des affaires générales a adopté le plan d'action[3] mettant en œuvre les conclusions du Conseil[4] sur la communication conjointe[5] au Parlement européen et au Conseil intitulée "Résilience, dissuasion et défense: doter l'Union européenne d'une cybersécurité solide". Le plan d'action traduisait l'ambition du Conseil de dégager une orientation générale sur la proposition pour juin 2018.

6. Au Parlement européen, M[me] Angelika NIEBLER (ITRE, PPE) a été nommée rapporteure. Il est prévu que la commission ITRE vote sur son rapport le 19 juin 2018.

7. Le Comité économique et social européen a adopté son avis le 14 février 2018.

II. TRAVAUX AU SEIN DU CONSEIL

8. Le 26 septembre 2017, la Commission a présenté la proposition et l'analyse d'impact y afférente au groupe horizontal "Questions liées au cyberespace" (ci-après dénommé "groupe"), qui a examiné l'analyse d'impact le 20 octobre 2017. Les discussions qui ont suivi ont été centrées sur la capacité opérationnelle de l'Agence, sur le degré d'interaction avec les autorités nationales compétentes, ainsi que sur l'incidence du cadre de certification sur le marché et la compétitivité des entreprises. De manière générale, tant l'analyse d'impact que la proposition ont reçu un accueil favorable de la part des délégations.

---

2 EUCO 14/17, point 11.
3 Doc. 15748/17.
4 Doc. 14435/17.
5 Doc. 12211/17.

9. Le groupe a commencé à examiner la proposition elle-même en novembre 2017, pendant la présidence estonienne, et a poursuivi ses travaux au cours de la présidence bulgare. Douze réunions ont été consacrées à cette proposition, qui ont abouti à huit versions révisées consécutives du texte, en vue de parvenir à un accord sur une orientation générale lors de la prochaine session du Conseil TTE (Télécommunications), qui doit se tenir le 8 juin 2018.

10. Les résultats des discussions intervenues au sein du groupe les 14 et 15 mai 2018, ainsi que le texte de compromis révisé de la présidence, figurent à l'annexe de la présente note. Les considérants ont été adaptés pour tenir compte des modifications apportées au dispositif. Les modifications par rapport à la proposition de la Commission sont toutes indiquées en **caractères gras** ou signalées par des crochets [...]. Les modifications par rapport au dernier document en date du groupe (8834/18) sont indiquées en **caractères gras et soulignés** et tous les passages supprimés sont signalés par le symbole **[...]**.

III. CONCLUSION

11. Le texte de compromis de la présidence, tel qu'il figure en annexe, reflète les efforts fournis par la présidence et les États membres pour parvenir à un équilibre adéquat.

12. Le 25 mai 2018, le Comité des représentants permanents est parvenu à un accord sur le texte de compromis de la présidence, sous réserve de modification à l'article 19, paragraphe 5, et à l'article 48, paragraphe 5, figurant en annexe.

13. Le Conseil est dès lors invité à adopter une orientation générale lors de sa session du 8 juin 2018 et à charger la présidence d'entamer des négociations avec les représentants du Parlement européen et de la Commission européenne sur ce dossier.

ANNEXE

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

relatif à l'ENISA, [...] *Agence de l'Union européenne pour la cybersécurité*, et abrogeant le règlement (UE) n° 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité)

(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[6],

vu l'avis du Comité des régions[7],

statuant conformément à la procédure législative ordinaire,

[6] JO C, p. .
[7] JO C, p. .

considérant ce qui suit:

(1) Les réseaux et systèmes d'information et les réseaux et services de télécommunications remplissent une fonction essentielle pour la société et sont devenus le nerf de la croissance économique. Les technologies de l'information et des communications sont le fondement des systèmes complexes qui rendent possibles les activités sociales; elles permettent à nos économies de fonctionner dans des secteurs clés comme la santé, l'énergie, la finance et les transports, et soutiennent en particulier le fonctionnement du marché intérieur.

(2) L'utilisation des réseaux et des systèmes d'information par les particuliers, les entreprises et les pouvoirs publics s'est généralisée dans l'Union tout entière. La numérisation et la connectivité caractérisent un nombre toujours croissant de produits et de services; avec l'avènement de l'internet des objets (IdO), ce sont des millions, sinon des milliards, de dispositifs numériques connectés qui devraient être mis en service dans l'UE au cours de la prochaine décennie. Alors qu'un nombre croissant de dispositifs sont connectés à l'internet, leur conception n'intègre pas suffisamment les impératifs de sécurité et de résilience, de sorte que la cybersécurité est insuffisante. Dans ce contexte, le recours limité à la certification entraîne un manque d'information des utilisateurs, qu'il s'agisse de particuliers ou d'organisations, sur les caractéristiques des produits et services TIC en matière de cybersécurité, sapant ainsi la confiance dans les solutions numériques.

(3) Une numérisation et une connectivité accrues entraînent une augmentation des risques en matière de cybersécurité, ce qui rend ainsi l'ensemble de la société plus vulnérable aux cybermenaces et exacerbe les dangers auxquels sont confrontés les individus, notamment les personnes vulnérables telles que les enfants. Afin d'atténuer ce risque pour la société, il convient de prendre toutes les mesures nécessaires pour améliorer la cybersécurité dans l'Union afin de mieux protéger les réseaux et systèmes d'information, les réseaux de télécommunication, les produits, services et appareils numériques utilisés par les particuliers, les pouvoirs publics et les entreprises — depuis les PME jusqu'aux opérateurs d'infrastructures critiques — contre les cybermenaces.

(4) Les cyberattaques sont en augmentation; une économie et une société connectées, qui sont plus vulnérables aux cybermenaces et aux cyberattaques, ont donc besoin de dispositifs de défense renforcés. Cependant, alors que les cyberattaques sont souvent de nature transnationale, les réponses apportées par les autorités chargées de la cybersécurité et les compétences en matière de répression sont surtout nationales. Des incidents de cybersécurité majeurs pourraient perturber la fourniture de services essentiels dans l'ensemble de l'UE. Il est donc indispensable de mettre sur pied une capacité de réaction et de gestion des crises à l'échelon de l'UE, sur la base de politiques spécifiques et d'instruments élargis aux fins de la solidarité européenne et de l'assistance mutuelle. En outre, il est important pour les décideurs, les entreprises et les utilisateurs que la situation en matière de cybersécurité et de résilience dans l'Union soit régulièrement évaluée à partir de données de l'Union fiables et d'une anticipation systématique des évolutions, défis et menaces futurs tant au niveau de l'Union qu'au niveau mondial.

(5) Compte tenu de l'augmentation des enjeux auxquels l'Union est confrontée dans le domaine de la cybersécurité, il est nécessaire de disposer d'une panoplie de mesures qui développent les actions déjà menées par l'Union et promeuvent des objectifs se renforçant mutuellement. Ces objectifs sont notamment la nécessité de continuer à renforcer les capacités et l'état de préparation des États membres et des entreprises, ainsi que d'améliorer la coopération et la coordination entre les États membres et les institutions, organes et organismes de l'UE. En outre, étant donné la nature universelle des cybermenaces, il est nécessaire d'augmenter, au niveau de l'Union, les capacités susceptibles de compléter l'action des États membres, notamment dans les cas d'incidents et crises transfrontières de cybersécurité majeurs. Des efforts supplémentaires sont également requis pour sensibiliser davantage les particuliers et les entreprises aux questions de cybersécurité. En outre, une information transparente sur le niveau de sécurité qui caractérise les produits et services TIC permettrait de renforcer la confiance dans le marché unique numérique. Une certification mise en œuvre à l'échelle de l'UE, prévoyant des exigences et des critères d'évaluation communs en matière de cybersécurité dans l'ensemble des marchés nationaux et des secteurs, peut faciliter cette transparence.

(6) En 2004, le Parlement européen et le Conseil ont adopté le règlement (CE) n° 460/2004[8] instituant l'ENISA en vue de contribuer à la réalisation des objectifs visant à assurer un niveau élevé de sécurité des réseaux et de l'information au sein de l'Union et à favoriser l'émergence d'une culture de la sécurité des réseaux et de l'information dans l'intérêt des citoyens, des consommateurs, des entreprises et des administrations publiques. En 2008, le Parlement européen et le Conseil ont adopté le règlement (CE) n° 1007/2008[9] prolongeant le mandat de l'Agence jusqu'en mars 2012. Le règlement (CE) n° 580/2011[10] a prolongé le mandat de l'Agence une nouvelle fois jusqu'au 13 septembre 2013. En 2013, le Parlement européen et le Conseil ont adopté le règlement (UE) n° 526/2013[11] concernant l'ENISA et abrogeant le règlement (CE) n° 460/2004, qui a prolongé le mandat de l'Agence jusqu'en juin 2020.

---

8 Règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information (JO L 77 du 13.3.2004, p. 1).

9 Règlement (CE) n° 1007/2008 du Parlement européen et du Conseil du 24 septembre 2008 modifiant le règlement (CE) n° 460/2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information en ce qui concerne sa durée (JO L 293 du 31.10.2008, p. 1).

10 Règlement (UE) n° 580/2011 du Parlement européen et du Conseil du 8 juin 2011 modifiant le règlement (CE) n° 460/2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information en ce qui concerne sa durée (JO L 165 du 24.6.2011, p. 3).

11 Règlement (UE) n° 526/2013 du Parlement européen et du Conseil du 21 mai 2013 concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et abrogeant le règlement (CE) n° 460/2004 (JO L 165 du 18.6.2013, p. 41).

(7) L'Union a déjà pris d'importantes mesures pour garantir la cybersécurité et renforcer la confiance dans les technologies numériques. En 2013, l'UE s'est dotée d'une stratégie de cybersécurité afin d'orienter la politique qu'elle entendait mener en réaction aux menaces et aux risques qui pèsent sur la cybersécurité. Dans le cadre de ses efforts pour mieux protéger les Européens en ligne, l'Union a adopté en 2016 le premier acte législatif dans le domaine de la cybersécurité, la directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (la "directive SRI"). La directive SRI a instauré des exigences concernant les capacités nationales dans le domaine de la cybersécurité, établi le premier mécanisme destiné à améliorer la coopération stratégique et opérationnelle entre les États membres, et introduit des obligations concernant les mesures de sécurité et la notification des incidents dans différents secteurs qui revêtent une importance vitale pour l'économie et la société, tels que l'énergie, les transports, l'eau, les banques, les infrastructures des marchés financiers, les soins de santé, les infrastructures numériques ainsi que les fournisseurs de services numériques fondamentaux (moteurs de recherche, services d'informatique en nuage et places de marché en ligne). L'ENISA s'est vu attribuer un rôle essentiel d'appui à la mise en œuvre de cette directive. En outre, lutter efficacement contre la cybercriminalité est l'une des principales priorités du programme européen en matière de sécurité et contribue à l'objectif global consistant à atteindre un niveau élevé de cybersécurité.

(8) Il est reconnu que, depuis l'adoption de la stratégie de cybersécurité de l'UE en 2013 et la dernière révision du mandat de l'Agence, le cadre d'action général a considérablement évolué, compte tenu notamment d'un environnement mondial plus incertain et moins sûr. Dans ce contexte, et dans le cadre de la nouvelle politique de cybersécurité de l'Union, il est nécessaire de réviser le mandat de l'ENISA pour définir son rôle dans le nouvel écosystème de la cybersécurité et faire en sorte qu'elle contribue efficacement à la réponse apportée par l'Union aux défis en matière de cybersécurité qui résultent de cette transformation radicale de la nature des menaces. L'évaluation de l'Agence a en effet conclu à une insuffisance du mandat actuel à cet égard.

(9) L'Agence établie par le présent règlement devrait succéder à l'ENISA telle qu'instituée par le règlement (UE) n° 526/2013. L'Agence devrait remplir les missions qui lui sont confiées par le présent règlement et par les actes législatifs de l'Union dans le domaine de la cybersécurité notamment en fournissant une expertise et des conseils et en jouant le rôle de centre d'information et de connaissance au niveau de l'Union. Elle devrait promouvoir l'échange des meilleures pratiques entre les États membres et les parties prenantes du secteur privé en proposant des mesures à la Commission européenne et aux États membres, en jouant le rôle de point de référence pour les initiatives politiques sectorielles au niveau de l'Union en ce qui concerne la cybersécurité, en favorisant la coopération opérationnelle entre les États membres et entre ceux-ci et les institutions, organes et organismes européens.

(10) Dans le cadre de la décision 2004/97/CE, Euratom adoptée lors de la réunion du Conseil européen du 13 décembre 2003, les représentants des États membres ont décidé que l'Agence aurait son siège dans une ville en Grèce que le gouvernement grec déterminerait. L'État membre d'accueil de l'Agence devrait offrir les meilleures conditions possibles pour un fonctionnement harmonieux et efficace de l'Agence. Il est impératif, pour l'accomplissement correct et efficace de ses missions, pour le recrutement et la fidélisation du personnel et pour une plus grande efficacité des activités de mise en réseau, que l'Agence soit établie dans un lieu approprié, offrant, entre autres, des liaisons de transport et des aménagements appropriés pour les conjoints et enfants accompagnant les membres du personnel de l'Agence. Les dispositions nécessaires devraient être arrêtées dans un accord conclu, après approbation du conseil d'administration de l'Agence, entre l'Agence et l'État membre d'accueil.

(11) Étant donné l'aggravation des défis en matière de cybersécurité auxquels l'Union est confrontée, il faudrait augmenter les ressources financières et humaines allouées à l'Agence pour tenir compte du renforcement de son rôle et de ses missions, ainsi que de sa position critique parmi les organisations qui défendent l'écosystème numérique européen.

(12) L'Agence devrait acquérir et maintenir un niveau élevé d'expertise et servir de point de référence, en instaurant la confiance dans le marché intérieur du fait de son indépendance, de la qualité des conseils fournis et des informations diffusées, de la transparence de ses procédures et modes de fonctionnement, et de sa diligence à exécuter ses missions. L'Agence devrait **soutenir les efforts déployés au niveau national et** contribuer de manière dynamique aux efforts consentis au niveau de l'Union, tout en s'acquittant de ses missions en totale coopération avec les institutions, organes et organismes de l'Union et les États membres. De plus, l'Agence devrait s'appuyer sur les informations fournies par le secteur privé et travailler en coopération avec celui-ci, ainsi qu'avec d'autres parties prenantes. Un ensemble de missions devrait déterminer la manière dont l'Agence doit atteindre ses objectifs tout en lui laissant une certaine souplesse de fonctionnement.

(13) L'Agence devrait assister la Commission sous la forme de conseils, d'avis et d'analyses sur toutes les questions européennes liées à l'élaboration, l'actualisation et la révision des politiques et de la législation dans le domaine de la cybersécurité **et de ses aspects sectoriels spécifiques, afin de renforcer la pertinence des politiques et de la législation de l'UE ayant une dimension liée à la cybersécurité et de permettre leur application cohérente au niveau national [...].** L'Agence devrait être un point de référence, par ses conseils et son expertise, pour les initiatives politiques et législatives sectorielles au niveau de l'Union dans tous les cas où la cybersécurité est en jeu.

(14) La mission fondamentale de l'Agence consiste à promouvoir la mise en œuvre cohérente du cadre législatif applicable, et notamment la mise en œuvre effective de la directive SRI, essentielle pour renforcer la cyberrésilience. Compte tenu de l'évolution rapide de l'éventail des menaces en matière de cybersécurité, il est clair que les États membres ont besoin de s'appuyer sur une approche plus globale, transsectorielle, du développement de la cyberrésilience.

(15) L'Agence devrait assister les États membres et les institutions, organes et organismes de l'Union dans leurs efforts pour mettre en place et développer les capacités et la préparation requises pour prévenir et détecter les [...] **cybermenaces** et incidents de cybersécurité et y réagir, et en ce qui concerne la sécurité des réseaux et des systèmes d'information. L'Agence devrait notamment soutenir le développement et l'amélioration des CSIRT nationaux, afin qu'ils atteignent un niveau de maturité commun élevé dans l'ensemble de l'Union. **Les activités entreprises par l'ENISA en liaison avec les capacités opérationnelles des États membres devraient uniquement compléter les mesures prises par les États membres eux-mêmes pour respecter leurs obligations découlant de la directive SRI et ne devraient donc pas s'y substituer [...].**

(15 *bis*) L'Agence devrait également contribuer à l'élaboration et à la mise à jour des stratégies de l'Union et, sur demande, des États membres en matière de sécurité des réseaux et systèmes d'information, notamment en matière de cybersécurité, promouvoir leur diffusion et suivre leur mise en œuvre. L'Agence devrait enfin proposer des formations et du matériel pédagogique aux organismes publics et, le cas échéant, "former les formateurs" en vue d'aider les États membres à mettre en place leurs propres capacités de formation.

(16) L'Agence devrait aider le groupe de coopération établi par la directive SRI à accomplir ses tâches, notamment en le faisant bénéficier de ses conseils et de son expertise, et en facilitant l'échange de bonnes pratiques en matière de risques et d'incidents, en particulier en ce qui concerne l'identification des opérateurs de services essentiels par les États membres, y compris au regard des dépendances transfrontalières.

(17) Afin de stimuler la coopération entre le secteur public et le secteur privé et au sein de ce dernier, [...] **l'Agence devrait** soutenir **le partage d'informations au sein des secteurs et entre ceux-ci, en particulier dans les secteurs énumérés à l'annexe II de la directive (UE) 2016/1148, en proposant des bonnes pratiques et des orientations sur les outils disponibles, ainsi que des procédures, et en indiquant comment traiter les questions de réglementation liées au partage d'informations, par exemple en facilitant** [...] la mise en place de centres d'échange et d'analyse d'informations (ISAC) sectoriels [...].

(18) L'Agence devrait agréger et analyser les rapports nationaux émanant des CSIRT et des CERT-UE qui sont **partagés volontairement**, **afin d'aider les États membres à établir** des [...] **procédures**, un langage et une terminologie communs pour l'échange d'informations. L'Agence devrait également assurer la participation du secteur privé, dans le cadre de la directive SRI, qui a fixé les bases d'un échange volontaire d'informations techniques à l'échelon opérationnel [...] **au sein** du réseau des CSIRT.

(19) L'Agence devrait contribuer à l'élaboration d'une réaction au niveau de l'UE en cas d'incidents ou de crises transfrontières de cybersécurité majeurs. Cette fonction devrait **être remplie conformément au mandat de l'Agence en application du présent règlement ainsi qu'**à une **approche devant faire l'objet d'un accord des États membres dans le contexte de la recommandation de la Commission sur la coordination des réactions aux incidents et crises de cybersécurité majeurs**. **Elle pourrait** comprendre la collecte d'informations pertinentes et un rôle de facilitateur entre le réseau des CSIRT et la communauté technique ainsi que les décideurs chargés de la gestion des crises. En outre, l'Agence pourrait soutenir le traitement des incidents sur le plan technique, en facilitant l'échange de solutions techniques pertinentes entre les États membres et en contribuant à l'élaboration des communications au public. L'Agence devrait soutenir le processus en testant les modalités de cette coopération grâce à des exercices de cybersécurité [...] **réguliers**.

(20) [...] **Pour soutenir la coopération** opérationnelle [...], l'Agence devrait recourir à l'expertise **technique et opérationnelle** disponible de la CERT-UE, grâce à une coopération structurée [...]. [...] Le cas échéant, des accords spécifiques entre les deux organisations devraient être conclus afin de définir les modalités pratiques de la mise en œuvre de cette coopération **et d'éviter une duplication des activités**.

(21) Dans le cadre de ses missions [...] **consistant à soutenir la coopération opérationnelle au sein du réseau des CSIRT**, l'Agence devrait être en mesure de fournir un appui aux États membres**, à leur demande,** par exemple [...] **en apportant** des conseils **sur la manière d'améliorer leurs capacités de prévention, de détection et de réaction en ce qui concerne les incidents, en [...] facilitant la gestion** technique **des incidents ayant un impact significatif ou substantiel**, ou encore en assurant l'analyse des menaces et incidents. **Dans le cadre de la facilitation de la gestion technique des incidents ayant un impact significatif ou substantiel, l'ENISA devrait en particulier soutenir le partage volontaire de solutions techniques entre États membres ou produire des informations techniques combinées, par exemple des solutions techniques partagées volontairement par les États membres.** La recommandation de la Commission sur la coordination des réactions aux incidents et crises de cybersécurité majeurs invite les États membres à coopérer de bonne foi et à partager dans les meilleurs délais, entre eux et avec l'ENISA, les informations relatives aux crises et incidents de cybersécurité majeurs. Ces informations devraient apporter une aide supplémentaire à l'ENISA pour [...] **soutenir la coopération** opérationnelle.

(22) Dans le cadre de la coopération technique régulière menée pour étayer l'appréciation de la situation au niveau de l'Union, l'Agence devrait, à intervalles réguliers **et en coopération étroite avec les États membres**, préparer le rapport de situation technique sur les incidents et menaces de cybersécurité dans l'UE, sur la base d'informations du domaine public, de sa propre analyse et de rapports que lui communiquent les CSIRT des États membres [...] ou les points de contact uniques au titre de la directive SRI **(sur une base volontaire dans les deux cas)**, le Centre européen de lutte contre la cybercriminalité (EC3) au sein d'Europol, la CERT-UE et, le cas échéant, le Centre de l'UE pour l'analyse des renseignements (INTCEN) au sein du Service européen pour l'action extérieure (SEAE). Le rapport devrait être mis à la disposition des instances compétentes du Conseil, de la Commission, de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité et du réseau des CSIRT.

(23) **Le soutien apporté par l'Agence aux** enquêtes techniques ex post [...] sur les incidents ayant un impact significatif [...], sur demande des États membres concernés [...], devrait être axé sur la prévention des incidents futurs [...]. **Les États membres concernés devraient fournir les informations requises pour permettre à l'Agence de soutenir efficacement l'enquête technique.**

(24) [...]

(25) Les États membres peuvent inviter les entreprises concernées par l'incident à coopérer en fournissant les renseignements et l'assistance nécessaires à l'Agence, sans préjudice de leur droit de protéger les informations commercialement sensibles.

(26) Pour mieux comprendre les défis dans le domaine de la cybersécurité et en vue de fournir aux États membres et aux institutions de l'Union des conseils stratégiques à long terme, l'Agence devrait analyser les risques actuels et émergents. À cet effet, l'Agence devrait, en coopération avec les États membres et, le cas échéant, avec des instituts de statistique et d'autres organismes, recueillir des informations pertinentes **disponibles publiquement ou partagées volontairement** sur les technologies émergentes, les soumettre à des analyses et fournir des évaluations thématiques spécifiques sur les effets sociétaux, juridiques, économiques et réglementaires à attendre des innovations technologiques sur la sécurité des réseaux et de l'information, et notamment sur la cybersécurité. L'Agence devrait en outre aider les États membres et les institutions, organes et organismes de l'Union à déceler les tendances nouvelles et à prévenir les **incidents de** [...] cybersécurité, en procédant à l'analyse des menaces et incidents.

(27) Afin de renforcer la résilience de l'Union, l'Agence devrait développer l'excellence en matière de **cyber**sécurité **des infrastructures soutenant en particulier les secteurs énumérés à l'annexe II de la directive SRI et de celles utilisées par les fournisseurs de services numériques énumérés à l'annexe III de ladite directive [...],** en fournissant des conseils, des orientations ou des bonnes pratiques. En vue de faciliter l'accès à des informations mieux structurées sur les risques de cybersécurité et les solutions possibles, l'Agence devrait mettre sur pied et gérer le "pôle d'information" de l'Union, un portail servant de guichet unique pour l'obtention d'informations sur la cybersécurité en provenance des institutions, organes et organismes de l'UE et nationaux.

(28) L'Agence devrait contribuer à sensibiliser le public aux risques liés à la cybersécurité et fournir, à l'intention des particuliers et des organisations, des orientations sur les bonnes pratiques à adopter par les utilisateurs. L'Agence devrait également contribuer à promouvoir les meilleures pratiques et solutions pour les particuliers et les organisations en collectant et en analysant des informations du domaine public sur les incidents significatifs, et en rédigeant des rapports en vue de fournir des orientations aux entreprises et aux particuliers, et d'améliorer le niveau global de préparation et de résilience. L'Agence devrait en outre organiser, en coopération avec les membres et les institutions, organes et organismes de l'Union, des campagnes d'information régulières et des campagnes publiques d'éducation s'adressant aux utilisateurs finaux, en vue de promouvoir une navigation en ligne plus sûre pour tous et de sensibiliser aux dangers potentiels du cyberespace, y compris la cybercriminalité notamment sous forme de hameçonnages, réseaux zombies, fraudes financières et bancaires, et de donner des conseils de base en matière d'authentification et de protection des données. L'Agence devrait jouer un rôle central dans l'accélération de la sensibilisation des utilisateurs finaux à la sécurité des appareils.

(29) Afin de soutenir les entreprises actives dans le secteur de la cybersécurité, ainsi que les utilisateurs qui recourent aux solutions de cybersécurité, l'Agence devrait mettre sur pied et gérer un "observatoire du marché" en procédant à des analyses régulières des principales tendances observées sur le marché de la cybersécurité, tant du côté de la demande que du côté de l'offre, et en diffusant ses observations.

(30) Pour réaliser pleinement ses objectifs, l'Agence devrait se concerter avec les institutions, organes et organismes compétents, notamment la CERT-UE, le Centre européen de lutte contre la cybercriminalité (EC3) au sein d'Europol, l'Agence européenne de défense (EDA), l'Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle (eu-LISA), l'Agence européenne de la sécurité aérienne (AESA), **l'Agence du GNSS européen (GSA)** et toute autre agence de l'UE jouant un rôle en matière de sécurité informatique. Elle devrait aussi coopérer avec les autorités chargées de la protection des données en vue de procéder à des échanges de savoir-faire et de bonnes pratiques et de leur fournir des conseils sur les aspects liés à la cybersécurité susceptibles d'avoir une incidence sur leurs activités. Les représentants des autorités répressives et des autorités chargées de la protection des données aux échelons national et de l'Union devraient pouvoir être représentés au sein du groupe permanent des parties prenantes de l'Agence. Dans ses relations avec les organismes chargés de l'application de la loi concernant les questions de sécurité des réseaux et de l'information susceptibles d'avoir une incidence sur leurs activités, l'Agence devrait utiliser les canaux d'information existants et les réseaux établis.

(31) L'Agence, [...] **dans son rôle de** secrétariat du réseau des CSIRT, devrait soutenir les CSIRT des États membres et la CERT-UE dans leur coopération opérationnelle ainsi que dans toutes les tâches pertinentes du réseau des CSIRT, telles que définies par la directive SRI. En outre, l'Agence devrait promouvoir et soutenir la coopération entre les CSIRT concernés en cas d'incidents, d'attaques ou de perturbations sur les réseaux ou infrastructures dont les CSIRT assurent la gestion ou la protection et impliquant, ou susceptibles d'impliquer, au moins deux CERT, tout en tenant dûment compte des procédures opératoires standard du réseau des CSIRT.

(32) Afin que l'Union soit mieux préparée pour réagir aux incidents de cybersécurité, l'Agence devrait organiser des exercices [...] **réguliers** de cybersécurité au niveau de l'Union et aider les États membres et les institutions, organes et organismes de l'UE à organiser des exercices s'ils en font la demande.

(33) L'Agence devrait continuer à développer et maintenir son expertise en matière de certification de cybersécurité en vue de soutenir la politique de l'Union dans ce domaine. L'Agence devrait promouvoir le recours à la certification de cybersécurité dans l'Union, notamment en contribuant à l'établissement et au maintien d'un cadre de certification de cybersécurité au niveau de l'Union, en vue de rendre plus transparente l'assurance de la cybersécurité des produits et services TIC et, partant, de rehausser la confiance dans le marché intérieur numérique.

(34) Des politiques de cybersécurité efficaces devraient reposer sur des méthodes d'évaluation des risques bien élaborées, dans le secteur public comme dans le secteur privé. Les méthodes d'évaluation des risques sont utilisées à différents niveaux et il n'existe pas de pratiques communes en ce qui concerne leur application efficace. La promotion et le développement des meilleures pratiques en matière d'évaluation des risques et de solutions interopérables de gestion des risques dans les organisations des secteurs public et privé relèveront le niveau de cybersécurité dans l'Union. À cette fin, l'Agence devrait favoriser la coopération entre parties prenantes au niveau de l'Union, en contribuant à leurs efforts concernant l'établissement et l'adoption de normes européennes et internationales en matière de gestion des risques et de sécurité mesurable des produits, systèmes, réseaux et services électroniques, lesquels, conjointement avec les logiciels, constituent les réseaux et systèmes d'information.

(35) L'Agence devrait encourager les États membres et les fournisseurs de services à renforcer leurs normes de sécurité générales, de manière que tous les utilisateurs d'internet puissent prendre les mesures nécessaires pour garantir leur propre cybersécurité. En particulier, les fournisseurs de services et les fabricants de produits devraient retirer ou recycler les produits et services qui ne satisfont pas aux normes de cybersécurité. En coopération avec les autorités compétentes, l'ENISA peut diffuser des informations sur le niveau de cybersécurité des produits et services offerts sur le marché intérieur, et émettre des alertes visant des fournisseurs et des fabricants et les contraignant à améliorer la sécurité de leurs produits, y compris leur cybersécurité.

(36) L'Agence devrait prendre pleinement en compte les activités en cours en matière de recherche, de développement et d'évaluation technologique, et plus particulièrement celles menées dans le cadre des différentes initiatives de recherche de l'Union, pour fournir des conseils aux institutions, organes et organismes de l'Union et, le cas échéant, à leur demande, aux États membres sur les besoins en matière de recherche dans le domaine de la cybersécurité [...]. **Pour recenser les besoins et les priorités en matière de recherche, l'Agence devrait également consulter les groupes d'utilisateurs concernés.**

(37) Les [...] **menaces** de cybersécurité sont des enjeux mondiaux. Il est nécessaire de renforcer la coopération internationale pour améliorer les normes de **cyber**sécurité, y compris en définissant des normes de comportement communes, et le partage des informations, en encourageant une collaboration internationale plus prompte en réponse aux problèmes de sécurité des réseaux et de l'information ainsi qu'une approche globale commune de ces problèmes. À cette fin, l'Agence devrait aider l'Union à poursuivre son engagement et sa coopération avec les pays tiers et les organisations internationales en mettant, le cas échéant, les compétences et l'analyse nécessaires au service des institutions, organes et organismes de l'Union concernés.

(38) L'Agence devrait être en mesure de réagir aux demandes de conseil et d'assistance ad hoc qui sont formulées par les États membres et les institutions, organes et organismes de l'UE et qui relèvent des objectifs de l'Agence.

(39) Il convient de mettre en œuvre certains principes en ce qui concerne la gouvernance de l'Agence afin de se conformer à la déclaration conjointe et à l'approche commune adoptées par le groupe de travail interinstitutionnel sur les agences décentralisées de l'Union en juillet 2012, le but de cette déclaration et de cette approche étant de rationaliser les activités des agences et d'améliorer leur efficacité. La déclaration conjointe et l'approche commune devraient également se refléter, le cas échéant, dans les programmes de travail, les évaluations, ainsi que les pratiques en matière d'établissement des rapports et les pratiques administratives de l'Agence.

(40) Le conseil d'administration, composé de représentants des États membres et de la Commission, devrait fixer l'orientation générale du fonctionnement de l'Agence et veiller à ce qu'elle exécute ses missions conformément au présent règlement. Le conseil d'administration devrait être doté des pouvoirs nécessaires pour établir le budget, vérifier son exécution, adopter les règles financières appropriées, instaurer des procédures de travail transparentes pour la prise de décisions par l'Agence, adopter le document unique de programmation de l'Agence, adopter son propre règlement intérieur, nommer le directeur exécutif et statuer sur la prolongation du mandat du directeur exécutif et sur l'expiration dudit mandat.

(41) Pour assurer le fonctionnement approprié et efficace de l'Agence, la Commission et les États membres devraient veiller à ce que les personnes désignées au conseil d'administration soient dotées de compétences professionnelles et d'une expérience appropriées dans des domaines opérationnels. La Commission et les États membres devraient s'efforcer de limiter le roulement de leurs représentants respectifs au sein du conseil d'administration, afin de garantir la continuité des travaux de ce dernier.

(42) Le bon fonctionnement de l'Agence exige que le directeur exécutif de celle-ci soit nommé sur la base de son mérite et de ses capacités attestées dans le domaine de l'administration et de la gestion, ainsi que de ses compétences et de son expérience pertinentes en matière de cybersécurité, et qu'il exerce ses fonctions en toute indépendance. Le directeur exécutif devrait élaborer une proposition de programme de travail pour l'Agence, après consultation de la Commission, et prendre toutes les mesures nécessaires pour garantir la bonne exécution de ce programme de travail. Le directeur exécutif devrait préparer un rapport annuel **portant notamment sur la mise en œuvre du programme de travail annuel de l'Agence**, à soumettre au conseil d'administration, établir un projet d'état prévisionnel des recettes et des dépenses de l'Agence et exécuter le budget. Le directeur exécutif devrait en outre avoir la possibilité de créer des groupes de travail ad hoc pour traiter de questions spécifiques, en particulier de nature scientifique, technique, juridique ou socio-économique. Le directeur exécutif devrait veiller à ce que les membres des groupes de travail ad hoc soient sélectionnés aux niveaux d'expertise les plus élevés, compte dûment tenu de la nécessité d'assurer une représentation équilibrée, en fonction des questions spécifiques concernées, des administrations publiques des États membres, des institutions de l'Union et du secteur privé, y compris des entreprises, des utilisateurs et des experts universitaires en matière de sécurité des réseaux et de l'information.

(43) Le conseil exécutif devrait contribuer au fonctionnement efficace du conseil d'administration. Dans le cadre de ses travaux préparatoires liés aux décisions du conseil d'administration, il devrait examiner de manière approfondie les informations pertinentes, étudier les options disponibles et proposer des conseils et des solutions.

(44) L'Agence devrait disposer, à titre d'organe consultatif, d'un groupe permanent des parties prenantes pour maintenir un dialogue régulier avec le secteur privé, les organisations de consommateurs et les autres parties prenantes. Le groupe permanent des parties prenantes, institué par le conseil d'administration sur proposition du directeur exécutif, devrait s'attacher à examiner des questions pertinentes pour les parties prenantes et à les porter à l'attention de l'Agence. La composition du groupe permanent des parties prenantes et les tâches assignées à ce groupe, qui doit être consulté en particulier sur le projet de [...] **p**rogramme de [...] **t**ravail, devraient assurer une représentation suffisante des parties prenantes dans le travail de l'Agence.

(45) L'Agence devrait disposer de règles en matière de prévention et de gestion des conflits d'intérêts. L'Agence devrait aussi appliquer les dispositions pertinentes du droit de l'Union en ce qui concerne l'accès du public aux documents prévu par le règlement (CE) n° 1049/2001 du Parlement européen et du Conseil[12]. Le traitement des données à caractère personnel devrait être régi par le règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données[13]. L'Agence devrait respecter les dispositions applicables aux institutions de l'Union et la législation nationale concernant le traitement des informations, notamment les informations non classifiées sensibles et les informations classifiées de l'UE.

---

12 Règlement (CE) n° 1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission (JO L 145 du 31.5.2001, p. 43).

13 JO L 8 du 12.1.2001, p. 1.

(46) Pour garantir l'autonomie et l'indépendance complètes de l'Agence et lui permettre d'effectuer des missions nouvelles et supplémentaires, y compris des missions urgentes imprévues, il conviendrait de la doter d'un budget suffisant et autonome dont l'essentiel des recettes provienne d'une contribution de l'Union et de contributions des pays tiers participant aux travaux de l'Agence. La plus grande partie des effectifs de l'Agence devrait se consacrer directement à la mise en œuvre opérationnelle du mandat de l'Agence. L'État membre d'accueil ou tout autre État membre devrait être autorisé à apporter des contributions volontaires aux recettes de l'Agence. La procédure budgétaire de l'Union devrait rester applicable en ce qui concerne toute subvention imputable sur le budget général de l'Union. En outre, la Cour des comptes devrait contrôler les comptes de l'Agence afin de garantir la transparence et la responsabilité.

(47) [...]

(48) La certification de cybersécurité est importante pour accroître la sécurité des produits et services et renforcer la confiance qui leur est accordée. Le marché unique numérique, et en particulier l'économie des données et l'internet des objets, ne peuvent prospérer que si le grand public est convaincu que ces produits et services offrent un certain niveau d'assurance de cybersécurité. Les voitures connectées et automatisées, les dispositifs médicaux électroniques, les systèmes de contrôle-commande industriels ou les réseaux intelligents ne sont que quelques exemples de secteurs dans lesquels la certification est déjà largement utilisée ou est susceptible de l'être dans un avenir proche. Les secteurs régis par la directive SRI sont également des secteurs où la certification de cybersécurité joue un rôle critique.

(49) Dans la communication de 2016 intitulée "Renforcer le système européen de cyberrésilience et promouvoir la compétitivité et la cybersécurité", la Commission a souligné le besoin de produits et de solutions de très bonne qualité, abordables et interopérables en matière de cybersécurité. L'offre de produits et services TIC au sein du marché unique reste très dispersée sur le plan géographique. Cela est dû au fait que le secteur de la cybersécurité en Europe s'est développé principalement en fonction de la demande des pouvoirs publics nationaux. Le manque de solutions interopérables (normes techniques), de pratiques et de mécanismes de certification à l'échelle de l'UE est l'une des autres lacunes affectant le marché unique dans le domaine de la cybersécurité. Il en résulte, d'une part, qu'il est difficile pour les entreprises européennes d'être concurrentielles aux niveaux national, européen et mondial, et, d'autre part, que le choix des technologies viables et utilisables en matière de cybersécurité qui s'offre aux particuliers et aux entreprises est restreint. Dans le même ordre d'idées, dans son examen à mi-parcours de la mise en œuvre de la stratégie pour le marché unique numérique, la Commission a insisté sur le besoin de produits et systèmes connectés qui soient sûrs, et a indiqué que la création d'un cadre européen de la sécurité des TIC fixant des règles sur les modalités d'organisation de la certification de sécurité des TIC dans l'UE pourrait à la fois préserver la confiance dans l'internet et lutter contre la fragmentation du marché de la cybersécurité.

(50) Actuellement, la certification de cybersécurité des **processus,** produits et services TIC n'est utilisée que de façon limitée. Lorsqu'elle existe, elle intervient généralement au niveau des États membres ou dans le cadre de systèmes pilotés par les entreprises concernées. Dans ce contexte, un certificat délivré par une autorité nationale de cybersécurité n'est pas, en principe, reconnu par d'autres États membres. Il arrive donc que les entreprises doivent certifier leurs produits et services dans les différents États membres où elles exercent leurs activités, par exemple pour participer à des procédures nationales de passation de marchés. En outre, alors que de nouveaux systèmes voient le jour, il ne semble pas exister d'approche cohérente et globale des questions de cybersécurité transversales, par exemple dans le domaine de l'internet des objets. Les systèmes existants présentent des lacunes importantes et des différences en termes de couverture des produits, de niveau d'assurance, de critères de fond et d'utilisation effective.

(51) Des efforts ont été réalisés dans le passé pour parvenir à une reconnaissance mutuelle des certificats en Europe, mais ils n'ont que partiellement abouti. L'exemple le plus marquant à cet égard est l'accord de reconnaissance mutuelle (ARM) du SOG-IS (groupe de hauts fonctionnaires pour la sécurité des systèmes d'information). Même s'il est le modèle le plus remarquable en ce qui concerne la coopération et la reconnaissance mutuelle en matière de certification de sécurité, [...] le SOG-IS ne réunit qu'une partie des États membres de l'Union. De ce fait, son ARM n'a eu qu'une efficacité limitée dans la perspective du marché intérieur.

(52) Compte tenu de ce qui précède, il est nécessaire d'établir un cadre européen de certification de cybersécurité définissant les principales exigences horizontales pour les systèmes de certification de cybersécurité à développer, et permettant la reconnaissance et l'utilisation dans tous les États membres des certificats **et des déclarations de conformité de l'UE pour les** produits et services TIC. Le cadre européen devrait poursuivre un double objectif. D'une part, il devrait contribuer à rehausser la confiance dans les produits et services TIC qui ont été certifiés conformément à de tels systèmes. D'autre part, il devrait éviter la multiplication de certifications de cybersécurité nationales contradictoires ou faisant double emploi, ce qui réduirait les coûts à charge des entreprises opérant dans le marché unique numérique. Les systèmes devraient être non discriminatoires et fondés sur des normes internationales et/ou [...] **européennes**, sauf si ces normes sont inefficaces ou inappropriées pour remplir les objectifs légitimes de l'UE à cet égard.

(53) La Commission devrait être habilitée à adopter des systèmes européens de certification de cybersécurité concernant des groupes spécifiques de **processus,** produits et services TIC. Ces systèmes devraient être mis en œuvre et contrôlés par des autorités nationales de [...] certification **de cybersécurité**, et les certificats délivrés au titre de ces systèmes devraient être valables et reconnus sur tout le territoire de l'Union. Les systèmes de certification gérés par les entreprises concernées ou d'autres organismes privés devraient être exclus du champ d'application du présent règlement. Toutefois, les organismes qui gèrent un système de ce type peuvent proposer à la Commission de le prendre pour base en vue de l'approuver en tant que système européen.

(54) Les dispositions du présent règlement devraient être sans préjudice de la législation de l'Union prévoyant des règles spécifiques concernant la certification des produits et services TIC. En particulier, le règlement général sur la protection des données (RGPD) contient des dispositions en vue de la mise en place de mécanismes de certification ainsi que de labels et de marques en matière de protection des données afin de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent ledit règlement. Ces mécanismes de certification et ces labels et marques en matière de protection des données devraient permettre aux personnes concernées d'évaluer rapidement le niveau de protection des données offert par les produits et services en question. Le présent règlement est sans préjudice de la certification des opérations de traitement des données au titre du RGPD, y compris lorsque ces opérations sont intégrées dans des produits et services.

(55) Les systèmes européens de certification de cybersécurité devraient avoir pour finalité de garantir que les **processus,** produits et services TIC certifiés selon un tel système sont conformes aux exigences spécifiées, [...] **l'objectif étant de** [...] **protéger** la disponibilité, l'authenticité, l'intégrité et la confidentialité de données stockées ou transmises ou traitées, ou les fonctions connexes des produits, processus, services et systèmes au sens du présent règlement, **tout au long de leur cycle de vie**, ou les services qu'ils offrent ou qui sont accessibles par leur intermédiaire. Il n'est pas possible d'exposer en détail dans le présent règlement les exigences de cybersécurité se rapportant à tous les **processus,** produits et services TIC. Les **processus,** produits et services TIC et les besoins de cybersécurité correspondants sont si diversifiés qu'il est très difficile d'établir des exigences de cybersécurité d'application universelle. Il est donc nécessaire d'adopter, aux fins de la certification, une notion large et générale de la cybersécurité, complétée par une série d'objectifs spécifiques en matière de cybersécurité qui devraient être pris en compte lors de la conception de systèmes européens de certification de cybersécurité. Les modalités selon lesquelles ces objectifs seront atteints pour des **processus,** produits et services TIC spécifiques devraient ensuite être précisées en détail au niveau des différents systèmes de certification adoptés par la Commission, par exemple en faisant référence à des normes ou à des spécifications techniques **lorsqu'il n'existe aucune norme appropriée**.

(55 *bis*) Les spécifications techniques à utiliser dans un système européen de certification de cybersécurité devraient être définies en respectant les principes énoncés à l'annexe II du règlement (UE) n° 1025/2012. Il pourrait toutefois être jugé nécessaire de s'écarter quelque peu de ces principes dans des cas dûment justifiés, lorsque ces spécifications techniques doivent être utilisées dans un système européen de certification de cybersécurité renvoyant à un niveau d'assurance élevé. Les motifs de ces écarts doivent être rendus publics.

(55 *ter*) L'évaluation certifiée de la conformité est le processus consistant à évaluer s'il est satisfait à certaines exigences liées à un processus, un produit ou un service TIC. Ce processus est réalisé par un tiers indépendant, autre que le fabricant du produit ou le fournisseur du service. Le processus de délivrance d'un certificat est consécutif au processus menant à une évaluation positive d'un processus, produit ou service TIC. Il convient de le considérer comme une confirmation que l'évaluation correspondante a été dûment réalisée. En fonction du niveau d'assurance, le système européen de cybersécurité devrait déterminer si le certificat est délivré par un organisme privé ou public. L'évaluation de la conformité et la certification ne peuvent garantir en soi que les produits et services TIC certifiés sont fiables du point de vue de la cybersécurité. Il s'agit plutôt d'une procédure et d'une méthodologie technique visant à attester que des produits et services TIC ont été soumis à des essais et qu'ils sont conformes à certaines exigences de cybersécurité définies par ailleurs, par exemple dans des normes techniques.

(55 *quater*) Le choix, effectué par les utilisateurs de certificats, du niveau approprié de certification et des exigences de sécurité correspondantes devrait se fonder sur une analyse des risques concernant l'utilisation du processus, produit ou service TIC. Le niveau d'assurance devrait donc être proportionnel au niveau de risque correspondant à l'utilisation prévue d'un processus, produit ou service TIC.

(55 *quinquies*) Un système européen de certification de cybersécurité pourrait prévoir une évaluation de la conformité devant être effectuée sous la seule responsabilité du fabricant ou du fournisseur de produits et services TIC (autoévaluation de la conformité). En pareils cas, il suffit que le fabricant ou le fournisseur effectue lui-même tous les contrôles pour garantir la conformité des processus, produits ou services TIC avec le système de certification. Ce type d'évaluation de la conformité devrait être considéré comme approprié pour les produits et services TIC de faible complexité (par exemple lorsque la conception et le mécanisme de production sont simples) qui présentent un risque faible du point de vue de l'intérêt général. En outre, seuls les produits et services TIC correspondant à un niveau d'assurance élémentaire pourraient faire l'objet d'une autoévaluation de la conformité.

(55 *sexies*) Un système européen de certification de cybersécurité pourrait permettre à la fois la certification et l'autoévaluation de la conformité des produits et services TIC. Dans ce cas, ce système devrait prévoir des modalités claires et compréhensibles permettant aux consommateurs ou aux autres utilisateurs de distinguer les produits et services évalués sous la responsabilité du fabricant ou du fournisseur des produits et services certifiés par un tiers.

(55 *septies*) Le fabricant ou le fournisseur de produits et services TIC qui effectue une autoévaluation de la conformité devrait établir et signer la déclaration de conformité de l'UE dans le cadre de la procédure d'évaluation de la conformité. La déclaration de conformité de l'UE est le document qui indique que le produit ou service TIC concerné est conforme aux exigences du système. En établissant et en signant la déclaration de conformité de l'UE, le fabricant ou le fournisseur assume la responsabilité de la conformité du produit ou service TIC avec les prescriptions légales du système. Une copie de la déclaration de conformité de l'UE devrait être soumise à l'autorité nationale de certification de cybersécurité et à l'ENISA.

(55 *octies*) Le fabricant ou le fournisseur de produits et de services TIC devrait garder à la disposition de l'autorité nationale compétente en matière de certification de cybersécurité, pour une durée fixée dans le système européen de certification de cybersécurité concerné, la déclaration de conformité de l'UE et la documentation technique concernant toutes les informations pertinentes liées à la conformité des produits ou services TIC avec un système. La documentation technique devrait préciser les exigences applicables et couvrir, dans la mesure nécessaire à l'évaluation, la conception, la fabrication et le fonctionnement du produit ou du service TIC. La documentation technique devrait être compilée de façon à permettre l'évaluation de la conformité d'un produit ou d'un service TIC avec les exigences applicables.

(55 *nonies*) Les États membres ainsi que les organisations intervenantes intéressées devraient être autorisés à proposer au Groupe européen de certification de cybersécurité la préparation d'un système candidat. Les organisations intervenantes intéressées sont les organisations représentant les entreprises concernées ou les consommateurs, y compris les représentants des organisations de PME qui ont un intérêt valable dans la conception d'un système européen de certification de cybersécurité spécifique. Les propositions faites en ce sens devraient être examinées à la lumière des critères définis par le Groupe européen de certification de cybersécurité en fonction de lignes directrices fondées sur les principes de transparence, d'ouverture, d'impartialité, de consensus, d'efficacité, de pertinence et de cohérence.

(56) La Commission **et le groupe** devraient être habilités à demander à l'ENISA de préparer **sans retard injustifié** des systèmes candidats pour des **processus,** produits ou services TIC spécifiques. Sur la base du système candidat que propose l'ENISA, la Commission devrait alors être habilitée à adopter le système européen de certification de cybersécurité par voie d'actes d'exécution. Compte tenu de la finalité générale du présent règlement et des objectifs de sécurité qui y sont définis, tout système européen de certification de cybersécurité adopté par la Commission devrait préciser un ensemble minimal d'éléments relatifs à l'objet, au champ d'application et au fonctionnement du système considéré. Ces éléments devraient comprendre notamment le champ d'application et l'objet de la certification de cybersécurité, notamment l'indication des catégories de **processus,** produits et services TIC couverts, la description détaillée des exigences de cybersécurité (par exemple par référence à des normes ou spécifications techniques), les critères et méthodes d'évaluation spécifiques, le niveau d'assurance visé, c'est-à-dire élémentaire, substantiel ou élevé, **ainsi que les niveaux d'évaluation lorsqu'il y a lieu.**

(56 *bis*) L'assurance que donne un système européen de certification est le fondement permettant de garantir qu'un processus, produit ou service TIC est conforme aux exigences de sécurité d'un système européen de certification de cybersécurité spécifique. Pour assurer la cohérence du cadre relatif aux processus, produits et services TIC certifiés, un système européen de certification de cybersécurité pourrait préciser les niveaux d'assurance pour les certificats européens de cybersécurité et les déclarations de conformité de l'UE délivrés dans le cadre de ce système. Chaque certificat pourrait renvoyer à l'un des niveaux d'assurance, à savoir élémentaire, substantiel ou élevé, tandis que la déclaration de conformité de l'UE ne pourrait renvoyer qu'au niveau d'assurance élémentaire. Les niveaux d'assurance prévoient un niveau correspondant d'efforts pour l'évaluation [...] et sont caractérisés sur la base de spécifications techniques, normes et procédures connexes, y compris les contrôles techniques, l'objectif étant de prévenir les incidents de cybersécurité ou d'en limiter les conséquences. Chaque niveau d'assurance devrait être cohérent dans les différents domaines sectoriels dans lesquels la certification s'applique.

(56 *ter*) **Un système européen de certification de cybersécurité peut spécifier plusieurs niveaux d'évaluation, selon la rigueur et l'ampleur de la méthode d'évaluation utilisée, celle-ci devant correspondre à l'un des niveaux d'assurance et à une combinaison appropriée de composantes d'assurance. Pour tous les niveaux d'assurance, le produit ou service TIC devrait contenir un certain nombre de fonctions sécurisées, définies dans le cadre du système, pouvant comprendre une configuration sécurisée prête à l'emploi, un code signé, une mise à jour sécurisée, la limitation de l'exploitation de failles ainsi que des protections complètes de la pile/du tas. Ces fonctions devraient faire l'objet d'un développement et d'une maintenance fondés sur des approches de développement mettant l'accent sur la sécurité et des outils correspondants, afin d'assurer que des mécanismes efficaces (au niveau tant du matériel que du logiciel) sont incorporés de manière fiable. Pour le niveau d'assurance élémentaire, l'évaluation devrait être orientée, au moins, par les composantes d'assurance suivantes: l'évaluation devrait comprendre au moins un examen, par l'organisme d'évaluation de la conformité, des documents techniques accompagnant le produit ou service TIC. Lorsque la certification inclut des processus TIC, le processus de conception, de développement et de maintenance d'un produit ou service TIC devrait également être soumis à l'examen technique. Lorsqu'un système européen de certification de cybersécurité prévoit une autoévaluation de la conformité, il devrait suffire que le fabricant ou le fournisseur ait effectué une autoévaluation de la conformité du processus, des produits ou des services TIC avec le système de certification. Pour le niveau d'assurance substantiel, l'évaluation devrait reposer au moins, en plus des éléments du niveau d'assurance élémentaire, sur la vérification de la conformité des fonctionnalités de sécurité du produit ou service TIC avec sa documentation technique. Pour le niveau d'assurance élevé, l'évaluation devrait reposer au moins, en plus des éléments du niveau d'assurance substantiel, sur un test d'efficacité évaluant la résistance des fonctionnalités de sécurité du produit ou service TIC face à des acteurs qui lancent des cyberattaques élaborées en s'appuyant sur des compétences et des ressources importantes.**

(56 *quater*) Lors de l'élaboration d'un système candidat, l'ENISA devrait consulter toutes les parties prenantes, par exemple les organisations européennes de normalisation, les autorités nationales concernées, les organismes fondés sur des accords de reconnaissance mutuelle, comme l'ARM du SOG-IS, les PME, les organisations de consommateurs ainsi que les intervenants en matière environnementale ou sociale.

(56 *quinquies*) L'ENISA devrait maintenir un site web fournissant des informations sur les systèmes européens de certification de cybersécurité et leur donnant une visibilité, qui devrait comprendre, notamment, les demandes d'élaboration d'un système européen de certification de cybersécurité candidat ainsi que les retours d'information reçus lors du processus de consultation réalisé par l'ENISA au cours de la phase préparatoire. Un tel site web devrait en outre fournir des informations sur les certificats et les déclarations de conformité de l'UE délivrées en application du présent règlement.

(57) Le recours à la certification européenne de cybersécurité **et à la déclaration de conformité de l'UE** devrait rester volontaire, sauf disposition contraire dans la législation de l'Union ou la législation nationale **adoptée conformément au droit de l'Union. En l'absence de législation harmonisée, les États membres peuvent adopter des réglementations techniques nationales conformément à la directive (UE) 2015/1535 prévoyant une certification obligatoire dans le cadre d'un système européen de certification de cybersécurité. Les États membres pourraient aussi recourir à la certification européenne de cybersécurité dans le contexte d'un marché public et de la directive 2014/24/UE.**

(57 *bis*) En vue de réaliser les objectifs du présent règlement et d'éviter la fragmentation du marché intérieur, les systèmes ou procédures nationaux de certification de cybersécurité applicables aux produits et services TIC couverts par un système européen de certification de cybersécurité devraient cesser de produire des effets à compter de la date arrêtée par la Commission par voie d'acte d'exécution. De plus, les États membres devraient s'abstenir d'instaurer de nouveaux systèmes de certification nationaux portant sur la cybersécurité de produits et services TIC déjà couverts par un système européen de certification de cybersécurité existant. Toutefois, il convient de ne pas empêcher les États membres d'adopter ou de maintenir des systèmes nationaux de certification à des fins de sécurité nationale.

(58) Une fois un système européen de certification de cybersécurité adopté, les fabricants de produits TIC ou les fournisseurs de services TIC devraient être en mesure de soumettre une demande de certification de leurs produits ou services à l'organisme d'évaluation de la conformité de leur choix. Les organismes d'évaluation de la conformité devraient être agréés par un organisme d'accréditation s'ils satisfont à certaines exigences précises énoncées dans le présent règlement. L'accréditation devrait être accordée pour une durée maximale de cinq ans et pouvoir être renouvelée dans les mêmes conditions pourvu que l'organisme d'évaluation de la conformité satisfasse aux exigences. Elle devrait être **limitée, suspendue ou** révoquée si les conditions de l'accréditation ne sont pas ou plus remplies ou si des mesures prises par l'organisme d'évaluation de la conformité enfreignent le présent règlement.

(59) [...] Les États membres [...] devraient désigner une **ou plusieurs** autorités [...] de certification de cybersécurité **afin de contrôler le respect des obligations découlant du présent règlement**. **Si un État membre le juge approprié, les tâches peuvent être confiées également à des autorités déjà existantes. Les États membres devraient également pouvoir décider, d'un commun accord avec un autre État membre, de désigner une ou plusieurs autorités de contrôle sur le territoire de cet autre État membre. En particulier, l'autorité devrait contrôler et faire respecter les obligations qui incombent au fabricant ou fournisseur de produits et services TIC établi sur le territoire en question en ce qui concerne la déclaration de conformité de l'UE, assister les organismes nationaux d'accréditation dans le contrôle et la supervision des activités des organismes d'évaluation de la conformité en leur fournissant une expertise et les informations utiles, autoriser les organismes d'évaluation de la conformité à accomplir leurs tâches lorsqu'ils respectent les exigences supplémentaires fixées dans un système, et suivre les évolutions pertinentes dans le domaine de la certification de cybersécurité [...]**. Les autorités nationales de [...] certification **de cybersécurité** devraient traiter les réclamations introduites par toute personne physique ou morale en rapport avec les certificats **qu'elles ont délivrés ou qui l'ont été par les organismes d'évaluation de la conformité en ce qui concerne le niveau d'assurance élevé** [...], examiner l'objet de la réclamation dans la mesure nécessaire et informer l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable. De plus, elles devraient coopérer avec les autres autorités nationales [...] de certification **de cybersécurité** ou d'autres autorités publiques, notamment en s'échangeant des informations sur l'éventuelle non-conformité de produits et services TIC aux exigences du présent règlement ou à celles de systèmes de certification de cybersécurité spécifiques.

(60) Afin d'assurer l'application cohérente du cadre européen de certification de cybersécurité, un Groupe européen de certification de cybersécurité (ci-après dénommé "Groupe"), constitué des **représentants des** autorités nationales de [...] certification de cybersécurité **ou d'autres autorités nationales concernées**, devrait être mis en place. Les tâches principales du Groupe devraient consister à conseiller et assister la Commission dans ses efforts pour assurer une mise en œuvre et une application cohérentes du cadre européen de certification de cybersécurité; à assister l'Agence et à coopérer étroitement avec elle dans la préparation des systèmes de certification de cybersécurité candidats; à recommander à la Commission qu'elle demande à l'Agence d'élaborer un système européen de certification de cybersécurité candidat; et à adopter des avis adressés à **l'Agence sur les systèmes candidats et à** la Commission concernant l'actualisation et le réexamen de systèmes européens de certification de cybersécurité existants.

(60 *bis*) Le Groupe devrait faciliter l'échange de bonnes pratiques et d'expertise entre les autorités nationales de certification de cybersécurité responsables de l'accréditation des organismes d'évaluation de la conformité et de la délivrance des certificats. **Le Groupe devrait soutenir l'élaboration d'un mécanisme d'examen par les pairs dans le contexte de la préparation d'un système candidat et de sa mise en œuvre pour les organismes qui délivrent des certificats européens de cybersécurité pour le niveau d'assurance élevé. Un tel examen par les pairs devrait notamment consister à évaluer si les organismes concernés disposent de l'expertise nécessaire et s'acquittent de leurs tâches de façon harmonisée. Les résultats des examens par les pairs devraient être rendus publics. Les organismes concernés devraient adopter des mesures appropriées pour adapter leurs pratiques et leur expertise.**

(61) Dans une optique de sensibilisation et pour faciliter l'acceptation de futurs systèmes européens de certification de cybersécurité, la Commission européenne peut publier des lignes directrices générales ou sectorielles dans le domaine de la cybersécurité, par exemple sur les bonnes pratiques ou les comportements responsables en matière de cybersécurité, en soulignant les effets positifs de l'utilisation de produits et services TIC certifiés.

(61 *bis*) Pour faciliter plus encore les échanges, et compte tenu du fait que les chaînes d'approvisionnement TIC sont mondiales, des accords de reconnaissance mutuelle concernant les certificats délivrés par des systèmes établis au titre du cadre européen de certification de cybersécurité peuvent être conclus par l'Union en application de l'article 218 du TFUE. La Commission, tenant compte de l'avis de l'ENISA et du Groupe européen de certification de cybersécurité, peut recommander l'ouverture de négociations à cette fin. Chaque système devrait prévoir des conditions spécifiques de reconnaissance mutuelle avec les pays tiers.

(62) […]

(63) [...]

(64) Afin d'assurer des conditions uniformes d'exécution du présent règlement, il convient de conférer des compétences d'exécution à la Commission lorsque le présent règlement le prévoit. Ces compétences devraient être exercées en conformité avec le règlement (UE) n° 182/2011.

(65) La procédure d'examen devrait être utilisée pour l'adoption d'actes d'exécution concernant les systèmes européens de certification de cybersécurité applicables à des produits et services TIC; concernant les modalités d'exécution des [...] **enquêtes** menées par l'Agence; et concernant les circonstances, les formats et les procédures de notification à la Commission, par les autorités nationales de [...] certification **de cybersécurité**, des organismes d'évaluation de la conformité accrédités.

(66) Le fonctionnement de l'Agence devrait faire l'objet d'une évaluation indépendante. Cette évaluation devrait s'intéresser à la réalisation des objectifs, aux méthodes de travail et à la pertinence des missions de l'Agence. L'évaluation devrait également porter sur l'impact, l'efficacité et l'efficience du cadre européen de certification de cybersécurité.

(67) Il y a lieu d'abroger le règlement (UE) n° 526/2013.

(68) Étant donné que les objectifs du présent règlement ne peuvent pas être réalisés de manière suffisante par les États membres, mais peuvent 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 ces objectifs,

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

TITRE I
DISPOSITIONS GÉNÉRALES

Article premier

Objet et champ d'application

1. En vue d'assurer le bon fonctionnement du marché intérieur tout en cherchant à atteindre un niveau élevé de cybersécurité, de cyberrésilience et de confiance au sein de l'Union, le présent règlement:

a) fixe les objectifs, les missions et les aspects organisationnels de l'ENISA, Agence de l'Union européenne pour la cybersécurité, ci-après dénommée "Agence"; et

b) instaure un cadre pour la mise en place de systèmes européens de certification de cybersécurité dans le but de garantir un niveau suffisant de cybersécurité des **processus,** produits et services TIC dans l'Union. Ce cadre s'applique sans préjudice des dispositions spécifiques d'autres actes de l'Union en matière de certification volontaire ou obligatoire.

2. **Le présent règlement est sans préjudice des compétences des États membres en ce qui concerne la cybersécurité et, en tout état de cause, sans préjudice des activités relatives à la sécurité publique, à la défense et à la sécurité nationale, et des activités de l'État dans les domaines du droit pénal.**

Article 2

Définitions

Aux fins du présent règlement, on entend par:

1) "cybersécurité", toutes les activités nécessaires pour protéger les réseaux et les systèmes d'information, leurs utilisateurs et les personnes exposées contre les cybermenaces;

2) "réseau et système d'information", un réseau et système d'information au sens de l'article 4, point 1), de la directive (UE) 2016/1148;

3) "stratégie nationale en matière de sécurité des réseaux et des systèmes d'information", un cadre au sens de l'article 4, point 3), de la directive (UE) 2016/1148;

4) "opérateur de services essentiels", une entité publique ou privée telle que définie à l'article 4, point 4), de la directive (UE) 2016/1148;

5) "fournisseur de service numérique", toute personne morale qui fournit un service numérique, tel que défini à l'article 4, point 6), de la directive (UE) 2016/1148;

6) "incident", tout événement tel que défini à l'article 4, point 7), de la directive (UE) 2016/1148;

7) "gestion d'incident", toute procédure telle que définie à l'article 4, point 8), de la directive (UE) 2016/1148;

8) "cybermenace", toute circonstance ou tout événement potentiels susceptibles **de nuire ou** de porter atteinte aux réseaux et systèmes d'information, à leurs utilisateurs et aux personnes exposées, **ou encore de provoquer des interruptions**;

9) "système européen de certification de cybersécurité", l'ensemble complet de règles, d'exigences techniques, de normes et de procédures définies à l'échelon de l'Union, qui s'appliquent à la certification **ou à l'évaluation de la conformité** des **processus,** produits et services des technologies de l'information et des communications (TIC) relevant de ce système spécifique;

9 *bis*) "système 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, qui s'appliquent à la certification ou à l'évaluation de la conformité des processus, produits et services TIC relevant de ce système spécifique;

10) "certificat européen de cybersécurité", un document [...] attestant qu'un **processus,** produit ou service TIC donné [...] **a été évalué au regard de sa conformité** aux exigences **de sécurité** spécifiques énoncées dans un système européen de certification de cybersécurité;

11) "produit [...] TIC", tout élément ou groupe d'éléments appartenant aux réseaux et systèmes d'information;

11 *bis*) "service TIC", tout service consistant intégralement ou principalement à transmettre, stocker, récupérer ou traiter des informations au moyen de réseaux et de systèmes d'information;

11 *ter*) "processus TIC", tout ensemble d'activités exécutées pour concevoir, développer, fournir et maintenir un produit ou service TIC;

12) "accréditation", l'accréditation telle que définie à l'article 2, point 10), du règlement (CE) n° 765/2008;

13) "organisme national d'accréditation", un organisme national d'accréditation tel que défini à l'article 2, point 11), du règlement (CE) n° 765/2008;

14) "évaluation de la conformité", l'évaluation de la conformité telle que définie à l'article 2, point 12), du règlement (CE) n° 765/2008;

15) "organisme d'évaluation de la conformité", un organisme d'évaluation de la conformité tel que défini à l'article 2, point 13), du règlement (CE) n° 765/2008;

16) "norme", une norme telle que définie à l'article 2, point 1), du règlement (UE) n° 1025/2012**;**

16 *bis*) "spécification technique", un document qui établit les exigences techniques auxquelles un processus, produit ou service TIC doit répondre;

16 *ter*) "niveau d'assurance", fondement permettant de garantir qu'un processus, produit ou service TIC est conforme aux exigences de sécurité d'un système européen de certification de cybersécurité spécifique et indiquant à quel niveau il a été évalué; le niveau d'assurance ne mesure pas la sécurité d'un processus, produit ou service TIC même.

TITRE II

ENISA, l'"*Agence de [...] l'Union européenne pour la cybersécurité*"

CHAPITRE I

MANDAT ET OBJECTIFS *[...]*

Article 3

Mandat

1. L'Agence exécute les missions qui lui sont assignées par le présent règlement dans le but de contribuer à assurer un niveau élevé de cybersécurité dans **l'ensemble de** l'Union, **notamment en aidant les États membres et les institutions, organes et organismes de l'Union à améliorer la cybersécurité**. **L'Agence sert de point de référence, par ses conseils et son expertise en matière de cybersécurité, pour les institutions, organes et organismes de l'Union.**

2. L'Agence exécute les missions qui lui sont confiées par des actes de l'Union établissant des mesures destinées à rapprocher les dispositions législatives, réglementaires et administratives des États membres relatives à la cybersécurité.

2 *bis*. Dans l'accomplissement de ses missions, l'Agence agit en toute indépendance et tient dûment compte de l'expertise nationale des autorités compétentes des États membres, tout en évitant la duplication des activités.

3. […]

Article 4

Objectifs

1. L'Agence est un centre d'expertise en matière de cybersécurité du fait de son indépendance, de la qualité scientifique et technique des conseils et de l'assistance qu'elle dispense et des informations qu'elle fournit, de la transparence de ses procédures et modes de fonctionnement, et de sa diligence à exécuter ses missions.

2. L'Agence assiste les institutions, organes et organismes de l'Union, ainsi que les États membres, dans l'élaboration et la mise en œuvre des politiques **de l'Union** liées à la cybersécurité**, y compris les politiques sectorielles en la matière**.

3. L'Agence soutient le renforcement des capacités et contribue à l'état de préparation au sein de l'Union en aidant **les institutions, organes et organismes de** l'Union, **ainsi que** les États membres et les parties prenantes des secteurs public et privé à accroître la protection de leurs réseaux et systèmes d'information, à développer **et à améliorer les capacités de résilience et de réaction dans le domaine cyber, et à développer** des aptitudes et des compétences dans le domaine de la cybersécurité [...].

4. L'Agence promeut la coopération et la coordination, au niveau de l'Union, entre les États membres, les institutions, organes et organismes de l'Union et les parties prenantes **des secteurs public et privé** concernées [...] en ce qui concerne les questions liées à la cybersécurité.

5. L'Agence **contribue à renforcer** [...] les capacités dans le domaine de la cybersécurité au niveau de l'Union afin **d'aider** les [...] États membres à prévenir les cybermenaces et à réagir à celles-ci, notamment en cas d'incidents transfrontières.

6. L'Agence promeut le recours à la certification, **en vue d'éviter la multiplication des systèmes de certification dans l'UE. En particulier, elle contribue** [...] à l'établissement et au maintien d'un cadre de certification de cybersécurité au niveau de l'Union, conformément au titre III du présent règlement, en vue de rendre plus transparente l'assurance de la cybersécurité des produits et services TIC et, partant, de rehausser la confiance dans le marché intérieur numérique.

7. L'Agence promeut un niveau élevé de sensibilisation des particuliers et des entreprises aux questions liées à la cybersécurité.

CHAPITRE I **bis**

MISSIONS

Article 5

[...] ***Élaboration et mise en œuvre de la politique et du droit de l'Union***

L'Agence contribue à l'élaboration et à la mise en œuvre de la politique et du droit de l'Union:

1. en apportant son concours et ses conseils, en particulier sous la forme d'avis indépendants et de travaux préparatoires, concernant l'élaboration et la révision de la politique et du droit de l'Union dans le domaine de la cybersécurité, ainsi que les initiatives politiques et législatives sectorielles mettant en jeu des questions liées à la cybersécurité;

2. en aidant les États membres à mettre en œuvre de manière cohérente la politique et le droit de l'Union en matière de cybersécurité, notamment en ce qui concerne la directive (UE) 2016/1148, y compris au moyen d'avis, de lignes directrices, de conseils et de bonnes pratiques sur des thèmes tels que la gestion des risques, le signalement des incidents et le partage d'informations, ainsi qu'en facilitant l'échange de bonnes pratiques entre les autorités compétentes à cet égard;

3. en contribuant, par son expertise et son concours, aux travaux du groupe de coopération institué en application de l'article 11 de la directive (UE) 2016/1148;

4. en soutenant:

   1) l'élaboration et la mise en œuvre de la politique de l'Union dans le domaine de l'identification électronique et des services de confiance, en particulier en fournissant des conseils et des lignes directrices techniques, ainsi qu'en facilitant l'échange de bonnes pratiques entre les autorités compétentes;

   2) l'amélioration du niveau de sécurité des communications électroniques, y compris en fournissant une expertise et des conseils, ainsi qu'en facilitant l'échange de bonnes pratiques entre les autorités compétentes;

5. en facilitant le réexamen périodique des activités liées aux politiques de l'Union, au moyen d'un rapport annuel sur l'avancement de la mise en œuvre du cadre juridique applicable en ce qui concerne:

   a) les notifications d'incidents transmises par le point de contact unique de chaque État membre au groupe de coopération conformément à l'article 10, paragraphe 3, de la directive (UE) 2016/1148;

   b) les notifications d'atteinte à la sécurité et de perte d'intégrité reçues des prestataires de services de confiance et transmises à l'Agence par les organes de contrôle, conformément à l'article 19, paragraphe 3, du règlement (UE) n° 910/2014;

   c) les notifications [...] **d'incidents de** sécurité reçues des entreprises fournissant des réseaux de communications publics ou des services de communications électroniques accessibles au public et transmises à l'Agence par les autorités compétentes, conformément à l'article 40 de la [directive établissant le code des communications électroniques européen].

Article 6

[...] ***Renforcement des capacités***

1. L'Agence assiste:

a) les États membres dans leurs efforts pour améliorer la prévention, la détection et l'analyse des [...] **menaces** et incidents en matière de cybersécurité, ainsi que la capacité d'y réagir, en leur fournissant les connaissances et l'expertise nécessaires;

b) les institutions, organes et organismes de l'Union dans leurs efforts pour améliorer la prévention, la détection et l'analyse des [...] **menaces** et incidents en matière de cybersécurité, ainsi que la capacité d'y réagir, **notamment** en apportant un soutien adapté à l'équipe d'intervention en cas d'urgence informatique pour les institutions, organes et organismes de l'Union (CERT-UE);

c) les États membres, à leur demande, dans la mise en place de centres de réponse aux incidents de sécurité informatique (CSIRT) nationaux, conformément à l'article 9, paragraphe 5, de la directive (UE) 2016/1148;

d) les États membres, à leur demande, dans l'élaboration de leur stratégie nationale en matière de sécurité des réseaux et des systèmes d'information, conformément à l'article 7, paragraphe 2, de la directive (UE) 2016/1148; en outre, l'Agence favorise la diffusion et **suit** [...] **la** mise en œuvre de ces stratégies dans l'Union afin de promouvoir les bonnes pratiques;

e) les institutions de l'Union dans l'élaboration et la révision des stratégies de l'Union en matière de cybersécurité, la promotion de leur diffusion et le suivi de l'avancement de leur mise en œuvre;

f) les CERT nationales et de l'UE dans le relèvement du niveau de leurs capacités, y compris en favorisant le dialogue et l'échange d'informations, pour faire en sorte que, en ce qui concerne l'état de la technologie, chaque CERT satisfasse à un socle commun de capacités minimales et fonctionne selon les meilleures pratiques;

g) les États membres en organisant [...] **régulièrement** les exercices de cybersécurité [...] au niveau de l'Union visés à l'article 7, paragraphe 6, et en formulant des recommandations en vue d'actions sur la base de l'évaluation de ces exercices et des enseignements qui en ont été tirés;

h) les organismes publics concernés en proposant des formations sur la cybersécurité, le cas échéant en coopération avec des parties prenantes;

i) le groupe de coopération [...] **pour ce qui est de l'échange** de [...] bonnes pratiques, notamment en ce qui concerne l'identification, par les États membres, des opérateurs de services essentiels, y compris au regard des dépendances transfrontalières, en matière de risques et d'incidents, conformément à l'article 11, paragraphe 3, point l), de la directive (UE) 2016/1148.

2. L'Agence **soutient le partage d'informations au sein des secteurs et entre ceux-ci** [...], en particulier dans les secteurs énumérés à l'annexe II de la directive (UE) 2016/1148, en proposant des bonnes pratiques et des orientations sur les outils disponibles, ainsi que des procédures, et en indiquant comment traiter les questions de réglementation liées au partage d'informations.

Article 7

[...] ***Coopération opérationnelle au niveau de l'Union***

1. L'Agence apporte son soutien à la coopération opérationnelle entre les **États membres, les institutions, organes et** organismes **de l'Union** [...], et entre les parties prenantes.

2. L'Agence coopère sur le plan opérationnel et crée des synergies avec les institutions, organes et organismes de l'Union, y compris la CERT-UE, les services traitant de la cybercriminalité et les autorités de contrôle responsables de la protection de la vie privée et des données à caractère personnel, en vue de traiter des questions d'intérêt commun, y compris:

   a) en échangeant savoir-faire et bonnes pratiques;

   b) en fournissant des conseils et des lignes directrices sur des questions pertinentes liées à la cybersécurité;

   c) en établissant, après consultation de la Commission, des arrangements pratiques pour l'exécution de missions spécifiques.

3. L'Agence assure le secrétariat du réseau des CSIRT, conformément à l'article 12, paragraphe 2, de la directive (UE) 2016/1148, et facilite **à ce titre** [...] le partage d'informations et la coopération entre les membres du réseau.

4. L'Agence **favorise** [...] la coopération sur le plan opérationnel au sein du réseau des CSIRT par le soutien qu'elle apporte**, à leur demande,** aux États membres:

   a) en prodiguant des conseils sur la façon d'améliorer leur capacité à prévenir et détecter les incidents, et à y réagir;

   b) [...] **en facilitant la gestion** technique [...] des incidents ayant un impact significatif ou substantiel**, en particulier en soutenant le partage volontaire de solutions techniques entre États membres**;

   c) en analysant les vulnérabilités [...] et les incidents**;**

   c *bis*) en apportant un soutien aux enquêtes techniques ex post sur les incidents ayant un impact significatif ou substantiel conformément à la directive (UE) 2016/1148.

Dans l'accomplissement de ces missions, l'Agence mène avec la CERT-UE une coopération structurée afin de tirer avantage des synergies [...] **et d'éviter une duplication des activités**.

5. […]

[…]

6. L'Agence organise **régulièrement** des exercices de cybersécurité [...] à l'échelle de l'Union, et aide, à leur demande, les États membres et les institutions, organes et organismes de l'UE à organiser de tels exercices. **Ces exercices à l'échelle de l'Union peuvent comporter des aspects techniques, opérationnels ou stratégiques** [...]. **Tous les deux ans, un exercice à grande échelle comportant tous ces aspects est organisé.** En outre, l'Agence contribue à des exercices de cybersécurité sectoriels, qu'elle aide à organiser le cas échéant, en collaboration avec des [...] **organisations** compétentes **qui peuvent** [...] participer également à des exercices de cybersécurité à l'échelle de l'Union.

7. L'Agence prépare à intervalles réguliers, **en coopération étroite avec les États membres,** un rapport de situation technique sur les incidents et menaces de cybersécurité dans l'UE, sur la base d'informations provenant de sources ouvertes, de ses propres analyses et des rapports que lui communiquent notamment: les CSIRT des États membres [...] ou les points de contact uniques au titre de la directive SRI (**sur une base volontaire dans les deux cas** [...]), le Centre européen de lutte contre la cybercriminalité (EC3) au sein d'Europol et la CERT-UE.

8. L'Agence contribue à l'élaboration d'une réaction concertée au niveau de l'UE en cas d'incidents ou de crises transfrontières de cybersécurité majeurs, principalement en:

   a) agrégeant des rapports provenant de sources nationales **partagés sur une base volontaire** en vue de contribuer à former une appréciation commune de la situation;

   b) assurant une circulation efficace de l'information et en proposant des mécanismes de remontée des décisions entre le réseau des CSIRT et les décideurs techniques et politiques au niveau de l'Union;

c) [...] **facilitant, à la demande des États membres,** la gestion technique des incidents ou des crises, [...] **en particulier** en [...] **favorisant** le partage **volontaire** de solutions techniques entre les États membres;

d) [...] **soutenant les institutions, organes et organismes de l'UE et, à leur demande, les États membres dans** la communication publique autour des incidents ou des crises;

e) **aidant les États membres, à leur demande, à** mettre [...] à l'épreuve les plans de coopération destinés à réagir à ces incidents ou crises.

Article 8

[...] ***Marché, certification de cybersécurité et normalisation***

L'Agence:

a) soutient et promeut l'élaboration et la mise en œuvre de la politique de l'Union en matière de certification de cybersécurité des **processus,** produits et services TIC, telle que décrite au titre III du présent règlement, en:

1) préparant des systèmes européens de certification de cybersécurité candidats pour des **processus,** produits et services TIC, **en coopération avec les entreprises du secteur et** conformément à l'article 44 du présent règlement;

2) aidant la Commission à assurer le secrétariat du Groupe européen de certification de cybersécurité, conformément à l'article 53 du présent règlement;

3) établissant et publiant des lignes directrices, ainsi qu'en mettant au point des bonnes pratiques en ce qui concerne les exigences de cybersécurité de produits et services TIC, en coopération avec les autorités nationales de certification [...] **de cybersécurité** et les entreprises concernées;

3 *bis*) recommandant des spécifications techniques appropriées pour le recours au développement des systèmes européens de certification de cybersécurité visés à l'article 47, paragraphe 1, point b) dans les cas où il n'existe aucune norme;

3 *ter*) contribuant à un renforcement suffisant des capacités en matière de processus d'évaluation et de certification, en établissant et publiant des lignes directrices ainsi qu'en fournissant un soutien aux États membres, à leur demande;

b) facilite l'établissement et l'adoption de normes européennes et internationales en matière de gestion des risques et de sécurité des **processus,** produits et services TIC [...]**;**

b *bis*) formule, en collaboration avec les États membres, des avis et des lignes directrices concernant les domaines techniques liés aux exigences de sécurité qui s'imposent aux opérateurs de services essentiels et aux fournisseurs de service numérique, et concernant les normes existantes, y compris les normes nationales des États membres, en application de l'article 19, paragraphe 2, de la directive (UE) 2016/1148;

c) effectue et diffuse, à intervalles réguliers, des analyses des principales tendances du marché de la cybersécurité, tant du côté de la demande que du côté de l'offre, en vue de stimuler le marché de la cybersécurité dans l'Union.

Article 9

[...] ***Connaissance et information*** [...]

L'Agence:

a) analyse les technologies émergentes et fournit des évaluations thématiques sur les incidences escomptées des innovations technologiques en matière de cybersécurité du point de vue sociétal, juridique, économique et réglementaire;

b) produit des analyses stratégiques à long terme des menaces et des incidents de cybersécurité afin d'identifier les tendances émergentes et de contribuer à prévenir [...] **les incidents de** cybersécurité;

c) fournit, en coopération avec des experts des États membres, des avis, des orientations et des bonnes pratiques en matière de sécurité des réseaux et des systèmes d'information, en particulier pour la sécurité [...] des infrastructures sur lesquelles s'appuient les secteurs énumérés à l'annexe II de la directive (UE) 2016/1148 **et de celles utilisées par les fournisseurs de services numériques énumérés à l'annexe III de ladite directive**;

d) regroupe, organise et met à la disposition du public, par l'intermédiaire d'un portail spécialisé, des informations sur la cybersécurité, fournies par les institutions, organes et organismes de l'Union **et, sur une base volontaire, par les États membres et les parties prenantes des secteurs publics et privés**;

e) […]

f) collecte et analyse des informations du domaine public sur les incidents significatifs, et rédige des rapports en vue de fournir des orientations aux entreprises et aux particuliers dans toute l'Union;

g) […].

Article 9 **bis**

Sensibilisation et éducation

L'Agence:

a) sensibilise le public aux risques liés à la cybersécurité et fournit, à l'intention des particuliers et des organisations, des orientations sur les bonnes pratiques à adopter par les utilisateurs;

b) organise à intervalles réguliers, en coopération avec les États membres, les institutions, organes et organismes de l'Union et les entreprises concernées, des campagnes d'information afin de renforcer la cybersécurité et d'en accroître la visibilité dans l'Union;

c) aide les États membres dans leurs efforts visant à mieux faire connaître la cybersécurité et à promouvoir l'éducation à la cybersécurité;

d) encourage une coordination plus étroite et l'échange de bonnes pratiques entre les États membres en matière d'éducation et de sensibilisation à la cybersécurité en favorisant la création et le maintien d'un réseau de points de contact nationaux en matière d'éducation.

Article 10

[...] ***Recherche et innovation***

En ce qui concerne la recherche et l'innovation, l'Agence:

a) conseille l'Union et les États membres sur les besoins et les priorités en matière de recherche dans le domaine de la cybersécurité, afin que des réponses efficaces puissent être apportées face aux risques et aux menaces actuels et émergents, y compris en ce qui concerne les technologies de l'information et de la communication nouvelles et émergentes, et afin que les technologies de prévention des risques soient utilisées d'une manière efficace;

b) participe, lorsque la Commission lui a délégué les pouvoirs correspondants, à la phase de mise en œuvre des programmes de financement de la recherche et de l'innovation, ou est bénéficiaire de ces programmes.

Article 11

[...] ***Coopération internationale***

L'Agence contribue aux efforts de l'Union pour coopérer avec les pays tiers et les organisations internationales, afin de promouvoir une coopération internationale sur les problèmes de cybersécurité, en:

a) s'impliquant, le cas échéant, en tant qu'observateur dans l'organisation d'exercices internationaux, ainsi qu'en analysant les résultats de ces exercices et en en rendant compte au conseil d'administration;

b) facilitant [...] l'échange de bonnes pratiques **au sein des cadres de coopération internationale pertinents** [...];

c) mettant son expertise à la disposition de la Commission si elle en fait la demande**;**

c *bis*) fournissant des conseils et un soutien à la Commission, en collaboration avec le Groupe européen de certification de cybersécurité établi en vertu de l'article 53, sur les questions relatives aux accords de reconnaissance mutuelle des certificats de cybersécurité avec des pays tiers.

CHAPITRE II
ORGANISATION DE L'AGENCE

Article 12

Structure

La structure administrative et de gestion de l'Agence comprend:

a) un conseil d'administration, qui exerce les fonctions définies à l'article 14;

b) un conseil exécutif, qui exerce les fonctions définies à l'article 18;

c) un directeur exécutif, qui assume les responsabilités définies à l'article 19; [...]

d) un groupe permanent des parties prenantes, qui exerce les fonctions définies à l'article 20**;**

d *bis*) un réseau des agents de liaison nationaux, qui exerce les fonctions définies à l'article 20 *bis*.

SECTION 1
CONSEIL D'ADMINISTRATION

Article 13

Composition du conseil d'administration

1. Le conseil d'administration est composé d'un représentant de chaque État membre, et de deux représentants nommés par la Commission. Tous les représentants disposent du droit de vote.

2. Chaque membre du conseil d'administration dispose d'un suppléant, qui le représente en cas d'absence.

3. Les membres du conseil d'administration et leurs suppléants sont nommés sur la base de leurs connaissances dans le domaine de la cybersécurité, compte tenu des compétences managériales, administratives et budgétaires requises. La Commission et les États membres s'efforcent de limiter le roulement de leurs représentants au sein du conseil d'administration, afin de garantir la continuité des travaux de celui-ci. La Commission et les États membres visent à atteindre une représentation équilibrée entre hommes et femmes au sein du conseil d'administration.

4. Le mandat des membres du conseil d'administration et de leurs suppléants a une durée de quatre ans. Ce mandat est renouvelable.

Article 14

Fonctions du conseil d'administration

1. Le conseil d'administration:

a) fixe l'orientation générale du fonctionnement de l'Agence et veille à ce que l'Agence travaille conformément aux règles et principes énoncés dans le présent règlement. Il assure aussi la cohérence des travaux de l'Agence avec les activités menées par les États membres ainsi qu'au niveau de l'Union;

b) adopte le projet de document unique de programmation de l'Agence visé à l'article 21, avant de le soumettre pour avis à la Commission;

c) adopte, en tenant compte de l'avis de la Commission, le document unique de programmation de l'Agence, à la majorité des deux tiers des membres et conformément à l'article 17;

c *bis*) supervise la mise en œuvre de la programmation annuelle et pluriannuelle contenue dans le document unique de programmation;

d) adopte le budget annuel de l'Agence à la majorité des deux tiers des membres et exerce d'autres fonctions liées au budget de l'Agence en application du chapitre III;

e) évalue et adopte le rapport annuel consolidé sur les activités de l'Agence et transmet, au plus tard le 1er juillet de l'année suivante, le rapport et son évaluation au Parlement européen, au Conseil, à la Commission et à la Cour des comptes. Le rapport annuel inclut les comptes et décrit la manière dont l'Agence atteint ses indicateurs de performance. Le rapport annuel est rendu public;

f) adopte les règles financières applicables à l'Agence, conformément à l'article 29;

g) adopte une stratégie antifraude qui est proportionnée aux risques de fraude compte tenu de l'analyse coût-bénéfice des mesures à mettre en œuvre;

h) adopte des règles en matière de prévention et de gestion des conflits d'intérêts concernant ses membres;

i) assure le suivi approprié des conclusions et des recommandations découlant des enquêtes de l'Office européen de lutte antifraude (OLAF) et des divers rapports d'audit et évaluations internes ou externes;

j) adopte son règlement intérieur;

k) conformément au paragraphe 2, exerce, à l'égard du personnel de l'Agence, les compétences qui sont dévolues, par le statut des fonctionnaires de l'Union européenne et le régime applicable aux autres agents de l'Union européenne, respectivement à l'autorité investie du pouvoir de nomination et à l'autorité habilitée à conclure les contrats d'engagement ("compétences de l'autorité investie du pouvoir de nomination");

l) arrête les modalités d'application du statut et du régime applicable aux autres agents conformément à la procédure prévue à l'article 110 du statut;

m) nomme le directeur exécutif et, le cas échéant, prolonge son mandat ou le démet de ses fonctions conformément à l'article 33 du présent règlement;

n) nomme un comptable, qui peut être le comptable de la Commission, qui est totalement indépendant dans l'exercice de ses fonctions;

o) prend toutes les décisions relatives à la mise en place des structures internes de l'Agence et, le cas échéant, à leur modification, en tenant compte des besoins liés à l'activité de l'Agence et en respectant le principe d'une gestion budgétaire saine;

p) autorise la conclusion d'arrangements de travail conformément aux articles 7 et 39.

2. Le conseil d'administration adopte, conformément à la procédure prévue à l'article 110 du statut, une décision fondée sur l'article 2, paragraphe 1, du statut et sur l'article 6 du régime applicable aux autres agents, déléguant au directeur exécutif les compétences correspondantes dévolues à l'autorité investie du pouvoir de nomination et définissant les conditions dans lesquelles cette délégation de compétences peut être suspendue. Le directeur exécutif est autorisé à sous-déléguer ces compétences.

3. Lorsque des circonstances exceptionnelles l'exigent, le conseil d'administration peut, par voie de décision, suspendre temporairement la délégation au directeur exécutif des compétences dévolues à l'autorité investie du pouvoir de nomination ainsi que de celles sous-déléguées par le directeur exécutif, pour les exercer lui-même ou les déléguer à un de ses membres ou à un membre du personnel autre que le directeur exécutif.

Article 15

Présidence du conseil d'administration

Le conseil d'administration élit, à la majorité des deux tiers des membres, son président et un vice-président parmi ses membres, pour une durée de quatre ans renouvelable une fois. Cependant, si le président ou le vice-président perd sa qualité de membre du conseil d'administration à un moment quelconque de son mandat, ledit mandat expire automatiquement à la même date. Le vice-président remplace d'office le président lorsque celui-ci n'est pas en mesure d'assumer ses fonctions.

Article 16

Réunions du conseil d'administration

1. Les réunions du conseil d'administration sont convoquées par son président.

2. Le conseil d'administration tient une réunion ordinaire au moins deux fois par an. Il tient aussi des réunions extraordinaires à l'initiative du président, à la demande de la Commission ou à la demande d'au moins un tiers de ses membres.

3. Le directeur exécutif participe sans droit de vote aux réunions du conseil d'administration.

4. Sur invitation du président, des membres du groupe permanent des parties prenantes peuvent participer sans droit de vote aux réunions du conseil d'administration.

5. Les membres du conseil d'administration et leurs suppléants peuvent, dans le respect du règlement intérieur, être assistés au cours des réunions par des conseillers ou des experts.

6. L'Agence assure le secrétariat du conseil d'administration.

Article 17

Règles de vote du conseil d'administration

1. Les décisions du conseil d'administration sont prises à la majorité de ses membres.

2. Une majorité des deux tiers de tous les membres du conseil d'administration est nécessaire pour adopter le document unique de programmation et le budget annuel, pour nommer le directeur exécutif, prolonger son mandat ou le révoquer.

3. Chaque membre dispose d'une voix. En l'absence d'un membre, son suppléant peut exercer son droit de vote.

4. Le président prend part au vote.

5. Le directeur exécutif ne prend pas part au vote.

6. Le règlement intérieur du conseil d'administration fixe les modalités détaillées du vote, notamment les conditions dans lesquelles un membre peut agir au nom d'un autre membre.

SECTION 2
CONSEIL EXÉCUTIF

Article 18

Conseil exécutif

1. Le conseil d'administration est assisté d'un conseil exécutif.

2. Le conseil exécutif:

   a) prépare les décisions qui doivent être adoptées par le conseil d'administration;

   b) assure, avec le conseil d'administration, le suivi approprié des conclusions et des recommandations découlant des enquêtes de l'OLAF ainsi que des divers rapports d'audit interne ou externe et des évaluations;

   c) sans préjudice des responsabilités du directeur exécutif définies à l'article 19, assiste et conseille celui-ci dans la mise en œuvre des décisions du conseil d'administration relatives à des questions administratives et budgétaires, conformément à l'article 19.

3. Le conseil exécutif est composé de cinq membres nommés parmi les membres du conseil d'administration, dont le président du conseil d'administration, qui peut également présider le conseil exécutif, et un des représentants de la Commission. Le directeur exécutif participe aux réunions du conseil exécutif, mais sans droit de vote.

4. La durée du mandat des membres du conseil exécutif est de quatre ans. Ce mandat est renouvelable.

5. Le conseil exécutif se réunit au moins une fois par trimestre. Le président du conseil exécutif convoque des réunions supplémentaires à la demande de ses membres.

6. Le conseil d'administration établit le règlement intérieur du conseil exécutif.

7. […]

SECTION 3
DIRECTEUR EXÉCUTIF

Article 19

Responsabilités du directeur exécutif

1. L'Agence est gérée par son directeur exécutif, qui est indépendant dans l'exécution de ses tâches. Le directeur exécutif rend compte de ses activités au conseil d'administration.

2. Le directeur exécutif fait rapport au Parlement européen sur l'exécution de ses tâches, lorsqu'il y est invité. Le Conseil peut inviter le directeur exécutif à lui faire rapport sur l'exécution de ses tâches.

3. Le directeur exécutif est chargé:

a) d'assurer l'administration courante de l'Agence;

b) de mettre en œuvre les décisions adoptées par le conseil d'administration;

c) de préparer le projet de document unique de programmation et de le soumettre au conseil d'administration pour approbation, avant qu'il ne soit soumis à la Commission;

d) de mettre en œuvre le document unique de programmation et d'en faire rapport au conseil d'administration;

e) de préparer le rapport annuel consolidé sur les activités de l'Agence**, y compris la mise en œuvre du programme de travail annuel,** et de le présenter au conseil d'administration pour évaluation et adoption;

f) de préparer un plan d'action faisant suite aux conclusions des évaluations rétrospectives et de faire rapport tous les deux ans à la Commission sur les progrès accomplis;

g) de préparer un plan d'action donnant suite aux conclusions des rapports d'audit internes ou externes, ainsi qu'aux enquêtes de l'Office européen de lutte antifraude (OLAF), et présenter des rapports semestriels à la Commission et des rapports réguliers au conseil d'administration sur les progrès accomplis;

h) d'élaborer le projet de règles financières applicables à l'Agence;

i) d'établir le projet d'état prévisionnel des recettes et dépenses de l'Agence et d'exécuter son budget;

j) de protéger les intérêts financiers de l'Union par l'application de mesures préventives contre la fraude, la corruption et d'autres activités illégales, par des contrôles efficaces et, si des irrégularités sont constatées, par le recouvrement des montants indûment payés et, le cas échéant, par des sanctions administratives et financières efficaces, proportionnées et dissuasives;

k) de préparer une stratégie antifraude pour l'Agence et de la présenter au conseil d'administration pour approbation;

l) d'établir et de maintenir le contact avec le secteur des entreprises et les organisations de consommateurs afin d'assurer un dialogue régulier avec les parties prenantes concernées;

l *bis*) d'avoir un échange régulier avec les institutions, organes et organismes de l'Union sur leurs activités en matière de cybersécurité, pour assurer la cohérence dans l'élaboration et dans la mise en œuvre de la politique de l'UE;

m) d'exécuter les autres tâches qui lui sont confiées par le présent règlement.

4. En tant que de besoin, dans le cadre du mandat de l'Agence et conformément aux objectifs et aux missions de l'Agence, le directeur exécutif peut créer des groupes de travail ad hoc composés d'experts, y compris des experts des autorités compétentes des États membres. Le conseil d'administration en est préalablement informé. Les modalités concernant en particulier la composition des groupes de travail, la nomination par le directeur exécutif des experts qui les composent et le fonctionnement de ces groupes sont précisées dans les règles internes de fonctionnement de l'Agence.

5. **Lorsque cela s'avère nécessaire, à l'effet d'exécuter les missions de l'Agence de manière efficiente et efficace et sur la base d'une analyse coût-bénéfice appropriée, le** directeur exécutif **peut** décider [...] **d'établir un ou plusieurs bureaux locaux dans un ou plusieurs États membres**. Avant d'arrêter une décision sur l'établissement d'un bureau local, le directeur exécutif **demande l'avis du ou des États membres concernés, notamment l'État membre dans lequel est situé le siège de l'Agence, et** obtient le consentement préalable de la Commission **et** du conseil d'administration [...]. **En cas de désaccord au cours de la procédure de consultation entre le directeur exécutif et les États membres concernés, la question est soumise à l'examen du Conseil.** La décision précise la portée des activités confiées à ce bureau local de manière à éviter les coûts inutiles et les doubles emplois dans les fonctions administratives de l'Agence.[...] **Les effectifs de l'ensemble des bureaux locaux sont maintenus au niveau le plus bas et ne dépassent pas, au total, 40 % des [...] effectifs en place dans l'État membre où se situe le siège de l'Agence. Les effectifs de chaque bureau local ne dépassent pas 10 % des [...] effectifs [...] en place dans l'État membre où se situe le siège de l'Agence.**

SECTION 4
GROUPE PERMANENT DES PARTIES PRENANTES

Article 20

Groupe permanent des parties prenantes

1. Le conseil d'administration crée, sur proposition du directeur exécutif, un groupe permanent des parties prenantes composé d'experts reconnus représentant les parties prenantes concernées, comme les entreprises du secteur des TIC, les fournisseurs de réseaux de communications électroniques ou de services accessibles au public, **les opérateurs de services essentiels,** les organisations de consommateurs, les experts universitaires en matière de cybersécurité et les représentants des autorités compétentes notifiées au titre de la [directive établissant le code des communications électroniques européen], ainsi que les autorités chargées du respect de la loi et de la protection des données.

2. Les procédures applicables au groupe permanent des parties prenantes, notamment en ce qui concerne le nombre de membres, la composition du groupe, la nomination des membres par le conseil d'administration, la proposition par le directeur exécutif et le fonctionnement du groupe sont précisées dans les règles internes de fonctionnement de l'Agence et sont rendues publiques.

3. Le groupe permanent des parties prenantes est présidé par le directeur exécutif ou par toute personne qu'il désigne à cet effet au cas par cas.

4. La durée du mandat des membres du groupe permanent des parties prenantes est de deux ans et demi. Les membres du conseil d'administration ne peuvent pas être membres du groupe permanent des parties prenantes. Des experts de la Commission et des États membres sont autorisés à assister aux réunions et à prendre part aux travaux du groupe permanent des parties prenantes. Des représentants d'autres organismes jugés intéressants par le directeur exécutif, qui ne sont pas membres du groupe permanent des parties prenantes, peuvent être invités à assister aux réunions du groupe permanent des parties prenantes et à prendre part à ses travaux.

5. Le groupe permanent des parties prenantes conseille l'Agence dans l'exercice de ses activités. Il conseille en particulier le directeur exécutif lors de l'élaboration d'une proposition de programme de travail pour l'Agence ainsi que pour la communication avec les parties prenantes concernées sur toutes les questions liées au programme de travail.

5 *bis*. Le groupe permanent des parties prenantes tient le conseil d'administration régulièrement informé de ses activités.

SECTION 4 *bis*
RÉSEAU DES AGENTS DE LIAISON NATIONAUX

Article 20 bis
Réseau des agents de liaison nationaux

1. Le conseil d'administration crée, sur proposition du directeur exécutif, un réseau des agents de liaison nationaux composé de représentants des États membres.

2. Le réseau des agents de liaison nationaux est composé de représentants de tous les États membres. Chaque État membre nomme un représentant. Les réunions du réseau peuvent se tenir dans différentes configurations d'expertise.

3. En particulier, le réseau des agents de liaison nationaux facilite l'échange d'informations entre l'ENISA et les États membres. Il aide notamment l'ENISA à faire connaître ses activités et à diffuser les résultats de ses travaux et recommandations auprès des parties prenantes concernées dans l'ensemble de l'UE.

4. Les agents de liaison nationaux servent de points focaux au niveau national pour faciliter la coopération entre l'ENISA et les experts nationaux dans le cadre de la mise en œuvre du programme de travail de l'ENISA.

5. Si les agents de liaison nationaux devraient coopérer étroitement avec les représentants du conseil d'administration de leurs pays respectifs, le réseau en lui-même ne doit dupliquer le travail ni du conseil d'administration ni d'autres instances de l'UE.

6. Les fonctions et les procédures du réseau des agents de liaison nationaux sont précisées dans les règles internes de fonctionnement de l'Agence et rendues publiques.

SECTION 5
FONCTIONNEMENT

Article 21

Document unique de programmation

1. L'Agence exécute ses tâches conformément à un document unique de programmation qui décrit sa programmation annuelle et pluriannuelle, et qui contient l'ensemble de ses activités planifiées.

2. Le directeur exécutif établit, chaque année, un projet de document unique de programmation contenant la programmation annuelle et pluriannuelle, ainsi que les ressources humaines et financières correspondantes, conformément à l'article 32 du règlement délégué (UE) n° 1271/2013[14] de la Commission, et tenant compte des lignes directrices fixées par la Commission.

3. Le Conseil d'administration adopte, au plus tard le 30 novembre de chaque année, le document unique de programmation visé au paragraphe 1 et le transmet au Parlement européen, au Conseil et à la Commission au plus tard le 31 janvier de l'année suivante, ainsi que toute version de ce document actualisée ultérieurement.

4. Le document unique de programmation devient définitif après l'adoption définitive du budget général de l'Union et, si nécessaire, il est adapté en conséquence.

5. Le programme de travail annuel expose des objectifs détaillés et les résultats escomptés, notamment des indicateurs de performance. Il contient, en outre, une description des actions à financer et une indication des ressources financières et humaines allouées à chaque action, conformément aux principes d'établissement du budget par activités et de la gestion fondée sur les activités. Le programme de travail annuel s'inscrit dans la logique du programme de travail pluriannuel visé au paragraphe 7. Il indique clairement les tâches qui ont été ajoutées, modifiées ou supprimées par rapport à l'exercice précédent.

[14] Règlement délégué (UE) n° 1271/2013 de la Commission du 30 septembre 2013 portant règlement financier-cadre des organismes visés à l'article 208 du règlement (UE, Euratom) n° 966/2012 du Parlement européen et du Conseil (JO L 328 du 7.12.2013, p. 42).

6. Le conseil d'administration modifie le programme de travail annuel adopté lorsqu'une nouvelle tâche est confiée à l'Agence. Toute modification substantielle du programme de travail annuel est soumise à une procédure d'adoption identique à celle applicable au programme de travail annuel initial. Le conseil d'administration peut déléguer au directeur exécutif le pouvoir d'apporter des modifications non substantielles au programme de travail annuel.

7. Le programme de travail pluriannuel expose la programmation stratégique globale comprenant les objectifs, les résultats escomptés et les indicateurs de performance. Il définit également la programmation des ressources, notamment le budget pluriannuel et les effectifs.

8. La programmation des ressources est actualisée chaque année. La programmation stratégique est actualisée en tant que de besoin, notamment pour tenir compte des résultats de l'évaluation visée à l'article 56.

Article 22

Déclaration d'intérêt

1. Les membres du conseil d'administration, le directeur exécutif et les fonctionnaires détachés par les États membres à titre temporaire font chacun une déclaration d'engagements et une déclaration indiquant l'absence ou la présence de tout intérêt direct ou indirect qui pourrait être considéré comme préjudiciable à leur indépendance. Les déclarations sont exactes et complètes, faites par écrit sur une base annuelle et actualisées si nécessaire.

2. Les membres du conseil d'administration, le directeur exécutif et les experts externes participant aux groupes de travail ad hoc déclarent chacun de manière exacte et complète, au plus tard au début de chaque réunion, les intérêts qui pourraient être considérés comme préjudiciables à leur indépendance eu égard aux points inscrits à l'ordre du jour, et s'abstiennent de prendre part aux discussions et de voter sur ces points.

3. L'Agence fixe, dans ses règles internes de fonctionnement, les modalités pratiques concernant les règles relatives aux déclarations d'intérêt visées aux paragraphes 1 et 2.

Article 23

Transparence

1. L'Agence exerce ses activités avec un niveau élevé de transparence et conformément aux dispositions de l'article 25.

2. L'Agence veille à ce que le public et toute partie intéressée reçoivent une information appropriée, objective, fiable et facilement accessible, notamment en ce qui concerne le résultat de ses travaux. Elle rend également publiques les déclarations d'intérêt faites conformément à l'article 22.

3. Le conseil d'administration peut, sur proposition du directeur exécutif, autoriser des parties intéressées à participer en tant qu'observateurs à certaines activités de l'Agence.

4. L'Agence fixe, dans ses règles internes de fonctionnement, les modalités pratiques d'application des règles de transparence visées aux paragraphes 1 et 2.

Article 24

Confidentialité

1. Sans préjudice de l'article 25, l'Agence ne divulgue pas à des tiers les informations qu'elle traite ou qu'elle reçoit et pour lesquelles une demande motivée de traitement confidentiel, en tout ou en partie, a été faite.

2. Les membres du conseil d'administration, le directeur exécutif, les membres du groupe permanent des parties prenantes, les experts externes participant aux groupes de travail ad hoc et les membres du personnel de l'Agence, y compris les fonctionnaires détachés par les États membres à titre temporaire, respectent l'obligation de confidentialité visée à l'article 339 du traité sur le fonctionnement de l'Union européenne, même après la cessation de leurs fonctions.

3. L'Agence fixe, dans ses règles internes de fonctionnement, les modalités pratiques d'application des règles de confidentialité visées aux paragraphes 1 et 2.

4. Si l'exécution des missions de l'Agence l'exige, le conseil d'administration décide d'autoriser l'Agence à traiter des informations classifiées. Dans ce cas, le conseil d'administration, en accord avec les services de la Commission, adopte des règles internes de fonctionnement respectant les principes de sécurité énoncés dans les décisions (UE, Euratom) 2015/443[15] et 2015/444[16]. Ces règles comprennent des dispositions relatives à l'échange, au traitement et à l'archivage des informations classifiées.

---

15 Décision (UE, Euratom) 2015/443 de la Commission du 13 mars 2015 relative à la sécurité au sein de la Commission (JO L 72 du 17.3.2015, p. 41).

16 Décision (UE, Euratom) 2015/444 de la Commission du 13 mars 2015 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne (JO L 72 du 17.3.2015, p. 53).

Article 25

Accès aux documents

1. Le règlement (CE) n° 1049/2001 s'applique aux documents détenus par l'Agence.

2. Le conseil d'administration adopte des dispositions pour la mise en œuvre du règlement (CE) n° 1049/2001 dans les six mois suivant la création de l'Agence.

3. Les décisions prises par l'Agence en application de l'article 8 du règlement (CE) n° 1049/2001 peuvent faire l'objet d'une plainte auprès du Médiateur au titre de l'article 228 du traité sur le fonctionnement de l'Union européenne ou d'un recours devant la Cour de justice de l'Union européenne au titre de l'article 263 du traité sur le fonctionnement de l'Union européenne.

CHAPITRE III
ÉTABLISSEMENT ET STRUCTURE DU BUDGET

Article 26

Établissement du budget

1. Chaque année, le directeur exécutif établit un projet d'état prévisionnel des recettes et des dépenses de l'Agence pour l'exercice budgétaire suivant et le transmet au conseil d'administration avec un projet de tableau des effectifs. Les recettes et les dépenses sont équilibrées.

2. Le conseil d'administration établit chaque année, sur la base du projet d'état prévisionnel des recettes et des dépenses visé au paragraphe 1, un état prévisionnel des recettes et des dépenses de l'Agence pour l'exercice budgétaire suivant.

3. Le conseil d'administration transmet, au plus tard le 31 janvier de chaque année, l'état prévisionnel visé au paragraphe 2, qui fait partie du projet de document unique de programmation, à la Commission et aux pays tiers avec lesquels l'Union européenne a conclu des accords conformément à l'article 39.

4. Sur la base de cet état prévisionnel, la Commission inscrit dans le projet de budget général de l'Union les prévisions qu'elle estime nécessaires en ce qui concerne le tableau des effectifs et le montant de la contribution à la charge du budget général et le soumet au Parlement européen et au Conseil conformément aux articles 313 et 314 du traité sur le fonctionnement de l'Union européenne.

5. Le Parlement européen et le Conseil autorisent les crédits au titre de la contribution destinée à l'Agence.

6. Le Parlement européen et le Conseil adoptent le tableau des effectifs de l'Agence.

7. Le conseil d'administration adopte le budget de l'Agence en même temps que le document unique de programmation. Ce budget devient définitif après l'adoption définitive du budget général de l'Union. Le cas échéant, le conseil d'administration ajuste le budget de l'Agence et le document unique de programmation conformément au budget général de l'Union.

Article 27

Structure du budget

1. Sans préjudice d'autres ressources, les recettes de l'Agence sont constituées:

   a) d'une contribution du budget de l'Union;

   b) de recettes allouées à des postes de dépense spécifiques conformément à ses règles financières visées à l'article 29;

   c) d'un financement de l'Union sous la forme de conventions de délégation ou de subventions ad hoc, conformément à ses règles financières visées à l'article 29 et aux dispositions des instruments pertinents appuyant les politiques de l'Union;

   d) de contributions de pays tiers participant aux travaux de l'Agence en vertu de l'article 39;

e) de toute contribution volontaire des États membres en espèces ou en nature. Les États membres qui apportent une contribution volontaire ne peuvent prétendre à aucun droit ou service spécifique du fait de celle-ci.

2. Les dépenses de l'Agence comprennent la rémunération du personnel, l'assistance administrative et technique, les dépenses d'infrastructure et de fonctionnement et les dépenses résultant de contrats passés avec des tiers.

Article 28

Exécution du budget

1. Le directeur exécutif est responsable de l'exécution du budget de l'Agence.

2. L'auditeur interne de la Commission exerce à l'égard de l'Agence les mêmes compétences que celles qui lui sont attribuées à l'égard des services de la Commission.

3. Au plus tard le 1er mars suivant l'achèvement de l'exercice (1er mars de l'année N + 1), le comptable de l'Agence transmet les comptes provisoires au comptable de la Commission et à la Cour des comptes.

4. À la réception des observations formulées par la Cour des comptes sur les comptes provisoires de l'Agence, le comptable de l'Agence établit les comptes définitifs de l'Agence sous sa propre responsabilité.

5. Le directeur exécutif transmet pour avis les comptes définitifs au conseil d'administration.

6. Au plus tard le 31 mars de l'année N + 1, le directeur exécutif transmet le rapport sur la gestion budgétaire et financière au Parlement européen, au Conseil, à la Commission et à la Cour des comptes.

7. Au plus tard le 1er juillet de l'année N + 1, le comptable transmet les comptes définitifs, accompagnés de l'avis du conseil d'administration, au Parlement européen, au Conseil, au comptable de la Commission et à la Cour des comptes.

8. À la même date que la transmission de ses comptes définitifs, le comptable transmet également à la Cour des comptes une lettre de déclaration portant sur ces comptes définitifs, avec copie au comptable de la Commission.

9. Le directeur exécutif publie les comptes définitifs avant le 15 novembre de l'année suivante.

10. Le directeur exécutif adresse à la Cour des comptes une réponse aux observations de celle-ci, le 30 septembre de l'année N + 1 au plus tard, et adresse également une copie de cette réponse au conseil d'administration et à la Commission.

11. Le directeur exécutif soumet au Parlement européen, à la demande de celui-ci, comme prévu à l'article 165, paragraphe 3, du règlement financier, toute information nécessaire au bon déroulement de la procédure de décharge pour l'exercice budgétaire en question.

12. Le Parlement européen, statuant sur recommandation du Conseil, donne avant le 15 mai de l'année N + 2, décharge au directeur exécutif sur l'exécution du budget de l'exercice N.

Article 29

Règles financières

Les règles financières applicables à l'Agence sont arrêtées par le conseil d'administration, après consultation de la Commission. Elles ne peuvent s'écarter du règlement (UE) n° 1271/2013 que si les exigences spécifiques du fonctionnement de l'Agence le nécessitent et moyennant l'accord préalable de la Commission.

Article 30

Lutte contre la fraude

1. Afin de faciliter la lutte contre la fraude, la corruption et d'autres activités illégales au titre du règlement (UE, Euratom) n° 883/2013 du Parlement européen et du Conseil[17], l'Agence, dans un délai de six mois à compter de son entrée en fonction, adhère à l'accord interinstitutionnel du 25 mai 1999 relatif aux enquêtes internes effectuées par l'Office européen de lutte antifraude (OLAF) et adopte les dispositions appropriées applicables à tout le personnel de l'Agence, en utilisant le modèle figurant à l'annexe dudit accord.

2. La Cour des comptes dispose d'un pouvoir d'audit, sur pièces et sur place, à l'égard de tous les bénéficiaires de subventions, contractants et sous-traitants qui ont reçu des fonds de l'Union en provenance de l'Agence.

[17] Règlement (UE, Euratom) n° 883/2013 du Parlement européen et du Conseil du 11 septembre 2013 relatif aux enquêtes effectuées par l'Office européen de lutte antifraude (OLAF) et abrogeant le règlement (CE) n° 1073/1999 du Parlement européen et du Conseil et le règlement (Euratom) n° 1074/1999 du Conseil (JO L 248 du 18.9.2013, p. 1).

3. L'OLAF peut effectuer des enquêtes, y compris des contrôles et vérifications sur place, selon les dispositions et modalités prévues par le règlement (UE, Euratom) n° 883/2013 du Parlement européen et du Conseil et le règlement (Euratom, CE) n° 2185/96[18] du Conseil du 11 novembre 1996 relatif aux contrôles et vérifications sur place effectués par la Commission pour la protection des intérêts financiers des Communautés européennes contre les fraudes et autres irrégularités, en vue d'établir l'existence éventuelle d'une fraude, d'un acte de corruption ou de toute autre activité illégale portant atteinte aux intérêts financiers de l'Union, dans le cadre d'une subvention ou d'un contrat financés par l'Agence.

4. Sans préjudice des paragraphes 1, 2 et 3, les accords de coopération conclus avec des pays tiers et des organisations internationales, les contrats, les conventions de subvention et les décisions de subvention de l'Agence contiennent des dispositions habilitant expressément la Cour des comptes et l'OLAF à procéder à ces audits et ces enquêtes, conformément à leurs compétences respectives.

CHAPITRE IV
PERSONNEL DE L'AGENCE

Article 31

Dispositions générales

Le statut et le régime applicable aux autres agents, ainsi que les réglementations arrêtées d'un commun accord des institutions de l'Union visant à exécuter le statut, s'appliquent au personnel de l'Agence.

---

18 Règlement (Euratom, CE) n° 2185/96 du Conseil du 11 novembre 1996 relatif aux contrôles et vérifications sur place effectués par la Commission pour la protection des intérêts financiers des Communautés européennes contre les fraudes et autres irrégularités (JO L 292 du 15.11.1996, p. 2).

Article 32

Privilèges et immunités

Le protocole nº 7 sur les privilèges et immunités de l'Union européenne annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne s'applique à l'Agence ainsi qu'à son personnel.

Article 33

Directeur exécutif

1. Le directeur exécutif est engagé en tant qu'agent temporaire de l'Agence conformément à l'article 2, point a), du régime applicable aux autres agents.

2. Le directeur exécutif est nommé par le conseil d'administration sur la base d'une liste de candidats proposés par la Commission, à la suite d'une procédure de sélection ouverte et transparente.

3. Aux fins de la conclusion du contrat du directeur exécutif, l'Agence est représentée par le président du conseil d'administration.

4. Avant d'être nommé, le candidat retenu par le conseil d'administration est invité à faire une déclaration devant la commission concernée du Parlement européen et à répondre aux questions des députés.

5. Le mandat du directeur exécutif est de **quatre** [...] ans. Avant la fin de cette période, la Commission procède à une évaluation qui tient compte de l'évaluation du travail accompli par le directeur exécutif et des missions et défis futurs de l'Agence.

6. Le conseil d'administration statue sur la nomination, la prolongation du mandat et la révocation du directeur exécutif à la majorité des deux tiers de ses membres disposant du droit de vote.

7. Le conseil d'administration, sur proposition de la Commission tenant compte de l'examen visé au paragraphe 5, peut proroger une fois le mandat du directeur exécutif, pour une durée n'excédant pas **quatre** [...] ans.

8. Le conseil d'administration informe le Parlement européen de son intention de prolonger le mandat du directeur exécutif. Dans les trois mois précédant cette prolongation, le directeur exécutif fait, s'il y est invité, une déclaration devant la commission concernée du Parlement européen et répond aux questions des députés.

9. Un directeur exécutif dont le mandat a été prolongé ne peut pas participer à une nouvelle procédure de sélection pour le même poste.

10. Le directeur exécutif ne peut être démis de ses fonctions que sur décision du conseil d'administration [...].

Article 34

Experts nationaux détachés et autre personnel

1. L'Agence peut avoir recours à des experts nationaux détachés ou à d'autres personnes qu'elle n'emploie pas. Le statut et le régime applicable aux autres agents ne s'appliquent pas à ces personnes.

2. Le conseil d'administration adopte une décision établissant le régime applicable aux experts nationaux détachés auprès de l'Agence.

CHAPITRE V
DISPOSITIONS GÉNÉRALES

Article 35

Statut juridique de l'Agence

1. L'Agence est un organisme de l'Union et est dotée de la personnalité juridique.

2. Dans chaque État membre, l'Agence jouit de la capacité juridique la plus étendue accordée aux personnes morales en droit national. Elle peut notamment acquérir ou aliéner des biens mobiliers et immobiliers et [...] ester en justice.

3. L'Agence est représentée par son directeur exécutif.

Article 36

Responsabilité de l'Agence

1. La responsabilité contractuelle de l'Agence est régie par la législation applicable au contrat en question.

2. La Cour de justice de l'Union européenne est compétente pour statuer en vertu de toute clause compromissoire contenue dans un contrat conclu par l'Agence.

3. En cas de responsabilité non contractuelle, l'Agence, conformément aux principes généraux communs aux droits des États membres, répare tout dommage causé par ses services ou par ses agents dans l'exercice de leurs fonctions.

4. La Cour de justice de l'Union européenne est compétente pour tout litige relatif à la réparation de tels dommages.

5. La responsabilité personnelle à l'égard de l'Agence de ses propres agents est régie par les dispositions pertinentes applicables au personnel de l'Agence.

Article 37

Régime linguistique

1. Les dispositions du règlement nº 1 du Conseil s'appliquent à l'Agence[19]. Les États membres et les autres organismes désignés par ceux-ci peuvent s'adresser à l'Agence et en recevoir une réponse dans la langue officielle des institutions de l'Union de leur choix.

2. Les services de traduction nécessaires au fonctionnement de l'Agence sont assurés par le Centre de traduction des organes de l'Union européenne.

Article 38

Protection des données à caractère personnel

1. Les opérations de traitement de données à caractère personnel effectuées par l'Agence sont soumises aux dispositions du règlement (CE) n° 45/2001 du Parlement européen et du Conseil[20].

2. Le conseil d'administration adopte les dispositions d'application visées à l'article 24, paragraphe 8, du règlement (CE) n° 45/2001. Le conseil d'administration peut adopter des mesures supplémentaires nécessaires pour l'application du règlement (CE) n° 45/2001 par l'Agence.

---

19 Règlement n° 1, portant fixation du régime linguistique de la Communauté européenne de l'énergie atomique (JO 17 du 6.10.1958, p. 401).

20 Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO L 8 du 12.1.2001, p. 1).

Article 39

Coopération avec des pays tiers et des organisations internationales

1. Dans la mesure où cela est nécessaire pour atteindre les objectifs énoncés dans le présent règlement, l'Agence peut coopérer avec les autorités compétentes de pays tiers et/ou avec des organisations internationales. À cet effet, l'Agence peut, sous réserve de l'approbation préalable de la Commission, établir des arrangements de travail avec les autorités de pays tiers et des organisations internationales. Ces arrangements ne créent pas d'obligations juridiques à l'égard de l'Union ou de ses États membres.

2. L'Agence est ouverte à la participation des pays tiers qui ont conclu des accords en ce sens avec l'Union européenne. Conformément aux dispositions pertinentes de ces accords, des arrangements sont élaborés pour préciser notamment la nature, l'étendue et les modalités de la participation de ces pays aux travaux de l'Agence. Ces arrangements comprennent notamment des dispositions relatives à la participation aux initiatives prises par l'Agence, aux contributions financières et au personnel. En ce qui concerne les questions relatives au personnel, lesdits arrangements respectent, en tout état de cause, le statut.

3. Le conseil d'administration adopte une stratégie en ce qui concerne les relations avec les pays tiers ou les organisations internationales sur les questions relevant de la compétence de l'Agence. La Commission veille à ce que l'Agence fonctionne dans les limites de son mandat et du cadre institutionnel existant en concluant un arrangement de travail approprié avec le directeur exécutif de l'Agence.

Article 40

Règles de sécurité en matière de protection des informations classifiées et des informations sensibles non classifiées

En consultation avec la Commission, l'Agence adopte ses propres règles de sécurité, en appliquant les principes de sécurité énoncés dans les règles de sécurité de la Commission visant à protéger les informations classifiées de l'Union européenne (ICUE) et les informations sensibles non classifiées, exposées dans les décisions (UE, Euratom) 2015/443 et 2015/444 de la Commission. Ces principes couvrent, entre autres, les dispositions relatives à l'échange, au traitement et au stockage de telles informations.

Article 41

Accord de siège et conditions de fonctionnement

1. Les dispositions relatives à l'implantation de l'Agence dans l'État membre du siège et aux prestations à fournir par cet État, ainsi que les règles particulières qui y sont applicables au directeur exécutif, aux membres du conseil d'administration, au personnel de l'Agence et aux membres de leurs familles sont arrêtées dans un accord de siège conclu entre l'Agence et l'État membre où son siège est situé, après approbation par le conseil d'administration et au plus tard [deux ans après l'entrée en vigueur du règlement].

2. L'État membre d'accueil de l'Agence offre des [...] conditions [...] **permettant d'**assurer le bon fonctionnement de l'Agence, notamment l'accessibilité de l'emplacement, l'existence de services d'éducation appropriés pour les enfants des membres du personnel et un accès adéquat au marché du travail, à la sécurité sociale et aux soins médicaux pour les enfants et les conjoints.

Article 42

Contrôle administratif

Les activités de l'Agence sont soumises au contrôle du Médiateur, conformément à l'article 228 du traité sur le fonctionnement de l'Union européenne.

TITRE III
CADRE DE CERTIFICATION DE CYBERSÉCURITÉ

Article 43

***Cadre européen de certification de cybersécurité* [...]**

1. **Le cadre européen de certification de cybersécurité est établi afin d'améliorer les conditions de fonctionnement du marché intérieur en renforçant le niveau de cybersécurité au sein de l'Union. Il instaure une gouvernance permettant de disposer, au niveau de l'UE, d'une approche harmonisée des systèmes européens de certification de cybersécurité, en vue de créer un marché unique numérique pour les processus, produits et services TIC.**

2. **Le cadre européen de certification de cybersécurité définit un mécanisme visant à établir des** [...] système**s** européen**s** de certification de cybersécurité [...] **et à** attester que les **processus,** produits et services TIC qui ont été [...] **évalués** conformément à ce**s** système**s** satisfont à des exigences **de sécurité** spécifiées [...], **l'objectif étant de protéger** la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou traitées ou des fonctions ou services associés qui sont offerts ou accessibles par ces produits, processus **et** services [...] **tout au long de leur cycle de vie**.

Article 44

Élaboration et adoption d'un système européen de certification de cybersécurité

1. À la suite d'une demande de la Commission **ou du Groupe européen de certification de cybersécurité (ci-après dénommé "Groupe") établi en vertu de l'article 53**, l'ENISA élabore un système européen de certification de cybersécurité candidat qui satisfait aux exigences énoncées aux articles 45, 46 et 47 du présent règlement. [...]

1 *bis*. L'élaboration d'un système européen de certification de cybersécurité candidat peut être proposée au Groupe par les États membres ou les organisations intervenantes intéressées. Le Groupe évalue les propositions faites en ce sens en fonction de critères qu'il définit au moyen de lignes directrices conformément à l'article 53, paragraphe 3, point c *bis*), et peut demander à l'ENISA d'élaborer un système européen de certification de cybersécurité candidat.

2. Lors de l'élaboration des systèmes candidats visés au paragraphe 1 du présent article, l'ENISA consulte toutes les parties prenantes concernées **au moyen de processus de consultation transparents** et travaille en étroite collaboration avec le Groupe. Celui-ci fournit aide et expertise à l'ENISA [...] dans le cadre de l'élaboration du système candidat **et adopte un avis sur celui-ci avant sa soumission à la Commission** [...]. **L'ENISA veille à ce que les systèmes candidats soient conformes à la norme harmonisée applicable utilisée pour l'accréditation de l'organisme d'évaluation de la conformité.**

3. L'ENISA **tient dûment compte de l'avis du Groupe avant de transmettre** à la Commission [...] le système [...] candidat élaboré conformément au paragraphe 2 du présent article.

4. La Commission, se fondant sur le système candidat proposé par l'ENISA, peut adopter des actes d'exécution, conformément à l'article 55, paragraphe 2, prévoyant des systèmes européens de certification de cybersécurité pour les **processus,** produits et services TIC qui satisfont aux exigences des articles 45, 46 et 47 du présent règlement.

5. […]

***Article 44* bis**

Actualisation des systèmes européens de certification de cybersécurité

1. L'Agence tient à jour un site web spécifique fournissant des informations sur les systèmes européens de certification de cybersécurité, les certificats et les déclarations de conformité de l'UE délivrées en vertu de l'article 47 *bis*, et leur assurant une publicité.

2. L'Agence, en coopération étroite avec le Groupe, réexamine tous les cinq ans au moins les systèmes européens de certification de cybersécurité adoptés, en tenant compte des informations reçues en retour des parties intéressées. S'ils le jugent nécessaire, la Commission ou le Groupe peuvent demander à l'Agence de lancer le processus d'élaboration d'un système candidat révisé, conformément à l'article 44, paragraphes 2 et 3.

Article 45

Objectifs de sécurité des systèmes européens de certification de cybersécurité

Un système européen de certification de cybersécurité est conçu de façon [...] **à réaliser**, le cas échéant, **au moins** les objectifs de sécurité suivants:

a) protéger les données stockées, transmises ou traitées d'une autre façon contre le stockage, le traitement, l'accès ou la diffusion accidentels ou non autorisés **durant l'ensemble du cycle de vie du processus, produit ou service**;

b) protéger les données stockées, transmises ou traitées d'une autre façon contre la destruction accidentelle ou non autorisée, la perte ou l'altération [...], **ou l'absence de disponibilité, durant l'ensemble du cycle de vie du processus, produit ou service**;

c) faire en sorte que les personnes autorisées, les programmes ou les machines puissent exclusivement accéder aux données, services ou fonctions concernés par leurs droits d'accès;

d) garder une trace des données, fonctions ou services qui ont été [...] **consultés, utilisés ou traités d'une autre façon**, du moment où ils l'ont été et par quelles personnes;

e) faire en sorte qu'il soit possible de vérifier quels sont les données, services ou fonctions qui ont été consultés**,** [...] utilisés **ou traités d'une autre façon**, à quel moment et par quelles personnes;

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

g) faire en sorte que les **processus,** produits et services TIC soient dotés de logiciels **et de matériel** à jour et sans vulnérabilités connues **du public**, et de mécanismes permettant d'assurer les mises à jour [...] en toute sécurité**;**

g *bis*) faire en sorte que les processus, produits et services TIC soient développés, fabriqués et fournis conformément aux exigences de sécurité énoncées dans le système concerné.

Article 46

Niveaux d'assurance des systèmes européens de certification de cybersécurité

1. Un système européen de certification de cybersécurité peut préciser un ou plusieurs des niveaux d'assurance suivants - élémentaire, substantiel et/ou élevé - pour les **processus,** produits et services TIC [...]. **Le niveau d'assurance est proportionnel au niveau de risque correspondant à l'utilisation prévue d'un processus, produit ou service TIC.**

2. Les niveaux d'assurance élémentaire, substantiel et élevé [...] **renvoient à un certificat ou à une déclaration de conformité de l'UE délivrés dans le cadre d'un système européen de certification de cybersécurité, qui prévoit, pour chaque niveau d'assurance, des exigences de sécurité respectives comprenant des fonctionnalités de sécurité, et le niveau correspondant d'efforts pour l'évaluation d'un processus, produit ou service TIC. Le certificat ou la déclaration de conformité de l'UE sont caractérisés sur la base de spécifications techniques, normes et procédures connexes, y compris les contrôles techniques, l'objectif étant de réduire le risque d'incidents de cybersécurité ou de prévenir ceux-ci, comme suit:**

a) **un certificat européen de cybersécurité ou une déclaration de conformité de l'UE qui atteste du** niveau d'assurance **"**élémentaire**" offre l'assurance que les processus, produits et services TIC respectent les exigences de sécurité respectives, y compris des fonctionnalités de sécurité, et qu'ils ont été évalués à un niveau qui vise à minimiser les risques élémentaires connus de cyberincidents et de cyberattaques. Les activités d'évaluation comprennent au moins un examen de la documentation technique ou, lorsque cela n'est pas possible, des activités de substitution ayant un effet équivalent** [...];

b) **un certificat européen de cybersécurité qui atteste du** niveau d'assurance **"**substantiel**" offre l'assurance que les processus, produits et services TIC respectent les exigences de sécurité respectives, y compris des fonctionnalités de sécurité, et qu'ils ont été évalués à un niveau qui vise à minimiser les risques, incidents et attaques cyber connus émanant d'acteurs dotés de connaissances et de ressources limitées. Les activités d'évaluation comprennent au moins: l'examen de la non-applicabilité de vulnérabilités connues du public et la vérification que les processus, produits ou services TIC mettent correctement en œuvre la fonctionnalité de sécurité nécessaire; ou, lorsque cela n'est pas possible, des activités de substitution ayant un effet équivalent** [...];

c) **un certificat européen de cybersécurité qui atteste du** niveau d'assurance **"**élevé**" offre l'assurance que les processus, produits et services TIC respectent les exigences de sécurité respectives, 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 dotés de connaissances et de ressources importantes. Les activités d'évaluation comprennent au moins: l'examen de la non-applicabilité de vulnérabilités connues du public, la vérification que les processus, produits ou services TIC mettent correctement en œuvre la fonctionnalité de sécurité nécessaire, au niveau le plus élevé, et l'évaluation de leur résistance à des attaques menées par des acteurs qualifiés, au moyen de tests de pénétration; ou, lorsque cela n'est pas possible, des activités de substitution ayant un effet équivalent.**

2 *bis*. Un système européen de certification de cybersécurité peut spécifier plusieurs niveaux d'évaluation selon la rigueur et l'ampleur de la méthode d'évaluation. Chaque niveau d'évaluation correspond à l'un des niveaux d'assurance et est défini par une combinaison appropriée de composantes d'assurance.

Article 47

Éléments des systèmes européens de certification de cybersécurité

1. Un système européen de certification de cybersécurité comprend **au moins** les éléments suivants:

a) l'objet et le champ d'application **du système de** certification, notamment le type ou les catégories de **processus,** produits et services TIC**, ainsi qu'une présentation de la manière dont le système de certification répond aux besoins des groupes cibles prévus**;

b) [...] une référence aux normes [...] internationales**, européennes ou nationales suivies dans le cadre de l'évaluation. Lorsqu'il n'existe aucune norme, il est fait référence à** [...] des spécifications techniques **qui respectent les exigences figurant à l'annexe II du règlement (UE) n° 1025/2012 ou, s'il n'y en a pas, à des spécifications techniques ou autres exigences de cybersécurité définies dans le système**;

c) le cas échéant, un ou plusieurs niveaux d'assurance;

c *bis*) le cas échéant, des exigences spécifiques ou supplémentaires applicables aux organismes d'évaluation de la conformité aux fins de garantir qu'ils disposent des compétences techniques nécessaires pour évaluer les exigences de cybersécurité;

d) les critères et méthodes d'évaluation spécifiques utilisés, notamment les types d'évaluation, afin de démontrer que les objectifs spécifiques visés à l'article 45 sont atteints;

e) **le cas échéant,** les informations nécessaires à la certification qu'un demandeur doit fournir aux organismes d'évaluation de la conformité **ou mettre à leur disposition d'une autre façon**;

f) lorsque le système prévoit des marques ou des labels, les conditions dans lesquelles ces marques ou labels peuvent être utilisés;

g) [...] les modalités relatives au contrôle du respect des exigences associées aux certificats **ou à la déclaration de conformité de l'UE**, notamment les mécanismes permettant de démontrer le respect constant des exigences de cybersécurité;

h) **le cas échéant,** les conditions permettant de délivrer **et de renouveler un certificat**, **ainsi que de** maintenir et poursuivre la certification et d'étendre ou de réduire son champ d'application;

i) les règles relatives aux conséquences de la non-conformité des produits et services TIC certifiés **ou autoévalués** aux exigences [...] **du système**;

j) les règles relatives aux modalités de signalement et de traitement des vulnérabilités de cybersécurité non détectées précédemment dans des **processus,** produits et services TIC;

k) **le cas échéant,** les règles relatives à la conservation des archives par les organismes d'évaluation de la conformité;

l) l'identification des systèmes nationaux **ou internationaux** de certification de cybersécurité couvrant le même type ou les mêmes catégories de **processus,** produits et services TIC**, exigences de sécurité et critères et méthodes d'évaluation**;

m) le contenu du certificat délivré **ou de la déclaration de conformité de l'UE;**

m *bis*) la période de stockage de la déclaration de conformité de l'UE et la documentation technique concernant toutes les informations pertinentes fournies par le fabricant ou le fournisseur de produits et services TIC;

m *ter* [...]) la durée maximale de validité des certificats;

m *quater* [...]) la politique de divulgation concernant les certificats accordés, modifiés et retirés;

m *quinquies* [...]) les conditions de reconnaissance mutuelle des systèmes de certification avec les pays tiers;

m *sexies* [...]) le cas échéant, les règles régissant un mécanisme d'examen par les pairs concernant les organismes qui délivrent des certificats européens de cybersécurité pour un niveau d'assurance élevé [...] conformément à l'article 48, paragraphe 4 *bis*.

2. Les exigences spécifiées du système ne sont pas contraires aux exigences légales applicables, notamment les exigences découlant de la législation harmonisée de l'Union.

3. Lorsqu'un acte spécifique de l'Union le prévoit, la certification **ou la déclaration de conformité de l'UE** au titre d'un système européen de certification de cybersécurité peut être utilisée pour démontrer la présomption de conformité aux exigences de cet acte.

4. En l'absence de législation harmonisée de l'Union, le droit d'un État membre peut aussi prévoir qu'un système européen de certification de cybersécurité soit utilisé pour établir la présomption de conformité aux exigences légales.

Article 47 **bis**

Autoévaluation de la conformité

1. Un système européen de certification de cybersécurité peut permettre la réalisation d'une évaluation de la conformité sous la seule responsabilité du fabricant ou fournisseur de produits et services TIC. Une telle évaluation de la conformité ne s'applique qu'aux produits et services TIC qui présentent un risque faible et une complexité limitée correspondant au niveau d'assurance élémentaire.

2. Le fabricant ou fournisseur de produits et services TIC peut délivrer une déclaration de conformité de l'UE indiquant que le respect des exigences énoncées dans le système a été démontré. En établissant une telle déclaration, le fabricant ou fournisseur de produits et services TIC assume la responsabilité de la conformité du produit ou service TIC avec les exigences énoncées dans le système.

3. Le fabricant ou fournisseur de produits et services TIC garde à la disposition de l'autorité nationale de certification de cybersécurité visée à l'article 50, paragraphe 1, pour une durée fixée dans le système européen de certification de cybersécurité correspondant, la déclaration de conformité de l'UE et la documentation technique concernant toutes les informations pertinentes liées à la conformité des produits ou services TIC avec un système. Une copie de la déclaration de conformité de l'UE est transmise à l'autorité nationale de certification de cybersécurité et à l'ENISA.

4. La délivrance d'une déclaration de conformité de l'UE est volontaire, sauf indication contraire dans le droit de l'Union ou de l'État membre.

5. La déclaration de conformité de l'UE délivrée au titre du présent article est reconnue dans tous les États membres.

Article 48

Certification de cybersécurité

1. Les **processus,** produits et services TIC qui ont été certifiés dans le cadre d'un système européen de certification de cybersécurité adopté conformément à l'article 44 sont présumés conformes aux exigences de ce système.

2. La certification est volontaire, sauf indication contraire dans le droit de l'Union **ou des États membres**.

3. Les organismes d'évaluation de la conformité visés à l'article 51 délivrent un certificat européen de cybersécurité au titre du présent article **attestant du niveau d'assurance élémentaire ou substantiel** sur la base des critères figurant dans le système européen de certification de cybersécurité adopté conformément à l'article 44.

4. Par dérogation au paragraphe 3, dans des cas dûment justifiés, un système européen **de certification** de cybersécurité particulier peut prévoir que seul un organisme public puisse délivrer un certificat européen de cybersécurité dans le cadre dudit système. Cet organisme [...] est l'une des entités suivantes:

a) une autorité nationale [...] de certification **de cybersécurité** visée à l'article 50, paragraphe 1;

b) un organisme **public** accrédité en tant qu'organisme d'évaluation de la conformité conformément à l'article 51, paragraphe 1 [...];

c) […].

4 *bis*. Dans le cas où un système européen de certification de cybersécurité au titre de l'article 44 exige un niveau d'assurance élevé, le certificat ne peut être délivré que par une autorité nationale de certification de cybersécurité visée à l'article 50, paragraphe 1, ou, dans les conditions ci-après, par un organisme d'évaluation de la conformité visé à l'article 51:

a) moyennant l'approbation préalable de l'autorité nationale de certification de cybersécurité pour chaque certificat délivré par un organisme d'évaluation de la conformité; ou

b) moyennant la délégation générale préalable de cette mission à un organisme d'évaluation de la conformité par l'autorité nationale de certification de cybersécurité.

5. La personne physique ou morale qui soumet ses **processus,** produits ou services TIC au mécanisme de certification [...] **met à la disposition de** l'organisme d'évaluation de la conformité visé à l'article 51 **ou de l'autorité nationale de certification de cybersécurité visée à l'article 50, lorsque cette autorité est l'organisme délivrant le certificat,** toutes les informations nécessaires pour mener la procédure de certification.

5 *bis*. Le titulaire d'un certificat informe l'organisme qui délivre le certificat de toute vulnérabilité ou irrégularité détectée ultérieurement concernant la sécurité du processus, produit ou service TIC certifié qui pourrait avoir un effet sur les exigences liées à la certification. L'organisme transmet ces informations sans retard injustifié à l'autorité nationale de certification de cybersécurité.

6. Les certificats sont délivrés pour [...] **la durée fixée dans le système de certification concerné** et peuvent être renouvelés, [...] pourvu que les exigences applicables continuent d'être satisfaites.

7. Un certificat européen de cybersécurité délivré au titre du présent article est reconnu dans tous les États membres.

Article 49

Systèmes nationaux de certification de cybersécurité et certificats

1. Sans préjudice du paragraphe 3, les systèmes nationaux de certification de cybersécurité et les procédures connexes pour les **processus,** produits et services TIC couverts par un système 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 44, paragraphe 4. Les systèmes nationaux de certification de cybersécurité et les procédures connexes pour les **processus,** produits et services TIC qui ne sont pas couverts par un système européen de certification de cybersécurité continuent à exister.

2. Les États membres s'abstiennent d'instaurer de nouveaux systèmes nationaux de certification de cybersécurité des **processus,** produits et services TIC couverts par un système européen de certification de cybersécurité en vigueur.

3. Les certificats existants, délivrés en vertu de systèmes nationaux de certification de cybersécurité **et relevant d'un système européen de certification de cybersécurité**, restent valables jusqu'à leur date d'expiration.

Article 50

Autorités nationales de [...] ***certification*** **de cybersécurité**

1. Chaque État membre désigne **une ou plusieurs autorités** nationales de [...] certification **de cybersécurité sur son territoire ou, d'un commun accord avec un autre État membre, désigne une ou plusieurs autorités établies dans cet autre État membre comme responsables des missions de supervision dans l'État membre qui procède à la désignation**.

2. Chaque État membre informe la Commission de l'identité **des autorités [...] désignées et des missions qui leur sont confiées**.

3. **Sans préjudice de l'article 48, paragraphe 4, point a), et paragraphe 4 *bis*,** [...] **c**haque autorité nationale de [...] certification **de cybersécurité** est indépendante, en ce qui concerne son organisation, ses décisions de financement, sa structure juridique et son processus décisionnel, des entités qu'elle surveille.

3 *bis*. Les États membres veillent à ce que les activités de l'autorité nationale de certification de cybersécurité liées à la délivrance de certificats en vertu de l'article 48, paragraphe 4, point a), et paragraphe 4 *bis*, observent une séparation stricte des rôles et responsabilités avec les activités de supervision visées au présent article, et à ce que les deux domaines d'activité fonctionnent indépendamment l'un de l'autre.

4. Les États membres veillent à ce que les autorités nationales de [...] certification **de cybersécurité** disposent de ressources adéquates pour exercer leurs pouvoirs et exécuter, de manière efficace et efficiente, les missions qui leur sont dévolues.

5. Afin d'assurer la mise en œuvre efficace du présent règlement, il convient que ces autorités participent, d'une manière active, efficace, efficiente et sécurisée, au Groupe européen de certification de cybersécurité institué en vertu de l'article 53.

6. Les autorités nationales de [...] certification **de cybersécurité**:

a) […]

a *bis*) contrôlent et font respecter les obligations qui incombent aux fabricants ou fournisseurs de produits et services TIC établis sur leurs territoires respectifs, visées à l'article 47 *bis*, paragraphes 2 et 3, et dans le système européen de certification de cybersécurité correspondant;

b) [...] **sans préjudice de l'article 51, paragraphe 1 *ter*, assistent les organismes nationaux d'accréditation dans le contrôle et la supervision des** activités des organismes d'évaluation de la conformité aux fins du présent règlement [...];

b *bis*) contrôlent et supervisent les activités des organismes visés à l'article 48, paragraphe 4;

b *ter*) agréent les organismes d'évaluation de la conformité visés à l'article 51, paragraphe 1 *ter*, et limitent, suspendent ou retirent les autorisations existantes en cas de non-conformité aux exigences du présent règlement;

c) traitent les réclamations introduites par une personne physique ou morale en rapport avec les certificats délivrés par [...] **l'autorité nationale de certification de cybersécurité ou, conformément à l'article 48, paragraphe 4 *bis*, par des organismes d'évaluation de la conformité**, examinent l'objet de la réclamation dans la mesure nécessaire et informent l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable;

d) coopèrent avec les autres autorités nationales de [...] certification **de cybersécurité** ou d'autres autorités publiques, notamment en partageant des informations sur l'éventuelle non-conformité de **processus,** produits et services TIC aux exigences du présent règlement ou à celles de systèmes de certification de cybersécurité spécifiques;

e) suivent les évolutions pertinentes dans le domaine de la certification de cybersécurité.

7. Chaque autorité nationale de [...] certification **de cybersécurité** dispose au moins des pouvoirs suivants:

a) demander aux organismes d'évaluation de la conformité**,** [...] aux titulaires d'un certificat européen de cybersécurité **et aux émetteurs de déclarations de conformité de l'UE** de lui communiquer toute information dont elle a besoin pour l'accomplissement de sa mission;

b) effectuer des enquêtes, sous la forme d'audits, auprès des organismes d'évaluation de la conformité**,** [...] des titulaires de certificats européens de cybersécurité **et des émetteurs de déclarations de conformité de l'UE** afin de vérifier le respect des dispositions en vertu du titre III;

c) prendre les mesures appropriées, conformément au droit national, afin de veiller à ce que les organismes d'évaluation de la conformité**,** [...] les titulaires d'un certificat **et les émetteurs de déclarations de conformité de l'UE** respectent le présent règlement ou un système européen de certification de cybersécurité;

d) obtenir l'accès à tous les locaux des organismes d'évaluation de la conformité et des titulaires de certificats européens de cybersécurité afin d'effectuer des enquêtes conformément au droit de l'Union ou au droit procédural des États membres;

e) retirer, conformément au droit national, les certificats **délivrés par l'autorité nationale de certification de cybersécurité ou, conformément à l'article 48, paragraphe 4 *bis*, par les organismes d'évaluation de la conformité** qui ne sont pas conformes au présent règlement ou à un système européen de certification de cybersécurité;

f) imposer des sanctions, comme prévu à l'article 54, conformément au droit national, et exiger la cessation immédiate des manquements aux obligations énoncées dans le présent règlement.

8. 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 **processus,** produits et services TIC.

Article 51

Organismes d'évaluation de la conformité

1. Les organismes d'évaluation de la conformité ne sont accrédités par l'organisme national d'accréditation désigné conformément au règlement (CE) n° 765/2008 du Parlement européen et du Conseil que lorsqu'ils satisfont aux exigences énoncées à l'annexe du présent règlement.

1 *bis*. Dans les cas où un certificat européen de cybersécurité est délivré par une autorité nationale de certification de cybersécurité en vertu de l'article 48, paragraphe 4, point a), et paragraphe 4 *bis*, l'organisme de certification de l'autorité nationale de certification de cybersécurité est accrédité en tant qu'organisme d'évaluation de la conformité conformément au paragraphe 1 du présent article.

1 *ter*. Le cas échéant, les organismes d'évaluation de la conformité sont autorisés par l'autorité nationale de certification de cybersécurité à accomplir ses missions lorsqu'ils respectent les exigences spécifiques ou supplémentaires fixées dans le système européen de certification conformément à l'article 47, paragraphe 1, point c *bis*).

2. L'accréditation est accordée pour une durée maximale de cinq ans et peut être renouvelée dans les mêmes conditions pourvu que l'organisme d'évaluation de la conformité satisfasse aux exigences énoncées au présent article. Les organismes d'accréditation **prennent, dans un délai raisonnable, toutes les mesures appropriées pour limiter, suspendre ou** révoqu**er** l'accréditation d'un organisme d'évaluation de la conformité accordée en vertu du paragraphe 1 lorsque les conditions de l'accréditation ne sont pas ou plus remplies ou que des mesures prises par l'organisme d'évaluation de la conformité enfreignent le présent règlement.

Article 52

Notification

1. Pour chaque système européen de certification de cybersécurité adopté en vertu de l'article 44, les autorités nationales de [...] certification **de cybersécurité** notifient à la Commission les organismes d'évaluation de la conformité accrédités **et, le cas échéant, autorisés au titre de l'article 51, paragraphe 1 *ter*, à** délivrer des certificats aux niveaux d'assurance spécifiés visés à l'article 46 et l'informent, sans délai indu, de toute modification ultérieure qui y est apportée.

2. Un an après la date d'entrée en vigueur d'un système européen de certification de cybersécurité, la Commission publie au Journal officiel une liste des organismes d'évaluation de la conformité notifiés.

3. Si la Commission reçoit une notification après expiration du délai visé au paragraphe **2** [...], elle publie au Journal officiel de l'Union européenne les modifications apportées à la liste visée au paragraphe 2 dans un délai de deux mois à compter de la date de réception de cette notification.

4. Une autorité nationale de [...] certification **de cybersécurité** peut présenter à la Commission une demande visant à retirer de la liste visée au paragraphe 2 du présent article un organisme d'évaluation de la conformité notifié par l'État membre en cause. La Commission publie au Journal officiel de l'Union européenne les modifications correspondantes apportées à la liste dans un délai d'un mois à compter de la date de réception de la demande présentée par l'autorité nationale de [...] certification **de cybersécurité**.

5. La Commission peut définir, au moyen d'actes d'exécution, les circonstances, formats et procédures des notifications visées au paragraphe 1. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 55, paragraphe 2.

Article 53

Groupe européen de certification de cybersécurité

1. Le Groupe européen de certification de cybersécurité (ci-après dénommé "Groupe") est institué.

2. Le Groupe est composé **de représentants** d'autorités nationales de [...] certification **de cybersécurité ou de représentants d'autres autorités nationales compétentes**. [...] **Un membre du Groupe ne peut représenter plus d'un autre État membre**.

3. Le Groupe a pour mission:

a) de conseiller et d'assister la Commission dans ses efforts pour assurer une mise en œuvre et une application cohérentes des dispositions du présent titre, notamment en ce qui concerne les questions de politique de certification de cybersécurité, la coordination des approches et l'élaboration de systèmes européens de certification de cybersécurité;

b) d'assister, de conseiller et de coopérer avec l'ENISA en ce qui concerne l'élaboration d'un système candidat conformément à l'article 44 du présent règlement;

b *bis*) d'adopter un avis sur le système candidat au titre de l'article 44 du présent règlement;

c) [...] de demander à l'Agence d'élaborer un système européen de certification de cybersécurité candidat conformément à l'article 44 du présent règlement;

c *bis*) de mettre au point et d'adopter des lignes directrices concernant les critères d'évaluation des propositions aux fins de l'élaboration d'un système candidat soumis au [...] Groupe en vertu de l'article 44, paragraphe 1 *bis*;

d) d'adopter des avis adressés à la Commission concernant l'actualisation et le réexamen de systèmes européens de certification de cybersécurité existants;

e) d'examiner les évolutions pertinentes dans le domaine de la certification de cybersécurité et de l'échange de bonnes pratiques sur les systèmes de certification de cybersécurité;

f) de faciliter la coopération entre les autorités nationales de [...] certification **de cybersécurité** en vertu du présent titre par **le renforcement des capacités et** l'échange d'informations, notamment en établissant des méthodes permettant un échange d'informations efficace sur toutes les questions relatives à la certification de cybersécurité**;**

f *bis*) de fournir un soutien à la mise en œuvre du mécanisme d'examen par les pairs conformément aux règles fixées dans un système européen de certification de cybersécurité au titre de l'article 47, paragraphe 1, point m *quinquies*), du présent règlement.

4. La Commission préside le Groupe **en qualité de modérateur** et en assure le secrétariat, avec l'aide de l'ENISA conformément à l'article 8, point a).

***Article 53* bis**

Droit d'introduire une réclamation auprès de l'autorité nationale de [...] ***certification de* cybersécurité**

1. Les personnes physiques ou morales ont le droit d'introduire une réclamation auprès de l'autorité nationale de certification de cybersécurité en ce qui concerne un certificat délivré par cette même autorité ou, conformément à l'article 48, paragraphe 4 *bis*), par des organismes d'évaluation de la conformité.

2. L'autorité nationale de certification de cybersécurité auprès de laquelle la réclamation a été introduite informe l'auteur de la réclamation de l'état d'avancement et de l'issue de la réclamation, y compris de la possibilité d'un recours juridictionnel en vertu de l'article 53 *ter*.

Article 53 **ter**

Droit à un recours juridictionnel effectif

1. Les personnes physiques ou morales ont droit à un recours juridictionnel effectif contre toute décision juridiquement contraignante rendue par une autorité nationale de certification de cybersécurité les concernant.

2. Les personnes physiques ou morales ont droit à un recours juridictionnel effectif lorsque l'autorité nationale de certification de cybersécurité ne traite pas une réclamation.

3. Les procédures engagées contre une autorité nationale de certification de cybersécurité sont portées devant les juridictions de l'État membre où l'autorité est établie.

Article 54

Sanctions

Les États membres fixent des règles relatives aux sanctions applicables en cas d'infraction aux dispositions du présent titre et des systèmes européens de certification de cybersécurité et prennent toutes les mesures nécessaires pour que ces règles soient appliquées. Les sanctions prévues sont effectives, proportionnées et dissuasives. Les États membres notifient ces règles et ces mesures à la Commission [au plus tard le ... /sans retard], et l'informent de toute modification ultérieure les concernant.

TITRE IV
DISPOSITIONS FINALES

Article 55

Procédure de comité

1. La Commission est assistée par un comité. Celui-ci est un comité au sens du règlement (UE) n° 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 5**, paragraphe 4, point b),** du règlement (UE) n° 182/2011 s'applique.

Article 56

Évaluation et révision

1. Au plus tard cinq ans après la date visée à l'article 58, et ensuite tous les cinq ans, la Commission évalue l'incidence, l'efficacité et l'efficience de l'Agence et de ses méthodes de travail, ainsi que la nécessité éventuelle de modifier le mandat de l'Agence et les conséquences financières d'une telle modification. L'évaluation tient compte de toute information communiquée en retour à l'Agence en réaction à ses activités. Lorsque la Commission estime que le maintien de l'Agence n'est plus justifié au regard des objectifs, du mandat et des missions qui lui ont été assignés, elle peut proposer que les dispositions du présent règlement relatives à l'Agence soient modifiées.

2. L'évaluation porte également sur l'impact, l'efficacité et l'efficience des dispositions du titre III au regard des objectifs consistant à garantir un niveau suffisant de cybersécurité des produits et services TIC dans l'Union et à améliorer le fonctionnement du marché intérieur.

3. La Commission transmet le rapport d'évaluation, accompagné de ses conclusions, au Parlement européen, au Conseil et au conseil d'administration. Les conclusions du rapport d'évaluation sont rendues publiques.

Article 57

Abrogation et succession

1. Le règlement (CE) n° 526/2013 est abrogé avec effet au […].

2. Les références au règlement (CE) n° 526/2013 et à l'ENISA s'entendent comme faites au présent règlement et à l'Agence.

3. L'Agence succède à l'Agence qui a été instituée par le règlement (CE) n° 526/2013 en ce qui concerne tous les droits de propriété, accords, obligations légales, contrats de travail, engagements financiers et responsabilités. Toutes les décisions du conseil d'administration et du conseil exécutif restent valables, pour autant qu'elles ne soient pas en contradiction avec les dispositions du présent règlement.

4. L'Agence est instituée pour une durée indéterminée à compter du [...].

5. Le directeur exécutif nommé en vertu de l'article 24, paragraphe 4, du règlement (CE) n° 526/2013 est le directeur exécutif de l'Agence pour la durée restante de son mandat.

6. Les membres, et leurs suppléants, du conseil d'administration nommés en application de l'article 6 du règlement (CE) n° 526/2013 sont les membres, et leurs suppléants, du conseil d'administration de l'Agence pour la durée restante de leur mandat.

Article 58

Entrée en vigueur

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

1 *bis*. Le présent règlement s'applique à partir du [...], à l'exception de ses articles 50, 51, 52, 53 *bis*, 53 *ter* et 54, qui s'appliquent à partir du [24 mois après la date de sa publication au Journal officiel de l'Union européenne].

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

Fait à Bruxelles, le

Par le Parlement européen	*Par le Conseil*
Le président	*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 indépendant de l'organisation ou des produits ou services TIC 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 ou services TIC qu'il évalue peut, pour autant que son indépendance et que l'absence de tout conflit d'intérêts soient démontrées, être considéré comme un organisme d'évaluation de la conformité.

4. Un organisme d'évaluation de la conformité, ses cadres supérieurs et le personnel chargé d'exécuter les tâches d'évaluation de la conformité ne peuvent être ni le concepteur, le fabricant, le fournisseur, l'installateur, l'acheteur, le propriétaire, l'utilisateur ou le responsable de l'entretien du produit ou service TIC qui est évalué, ni le mandataire d'aucune de ces parties. Cela n'exclut pas l'utilisation de produits évalués qui sont nécessaires au fonctionnement de l'organisme d'évaluation de la conformité ou l'utilisation de ces produits à des fins personnelles.

5. Un organisme d'évaluation de la conformité, ses cadres supérieurs et le personnel chargé d'exécuter les tâches d'évaluation de la conformité ne peuvent intervenir, ni directement ni comme mandataires, dans la conception, la fabrication ou la construction, la commercialisation, l'installation, l'utilisation ou l'entretien des produits ou services TIC. Ils ne peuvent participer à aucune activité qui peut entrer en conflit avec l'indépendance de leur jugement et l'intégrité des activités d'évaluation de la conformité pour lesquelles ils sont notifiés. Cela vaut en particulier pour les services de conseil.

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

7. 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, notamment d'ordre financier, susceptible d'influencer leur jugement ou les résultats de leurs travaux d'évaluation de la conformité, en particulier de la part de personnes ou de groupes de personnes intéressés par ces résultats.

8. L'organisme d'évaluation de la conformité est capable d'exécuter toutes les tâches d'évaluation de la conformité pour lesquelles il a été désigné 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.

9. En toutes circonstances et pour chaque procédure d'évaluation de la conformité, ainsi que pour tout type ou toute catégorie ou sous-catégorie de produits ou services TIC, l'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 selon lesquelles l'évaluation de la conformité est effectuée, garantissant la transparence et à 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 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 ou service TIC en question et de la nature, en masse ou en série, du processus de production.

10. 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.

11. Le personnel chargé d'accomplir des activités d'évaluation de la conformité possède:

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 qu'il effectue 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 effectuées.

12. L'impartialité des organismes d'évaluation de la conformité, de leurs cadres supérieurs et de leur personnel effectuant l'évaluation est garantie.

13. La rémunération des cadres supérieurs et du personnel chargé de l'évaluation au sein d'un organisme d'évaluation de la conformité ne dépend pas du nombre d'évaluations effectuées ni de leurs résultats.

14. 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 en vertu du droit national ou que l'évaluation de la conformité ne soit effectuée sous la responsabilité directe de l'État membre.

15. Le personnel d'un organisme d'évaluation de la conformité est lié par le secret professionnel pour toutes les informations obtenues dans l'exercice de ses fonctions au titre du présent règlement ou de toute disposition de droit national lui donnant effet, sauf à l'égard des autorités compétentes de l'État membre où il exerce ses activités.

16. Les organismes d'évaluation de la conformité respectent les exigences de la norme [...] **pertinente harmonisée au titre du règlement (CE) n° 765/2008 en ce qui concerne l'accréditation des organismes d'évaluation de la conformité chargés de la certification de processus, produits ou services** [...].

17. 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 harmonisée au titre du règlement (CE) n° 765/2008 en ce qui concerne l'accréditation de laboratoires qui réalisent des essais** [...].