AMENDEMENTS 001-257
déposés par la commission de l'industrie, de la recherche et de l'énergie

Rapport
Angelika Niebler **A8-0264/2018**
Règlement sur la cybersécurité

Proposition de règlement (COM(2017)0477 – C8-0310/2017 – 2017/0225(COD))

Amendement 1

Proposition de règlement
Considérant 1

Texte proposé par la Commission	*Amendement*
(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.	(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 ***(ci-après, les «TIC»)*** sont le fondement des systèmes complexes qui rendent possibles les activités sociales ***courantes***; 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.

Amendement 2

Proposition de règlement
Considérant 2

Texte proposé par la Commission	*Amendement*
(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.	(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***, processus*** et services TIC en matière de cybersécurité, sapant ainsi la confiance dans les solutions numériques. ***Cette ambition figure au cœur du programme de réforme de la Commission européenne pour la réalisation du marché unique du numérique étant donné que les réseaux des technologies de l'information constituent l'épine dorsale sur laquelle se greffent les produits et les services numériques qui peuvent nous assister dans tous les aspects de notre vie et constituer le moteur de la croissance économique en Europe. Pour faire en sorte que les objectifs du marché unique numérique soient pleinement atteints, les composantes technologiques essentielles sur lesquelles reposent des domaines importants tels que la santé en ligne, l'internet des objets, l'intelligence artificielle, les technologies quantiques ainsi que les systèmes de transport intelligents et les techniques avancées de production, doivent être mises en place.***

Amendement 3

Proposition de règlement
Considérant 3

Texte proposé par la Commission	*Amendement*
(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.	(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. ***À cet égard, le plan d'action en matière d'éducation numérique publié par la Commission européenne le 17 janvier 2018 constitue une avancée dans la bonne direction, en particulier la campagne de sensibilisation à l'échelle de l'Union européenne destinée aux éducateurs, aux parents et aux jeunes et visant à encourager la sécurité en ligne, l'hygiène informatique et l'éducation aux médias, ainsi que l'initiative d'enseignement de la sécurité informatique élaborée sur la base du cadre européen des compétences numériques pour les citoyens, afin de donner les moyens à tous d'utiliser les technologies de façon sûre et responsable.***

Amendement 4

Proposition de règlement
Considérant 3 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(3 bis) Les objectifs et les activités de l'ENISA devraient être davantage alignés sur la communication conjointe en ce qui concerne la référence de cette dernière à la promotion d'une hygiène informatique et d'une sensibilisation à la cybersécurité; relève qu'il est possible de parvenir à la cyberrésilience par l'application de principes d'hygiène informatique de base;

Amendement 5

Proposition de règlement
Considérant 3 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	(3 ter) L'ENISA devrait apporter un soutien plus concret et fondé sur des informations au secteur de la cybersécurité de l'Union européenne, en particulier aux PME et aux jeunes pousses, sources fondamentales de solutions innovantes dans le domaine de la cyberdéfense, et devrait promouvoir une coopération plus étroite avec les organismes universitaires de recherche et les acteurs de plus grande taille, afin de réduire les dépendances vis-à-vis des produits de cybersécurité provenant de sources externes et de créer une chaîne d'approvisionnement stratégique au sein de l'Union.

Amendement 6

Proposition de règlement
Considérant 4

Texte proposé par la Commission	*Amendement*
(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	(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.	renforcés ***et plus sûrs***. 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***. Les besoins de formation dans le domaine de la cyberdéfense sont considérables et augmentent, et la façon la plus efficace de les satisfaire est de coopérer à l'échelle de l'Union.*** 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.

Amendement 7

Proposition de règlement
Considérant 5

Texte proposé par la Commission	*Amendement*
(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	(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.

coopération***, la coordination*** et ***le partage d'informations*** 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***, tout en insistant sur l'importance de préserver et de renforcer les capacités de réaction des États membres en cas de menaces informatiques de tous types***. Des efforts supplémentaires sont également requis pour ***mettre en place une action coordonnée à l'échelle de l'Union et*** sensibiliser davantage les particuliers et les entreprises aux questions de cybersécurité. En outre, ***étant donné que les cyberincidents sapent la confiance dans les fournisseurs de services numériques et dans le marché unique numérique, notamment parmi les consommateurs,*** une information transparente sur le niveau de sécurité qui caractérise les produits***, processus*** et services permettrait de renforcer la confiance dans le marché unique numérique***, en précisant que la certification en matière de sécurité informatique, aussi élevée soit-elle, ne peut garantir que le produit ou service certifié soit complètement fiable***. 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, ***ainsi que la promotion de l'habileté numérique, peuvent*** faciliter cette transparence. ***Parallèlement à la certification à l'échelle de l'Union et compte tenu de la disponibilité croissante de dispositifs IdO, le secteur privé devrait prendre une série de mesures volontaires dans l'optique de renforcer la confiance dans la sécurité des produits, processus et services TIC, telles que le cryptage et les technologies de chaînes de blocs. Les enjeux à relever***

devraient être proportionnellement pris en compte dans l'enveloppe budgétaire allouée à l'Agence, de façon à garantir son fonctionnement optimal dans les circonstances actuelles.

Amendement 8

Proposition de règlement
Considérant 5 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(5 bis) En vue de renforcer les structures européennes de sécurité et de cyberdéfense, il est important de préserver et de développer les capacités de réaction globale des États membres en cas de cybermenaces, y compris en cas d'incidents transfrontières, tout en veillant à ce que la coordination par l'Agence à l'échelle de l'Union n'entraîne pas une diminution des capacités ou des efforts des États membres.

Amendement 9

Proposition de règlement
Considérant 5 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	(5 ter) Les entreprises devraient disposer, au même titre que les consommateurs individuels, d'informations précises sur le niveau de sécurité de leurs produits TIC. Dans le même temps, il convient d'accepter qu'aucun produit n'est fiable sur le plan de la cybersécurité et que des règles fondamentales d'hygiène informatique doivent être promues et privilégiées.

Amendement 10

Proposition de règlement

Considérant 7

Texte proposé par la Commission	*Amendement*
(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.	(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, dont le succès dépend largement de la mise en œuvre effective par les États membres, répond à la stratégie pour le marché unique numérique et instaure, en combinaison avec d'autres instruments tels que la directive établissant le code des communications électroniques européen, le règlement (UE) 2016/679 et la directive 2002/58/CE, instaure*** 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.

Amendement 11

Proposition de règlement
Considérant 8

Texte proposé par la Commission	*Amendement*
(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.	(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 ***compte tenu du rôle positif que l'Agence a joué au fil des ans en matière de mise en commun des compétences, de coordination et de renforcement des capacités, ainsi que*** 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.

Amendement 12

Proposition de règlement
Considérant 11

Texte proposé par la Commission	*Amendement*
(11) Étant donné l'aggravation des défis en matière de cybersécurité auxquels	(11) Étant donné l'aggravation des défis ***et des menaces*** en matière de cybersécurité

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.

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***, et lui permettre de remplir efficacement les tâches qui lui incombent en vertu du présent règlement***.

Amendement 13

Proposition de règlement
Considérant 12

Texte proposé par la Commission	*Amendement*
(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 contribuer de manière dynamique aux efforts consentis aux niveaux national et 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.	(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 contribuer de manière dynamique aux efforts consentis aux niveaux national et 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***, en évitant les doubles emplois, en favorisant les synergies et la complémentarité et, partant, en renforçant la coordination et en réalisant des économies budgétaires***. De plus, l'Agence devrait s'appuyer sur les informations fournies par ***les secteurs public et*** privé et travailler en coopération avec ***ceux-ci***, ainsi qu'avec d'autres parties prenantes. Un ***calendrier précis et un*** ensemble de missions ***et d'objectifs clairement définis devraient*** déterminer la manière dont l'Agence doit atteindre ses objectifs tout en ***tenant dûment compte de la*** souplesse ***nécessaire pour son*** fonctionnement. ***Dans la mesure du***

possible, le plus haut niveau de transparence et de diffusion de l'information doit être maintenu.

Amendement 14

Proposition de règlement
Considérant 12 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(12 bis) Le rôle de l'Agence devrait être soumis à une évaluation continue et à des examens opportuns, en particulier quant à son rôle de coordination vis-à-vis des États membres et de leurs autorités nationales, ainsi que concernant son rôle potentiel de «guichet unique» pour les États membres et les institutions et organes de l'Union européenne. Le rôle que joue l'Agence dans la prévention de la fragmentation du marché intérieur ainsi que dans l'introduction éventuelle de systèmes de certification de cybersécurité obligatoires, si la situation à venir exige une telle évolution, devrait également être évalué, tout comme son rôle dans la vérification des produits en provenance de pays tiers qui entrent sur le marché de l'Union ainsi que dans l'élaboration éventuelle d'une liste noire des sociétés qui ne satisfont pas aux exigences de l'Union.

Amendement 15

Proposition de règlement
Considérant 12 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	(12 ter) Pour être en mesure d'apporter un soutien adéquat à la coopération opérationnelle avec les États membres, l'ENISA devrait renforcer davantage ses propres capacités et

compétences techniques. À cette fin, l'Agence devrait renforcer progressivement son personnel consacré à cette tâche afin de pouvoir collecter et analyser de manière autonome les différents types d'un large éventail de menaces et de logiciels malveillants en matière de cybersécurité, procéder à des analyses scientifiques et aider les États membres à réagir aux incidents de grande ampleur. Afin d'éviter toute duplication des capacités existantes dans les États membres, l'ENISA devrait accroître son savoir-faire et ses capacités sur la base des ressources existantes dans les États membres, notamment en détachant des experts nationaux auprès de l'Agence, en créant des groupes d'experts, des programmes d'échanges de personnel, etc. Lors de la sélection du personnel compétent, l'Agence devrait progressivement s'assurer qu'il respecte les critères appropriés pour fournir un soutien adéquat.

Amendement 16

Proposition de règlement
Considérant 13

Texte proposé par la Commission	*Amendement*
(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, y compris la protection des infrastructures critiques et la cyberrésilience. 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.	(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, y compris la protection des infrastructures critiques et la cyberrésilience. 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. ***Ses compétences seront particulièrement nécessaires lors de l'élaboration du programme de travail***

pluriannuel de l'Union pour les systèmes européens de certification de cybersécurité. L'Agence devrait régulièrement tenir le Parlement informé des mises à jour, des analyses et des examens dans le domaine de la cybersécurité, ainsi que de l'état d'avancement de ses travaux.

Amendement 17

Proposition de règlement
Considérant 14

Texte proposé par la Commission	*Amendement*
(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.	(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, ***de la directive établissant le code des communications électroniques européen, du règlement (UE) 2016/679 et de la directive 2002/58/CE, essentiels*** 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.

Amendement 18

Proposition de règlement
Considérant 15

Texte proposé par la Commission	*Amendement*
(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 problèmes et incidents de cybersécurité et y réagir, et en ce qui concerne la sécurité des réseaux et	(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 problèmes 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. L'Agence devrait également contribuer à l'élaboration et à la mise à jour des stratégies de l'Union et des États membres en matière de sécurité des réseaux et systèmes d'information, notamment en matière de cybersécurité, promouvoir leur diffusion et suivre l'avancement de 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.	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. L'Agence devrait également contribuer à l'élaboration et à la mise à jour des stratégies de l'Union et des États membres en matière de sécurité des réseaux et systèmes d'information, notamment en matière de cybersécurité, promouvoir leur diffusion et suivre l'avancement de leur mise en œuvre. ***Étant donné que les erreurs humaines constituent l'un des risques les plus susceptibles de toucher la cybersécurité,*** l'Agence devrait ***aussi*** proposer des formations et du matériel pédagogique aux organismes publics et, ***autant que possible***, «former les formateurs» en vue d'aider les États membres ***ainsi que les institutions et organes de l'Union*** à mettre en place leurs propres capacités de formation. ***L'Agence devrait enfin servir de point de contact pour les États membres et les institutions de l'Union, lesquels devraient avoir la possibilité de demander son assistance dans la limite des compétences et des fonctions qui lui sont assignées.***

Amendement 19

Proposition de règlement
Considérant 18

Texte proposé par la Commission	*Amendement*
(18) L'Agence devrait agréger et analyser les rapports nationaux émanant des CSIRT et des CERT-UE, en établissant des règles, 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 avec la création du réseau des CSIRT.	(18) L'Agence devrait agréger et analyser les rapports nationaux émanant des CSIRT et des CERT-UE, en établissant des règles, un langage et une terminologie communs pour l'échange d'informations. L'Agence devrait également assurer la participation ***des secteurs public et*** privé, dans le cadre de la directive SRI, qui a fixé les bases d'un échange volontaire d'informations techniques à l'échelon opérationnel avec la création du réseau des CSIRT.

Amendement 20

Proposition de règlement
Considérant 19

Texte proposé par la Commission	*Amendement*
(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 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 annuels.	(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 comprendre la ***convocation des autorités des États membres et l'assistance à la coordination de leur réaction, 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, ***par exemple*** 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 annuels. ***L'Agence devrait respecter les compétences des États membres en ce qui concerne la cybersécurité, en particulier les compétences relatives à la sécurité publique, à la défense et à la sûreté de l'État, et les activités de l'État dans les domaines du droit pénal.***

Amendement 21

Proposition de règlement
Considérant 25

Texte proposé par la Commission	*Amendement*
(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	(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.	préjudice de leur droit de protéger les informations commercialement sensibles ***et les informations relatives à la sécurité publique***.

Amendement 22

Proposition de règlement
Considérant 26

Texte proposé par la Commission	*Amendement*
(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 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 problèmes liés à la cybersécurité, en procédant à l'analyse des menaces et ***incidents***.	(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***, les incidents, les menaces et les vulnérabilités*** 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 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 problèmes liés à la cybersécurité, en procédant à l'analyse des menaces***, des incidents*** et ***des vulnérabilités***.

Amendement 23

Proposition de règlement
Considérant 27

Texte proposé par la Commission	*Amendement*
(27) Afin de renforcer la résilience de l'Union, l'Agence devrait développer	(27) Afin de renforcer la résilience de l'Union, l'Agence devrait développer

l'excellence en matière de sécurité des infrastructures internet et des infrastructures critiques 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.	l'excellence en matière de sécurité des infrastructures internet et des infrastructures critiques 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. ***Un accès facilité à des informations mieux structurées sur les risques de cybersécurité et d'éventuelles mesures correctives devraient aider les États membres à consolider leurs capacités et à uniformiser leurs pratiques et, partant, à améliorer leur résilience générale face aux attaques.***

Amendement 24

Proposition de règlement
Considérant 28

Texte proposé par la Commission	*Amendement*
(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	(28) L'Agence devrait contribuer à sensibiliser le public aux risques liés à la cybersécurité***, y compris en favorisant l'éducation,*** et fournir, à l'intention des particuliers***, des organisations*** et des ***entreprises***, des orientations sur les bonnes pratiques à adopter par les utilisateurs. L'Agence devrait également contribuer à promouvoir les meilleures pratiques ***en matière d'hygiène informatique, qui couvrent plusieurs pratiques qui devraient être mises en œuvre et réalisées régulièrement pour protéger les utilisateurs et les entreprises en ligne,*** et solutions pour les particuliers***, les organisations*** et les ***entreprises*** en collectant et en analysant des informations du domaine public sur les incidents significatifs, et en rédigeant ***et publiant*** des

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.

rapports ***et des guides*** en vue de fournir des orientations aux entreprises et aux particuliers, et d'améliorer le niveau global de préparation et de résilience. ***L'ENISA devrait s'efforcer également de fournir aux consommateurs des informations pertinentes concernant les systèmes de certification en vigueur, par exemple en fournissant des orientations et des recommandations aux marchés en ligne et hors ligne.*** L'Agence devrait en outre organiser, ***conformément au plan d'action en matière d'éducation numérique et*** 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***, les compétences numériques*** 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 ***multifactorielle, de correctifs, de cryptage, d'anonymisation*** 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 ***et la sécurisation de l'utilisation des services, la généralisation au niveau de l'Union des concepts de sécurité dès la conception et de protection de la vie privée dès la conception et la communication des incidents et des solutions associées. Pour atteindre cet objectif, l'Agence doit utiliser au mieux les meilleures pratiques et expériences disponibles, notamment celles issues du monde universitaire et du domaine de la recherche en sécurité informatique. Étant donné que les erreurs individuelles et la méconnaissance des risques informatiques constituent l'un des principaux facteurs d'insécurité cybernétique, l'Agence devrait être dotée***

	de ressources suffisantes pour exercer au mieux cette fonction.

Amendement 25

Proposition de règlement
Considérant 28 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(28 bis) L'Agence doit sensibiliser le public aux risques de falsification ou de vol de données qui peuvent porter gravement atteinte aux droits fondamentaux des personnes, constituer une menace pour l'état de droit et mettre en danger la stabilité de nos sociétés démocratiques, y compris des processus démocratiques dans les États membres.

Amendement 26

Proposition de règlement
Considérant 30

Texte proposé par la Commission	*Amendement*
(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) et toute autre agence de l'UE jouant un rôle en matière de cybersécurité. 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	(30) Pour réaliser pleinement ses objectifs, l'Agence devrait se concerter avec les institutions, ***agences et*** organes ***compétents, ainsi qu'avec les autorités européennes de contrôle*** et ***autres autorités compétentes***, 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 ***du GNSS européen (GSA), l'Organe des régulateurs européens des communications électroniques (ORECE), l'Agence*** européenne pour la gestion opérationnelle des systèmes d'information à grande échelle (eu-LISA), ***la Banque centrale européenne (BCE), l'Autorité bancaire européenne (ABE), le comité européen de la protection des données,*** l'Agence européenne de la sécurité aérienne (AESA)

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.

et toute autre agence de l'UE jouant un rôle en matière de cybersécurité. Elle devrait aussi coopérer avec les ***organisations européennes de normalisation (OEN), les parties prenantes concernées et 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 ***consultatif*** de ***l'ENISA***. 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. ***Des partenariats devraient être noués avec des établissements universitaires menant des initiatives de recherche dans les domaines en question, et il convient que les organisations de consommateurs et autres disposent de canaux adéquats pour leurs contributions, lesquelles devraient toujours être analysées.***

Amendement 27

Proposition de règlement
Considérant 31

Texte proposé par la Commission	*Amendement*
(31) L'Agence, en tant que membre du réseau des CSIRT chargé en outre d'en assurer le secrétariat, 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	(31) L'Agence, en tant que membre du réseau des CSIRT chargé en outre d'en assurer le secrétariat, 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.	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. ***L'Agence peut, à la demande de la Commission ou d'un État membre, procéder régulièrement à des audits des infrastructures transfrontalières critiques dans le domaine de la sécurité informatique dans le but de recenser les risques éventuels de cybersécurité et de formuler des recommandations visant à renforcer leur résilience.***

Amendement 28

Proposition de règlement
Considérant 33

Texte proposé par la Commission	*Amendement*
(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.	(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 ***s'appuyer sur les bonnes pratiques existantes et*** 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.

Amendement 29

Proposition de règlement
Considérant 35

Texte proposé par la Commission	*Amendement*
(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 ***et*** services, y compris leur cybersécurité.	(35) L'Agence devrait encourager les États membres***, les fabricants*** et les fournisseurs de services à renforcer ***les*** normes de sécurité générales ***de leurs produits, processus, services et systèmes TIC qui devraient satisfaire à des exigences élémentaires de sécurité conformément aux principes de sécurité dès la conception et de sécurité par défaut, en particulier en fournissant les mises à jour nécessaires***, de manière que tous les utilisateurs d'internet puissent ***être protégés et encouragés à*** prendre les mesures nécessaires pour garantir leur propre cybersécurité. En particulier, les fournisseurs de services et les fabricants de produits devraient ***rappeler,*** retirer ou recycler les produits et services qui ne satisfont pas aux ***exigences élémentaires*** de cybersécurité***, tandis que les importateurs et les distributeurs devraient veiller à ce que les produits, processus, services et systèmes TIC qu'ils mettent sur le marché de l'Union soient conformes aux exigences applicables et ne présentent aucun risque pour les consommateurs européens***. 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***, processus,*** services ***et systèmes***, y compris leur cybersécurité. ***L'Agence devrait collaborer avec les parties prenantes en vue d'élaborer une approche responsable de la divulgation des vulnérabilités à l'échelle de l'Union et promouvoir les meilleures pratiques dans ce domaine.***

Amendement 30

Proposition de règlement
Considérant 36

Texte proposé par la Commission	*Amendement*
(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 sécurité des réseaux et de l'information, et en particulier de la 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 sécurité des réseaux et de l'information, et en particulier de la cybersécurité. ***Plus précisément, il convient de mettre en place une coopération avec le Conseil européen de la recherche (CER) et l'Institut européen d'innovation et de technologie (EIT) et d'intégrer la recherche en matière de sécurité dans le neuvième programme-cadre de recherche et dans le programme Horizon 2020.***

Amendement 31

Proposition de règlement
Considérant 36 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(36 bis) Les normes constituent un instrument volontaire, ajusté aux conditions du marché, offrant des exigences et des conseils techniques et découlant d'un processus ouvert, transparent et exhaustif. L'Agence devrait consulter régulièrement les organismes européens de normalisation et collaborer avec eux, notamment lors de l'élaboration des systèmes européens de certification de cybersécurité.

Amendement 32

Proposition de règlement
Considérant 37

Texte proposé par la Commission	*Amendement*
(37) Les problèmes de cybersécurité sont des enjeux mondiaux. Il est nécessaire de renforcer la coopération internationale pour améliorer les normes de 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.	(37) Les problèmes de cybersécurité sont des enjeux mondiaux. Il est nécessaire de renforcer la coopération internationale pour améliorer les normes de sécurité, y compris en définissant des normes de comportement communes, ***en élaborant des codes de conduite et en recourant à des normes internationales,*** 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.

Amendement 33

Proposition de règlement
Considérant 40

Texte proposé par la Commission	*Amendement*
(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	(40) Le conseil d'administration, ***qui représente les*** États membres et la Commission ***ainsi que les parties prenantes pertinentes pour les objectifs de l'Agence***, 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

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.

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. ***Compte tenu des tâches hautement techniques et scientifiques de l'Agence, les membres du conseil d'administration devraient avoir l'expérience appropriée et être dotés d'un niveau d'expertise élevé sur les questions relevant du mandat de l'Agence.***

Amendement 34

Proposition de règlement
Considérant 41

Texte proposé par la Commission	*Amendement*
(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.	(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. ***En raison de la haute valeur sur le marché des compétences recherchées pour le travail de l'Agence, il faut veiller à ce que les salaires et les conditions sociales proposés à tous les membres du personnel de l'Agence soient compétitifs et à même d'attirer les meilleurs professionnels.***

Justification

Afin de disposer du niveau de compétences suffisant, l'ENISA doit être un employeur compétitif dans un marché très compétitif.

Amendement 35

Proposition de règlement
Considérant 42

Texte proposé par la Commission	*Amendement*
(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 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.	(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 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, ***notamment entre les hommes et les femmes,*** 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.

Amendement 36

Proposition de règlement
Considérant 44

Texte proposé par la Commission	*Amendement*
(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 programme de travail, devraient assurer une représentation suffisante des parties prenantes dans le travail de l'Agence.	(44) L'Agence devrait disposer, à titre d'organe consultatif, d'un groupe ***consultatif de l'ENISA*** pour maintenir un dialogue régulier avec le secteur privé, les organisations de consommateurs***, le monde universitaire*** et les autres parties prenantes. Le groupe ***consultatif de l'ENISA***, 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 programme de travail, devraient assurer une représentation suffisante des parties prenantes dans le travail de l'Agence. ***Compte tenu de l'importance des exigences en matière de certification pour assurer la confiance dans l'IdO, la Commission envisagera tout particulièrement la mise en place de mesures visant à assurer une harmonisation paneuropéenne des normes de sécurité pour les dispositifs de l'IdO.***

Amendement 37

Proposition de règlement
Considérant 44 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(44 bis) L'Agence devrait disposer, à titre d'organe consultatif, d'un groupe des parties prenantes pour la certification

pour maintenir un dialogue régulier avec le secteur privé, les organisations de consommateurs, le monde universitaire et les autres parties prenantes. Le groupe des parties prenantes pour la certification, institué par le directeur exécutif, devrait être composé d'un comité consultatif général chargé de fournir des contributions sur les produits et services TIC qui devront être couverts par les futurs systèmes européens de certification en matière de sécurité informatique, et les comités ad hoc chargés de fournir des contributions pour la proposition, le développement et l'adoption des systèmes de cybersécurité européens candidats demandés.

Amendement 38

Proposition de règlement
Considérant 46

Texte proposé par la Commission	*Amendement*
(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***	(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. ***Doter l'Agence d'un budget adéquat est d'une importance capitale pour garantir qu'elle dispose de ressources suffisantes en vue de réaliser ses objectifs et ses tâches qui ne cessent de croître.*** 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

responsabilité.	budget général de l'Union. En outre, la Cour des comptes devrait contrôler les comptes de l'Agence afin de garantir la transparence***, la responsabilité*** et ***l'efficacité des dépenses***.

Amendement 39

Proposition de règlement
Considérant 47

Texte proposé par la Commission	*Amendement*
(47) L'évaluation de la conformité est le processus destiné à établir si les exigences spécifiées relatives à un produit, à un processus, à un service, à un système, à une personne ou à un organisme ont été respectées. Aux fins du présent règlement, il y a lieu de considérer la certification comme un type d'évaluation de la conformité portant sur les caractéristiques de cybersécurité d'un produit, processus, service, système, ou d'une combinaison de ceux-ci («produits et services TIC») effectuée par un tiers indépendant, ***distinct*** du fabricant du produit ou du fournisseur du service. En soi, la certification ne peut garantir 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.	(47) L'évaluation de la conformité est le processus destiné à établir si les exigences spécifiées relatives à un produit, à un processus, à un service, à un système, à une personne ou à un organisme ont été respectées. Aux fins du présent règlement, il y a lieu de considérer la certification comme un type d'évaluation de la conformité portant sur les caractéristiques de cybersécurité d'un produit, processus, service, système, ou d'une combinaison de ceux-ci («produits***, processus*** et services TIC») effectuée par un tiers indépendant, ***ou, lorsque cela est possible, par une auto-évaluation*** du fabricant du produit ou du fournisseur du service. ***L'auto-évaluation peut être entreprise par le fabricant d'un produit, les PME ou le fournisseur d'un service, conformément aux dispositions du présent règlement, et, le cas échéant, conformément aux prévisions et aux dispositions du nouveau cadre législatif. En outre, elle peut être entreprise par le fabricant d'un produit ou l'exploitant lorsque l'on ne s'attend pas à ce qu'un tel produit comporte un risque élevé ou important qu'un incident de cybersécurité se produise, et/ou qu'un tel incident cause un préjudice important à la société ou à une grande partie des citoyens, compte tenu de l'utilisation prévue par le fabricant ou le fournisseur du produit ou service concerné.*** En soi, la certification ne peut garantir que les produits***, processus*** et services TIC

	couverts sont fiables du point de vue de la cybersécurité***, et il convient d'en informer dûment les consommateurs et les entreprises***. Il s'agit plutôt d'une procédure et d'une méthodologie technique visant à attester que des produits***, processus*** 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. ***Ces normes techniques indiquent si un produit, processus ou service TIC est apte à remplir ses fonctions comme prévu lorsqu'il n'est pas connecté à l'internet.***

Amendement 40

Proposition de règlement
Considérant 48

Texte proposé par la Commission	*Amendement*
(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.	(48) La certification ***européenne*** de cybersécurité est ***essentielle*** pour accroître la sécurité des produits***, processus*** 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 ***haut*** 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.

Amendement 41

Proposition de règlement

Considérant 49

Texte proposé par la Commission	*Amendement*
(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.	(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***, de processus*** 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.

Amendement 42

Proposition de règlement

Considérant 50

Texte proposé par la Commission	*Amendement*
(50) Actuellement, la certification de cybersécurité des 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 l'industrie. 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.	(50) Actuellement, la certification de cybersécurité des produits***, processus*** 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 l'industrie. 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***, processus*** et services dans les différents États membres où elles exercent leurs activités, par exemple pour participer à des procédures nationales de passation de marchés***, ce qui implique des coûts supplémentaires***. 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 ***fondée sur le risque***, de critères de fond et d'utilisation effective. ***La reconnaissance mutuelle et la confiance entre les États membres sont des éléments clés à cet égard. L'ENISA a un rôle important à jouer dans la fourniture d'une aide aux États membres afin que ceux-ci mettent en place une structure institutionnelle solide et acquièrent une expertise en matière de protection contre des attaques informatiques potentielles. Une approche au cas par cas est nécessaire afin de garantir que les services, processus et produits sont soumis à des systèmes de certification appropriés. En outre, une approche fondée sur les risques est nécessaire afin de déceler et d'atténuer efficacement les risques tout en reconnaissant qu'une solution «passe-***

partout» n'est pas possible.

Amendement 43

Proposition de règlement
Considérant 52

Texte proposé par la Commission	*Amendement*
(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 applicables aux 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.	(52) Compte tenu de ce qui précède, il est nécessaire ***d'adopter une approche commune et*** 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 applicables aux produits***, processus*** et services TIC. ***Ce faisant, il est essentiel de s'appuyer sur des systèmes nationaux et internationaux existants, ainsi que sur des systèmes de reconnaissance mutuelle, notamment du SOG-IS (groupe de hauts fonctionnaires pour la sécurité des systèmes d'information) et de créer les conditions d'une transition en douceur entre les systèmes existants relevant de ces systèmes et les systèmes relevant du nouveau cadre européen.*** Le cadre européen devrait poursuivre un double objectif. D'une part, il devrait contribuer à rehausser la confiance dans les produits***, processus*** 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. ***Lorsqu'une certification européenne de cybersécurité a remplacé un système national, les certificats délivrés au titre du système européen devraient être considérés comme valables dans les cas où une certification au titre du système national était requise.*** Les systèmes devraient

s'inspirer du principe de la sécurité dès la conception et des principes énoncés dans le règlement (UE) 2016/679. Ils devraient également 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.

Amendement 44

Proposition de règlement
Considérant 52 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(52 bis) Ce cadre européen de certification de cybersécurité doit être établi de manière homogène dans tous les États membres afin d'éviter la pratique du "shopping de certifications" en raison de différences de coûts ou de niveaux d'exigence entre les États membres.

Amendement 45

Proposition de règlement
Considérant 52 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	(52 ter) Les systèmes de certification devraient être élaborés à partir de ceux qui existent déjà aux niveaux national et international, en tirant des enseignements des points forts actuels ainsi qu'en évaluant et en corrigeant les faiblesses.

Amendement 46

Proposition de règlement
Considérant 52 quater (nouveau)

Texte proposé par la Commission	*Amendement*
	(52 quater) Des solutions de cybersécurité flexibles sont nécessaires pour que les

entreprises du secteur gardent une longueur d'avance sur les menaces et les attaques malveillantes, d'où l'importance d'éviter le risque d'obsolescence rapide des systèmes de certification.

Amendement 47

Proposition de règlement
Considérant 53

Texte proposé par la Commission	*Amendement*
(53) La Commission devrait être habilitée à adopter des systèmes européens de certification de cybersécurité concernant des groupes spécifiques de produits et services TIC. Ces systèmes devraient être mis en œuvre et contrôlés par des autorités nationales de contrôle de la certification, 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 l'industrie 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.	(53) La Commission devrait être habilitée à adopter des systèmes européens de certification de cybersécurité concernant des groupes spécifiques de produits***, de processus*** et services TIC. Ces systèmes devraient être mis en œuvre et contrôlés par des autorités nationales de contrôle de la certification, 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 l'industrie 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. ***L'Agence devrait recenser et évaluer les systèmes déjà mis en œuvre par l'industrie ou des organisations privées afin de choisir les meilleures pratiques qui pourraient faire partie d'un système européen. Les entreprises du secteur peuvent auto-évaluer leurs produits ou services en amont de la certification, indiquant ainsi que leur produit ou service est prêt à entamer le processus de certification, le cas échéant.***

Amendement 48

Proposition de règlement
Considérant 53 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(53 bis) L'Agence et la Commission devraient utiliser au mieux les systèmes de certification existants aux niveaux européen et international. L'ENISA devrait être en mesure d'apprécier ceux des systèmes actuels qui sont adaptés à l'usage prévu et qui peuvent être introduits dans la législation européenne en coopération avec les organisations européennes de normalisation et, autant que possible, reconnus au niveau international. Les données sur les bonnes pratiques existantes devraient être collectées et partagées entre les États membres.

Amendement 49

Proposition de règlement
Considérant 54

Texte proposé par la Commission	*Amendement*
(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	(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***, processus*** 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.

lorsque ces opérations sont intégrées dans des produits et services.

Amendement 50

Proposition de règlement
Considérant 55

Texte proposé par la Commission	*Amendement*
(55) Les systèmes européens de certification de cybersécurité devraient avoir pour finalité de garantir que les produits et ***services*** TIC certifiés selon un tel système sont conformes aux exigences spécifiées. Ces exigences concernent l'aptitude à résister, à un niveau ***d'assurance*** donné, aux actions qui visent à compromettre 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, 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 produits et ***services*** TIC. Les 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 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	(55) Les systèmes européens de certification de cybersécurité devraient avoir pour finalité de garantir que les produits***, services*** et ***processus*** TIC certifiés selon un tel système sont conformes aux exigences spécifiées. Ces exigences concernent l'aptitude à résister, à un niveau ***de risque*** donné, aux actions qui visent à compromettre 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, 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 produits***, services*** et ***processus*** TIC. Les produits***, services*** et ***processus*** 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 produits***, services*** et ***processus*** 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.

spécifications techniques. ***Tous les acteurs d'une chaîne d'approvisionnement donnée devraient être encouragés à élaborer et à adopter des normes de sécurité, des normes techniques et des principes de sécurité dès la conception, à tous les stades du cycle de vie du produit, service ou processus. Chaque système européen de certification de cybersécurité devrait être conçu dans cette optique.***

Amendement 51

Proposition de règlement
Considérant 56

Texte proposé par la Commission	*Amendement*
(56) La Commission devrait être habilitée à demander à l'ENISA de préparer des systèmes candidats pour des 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 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, ainsi que le niveau d'assurance visé, ***c.-à-d.*** élémentaire, substantiel ou ***supérieur***.	(56) La Commission devrait être habilitée à demander à l'ENISA de préparer des systèmes candidats pour des produits***,*** ***processus*** ou services TIC spécifiques sur la base ***de motifs valables, à savoir les systèmes nationaux de certification de cybersécurité qui fragmentent le marché intérieur; un besoin actuel ou prévu de soutenir le droit de l'Union; ou l'avis du groupe de certification des États membres ou du groupe de certification des parties prenantes. Après avoir évalué les systèmes de certification candidats*** que propose l'ENISA, ***sur la base de la demande de*** la Commission***, la Commission serait*** alors habilitée à adopter ***les systèmes européens*** de certification de cybersécurité par voie d'actes ***délégués***. 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 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 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, ainsi que le niveau d'assurance visé, élémentaire, substantiel ***et/***ou ***élevé***.

Amendement 52

Proposition de règlement
Considérant 56 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(56 bis) L'Agence devrait être le point de référence des informations sur les systèmes européens de cybersécurité. Elle devrait tenir à jour un site web contenant toutes les informations utiles, notamment en ce qui concerne les certificats retirés et périmés et les certifications nationales concernées. L'Agence devrait veiller à ce qu'une partie adéquate du contenu de son site internet soit compréhensible pour les consommateurs ordinaires.

Amendement 53

Proposition de règlement
Considérant 56 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	(56 ter) Il est indispensable de définir les niveaux d'assurance pour les certificats afin de donner une indication à l'utilisateur final du type attendu de menaces informatiques que les mesures de cybersécurité contenues dans le produit, le processus ou le service visent à empêcher. La cybermenace doit être définie en tenant compte du risque attendu et des capacités de l'auteur ou des auteurs de l'attaque dans le contexte de l'utilisation prévue du produit, du processus ou du service de TIC couvert. Le niveau d'assurance «de base» désigne

	la capacité à résister aux attaques qui peuvent être évitées avec des mesures de cybersécurité de base et qui peuvent être contrôlées facilement en examinant la documentation technique. Le niveau d'assurance «substantiel» fait référence à la capacité de résister aux types d'attaques connus d'un agresseur à un niveau de sophistication précis, mais disposant de ressources limitées. Le niveau d'assurance «élevé» renvoie à la capacité de résister à des vulnérabilités inconnues et aux attaques sophistiquées impliquant des techniques de pointe et des ressources importantes telles que des équipes pluridisciplinaires financées.

Amendement 54

Proposition de règlement
Considérant 56 quater (nouveau)

Texte proposé par la Commission	*Amendement*
	(56 quater) Afin d'éviter la fragmentation du marché intérieur due aux systèmes nationaux de cybersécurité, de soutenir les futures législations et de renforcer la confiance et la sécurité, il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne en ce qui concerne la fixation des priorités en matière de certification européenne de cybersécurité, l'adoption du programme continu et l'adoption des systèmes de certification européens. Il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts, et que ces consultations soient menées conformément aux principes définis dans l'accord interinstitutionnel «Mieux légiférer» du 13 avril 2016. En particulier, pour assurer leur égale participation à la préparation des actes

délégués, le Parlement européen et le Conseil reçoivent tous les documents au même moment que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission traitant de l'élaboration des actes délégués.

Amendement 55

Proposition de règlement
Considérant 56 quinquies (nouveau)

Texte proposé par la Commission	*Amendement*
	(52 quinquies) Parmi les méthodes et les procédures d'évaluation associées à chaque système européen de certification de sécurité, il conviendrait de promouvoir, au niveau de l'Union, le piratage contrôlé, dont l'objectif est d'identifier les faiblesses et vulnérabilités des appareils et des systèmes d'information en anticipant les actions et les capacités des pirates malveillants.

Amendement 56

Proposition de règlement
Considérant 57

Texte proposé par la Commission	*Amendement*
(57) Le recours à la certification européenne de cybersécurité devrait rester volontaire, sauf disposition contraire dans la législation de l'Union ou la législation nationale. Toutefois, 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	(57) Le recours à la certification européenne de cybersécurité devrait rester volontaire, sauf disposition contraire dans la législation de l'Union ou la législation nationale. Toutefois, 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***, processus*** et services TIC couverts par un système européen de certification de cybersécurité devraient

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.	cesser de produire des effets à compter de la date arrêtée par la Commission par voie d'acte ***délégué***. 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. ***Cependant, le présent règlement devrait s'appliquer sans préjudice des systèmes nationaux qui relèvent du droit souverain des États membres de gérer les produits, processus et services TIC utilisés pour les besoins de leurs activités souveraines.***

Amendement 57

Proposition de règlement
Considérant 57 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(57 bis) L'obligation de délivrer une déclaration de produit contenant des informations structurées sur la certification du produit, processus ou service est introduite afin de fournir au consommateur davantage d'informations et de lui permettre de faire un choix éclairé.

Amendement 58

Proposition de règlement
Considérant 57 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	(52 ter) Lorsqu'ils proposent de nouveaux systèmes européens de cybersécurité, l'ENISA et les autres organes concernés devraient accorder une attention particulière à la dynamique concurrentielle de la proposition, notamment en veillant à ce que, lorsque les secteurs concernés comptent un grand

	nombre de petites et moyennes entreprises, comme celui du développement de logiciels, les systèmes de certification n'entravent pas l'entrée sur le marché de nouvelles entreprises et d'innovations.

Amendement 59

Proposition de règlement
Considérant 57 quater (nouveau)

Texte proposé par la Commission	*Amendement*
	(52 quater) Les systèmes européens de cybersécurité contribueront à harmoniser et à unifier les pratiques de cybersécurité au sein de l'Union. Cependant, ils ne doivent pas constituer le niveau minimal de cybersécurité. La conception des systèmes européens de certification de cybersécurité devrait également prendre en compte et permettre la mise au point d'innovations dans le domaine de la cybersécurité.

Amendement 60

Proposition de règlement
Considérant 58

Texte proposé par la Commission	*Amendement*
(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	(58) Une fois un système européen de certification de cybersécurité adopté, les fabricants de produits TIC ou les fournisseurs de ***processus ou de*** services TIC devraient être en mesure de soumettre une demande de certification de leurs produits ou services à ***un organisme*** d'évaluation de la conformité de leur choix ***établi n'importe où dans l'Union européenne***. 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

renouvelée dans les mêmes conditions pourvu que l'organisme d'évaluation de la conformité satisfasse aux exigences. Elle devrait être 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.	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 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. ***L'Agence devrait conduire des audits pour garantir un niveau équivalent de qualité et de diligence des organismes de vérification de la conformité, afin d'éviter un arbitrage réglementaire. Les résultats des audits devraient être communiqués à l'Agence, à la Commission ainsi qu'au Parlement, et être rendus publics.***

Amendement 61

Proposition de règlement
Considérant 58 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(58 bis) L'utilisation obligatoire de la certification européenne de cybersécurité devrait être limitée aux cas où l'analyse de risque justifie le coût pour l'industrie, les citoyens et les consommateurs. Les incidents qui perturbent la fourniture de services essentiels peuvent nuire à l'exercice d'activités économiques, entraîner des pertes financières importantes, entamer la confiance des utilisateurs et porter un grand préjudice à l'économie de l'Union. L'utilisation obligatoire de la certification européenne de cybersécurité par les opérateurs de services essentiels devrait se limiter aux éléments qui sont essentiels pour leur fonctionnement et ne devrait pas être étendue à des produits, des processus et des services de portée générale, ce qui entraînerait un coût injustifié pour l'industrie et les consommateurs. La Commission devrait collaborer avec le

groupe de coopération créé en vertu de l'article 11 de la directive (UE) 2016/1148 pour définir une liste de catégories de produits, de processus et de services spécifiquement destinés à l'utilisation par les opérateurs de services essentiels et dont le dysfonctionnement en cas d'incident pourrait avoir un effet perturbateur important sur le service essentiel. Cette liste devrait être établie progressivement et mise à jour si nécessaire. Seuls les produits, processus et services figurant sur cette liste devraient être obligatoires pour les opérateurs des exigences essentielles.

Amendement 62

Proposition de règlement
Considérant 58 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	(58 ter) La présence de références croisées dans la législation nationale qui font référence à une norme nationale qui a cessé de produire des effets juridiques en raison de l'entrée en vigueur d'un système de certification européen peut être une source de confusion pour les fabricants et les utilisateurs finaux. Afin d'éviter que les fabricants continuent à mettre en œuvre des spécifications correspondant à des certificats nationaux qui ne sont plus en vigueur, les États membres devraient, conformément aux obligations qui leur incombent en vertu des traités, adapter leur législation nationale pour tenir compte de l'adoption d'un système de certification européen.

Amendement 63

Proposition de règlement
Considérant 59

Texte proposé par la Commission	*Amendement*
(59) Il est nécessaire d'exiger que tous les États membres désignent une autorité de contrôle de la certification de cybersécurité afin de contrôler que les organismes d'évaluation de la conformité et les certificats délivrés par les organismes d'évaluation de la conformité établis sur leur territoire respectent les exigences du présent règlement et des systèmes de certification de cybersécurité pertinents. Les autorités nationales de contrôle de la certification devraient traiter les réclamations introduites par toute personne physique ou morale en rapport avec les certificats délivrés par des organismes d'évaluation de la conformité établis sur leur territoire, 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 contrôle de la certification 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.	(59) Il est nécessaire d'exiger que tous les États membres désignent une autorité de contrôle de la certification de cybersécurité afin de contrôler que les organismes d'évaluation de la conformité et les certificats délivrés par les organismes d'évaluation de la conformité établis sur leur territoire respectent les exigences du présent règlement et des systèmes de certification de cybersécurité pertinents***, ainsi que de veiller à ce que les certificats européens de cybersécurité soient reconnus sur leur territoire***. Les autorités nationales de contrôle de la certification devraient traiter les réclamations introduites par toute personne physique ou morale en rapport avec les certificats délivrés par des organismes d'évaluation de la conformité établis sur leur territoire ***ou avec des allégations de non-reconnaissance de certificats sur leur territoire***, 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 contrôle de la certification ou d'autres autorités publiques, notamment en s'échangeant des informations sur l'éventuelle non-conformité de produits***, processus*** et services TIC aux exigences du présent règlement ou à celles de systèmes de certification de cybersécurité spécifiques***, ou sur la non-reconnaissance des certificats européens de cybersécurité. Elles devraient en outre superviser et contrôler la conformité des autodéclarations de conformité et s'assurer que les certificats européens de cybersécurité ont été délivrés par des organismes d'évaluation de la conformité dans le respect des exigences énoncées dans le présent règlement, notamment des règles adoptées par le groupe européen de certification de cybersécurité et des exigences énoncées dans le système***

européen de certification de cybersécurité correspondant. Une coopération efficace entre les autorités nationales de contrôle de la certification est indispensable à la mise en œuvre correcte des systèmes européens de certification de cybersécurité et des aspects techniques concernant la cybersécurité des produits et services TIC. La Commission devrait faciliter cet échange d'informations grâce à la mise à disposition d'un système général de soutien à l'information électronique, par exemple, le système d'information et de communication pour la surveillance des marchés (ICSMS) et le système européen d'alerte rapide pour les produits dangereux (RAPEX) déjà utilisés par les autorités de surveillance du marché conformément au règlement (CE) nº 765/2008.

Amendement 64

Proposition de règlement
Considérant 60

Texte proposé par la Commission	*Amendement*
(60) Afin d'assurer l'application cohérente du cadre européen de certification de cybersécurité, un Groupe européen de certification ***de cybersécurité (ci-après le «groupe»),*** constitué des autorités nationales de contrôle de la certification, 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 la	(60) Afin d'assurer l'application cohérente du cadre européen de certification de cybersécurité, un Groupe européen de certification ***des États membres*** constitué des autorités nationales de contrôle de la certification, devrait être mis en place. Les tâches principales du groupe ***de certification des États membres*** 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 la

Commission concernant l'actualisation et le réexamen de systèmes européens de certification de cybersécurité existants.	Commission concernant l'actualisation et le réexamen de systèmes européens de certification de cybersécurité existants.

Amendement 65

Proposition de règlement
Considérant 60 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(60 bis) Pour garantir l'équivalence des niveaux de compétence des organismes d'évaluation de la conformité, faciliter la reconnaissance mutuelle et promouvoir l'acceptation généralisée des certificats et des résultats d'évaluation de la conformité délivrés par les organismes d'évaluation de la conformité, il faut que les autorités nationales de contrôle de la certification mettent en œuvre un système d'évaluation par les pairs rigoureux et transparent et se soumettent régulièrement à une telle évaluation.

Amendement 66

Proposition de règlement
Considérant 60 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	(60 ter) Une coopération efficace entre les autorités nationales de contrôle de la certification revêt une importance cruciale pour la bonne mise en œuvre de l'évaluation par les pairs, de même que pour l'accréditation transfrontalière. Dans l'intérêt de la transparence, il convient dès lors de faire obligation aux autorités nationales de contrôle de la certification de s'échanger les informations et de communiquer les informations pertinentes aux autorités nationales et à la Commission. Il convient également de rendre publiques, et donc de rendre accessibles en particulier aux

organismes d'évaluation de la conformité, des informations actualisées et exactes sur les activités d'accréditation proposées par les organismes nationaux d'accréditation.

Amendement 67

Proposition de règlement
Considérant 61

Texte proposé par la Commission	*Amendement*
(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) 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***, processus*** et services TIC certifiés.

Amendement 68

Proposition de règlement
Considérant 63

Texte proposé par la Commission	*Amendement*
(63) Afin de préciser les critères d'accréditation des organismes d'évaluation de la conformité, le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne devrait être délégué à la Commission. Il convient que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts. Ces consultations devraient être menées conformément aux principes définis dans l'accord interinstitutionnel «Mieux légiférer» du 13 avril 2016. En particulier, pour assurer leur égale participation à la	(63) Afin de préciser les critères d'accréditation des organismes d'évaluation de la conformité, le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne devrait être délégué à la Commission. Il convient que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts ***et des parties prenantes concernées, le cas échéant***. Ces consultations devraient être menées conformément aux principes définis dans l'accord interinstitutionnel «Mieux légiférer» du 13 avril 2016. En

préparation des actes délégués, le Parlement européen et le Conseil devraient recevoir tous les documents au même moment que les experts des États membres, et leurs experts avoir systématiquement accès aux réunions des groupes d'experts de la Commission traitant de la préparation des actes délégués.

particulier, pour assurer leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil devraient recevoir tous les documents au même moment que les experts des États membres, et leurs experts avoir systématiquement accès aux réunions des groupes d'experts de la Commission traitant de la préparation des actes délégués.

Amendement 69

Proposition de règlement
Considérant 65

Texte proposé par la Commission	*Amendement*
(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 contrôle de la certification, des organismes d'évaluation de la conformité accrédités.	(65) ***Des actes délégués pourraient par ailleurs être adoptés*** concernant les systèmes européens de certification de cybersécurité applicables à des produits***, processus*** 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 contrôle de la certification, des organismes d'évaluation de la conformité accrédités.

Amendement 70

Proposition de règlement
Considérant 66

Texte proposé par la Commission	*Amendement*
(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***.	(66) Le fonctionnement de l'Agence devrait faire l'objet d'une évaluation ***continue et*** indépendante. Cette évaluation devrait s'intéresser à la réalisation des objectifs, aux méthodes de travail et à la pertinence des missions de l'Agence***, en particulier quant à son rôle de coordination des États membres et de leurs autorités nationales***. ***Lors d'un***

réexamen, la Commission devrait ***évaluer la possibilité pour l'Agence de faire office de «guichet unique» pour les États membres*** et ***les institutions et organes*** de ***l'Union européenne***.

Amendement 71

Proposition de règlement
Considérant 66 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(66 bis) L'évaluation devrait également porter sur les effets, l'efficacité et l'efficience du cadre européen de certification de cybersécurité. Dans le cadre d'un réexamen, la Commission pourrait évaluer le rôle que l'Agence pourrait jouer dans l'évaluation des produits et des services de pays tiers qui pénètrent sur le marché de l'Union et la possibilité d'établir une liste noire des entreprises qui ne respectent pas les règles de l'Union.

Amendement 72

Proposition de règlement
Considérant 66 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	(66 ter) L'évaluation devrait analyser le niveau de cybersécurité des produits et services vendus dans l'Union. Dans le cas d'un réexamen, la Commission devrait évaluer s'il y a lieu d'inclure les exigences essentielles en matière de cybersécurité comme condition d'accès au marché intérieur.

Amendement 73

Proposition de règlement
Article 1 – alinéa 1 – point a

Texte proposé par la Commission	*Amendement*
(a) fixe les objectifs, les missions et les aspects organisationnels de ***l'ENISA, Agence*** de l'Union européenne ***pour*** la ***cybersécurité,*** ci-après dénommée l'«Agence»; et	a) fixe les objectifs, les missions et les aspects organisationnels de ***l'Agence*** de l'Union européenne ***chargée de*** la ***sécurité des réseaux et de l'information (***ci-après dénommée l'«Agence»***)***; et

Amendement 74

Proposition de règlement
Article 1 – alinéa 1 – point b

Texte proposé par la Commission	*Amendement*
(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 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.	b) instaure un cadre pour la mise en place de systèmes européens de certification de cybersécurité dans le but ***d'éviter une fragmentation des systèmes de certification dans l'Union et*** de garantir un niveau suffisant de cybersécurité des ***processus,*** produits et services TIC dans ***l'Union qui*** s'applique sans préjudice des dispositions spécifiques en matière de certification volontaire ***et, le cas échéant,*** obligatoire***, lorsque cela est prévu par le présent règlement ou d'autres actes de l'Union***.

Amendement 75

Proposition de règlement
Article 1 – alinéa 1 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	L'Agence exécute ses tâches sans préjudice des compétences des États membres en matière de cybersécurité, et notamment des compétences des États membres en ce qui concerne la sécurité publique, la défense, la sûreté de l'État et le droit pénal.

Amendement 76

Proposition de règlement
Article 2 – alinéa 1 – point 1

Texte proposé par la Commission	*Amendement*
(1) «cybersécurité», toutes les activités nécessaires pour protéger les réseaux et les systèmes d'information, leurs utilisateurs et les personnes exposées contre les cybermenaces;	*(Ne concerne pas la version française.)*

Amendement 77

Proposition de règlement
Article 2 – alinéa 1 – point 2

Texte proposé par la Commission	*Amendement*
(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;	*(Ne concerne pas la version française.)*

Amendement 78

Proposition de règlement
Article 2 – alinéa 1 – point 3

Texte proposé par la Commission	*Amendement*
(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;	3) «stratégie nationale en matière de sécurité des réseaux et des systèmes d'information», ***une stratégie nationale en matière*** de ***sécurité des réseaux et des systèmes d'information telle que définie à*** l'article 4, point 3), de la directive (UE) 2016/1148;

Amendement 79

Proposition de règlement
Article 2 – alinéa 1 – point 4

Texte proposé par la Commission	*Amendement*
(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;	4) «opérateur de services essentiels», ***un opérateur de services essentiels tel*** que ***défini*** à l'article 4, point 4), de la directive (UE) 2016/1148;

Amendement 80

Proposition de règlement
Article 2 – alinéa 1 – point 5

Texte proposé par la Commission	*Amendement*
(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;	5) «fournisseur de service numérique», ***un fournisseur de*** service numérique tel que défini à l'article 4, point 6), de la directive (UE) 2016/1148;

Amendement 81

Proposition de règlement
Article 2 – alinéa 1 – point 6

Texte proposé par la Commission	*Amendement*
(6) «incident», ***tout événement*** tel que défini à l'article 4, point 7), de la directive (UE) 2016/1148;	6) «incident», ***un incident*** tel que défini à l'article 4, point 7), de la directive (UE) 2016/1148;

Amendement 82

Proposition de règlement
Article 2 – alinéa 1 – point 7

Texte proposé par la Commission	*Amendement*
(7) «gestion d'incident», ***toute procédure*** telle que définie à l'article 4, point 8), de la directive (UE) 2016/1148;	7) «gestion d'incident», ***une gestion d'incident*** telle que définie à l'article 4, point 8), de la directive (UE) 2016/1148;

Amendement 83

Proposition de règlement
Article 2 – alinéa 1 – point 8

Texte proposé par la Commission	*Amendement*
(8) ***«cybermenace»***, toute circonstance ***ou*** tout événement potentiels susceptibles de porter atteinte aux réseaux et systèmes ***d'information***, à leurs utilisateurs et aux personnes exposées;	8) ***"cybermenace"***, toute circonstance***,*** tout événement potentiels ***ou toute action intentionnelle, y compris une commande automatisée,*** susceptibles de porter atteinte aux réseaux et systèmes ***d'information***, à leurs utilisateurs et aux personnes exposées***, d'endommager lesdits réseaux et systèmes ou de provoquer des interruptions***;

Amendement 84

Proposition de règlement
Article 2 – alinéa 1 – point 8 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	8 bis) «hygiène informatique», les mesures simples de routine qui, lorsqu'elles sont mises en œuvre et effectuées régulièrement par les utilisateurs et les entreprises en ligne, réduisent au minimum leur exposition aux risques liés aux menaces informatiques.

Amendement 85

Proposition de règlement
Article 2 – alinéa 1 – point 9

Texte proposé par la Commission	*Amendement*
(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 des produits et services des technologies de l'information et des communications (TIC) relevant de ce système spécifique;	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, ***conformément aux normes internationales et européennes approuvées et aux spécifications TIC répertoriées par l'Agence,*** qui s'appliquent à la certification des produits***, processus*** et services des technologies de l'information

et des communications (TIC) relevant de ce système spécifique;

Amendement 86

Proposition de règlement
Article 2 – alinéa 1 – point 10

Texte proposé par la Commission	*Amendement*
*(*10) «certificat européen de cybersécurité», un document délivré par un organisme d'évaluation de la conformité attestant qu'un produit ou service TIC donné satisfait aux exigences spécifiques énoncées dans un système européen de certification de cybersécurité;	10) «certificat européen de cybersécurité», un document délivré par un organisme d'évaluation de la conformité attestant qu'un produit***,*** ou service ***ou processus*** TIC donné satisfait aux exigences spécifiques énoncées dans un système européen de certification de cybersécurité;

Amendement 87

Proposition de règlement
Article 2 – alinéa 1 – point 11 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	11 bis) «processus TIC», un ensemble d'activités exécutées pour concevoir, développer, maintenir et fournir un produit ou un service TIC;

Amendement 88

Proposition de règlement
Article 2 – alinéa 1 – point 11 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	11 ter) «appareil électronique grand public», un appareil composé de matériel et d'un logiciel permettant de traiter des données à caractère personnel ou de se connecter à l'internet pour utiliser des appareils de domotique, de contrôle à usage domestique et de bureautique, des équipements de routage ainsi que des

	appareils connectés en réseau, tels que les télévisions intelligentes, les jouets et les consoles de jeux, les assistants virtuels ou numériques personnels, les appareils de lecture continue connectés, les appareils portables, les systèmes de commande vocale ou de réalité virtuelle;

Amendement 89

Proposition de règlement
Article 2 – alinéa 1 – point 16

Texte proposé par la Commission	*Amendement*
(16) ***«norme»***, ***une*** norme ***telle*** que ***définie*** à l'article 2, ***point*** 1), du règlement (UE) nº 1025/2012***.***	16) ***«norme, spécification technique et spécification technique des TIC »***, norme***, spécification technique ou spécification technique des TIC, telles*** que ***définies*** à l'article 2, ***points*** 1), ***4) et 5)*** du règlement (UE) nº 1025/2012***;***

Amendement 90

Proposition de règlement
Article 2 – alinéa 1 – point 16 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	16 bis) «autorité nationale de contrôle de la certification», un organe désigné par chaque État membre conformément à l'article 50 du présent règlement;

Amendement 91

Proposition de règlement
Article 2 – alinéa 1 – point 16 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	16 ter) «auto-évaluation», la déclaration de conformité par laquelle le fabricant déclare que les exigences spécifiques relatives aux produits, processus et services établies dans un

	système de certification, ont été respectées;

Amendement 92

Proposition de règlement
Article 2 – alinéa 1 – point 16 quater (nouveau)

Texte proposé par la Commission	*Amendement*
	16 quater) «sécurité par défaut», une situation dans laquelle si un produit, un logiciel ou un processus peut être mis en place de manière à assurer un degré de sécurité plus élevé, le premier utilisateur devrait recevoir la configuration par défaut avec les réglages les plus sûrs possibles. Si, au cas par cas, une analyse des risques et de la facilité d'utilisation aboutit à la conclusion qu'un tel dispositif n'est pas réalisable, les utilisateurs devraient être incités à choisir le réglage le plus sûr.

Amendement 93

Proposition de règlement
Article 2 – alinéa 1 – point 16 quinquies (nouveau)

Texte proposé par la Commission	*Amendement*
	16 quinquies) «opérateurs de services essentiels», les opérateurs de services essentiels tels que définis à l'article 4, point 4), de la directive (UE) 2016/1148.

Amendement 94

Proposition de règlement
Article 3 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. L'Agence exécute les missions qui lui sont assignées par le présent règlement ***dans le but de contribuer à assurer*** un	1. L'Agence exécute les missions qui lui sont assignées par le présent règlement ***et est renforcée dans le but d'atteindre*** un

niveau élevé de cybersécurité dans l'Union.	niveau élevé de cybersécurité***, afin d'éviter les cyberattaques*** dans l'Union***; de réduire la fragmentation du marché intérieur et d'améliorer son fonctionnement; et d'assurer la cohérence en tenant compte des résultats obtenus par les États membres en matière de coopération dans le cadre de la directive relative à la cybersécurité («directive SRI»)***.

Amendement 95

Proposition de règlement
Article 4 – paragraphe 1

Texte proposé par la Commission	*Amendement*
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.	1. L'Agence est un centre d'expertise ***théorique et pratique*** 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.

Amendement 96

Proposition de règlement
Article 4 – paragraphe 2

Texte proposé par la Commission	*Amendement*
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 de politiques liées à la cybersécurité.	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 de politiques liées à la cybersécurité ***ainsi que dans la sensibilisation des citoyens et des entreprises***.

Amendement 97

Proposition de règlement
Article 4 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. L'Agence soutient le renforcement des capacités et contribue à l'état de préparation ***au sein*** de l'Union en aidant ***l'Union,*** 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 des aptitudes et des compétences dans le domaine de ***la cybersécurité*** et à parvenir à la cyberrésilience.	3. L'Agence soutient le renforcement des capacités et contribue à l'état de préparation ***dans les institutions, agences et organes*** de l'Union***,*** en aidant 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 aux incidents informatiques, à accroître la sensibilisation et à développer*** des aptitudes et des compétences dans le domaine de ***la cybersécurité*** et à parvenir à la cyberrésilience.

Amendement 98

Proposition de règlement
Article 4 – paragraphe 4

Texte proposé par la Commission	*Amendement*
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 concernées***, y compris le secteur privé***, sur les questions liées à la cybersécurité.	4. L'Agence promeut la coopération***, la coordination*** et ***le partage d'informations*** au niveau de l'Union entre les États membres, les institutions, organes et organismes de l'Union et les parties prenantes concernées, sur les questions liées à la cybersécurité.

Amendement 99

Proposition de règlement
Article 4 – paragraphe 5

Texte proposé par la Commission	*Amendement*
5. L'Agence ***accroît*** les capacités dans le domaine de la cybersécurité au niveau de l'Union afin de compléter l'action des États membres en matière de prévention des cybermenaces et de réaction à celles-ci, notamment en cas d'incidents transfrontières.	5. L'Agence ***contribue à accroître*** les capacités dans le domaine de la cybersécurité au niveau de l'Union afin de compléter l'action des États membres en matière de prévention des cybermenaces et de réaction à celles-ci, notamment en cas d'incidents transfrontières***, ainsi qu'afin de***

	remplir l'aspect de son mandat consistant à assister les institutions de l'Union dans l'élaboration de politiques relatives à la cybersécurité.

Amendement 100

Proposition de règlement
Article 4 – paragraphe 6

Texte proposé par la Commission	*Amendement*
6. L'Agence promeut le recours à la certification, notamment en contribuant 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.	6. L'Agence promeut le recours à la certification ***en vue d'éviter la fragmentation du marché intérieur et d'améliorer son fonctionnement***, notamment en contribuant 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***, processus*** et services TIC et, partant, de rehausser la confiance dans le marché intérieur numérique***, ainsi que d'accroître la compatibilité entre les systèmes de certification nationaux et internationaux existants***.

Amendement 101

Proposition de règlement
Article 4 – paragraphe 7

Texte proposé par la Commission	*Amendement*
7. L'Agence promeut un niveau élevé de sensibilisation des particuliers et des entreprises aux questions liées à la cybersécurité.	7. L'Agence promeut ***et soutient des projets contribuant à*** un niveau élevé de sensibilisation***, d'hygiène informatique et d'habileté numérique*** des particuliers et des entreprises aux questions liées à la cybersécurité.

Amendement 102

Proposition de règlement
Article 5 – alinéa 1 – point 1

Texte proposé par la Commission	*Amendement*
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;	1) en apportant son concours et ses conseils, en particulier sous la forme d'avis indépendants***, d'analyses d'activités pertinentes dans le cyberespace*** 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;

Amendement 103

Proposition de règlement
Article 5 – alinéa 2 – point 2

Texte proposé par la Commission	*Amendement*
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;	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, ***la directive ... établissant le code des communications électroniques européen, le règlement (UE) 2016/679 et la directive 2002/58/CE,*** y compris au moyen d'avis, de lignes directrices, de conseils et de bonnes pratiques sur des thèmes tels que ***le développement de logiciels et de systèmes fiables,*** la gestion des risques, le signalement des incidents***,*** le partage d'informations ***et les mesures techniques et organisationnelles, notamment la mise en place de programmes de divulgation coordonnée des vulnérabilités***, ainsi qu'en facilitant l'échange de bonnes pratiques entre les autorités compétentes à cet égard;

Amendement 104

Proposition de règlement
Article 5 – alinéa 1 – point 2 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	2 bis) l'élaboration et la promotion de politiques visant à maintenir la disponibilité ou l'intégrité générale du noyau public de l'internet ouvert, qui joue un rôle essentiel dans la fonction de l'internet en général et soutient son fonctionnement normal, y compris, sans s'y limiter, la sécurité et la stabilité des protocoles clés (notamment DNS, BGP et IPv6), le fonctionnement du système de noms de domaines (y compris tous les domaines de premier niveau) et le fonctionnement de la zone racine.

Amendement 105

Proposition de règlement
Article 5 – alinéa 1 – point 4 – sous-point 2

Texte proposé par la Commission	*Amendement*
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;	2) l'amélioration du niveau de sécurité des communications électroniques, ***du stockage des données et du traitement des données,*** y compris en fournissant une expertise et des conseils, ainsi qu'en facilitant l'échange de bonnes pratiques entre les autorités compétentes;

Amendement 106

Proposition de règlement
Article 5 – alinéa 1 – point 5 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	5 bis) en aidant les États membres à mettre en œuvre de manière cohérente la politique et la législation de l'Union relatives à la protection des données, notamment en ce qui concerne le règlement (UE) 2016/679, ainsi qu'en

aidant le Comité européen de la protection des données à élaborer des lignes directrices concernant l'application du règlement (UE) 2016/679 à des fins de cybersécurité. Le Comité européen de la protection des données consulte l'Agence chaque fois qu'il émet un avis ou qu'il prend une décision relative à la mise en œuvre du règlement général sur la protection des données et à la cybersécurité, de manière non exhaustive sur des questions liées aux analyses d'impact sur la vie privée, aux notifications de violation des données, au traitement de la sécurité, aux exigences de sécurité et au respect de la vie privée dès la conception;

Amendement 107

Proposition de règlement
Article 6 – paragraphe 1 – point a bis (nouveau)

Texte proposé par la Commission	*Amendement*
	a bis) les États membres et les institutions de l'Union dans la mise en place et mise en œuvre de politiques de divulgation coordonnée des vulnérabilités et de procédures d'examen des divulgations de vulnérabilités par les acteurs gouvernementaux, dont les pratiques et les conclusions doivent être transparentes et soumises à un contrôle indépendant;

Amendement 108

Proposition de règlement
Article 6 – paragraphe 1 – point a ter (nouveau)

Texte proposé par la Commission	*Amendement*
	a ter) L'Agence facilite la mise en place et le lancement d'un projet européen à long terme sur la sécurité des technologies de l'information afin d'encourager davantage la recherche sur la

	cybersécurité dans l'Union et dans les États membres, en coopération avec le Conseil européen de la recherche (CER) et l'Institut européen d'innovation et de technologie (EIT) et dans le cadre des programmes de recherche de l'Union;

Amendement 109

Proposition de règlement
Article 6 – paragraphe 1 – point g

Texte proposé par la Commission	*Amendement*
(g) les États membres en organisant chaque année les exercices de cybersécurité à grande échelle 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;	g) les États membres en organisant ***régulièrement et au moins*** chaque année les exercices de cybersécurité à grande échelle au niveau de l'Union visés à l'article 7, paragraphe 6, et en formulant des recommandations ***et en échangeant les meilleures pratiques*** en vue d'actions sur la base de l'évaluation de ces exercices et des enseignements qui en ont été tirés;

Amendement 110

Proposition de règlement
Article 6 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. L'Agence facilite la mise en place de centres d'échange et d'analyse d'informations (ISAC) sectoriels et leur apporte un soutien continu, en particulier dans les secteurs énumérés à l'annexe II de la directive (UE) 2016/1148, en proposant de bonnes pratiques et des orientations sur les outils disponibles, les procédures et sur la manière d'aborder les questions réglementaires relatives au partage d'informations.	2. L'Agence facilite la mise en place de centres d'échange et d'analyse d'informations (ISAC) sectoriels et leur apporte un soutien continu, en particulier dans les secteurs énumérés à l'annexe II de la directive (UE) 2016/1148, en proposant de bonnes pratiques et des orientations sur les outils disponibles, les procédures et ***les principes d'hygiène informatique ainsi que*** sur la manière d'aborder les questions réglementaires relatives au partage d'informations.

Amendement 111

Proposition de règlement
Article 7 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. L'Agence apporte son soutien à la coopération opérationnelle entre les ***organismes publics compétents***, et entre les parties prenantes.	1. L'Agence apporte son soutien à la coopération opérationnelle entre les ***États membres, les institutions***, ***les agences et organes de l'Union*** et entre les parties prenantes***, en vue de parvenir à une collaboration, en analysant et en évaluant les systèmes nationaux existants, en élaborant et en mettant en œuvre un plan et en utilisant les instruments appropriés pour atteindre le niveau le plus élevé de certification en matière de cybersécurité dans l'Union et dans les États membres***.

Amendement 112

Proposition de règlement
Article 7 – paragraphe 4 – alinéa 1 – point b

Texte proposé par la Commission	*Amendement*
(b) en fournissant, à leur demande, une assistance technique en cas d'incidents ayant un impact important ou significatif;	b) en fournissant, à leur demande, une assistance technique ***sous la forme d'un partage d'informations ou d'expertise*** en cas d'incidents ayant un impact important ou significatif;

Amendement 113

Proposition de règlement
Article 7 – paragraphe 4 – alinéa 1 – point b bis (nouveau)

Texte proposé par la Commission	*Amendement*
	b bis) lorsqu'une situation exige une action urgente en présence d'un incident qui a un effet perturbateur non négligeable, un État membre peut demander l'assistance d'experts de l'Agence pour évaluer la situation. La demande comprend une description de la situation, des éventuels objectifs et des besoins envisagés;

Amendement 114

Proposition de règlement
Article 7 – paragraphe 5 – alinéa 1

Texte proposé par la Commission	*Amendement*
À la demande d'au moins ***deux États membres concernés*** et dans le seul but de fournir ***des*** conseils sur la prévention des incidents, l'Agence apporte son concours ou procède elle-même à une enquête technique ex post à la suite de la notification, par les entreprises exposées, d'incidents ayant un impact important ou significatif conformément à la directive (UE) 2016/1148. L'Agence procède également à une enquête de ce type à la demande dûment justifiée de la Commission, en accord avec les États membres concernés, lorsque les incidents atteignent plus ***de deux*** États membres.	À la demande d'au moins ***un État membre concerné*** et dans le seul but de fournir ***une assistance, soit sous la forme de*** conseils sur la prévention des incidents, ***soit sous la forme d'une aide pour faire face à des incidents majeurs en cours,*** l'Agence apporte son concours ou procède elle-même à une enquête technique ex post à la suite de la notification, par les entreprises exposées, d'incidents ayant un impact important ou significatif conformément à la directive (UE) 2016/1148. L'Agence ***accomplit ces tâches en recueillant des informations pertinentes fournies par les États membres concernés et en utilisant ses propres ressources d'analyse des menaces et de réaction aux incidents. L'Agence*** procède également à une enquête de ce type à la demande dûment justifiée de la Commission, en accord avec les États membres concernés, lorsque les incidents atteignent plus ***d'un État membre. Ce faisant, l'Agence veille à ne pas divulguer les mesures prises par les*** États membres ***pour sauvegarder leurs fonctions étatiques essentielles, notamment celles qui concernent la sécurité nationale***.

Amendement 115

Proposition de règlement
Article 7 – paragraphe 6

Texte proposé par la Commission	*Amendement*
6. L'Agence organise des exercices de cybersécurité ***annuels*** à l'échelle de l'Union, et aide, à leur demande, les États membres et les institutions, organes et	6. L'Agence organise ***régulièrement, et en tout état de cause au moins une fois par an,*** des exercices de cybersécurité à l'échelle de l'Union, et aide, à leur

organismes de l'UE à organiser de tels exercices. Les exercices annuels à l'échelle de l'Union comportent des aspects techniques, opérationnels et stratégiques, et contribuent à la préparation de la réaction concertée à l'échelle de l'Union en cas d'incidents transfrontières de cybersécurité majeurs. En outre, l'Agence contribue à des exercices de cybersécurité sectoriels, qu'elle aide à organiser le cas échéant, en collaboration avec les ISAC compétents, et permet à des ISAC de participer également à des exercices de cybersécurité au niveau de l'Union.	demande, les États membres et les institutions, organes et organismes de l'UE à organiser de tels exercices. Les exercices annuels à l'échelle de l'Union comportent des aspects techniques, opérationnels et stratégiques, et contribuent à la préparation de la réaction concertée à l'échelle de l'Union en cas d'incidents transfrontières de cybersécurité majeurs. En outre, l'Agence contribue à des exercices de cybersécurité sectoriels, qu'elle aide à organiser le cas échéant, en collaboration avec les ISAC compétents, et permet à des ISAC de participer également à des exercices de cybersécurité au niveau de l'Union.

Amendement 116

Proposition de règlement
Article 7 – paragraphe 7

Texte proposé par la Commission	*Amendement*
7. L'Agence prépare, à intervalle régulier, 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 (sur une base volontaire) ou les points de contact uniques au titre de la directive SRI (conformément à l'article 14, paragraphe 5, de la directive SRI), le Centre européen de lutte contre la cybercriminalité (EC3) au sein d'Europol, la CERT-UE.	7. L'Agence prépare, à intervalle régulier, un rapport ***approfondi*** 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 (sur une base volontaire) ou les points de contact uniques au titre de la directive SRI (conformément à l'article 14, paragraphe 5, de la directive SRI), le Centre européen de lutte contre la cybercriminalité (EC3) au sein d'Europol, la CERT-UE. ***Le directeur exécutif présente, s'il y a lieu, les conclusions publiques au Parlement européen.***

Amendement 117

Proposition de règlement
Article 7 – paragraphe 7 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	7 bis. L'Agence contribue, le cas échéant et sous réserve de l'approbation préalable de la Commission, à la coopération informatique avec le Centre d'excellence pour la cyberdéfense en coopération et l'école des systèmes d'information et de communication de l'OTAN.

Amendement 118

Proposition de règlement
Article 7 – paragraphe 8 – point a

Texte proposé par la Commission	*Amendement*
(a) ***agrégeant*** des rapports provenant de sources nationales en vue de contribuer à former une appréciation commune de la situation;	a) ***analysant et agrégeant*** des rapports provenant de sources nationales en vue de contribuer à former une appréciation commune de la situation;

Amendement 119

Proposition de règlement
Article 7 – paragraphe 8 – point c

Texte proposé par la Commission	*Amendement*
(c) soutenant la gestion technique des incidents ou des crises, y compris en facilitant le partage de solutions techniques entre les États membres;	c) soutenant la gestion technique des incidents ou des crises, ***à l'aide de son expertise indépendante et de ses propres ressources,*** y compris en facilitant le partage ***volontaire*** de solutions techniques entre les États membres;

Amendement 120

Proposition de règlement
Article 7 – paragraphe 8 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	8 bis. L'Agence organise, s'il y a lieu, un échange de vues et soutient les autorités

des États membres dans la coordination de leur réaction, conformément aux principes de subsidiarité et de proportionnalité.

Amendement 121

Proposition de règlement
Article 7 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	Article 7 bis
	Capacités techniques de l'Agence
	1. En vue d'atteindre les objectifs fixés à l'article 7, et conformément au programme de travail de l'Agence, celle-ci développe, entre autres, les capacités et les compétences techniques suivantes:
	a) la capacité de collecter des informations sur les menaces de cybersécurité auprès de sources ouvertes; et
	b) la capacité de déployer à distance un équipement technique, des outils et une expertise.
	2. Afin d'acquérir les capacités techniques visées au paragraphe 1 du présent article et de développer les compétences appropriées, l'Agence:
	a) veille à ce que ses procédures de recrutement tiennent compte des différentes compétences techniques nécessaires; et
	b) coopère avec la CERT-UE et Europol conformément aux dispositions de l'article 7, paragraphe 2, du présent règlement.

Amendement 122

Proposition de règlement
Article 8 – alinéa 1 – point a – partie introductive

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

Amendement 123

Proposition de règlement
Article 8 – alinéa 1 – point a – sous-point -1 (nouveau)

Texte proposé par la Commission	*Amendement*
	-1) identifiant en permanence les normes, les spécifications techniques et les spécifications techniques en matière de TIC;

Amendement 124

Proposition de règlement
Article 8 – alinéa 1 – point a – sous-point 1

Texte proposé par la Commission	*Amendement*
(1) préparant des systèmes européens de certification de cybersécurité candidats pour des produits et ***services*** TIC, conformément à l'article 44 du présent règlement;	1) préparant***, en coopération avec les parties prenantes du secteur et les organisations de normalisation dans le cadre d'un processus formel, normalisé et transparent,*** des systèmes européens de certification de cybersécurité candidats pour des produits***, services*** et ***processus*** TIC, conformément à l'article 44 du présent règlement;

Amendement 125

Proposition de règlement
Article 8 – alinéa 1 – point a – sous-point 1 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	1 bis) procédant, en coopération avec le groupe des États membres pour la certification visé à l'article 53 du présent règlement, aux évaluations des procédures pour la délivrance des certificats européens de cybersécurité mises en place par les organismes d'évaluation de la conformité visés à l'article 51 du présent règlement, en vue d'assurer une application uniforme du présent règlement par les organismes d'évaluation de la conformité lorsqu'ils délivrent des certificats;

Amendement 126

Proposition de règlement
Article 8 – alinéa 1 – point a – sous-point 1 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	1 ter) réalisant des contrôles réguliers indépendants ex post de la conformité des produits, processus et services TIC certifiés par les systèmes européens de certification de cybersécurité;

Amendement 127

Proposition de règlement
Article 8 – alinéa 1 – point a – sous-point 2

Texte proposé par la Commission	*Amendement*
(2) aidant la Commission à assurer le secrétariat du Groupe ***européen de certification de cybersécurité***, conformément à l'article 53 du présent règlement;	2) aidant la Commission à assurer le secrétariat du groupe ***des États membres pour la certification***, conformément à l'article 53 du présent règlement;

Amendement 128

Proposition de règlement
Article 8 – alinéa 1 – point a – sous-point 3

Texte proposé par la Commission	*Amendement*
(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 contrôle de la certification et l'industrie;	3) établissant et publiant des lignes directrices, ainsi qu'en mettant au point des bonnes pratiques***, y compris sur les principes d'hygiène informatique,*** en ce qui concerne les exigences de cybersécurité de produits***, processus*** et services TIC, en coopération avec les autorités nationales de contrôle de la certification et l'industrie ***dans le cadre d'un processus formel, normalisé et transparent***;

Amendement 129

Proposition de règlement
Article 8 – alinéa 1 – point b

Texte proposé par la Commission	*Amendement*
(b) facilite l'établissement et l'adoption de normes européennes et internationales en matière de gestion des risques et de sécurité des produits et services TIC; 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;	b) facilite l'établissement et l'adoption de normes européennes et internationales en matière de gestion des risques et de sécurité des produits***, processus*** et services TIC; formule, en collaboration avec les États membres ***et le secteur***, 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 ***et partage ces informations avec les États membres***;

Amendement 130

Proposition de règlement
Article 9 – alinéa 1 – point c

Texte proposé par la Commission	*Amendement*
(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 de l'infrastructure internet et des infrastructures sur lesquelles s'appuient les secteurs énumérés à l'annexe II de la directive (UE) 2016/1148;	c) fournit, en coopération avec des experts des États membres ***et les parties prenantes concernées***, des avis, des orientations et des bonnes pratiques en matière de sécurité des réseaux et des systèmes d'information, en particulier pour la sécurité de l'infrastructure internet et des infrastructures sur lesquelles s'appuient les secteurs énumérés à l'annexe II de la directive (UE) 2016/1148;

Amendement 131

Proposition de règlement
Article 9 – alinéa 1 – point e

Texte proposé par la Commission	*Amendement*
(e) sensibilise le public ***sur les*** 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;	e) sensibilise ***en permanence*** le public ***aux*** risques liés à la cybersécurité***,*** fournit, à l'intention des particuliers et des organisations, des ***formations et des*** orientations sur les bonnes pratiques à adopter par les utilisateurs***, et encourage l'adoption de mesures renforcées de prévention en matière de sécurité informatique et de protection fiable des données et de la vie privée***;

Amendement 132

Proposition de règlement
Article 9 – alinéa 1 – point g

Texte proposé par la Commission	*Amendement*
(g) organise à intervalle régulier, en coopération avec les États membres et les institutions, organes et organismes de l'Union, des campagnes ***d'information afin*** de ***relever le niveau*** de ***la cybersécurité et d'accroître sa visibilité dans l'Union***.	g) organise à intervalle régulier, en coopération avec les États membres et les institutions, organes et organismes de l'Union, des campagnes de ***communication afin*** de ***susciter un large débat public***.

Amendement 133

Proposition de règlement
Article 9 – alinéa 1 – point g bis (nouveau)

Texte proposé par la Commission	*Amendement*
	g bis) soutient l'étroite coordination et l'échange de bonnes pratiques entre les États membres en matière de culture de la cybersécurité et d'éducation à celle-ci, d'hygiène informatique et de sensibilisation.

Amendement 134

Proposition de règlement
Article 10 – alinéa 1 – point a

Texte proposé par la Commission	*Amendement*
(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;	a) ***assure la consultation préalable des groupes d'utilisateurs concernés et conseille*** l'Union et les États membres sur les besoins et les priorités en matière de recherche dans ***les domaines*** de la cybersécurité***, de la protection des données et du respect de la vie privée***, 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;

Amendement 135

Proposition de règlement
Article 10 – alinéa 1 – point b bis (nouveau)

Texte proposé par la Commission	*Amendement*
	b bis) commande ses propres activités de recherche dans des domaines d'intérêt qui ne sont pas encore couverts par d'autres

	programmes de recherche existants de l'Union, lorsqu'il existe une valeur ajoutée européenne clairement définie.

Amendement 136

Proposition de règlement
Article 11 – alinéa 1 – point c bis (nouveau)

Texte proposé par la Commission	*Amendement*
	c bis) fournissant des conseils et un soutien à la Commission, en collaboration avec le groupe des États membres pour la certification constitué en vertu de l'article 53, sur les questions relatives aux accords de reconnaissance mutuelle des certificats de cybersécurité avec des pays tiers.

Amendement 137

Proposition de règlement
Article 12 – alinéa 1 – point d

Texte proposé par la Commission	*Amendement*
(d) un groupe ***permanent des parties prenantes***, qui exerce les fonctions définies à l'article 20.	d) un groupe ***consultatif de l'ENISA***, qui exerce les fonctions définies à l'article 20.

Amendement 138

Proposition de règlement
Article 14 – paragraphe 1 – point e

Texte proposé par la Commission	*Amendement*
(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	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***, décrit l'adéquation des crédits***

atteint ses indicateurs de performance. Le rapport annuel est rendu public;	***engagés*** et ***évalue*** la manière dont l'Agence ***a été efficace et a*** atteint ses indicateurs de performance. Le rapport annuel est rendu public;

Amendement 139

Proposition de règlement
Article 14 – paragraphe 1 – point m

Texte proposé par la Commission	*Amendement*
(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;	m) nomme le directeur exécutif ***sur la base d'une sélection fondée sur des critères professionnels*** et, le cas échéant, prolonge son mandat ou le démet de ses fonctions conformément à l'article 33 du présent règlement;

Amendement 140

Proposition de règlement
Article 14 – paragraphe 1 – point o

Texte proposé par la Commission	*Amendement*
(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;	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 ***telle que décrite dans le présent règlement*** et en respectant le principe d'une gestion budgétaire saine;

Amendement 141

Proposition de règlement
Article 16 – paragraphe 4

Texte proposé par la Commission	*Amendement*
4. Sur invitation du président, des membres du groupe ***permanent des parties prenantes*** peuvent participer sans droit de vote aux réunions du conseil	4. Sur invitation du président, des membres du groupe ***consultatif de l'ENISA*** peuvent participer sans droit de vote aux réunions du conseil

d'administration.	d'administration.

Amendement 142

Proposition de règlement
Article 18 – paragraphe 3

Texte proposé par la Commission	*Amendement*
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.	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. ***Les nominations visent à parvenir à une représentation équilibrée des sexes au sein du conseil exécutif.***

Justification

Cet ajout est cohérent avec les dispositions de l'article 13, paragraphe 3, relatives au conseil d'administration. Les nominations au conseil exécutif doivent elles aussi viser la parité des sexes.

Amendement 143

Proposition de règlement
Article 19 – paragraphe 2

Texte proposé par la Commission	*Amendement*
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.	2. Le directeur exécutif fait rapport au Parlement européen sur l'exécution de ses tâches, ***chaque année ou*** lorsqu'il y est invité. Le Conseil peut inviter le directeur exécutif à lui faire rapport sur l'exécution de ses tâches.

Amendement 144

Proposition de règlement
Article 19 – paragraphe 5 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	5 bis. Le directeur exécutif est également habilité à agir en tant que conseiller institutionnel spécial en matière de politique de cybersécurité auprès du président de la Commission européenne, dans l'exercice du mandat défini dans la décision de la Commission C(2014) 541 du 6 février 2014.

Amendement 145

Proposition de règlement
Article 20 – titre

Texte proposé par la Commission	*Amendement*
Groupe ***permanent des parties prenantes***	Groupe ***consultatif de l'ENISA***
	(Cette modification s'applique à l'ensemble du texte législatif à l'examen; son adoption impose des adaptations techniques dans tout le texte.)

Amendement 146

Proposition de règlement
Article 20 – paragraphe 1

Texte proposé par la Commission	*Amendement*
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 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	1. Le conseil d'administration crée, sur proposition du directeur exécutif, ***de manière transparente,*** un groupe ***consultatif de l'ENISA*** composé d'experts ***en sécurité*** reconnus représentant les parties prenantes concernées, comme les entreprises du secteur des TIC, ***y compris les PME, les opérateurs de services essentiels au sens de la directive SRI,*** les fournisseurs de réseaux de communications électroniques ou de services accessibles au public, les organisations de consommateurs, les experts universitaires en matière de cybersécurité***, les organisations européennes de normalisation (OEN), les organes de***

données.	***l'Union*** 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. ***Le conseil d'administration garantit un équilibre approprié entre les différents groupes de parties prenantes.***

Amendement 147

Proposition de règlement
Article 20 – paragraphe 2

Texte proposé par la Commission	*Amendement*
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.	2. Les procédures applicables au groupe ***consultatif de l'ENISA***, 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.

Amendement 148

Proposition de règlement
Article 20 – paragraphe 3

Texte proposé par la Commission	*Amendement*
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.	3. Le groupe ***consultatif de l'ENISA*** est présidé par le directeur exécutif ou par toute personne qu'il désigne à cet effet au cas par cas.

Amendement 149

Proposition de règlement
Article 20 – paragraphe 4

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

Amendement 150

Proposition de règlement
Article 20 – paragraphe 4 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	4 bis. Le groupe consultatif de l'ENISA fournit régulièrement, au long de l'année, des mises à jour sur son programme de travail, et fixe les objectifs de son programme de travail, qui est rendu public tous les six mois pour en garantir la transparence.

Amendement 151

Proposition de règlement
Article 20 – paragraphe 5

Texte proposé par la Commission	*Amendement*
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	5. Le groupe ***consultatif de l'ENISA*** conseille l'Agence dans l'exercice de ses activités***, excepté celles visées au titre III du présent règlement***. Il conseille en

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.	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 les questions liées au programme de travail.

Amendement 152

Proposition de règlement
Article 20 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	Article 20 bis
	Groupe des parties prenantes pour la certification
	1. Le directeur exécutif crée un groupe des parties prenantes pour la certification, composé d'un comité consultatif général qui fournit des conseils d'ordre général sur l'application du titre III du présent règlement. Il crée également des comités ad hoc chargés de proposer, de mettre au point et d'adopter chaque système candidat. Les membres de ce groupe sont choisis parmi des experts en sécurité reconnus représentant les parties prenantes concernées, comme les entreprises du secteur des TIC, y compris les PME, les opérateurs de services essentiels au sens de la directive SRI, les fournisseurs de réseaux de communications électroniques ou de services accessibles au public, les organisations de consommateurs, les experts universitaires en matière de cybersécurité, les organisations européennes de normalisation (OEN) 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 des parties prenantes pour la

certification, notamment en ce qui concerne le nombre de membres, la composition du groupe et la nomination des membres par le directeur exécutif, sont précisées dans les règles internes de fonctionnement de l'Agence, suivent les meilleures pratiques en matière de représentation équitable et d'égalité des droits pour toutes les parties prenantes et sont rendues publiques.

3. Les membres du conseil d'administration ne peuvent pas être membres du groupe des parties prenantes pour la certification. Les membres du groupe consultatif de l'ENISA peuvent être membres également du groupe des parties prenantes pour la certification. Des experts de la Commission et des États membres sont autorisés, lorsqu'ils y sont invités, à assister aux réunions du groupe des parties prenantes pour la certification. Des représentants d'autres organismes jugés pertinents par le directeur exécutif peuvent être invités à assister aux réunions dudit groupe et à prendre part à ses travaux.

4. Le groupe des parties prenantes pour la certification conseille l'Agence dans l'exercice de ses activités visées au titre III du présent règlement. Il est en particulier habilité à proposer à la Commission la préparation d'un système européen de certification de cybersécurité candidat, conformément à l'article 44 du présent règlement, ainsi qu'à participer aux procédures visées aux articles 43 à 48 et à l'article 53 du présent règlement en vue de l'approbation desdits systèmes.

Amendement 153

Proposition de règlement
Article 21 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	Article 21 bis

	Demandes adressées à l'Agence
	1. L'Agence établit et gère un guichet unique pour répondre aux demandes de conseil et d'assistance entrant dans le cadre des objectifs et des tâches de l'Agence. Ces demandes sont accompagnées d'informations expliquant la question à traiter. L'Agence prévoit les ressources potentielles que cela implique et, en temps utile, donne suite aux demandes. Si l'Agence rejette une demande, elle doit motiver son refus.
	2. Les demandes visées au paragraphe 1 peuvent être introduites par:
	a) le Parlement européen;
	b) le Conseil;
	c) la Commission; et
	d) tout organisme compétent désigné par un État membre, telle une autorité réglementaire nationale au sens de l'article 2 de la directive 2002/21/CE.
	3. Les modalités pratiques d'application des paragraphes 1 et 2 en ce qui concerne notamment la présentation, la hiérarchisation et le suivi de ces demandes sont prévues par le conseil d'administration dans les règles internes de fonctionnement de l'Agence.

Amendement 154

Proposition de règlement
Article 24 – paragraphe 2

Texte proposé par la Commission	*Amendement*
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	2. Les membres du conseil d'administration, le directeur exécutif, les membres du groupe ***consultatif de l'ENISA***, 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.	visée à l'article 339 du traité sur le fonctionnement de l'Union européenne, même après la cessation de leurs fonctions.

Amendement 155

Proposition de règlement
Article 26 – paragraphe 1– alinéa 1 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	Le projet d'état prévisionnel se fonde sur les objectifs et les résultats escomptés du document unique de programmation visé à l'article 21, paragraphe 1, du présent règlement et tient compte des ressources financières nécessaires pour les atteindre, conformément au principe de budgétisation axée sur les performances.

Amendement 156

Proposition de règlement
Article 30 – paragraphe 2

Texte proposé par la Commission	*Amendement*
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.	2. La Cour des comptes dispose d'un pouvoir d'audit, sur pièces et ***à partir de vérifications*** 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.

Amendement 157

Proposition de règlement
Article 36 – paragraphe 5

Texte proposé par la Commission	*Amendement*
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.	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. ***L'Agence assure un***

recrutement efficace de personnel.

Amendement 158

Proposition de règlement
Article 37 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Les services de traduction nécessaires au fonctionnement de l'Agence sont assurés par le Centre de traduction des organes de l'Union européenne.	2. Les services de traduction nécessaires au fonctionnement de l'Agence sont assurés par le Centre de traduction des organes de l'Union européenne ***ou par d'autres prestataires de services de traduction, conformément aux règles de passation des marchés publics et dans les limites établies par les dispositions financières applicables***.

Amendement 159

Proposition de règlement
Article 39 – paragraphe 1

Texte proposé par la Commission	*Amendement*
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.	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. ***La coopération avec l'OTAN, le cas échéant, peut comprendre des exercices communs en matière de cybersécurité et la coordination conjointe de la réaction aux incidents.*** Ces arrangements ne créent pas d'obligations juridiques à l'égard de l'Union ou de ses États membres.

Justification

Compte tenu de la nature transfrontalière des incidents informatiques, l'ENISA devrait agir

en collaboration avec les acteurs européens en matière de cybersécurité, tels que l'OTAN, lorsque cela s'avère approprié. Cela est d'autant plus important que l'OTAN peut disposer de capacités informatiques que n'a pas l'ENISA, et vice versa. Étant donné l'augmentation du nombre d'attaques informatiques à l'encontre des États dans leur ensemble, il est impératif pour la sécurité européenne que l'ENISA coopère avec les organisations internationales telles que l'OTAN à l'échelle internationale.

Amendement 160

Proposition de règlement
Article 41 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. L'État membre d'accueil de l'Agence offre les meilleures conditions possibles pour 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.	2. L'État membre d'accueil de l'Agence offre les meilleures conditions possibles pour assurer le bon fonctionnement de l'Agence, notamment ***un emplacement unique pour toute l'Agence,*** 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.

Justification

La structure actuelle de l'Agence, dont le siège administratif se trouve à Héraklion et le centre opérationnel à Athènes, s'avère inefficace et coûteuse. Tous les agents de l'ENISA devraient donc travailler dans la même ville. Vu les critères mentionnés dans ce paragraphe, cette ville devrait être Athènes.

Amendement 161

Proposition de règlement
Article 43 – alinéa 1

Texte proposé par la Commission	*Amendement*
Un système européen de certification de cybersécurité atteste que les produits et services TIC ***qui ont été certifiés conformément à ce système*** satisfont à des exigences spécifiées concernant leur capacité à résister, à un niveau d'assurance donné, à des actions visant à compromettre la disponibilité, l'authenticité, l'intégrité ou	Un système européen de certification de cybersécurité atteste que les produits***,*** ***processus*** et services TIC ***couverts ne présentent aucune vulnérabilité au moment de la certification et*** satisfont à des exigences spécifiées ***qui peuvent faire référence à des normes européennes ou internationales, à des spécifications***

la confidentialité des données stockées, transmises ou traitées ou des fonctions ou services associés qui sont offerts ou accessibles par ces produits, processus**,** services et ***systèmes***.	***techniques et à des spécifications techniques en matière de TIC*** concernant leur capacité à résister***, tout au long de leur cycle de vie***, à un niveau d'assurance donné, à des actions visant à compromettre 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**,** et ***répondent aux objectifs de sécurité spécifiés***.

Amendement 162

Proposition de règlement
Article 44 – paragraphe -1 (nouveau)

Texte proposé par la Commission	*Amendement*
	-1. La Commission adopte des actes délégués, conformément à l'article 55 bis, pour compléter le présent règlement en établissant un programme de travail glissant de l'Union pour les systèmes européens de certification de cybersécurité. Ces actes délégués recensent les actions communes à entreprendre au niveau de l'Union et les priorités stratégiques. Le programme de travail glissant de l'Union comprend notamment une liste prioritaire des produits, processus et services TIC susceptibles d'être soumis à un système européen de certification de cybersécurité, ainsi qu'une analyse visant à déterminer s'il existe un niveau équivalent de qualité, de savoir-faire et d'expertise parmi les organismes d'évaluation de la conformité et les autorités nationales de surveillance de la certification et, le cas échéant, une proposition de mesures permettant de parvenir à un tel niveau.
	Le premier programme de travail glissant de l'Union est établi au plus tard le ... [six mois après l'entrée en vigueur du présent règlement]. Il est mis à jour lorsque cela est nécessaire et, en tout état de cause, au

moins tous les deux ans par la suite. Le programme de travail glissant de l'Union est rendu public.

Avant d'adopter ou de mettre à jour le programme de travail glissant de l'Union, la Commission consulte le groupe des États membres pour la certification, l'Agence et le groupe des parties prenantes pour la certification dans le cadre d'une consultation ouverte, transparente et inclusive.

Amendement 163

Proposition de règlement
Article 44 – paragraphe -1 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	-1 bis. S'il y a lieu, la Commission peut demander à l'Agence d'élaborer un système européen de certification de cybersécurité candidat. Une telle demande s'appuie sur le programme de travail glissant de l'Union.

Amendement 164

Proposition de règlement
Article 44 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. ***À la suite d'une*** demande ***de la Commission, 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.*** Les ***États membres ou le Groupe européen de certification de cybersécurité (le «Groupe») établi*** en ***vertu de l'article 53 peuvent proposer à*** la Commission ***l'élaboration d'un système européen de*** certification ***de cybersécurité candidat***.	1. ***La*** demande ***d'élaboration d'un*** système européen de certification de cybersécurité candidat ***comprend le champ d'application, les objectifs de sécurité applicables visés à l'article 45,*** les ***éléments applicables visés à l'article 47, et une date butoir pour la mise*** en ***œuvre du système candidat concerné. Lorsqu'elle prépare sa demande,*** la Commission ***peut consulter l'Agence, le groupe des États membres pour la*** certification ***et le groupe des parties prenantes pour la certification***.

Amendement 165

Proposition de règlement
Article 44 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Lors de l'élaboration des systèmes candidats visés au paragraphe 1, ***l'ENISA*** consulte toutes les parties prenantes concernées et travaille en étroite collaboration avec le Groupe. ***Celui-ci fournit*** à ***l'ENISA*** l'aide et l'expertise dont elle a besoin dans le cadre de l'élaboration du système candidat, notamment en formulant des avis si nécessaire.	2. Lors de l'élaboration des systèmes candidats visés au paragraphe **-**1, ***l'Agence*** consulte toutes les parties prenantes concernées ***par des processus de consultation officiels, transparents, ouverts et inclusifs*** et travaille en étroite collaboration avec le groupe ***des États membres pour la certification, le groupe des parties prenantes pour la certification, les comités ad hoc visés à l'article 20 bis du présent règlement et les organismes européens de normalisation***. ***Ceux-ci fournissent*** à ***l'Agence*** l'aide et l'expertise dont elle a besoin dans le cadre de l'élaboration du système candidat, notamment en formulant des avis si nécessaire.

Amendement 166

Proposition de règlement
Article 44 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. L'Agence transmet à la Commission le système ***européen de certification de cybersécurité candidat élaboré conformément au paragraphe 2***.	3. L'Agence transmet à la Commission le système ***candidat élaboré conformément aux paragraphes 1 et 2 du présent article***.

Amendement 167

Proposition de règlement
Article 44 – paragraphe 4

Texte proposé par la Commission	*Amendement*
4. La Commission, se fondant sur le système candidat proposé par ***l'ENISA***, peut adopter des actes ***d'exécution***,	4. La Commission, se fondant sur le système candidat proposé par ***l'Agence***, peut adopter des actes ***délégués***,

conformément à l'article 55, ***paragraphe 1,*** prévoyant des systèmes européens de certification de cybersécurité pour les produits et services TIC qui satisfont aux exigences des articles 45, 46 et 47 ***du présent règlement.***	conformément à l'article 55 ***bis***, ***pour compléter le présent règlement en*** prévoyant des systèmes européens de certification de cybersécurité pour les produits***, processus*** et services TIC qui satisfont aux exigences des articles 45, 46 et 47

Amendement 168

Proposition de règlement
Article 44 – paragraphe 5

Texte proposé par la Commission	*Amendement*
5. ***L'ENISA*** tient à jour un site Web spécifique fournissant des informations sur les systèmes européens de certification de cybersécurité et leur assurant une publicité.	5. ***L'Agence*** tient à jour un site Web spécifique fournissant des informations sur les systèmes européens de certification de cybersécurité***, notamment les certificats retirés et expirés et les certifications nationales couvertes,*** et leur assurant une publicité. ***Lorsqu'un système européen de certification de cybersécurité répond aux exigences qu'il vise à satisfaire et qui sont définies dans la législation d'harmonisation de l'Union correspondante, la Commission publie sans tarder une référence à cet égard au Journal officiel de l'Union européenne et par tout autre moyen, dans le respect des conditions fixées dans l'acte correspondant de la législation d'harmonisation de l'Union.***

Amendement 169

Proposition de règlement
Article 44 – paragraphe 5 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	5 bis. L'Agence réexamine les systèmes adoptés, conformément à la structure mise en place au titre du présent règlement, à la fin de leur période de validité conformément à l'article 47,

	paragraphe 1, point a ter), ou sur demande de la Commission, en tenant compte des remarques formulées par les parties prenantes concernées.

Amendement 170

Proposition de règlement
Article 45 – alinéa 1 – partie introductive

Texte proposé par la Commission	*Amendement*
Un système européen de certification de cybersécurité est conçu de façon à prendre en compte, le cas échéant, les objectifs de sécurité ***suivants***:	Un système européen de certification de cybersécurité est conçu de façon à prendre en compte, le cas échéant, les objectifs de sécurité ***qui permettent***:

Amendement 171

Proposition de règlement
Article 45 – alinéa 1 – point a

Texte proposé par la Commission	*Amendement*
(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***;	a) ***d'assurer la confidentialité, l'intégrité***, ***la disponibilité et la confidentialité des services***, ***des fonctions et des données***;

Amendement 172

Proposition de règlement
Article 45 – alinéa 1 – point b

Texte proposé par la Commission	*Amendement*
(b) ***protéger les données stockées, transmises ou traitées d'une autre façon contre la destruction accidentelle ou non autorisée, la perte*** ou ***l'altération accidentelles***;	b) ***de veiller à ce que les services, fonctions et données ne puissent être consultés et utilisés que par des personnes autorisées et/***ou ***des systèmes et programmes autorisés***;

Amendement 173

Proposition de règlement
Article 45 – alinéa 1 – point c

Texte proposé par la Commission	*Amendement*
(c) ***garantir que les personnes autorisées, les programmes ou les machines peuvent exclusivement accéder aux données, services ou fonctions concernés par leurs droits d'accès***;	c) ***de veiller à ce qu'un processus soit en place pour répertorier et documenter toutes les dépendances et les vulnérabilités connues des produits, processus et services TIC***;

Amendement 174

Proposition de règlement
Article 45 – alinéa 1 – point d

Texte proposé par la Commission	*Amendement*
(d) ***garder une trace des données, fonctions ou services qui ont été communiqués***, ***du moment où ils l'ont été et des personnes qui les ont communiqués***;	d) ***de veiller à ce que les produits***, ***processus et services TIC ne contiennent pas de vulnérabilités connues***;

Amendement 175

Proposition de règlement
Article 45 – alinéa 1 – point e

Texte proposé par la Commission	*Amendement*
(e) ***garantir la possibilité de vérifier quels sont les données, services ou fonctions qui ont été consultés ou utilisés***, ***à quel moment et par quelles personnes***;	e) ***de veiller à ce qu'un processus soit en place pour traiter les nouvelles vulnérabilités découvertes dans les produits***, ***processus et services TIC***;

Amendement 176

Proposition de règlement
Article 45 – alinéa 1 – point f

Texte proposé par la Commission	*Amendement*
(f) ***rétablir la disponibilité des données, services et fonctions ainsi*** que ***l'accès à ceux-ci dans les plus brefs délais en cas***	f) ***de faire en sorte*** que ***les produits, processus et services TIC soient sûrs par défaut et dès la conception***;

d'incident physique ou technique;

Amendement 177

Proposition de règlement
Article 45 – alinéa 1 – point g

Texte proposé par la Commission	*Amendement*
(g) ***veiller*** à ce que les produits et services TIC soient dotés de logiciels à jour et sans vulnérabilités connues, et de mécanismes permettant d'assurer les mises à jour des logiciels en toute sécurité.	g) ***de veiller*** à ce que les produits et services TIC soient dotés de logiciels à jour et sans vulnérabilités connues, et de mécanismes permettant d'assurer les mises à jour des logiciels en toute sécurité.

Amendement 178

Proposition de règlement
Article 45 – alinéa 1 – point g bis (nouveau)

Texte proposé par la Commission	*Amendement*
	g bis) de réduire au maximum les autres risques liés aux incidents de cybersécurité, tels que les risques pour la vie humaine, la santé, l'environnement et d'autres intérêts juridiques importants.

Amendement 179

Proposition de règlement
Article 46 – paragraphe 1

Texte proposé par la Commission	*Amendement*
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 produits et services TIC certifiés dans le cadre de ce système.	1. Un système européen de certification de cybersécurité peut préciser***, en fonction du contexte et de l'utilisation prévue des produits, processus et services TIC,*** un ou plusieurs des niveaux d'assurance suivants***, fondés sur les risques***: élémentaire, substantiel et/ou élevé, pour les produits***, processus*** et services TIC certifiés dans le cadre de ce système.

Amendement 180

Proposition de règlement
Article 46 – paragraphe 2 – point a

Texte proposé par la Commission	*Amendement*
(a) le niveau d'assurance élémentaire ***renvoie*** à un ***certificat délivré dans le cadre d'un système européen de certification de cybersécurité qui accorde un degré limité de fiabilité aux qualités de cybersécurité revendiquées*** ou ***prétendues d'un produit ou d'un*** service TIC***, et caractérisé sur la base*** de ***spécifications techniques, normes et procédures y afférents, y compris les contrôles techniques, dont l'objectif est*** de ***réduire le risque d'incidents*** de cybersécurité;	a) le niveau d'assurance élémentaire ***correspond*** à un ***risque faible, en ce qui concerne tant la survenue d'un incident que les dégâts que causerait celui-ci, lié à un produit, processus*** ou service TIC ***en fonction du contexte et*** de ***son utilisation prévue. Ce niveau d'assurance garantit la résistance aux risques*** de ***base connus en matière*** de cybersécurité;

Amendement 181

Proposition de règlement
Article 46 – paragraphe 2 – point b

Texte proposé par la Commission	*Amendement*
(b) le niveau d'assurance substantiel ***renvoie*** à un ***certificat délivré dans le cadre d'un système européen de certification de cybersécurité qui accorde un degré substantiel de fiabilité aux qualités de cybersécurité revendiquées ou prétendues d'un*** produit ***ou d'un*** service TIC***, et caractérisé sur la base de spécifications techniques, normes et procédures y afférents***, ***y compris les contrôles techniques, dont l'objectif est de réduire substantiellement le risque d'incidents de cybersécurité***;	b) le niveau d'assurance substantiel ***correspond*** à un ***risque moyen, en ce qui concerne tant la survenue d'un incident que les dégâts que causerait celui-ci, lié à un*** produit***, processus ou*** service TIC***. Ce niveau d'assurance garantit la prévention des risques connus en matière de cybersécurité***, ***ainsi que la capacité à résister à des cyberattaques menées avec des ressources limitées***;

Amendement 182

Proposition de règlement
Article 46 – paragraphe 2 – point c

Texte proposé par la Commission	*Amendement*
(c) le niveau d'assurance élevé ***renvoie*** à un ***certificat délivré dans le cadre d'un système européen de certification de cybersécurité*** qui ***accorde un degré de fiabilité aux qualités de cybersécurité revendiquées ou prétendues d'un*** produit ou service TIC ***plus élevé que les certificats ayant le*** niveau d'assurance ***substantiel, et caractérisé sur*** la ***base de spécifications techniques, normes et procédures y afférents***, ***y compris les contrôles techniques, dont l'objectif est*** de ***prévenir les incidents de cybersécurité;***	c) le niveau d'assurance élevé ***correspond*** à un ***risque élevé en ce*** qui ***concerne les dégâts que causerait un incident à un*** produit***, processus*** ou service TIC***. Ce*** niveau d'assurance ***garantit*** la ***prévention des risques en matière de cybersécurité***, ***ainsi que la capacité à résister à des cyberattaques*** de ***pointe menées avec des ressources considérables.***

Amendement 183

Proposition de règlement
Article 46 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	Article 46 bis
	Évaluation des niveaux d'assurance des systèmes européens de certification de cybersécurité
	1. Pour le niveau d'assurance élémentaire, le fabricant ou le fournisseur de produits, processus et services TIC a la possibilité, sous sa seule responsabilité, d'effectuer une auto-évaluation de conformité.
	2. Pour le niveau d'assurance substantiel, l'évaluation est guidée au moins par la vérification de la conformité des fonctionnalités de sécurité du produit, processus ou service par rapport à sa documentation technique.
	3. Pour le niveau d'assurance élevé, la méthode d'évaluation est guidée au moins par un test d'efficacité qui évalue la résistance des fonctionnalités de sécurité à des attaquants disposant de ressources considérables.

Amendement 184

Proposition de règlement
Article 47 – paragraphe 1 – point a

Texte proposé par la Commission	*Amendement*
(a) l'objet et le champ d'application de la certification, notamment le type ou les catégories de produits et services TIC;	a) l'objet et le champ d'application de la certification, notamment le type ou les catégories de produits***, de processus*** et ***de*** services TIC;

Amendement 185

Proposition de règlement
Article 47 – paragraphe 1 – point a bis (nouveau)

Texte proposé par la Commission	*Amendement*
	a bis) le champ d'application et les exigences en matière de cybersécurité, qui, le cas échéant, reproduisent fidèlement ceux de la certification nationale de cybersécurité qu'il remplace ou qui sont prévus par des actes juridiques;

Amendement 186

Proposition de règlement
Article 47 – paragraphe 1 – point a ter (nouveau)

Texte proposé par la Commission	*Amendement*
	a ter) la période de validité du système de certification;

Amendement 187

Proposition de règlement
Article 47 – paragraphe 1 – point b

Texte proposé par la Commission	*Amendement*
(b) une description détaillée des exigences de cybersécurité utilisées pour évaluer les produits et services TIC, par ***exemple*** par ***référence*** aux normes ou spécifications techniques européennes ou internationales;	b) une description détaillée des exigences de cybersécurité utilisées pour évaluer les produits***, processus*** et services TIC, par ***référence*** par ***exemple*** aux normes***, spécifications techniques*** ou spécifications techniques ***en matière de TIC*** européennes ou internationales***, définies de telle manière que la certification puisse être intégrée dans, ou reposer sur, les processus de sécurité systématiques du producteur, suivis pendant l'élaboration et le cycle de vie du produit, processus ou service en question***;

Amendement 188

Proposition de règlement
Article 47 – paragraphe 1 – point b bis (nouveau)

Texte proposé par la Commission	*Amendement*
	b bis) des informations sur les cybermenaces qui ne sont pas couvertes par la certification et des orientations pour les contrer;

Amendement 189

Proposition de règlement
Article 47 – paragraphe 1 – point c

Texte proposé par la Commission	*Amendement*
(c) le cas échéant, un ou plusieurs niveaux d'assurance;	c) le cas échéant, un ou plusieurs niveaux d'assurance ***tenant compte, entre autres, d'une approche fondée sur le risque***;

Amendement 190

Proposition de règlement
Article 47 – paragraphe 1 – point c bis (nouveau)

Texte proposé par la Commission	*Amendement*
	c bis) une indication précisant si l'auto-évaluation de la conformité est autorisée dans le cadre du système, et la procédure applicable à l'évaluation de la conformité ou à l'auto-déclaration de la conformité ou aux deux;

Amendement 191

Proposition de règlement
Article 47 – alinéa 1 – point d

Texte proposé par la Commission	*Amendement*
(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;	d) les critères***, types*** d'évaluation ***de la conformité et méthodes*** d'évaluation ***spécifiques***, afin de démontrer que les objectifs spécifiques visés à l'article 45 sont atteints;

Amendement 192

Proposition de règlement
Article 47 – paragraphe 1 – point e

Texte proposé par la Commission	*Amendement*
(e) les informations nécessaires à la certification qu'un demandeur doit fournir aux organismes d'évaluation de la conformité;	*(Ne concerne pas la version française.)*

Amendement 193

Proposition de règlement
Article 47 – paragraphe 1 – point f

Texte proposé par la Commission	*Amendement*
(f) ***lorsque le système prévoit des marques ou des labels***, ***les conditions dans lesquelles ces marques ou labels peuvent être utilisés***;	f) ***les informations en matière de cybersécurité***, ***conformément à l'article 47 bis du présent règlement***;

Amendement 194

Proposition de règlement
Article 47 – paragraphe 1 – point g

Texte proposé par la Commission	*Amendement*
(g) ***lorsque le système comprend une surveillance, les*** modalités relatives au contrôle du respect des exigences associées aux certificats, notamment les mécanismes permettant de démontrer le respect constant des exigences de cybersécurité;	g) ***les*** modalités relatives au contrôle du respect des exigences associées aux certificats, notamment les mécanismes permettant de démontrer le respect constant des exigences de cybersécurité;

Amendement 195

Proposition de règlement
Article 47 – paragraphe 1 – point h

Texte proposé par la Commission	*Amendement*
(h) les conditions permettant de délivrer, maintenir et ***poursuivre*** la certification et d'étendre ou de réduire ***son*** champ d'application;	h) les conditions permettant de délivrer, maintenir***, poursuivre, réexaminer*** et ***renouveler*** la certification et d'étendre ou de réduire ***le*** champ d'application ***et la période de validité du certificat***;

Amendement 196

Proposition de règlement
Article 47 – paragraphe 1 – point h bis (nouveau)

Texte proposé par la Commission	*Amendement*
	h bis) les règles visant à corriger les vulnérabilités susceptibles d'apparaître après la délivrance de la certification, par la mise en place d'un processus organisationnel dynamique et continu associant tant les fournisseurs que les utilisateurs;

Amendement 197

Proposition de règlement
Article 47 – paragraphe 1 – point i

Texte proposé par la Commission	*Amendement*
(i) les règles relatives aux conséquences de la non-conformité des produits et services TIC certifiés ***aux exigences en matière de certification***;	i) les règles relatives aux conséquences de la non-conformité ***avec les exigences en matière de certification*** des produits et services TIC certifiés ***ou auto-évalués***;

Amendement 198

Proposition de règlement
Article 47 – paragraphe 1 – point j

Texte proposé par la Commission	*Amendement*
(j) les règles relatives aux modalités de signalement et de traitement des vulnérabilités de cybersécurité non ***détectées précédemment*** dans des produits et services TIC;	j) les règles relatives aux modalités de signalement et de traitement des vulnérabilités de cybersécurité non ***connues du public*** dans des produits et services TIC***, une fois que ces vulnérabilités sont détectées***;

Amendement 199

Proposition de règlement
Article 47 – paragraphe 1 – point l

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

Amendement 200

Proposition de règlement
Article 47 – paragraphe 1 – point m bis (nouveau)

Texte proposé par la Commission	*Amendement*
	m bis) les conditions de reconnaissance mutuelle des systèmes de certification avec les pays tiers.

Amendement 201

Proposition de règlement
Article 47 – paragraphe 1 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	1 bis. Les processus de maintenance comprenant des mises à jours n'invalident pas la certification, sauf si ces mises à jours ont un effet préjudiciable non négligeable sur la sécurité du produit, du processus ou du service TIC concerné.

Amendement 202

Proposition de règlement
Article 47 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	Article 47 bis
	Informations en matière de cybersécurité pour les produits, processus et services certifiés
	1. Le fabricant ou le fournisseur de produits, processus ou services TIC relevant d'un système de certification au titre du présent règlement fournit à l'utilisateur final un document, au format papier ou électronique, qui comprend au moins les informations suivantes: le niveau d'assurance du certificat lié à l'utilisation prévue du produit, processus ou service TIC; une description des risques contre lesquels la certification garantit une résistance; des recommandations sur la manière dont les utilisateurs peuvent renforcer davantage

	la cybersécurité du produit, processus ou service, la régularité des mises à jour et la période d'assistance technique suite aux mises à jour; le cas échéant, des informations sur la manière dont les utilisateurs peuvent conserver les principales fonctionnalités du produit, processus ou service en cas de cyberattaque.
	2. Le document visé au paragraphe 1 du présent article reste disponible tout au long du cycle de vie du produit, processus ou service, tant que celui-ci n'est pas retiré du marché, et pour une durée minimum de cinq ans.
	3. La Commission adopte un acte d'exécution établissant un format pour ledit document. La Commission peut demander à l'Agence de proposer un projet de format. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 55 du présent règlement.

Amendement 203

Proposition de règlement
Article 48 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Les 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.	1. Les produits***, processus*** 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.

Amendement 204

Proposition de règlement
Article 48 – paragraphe 4 – partie introductive

Texte proposé par la Commission	*Amendement*
4. Par dérogation au paragraphe 3, dans	4. Par dérogation au paragraphe 3, ***et***

des cas dûment justifiés, un système européen de cybersécurité particulier peut prévoir que seul un organisme public puisse délivrer un certificat européen de cybersécurité dans le cadre dudit système. Cet organisme public est ***l'une des entités suivantes:***	***uniquement*** dans des cas dûment justifiés, ***comme par exemple pour des motifs de sécurité nationale,*** 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 public est ***un organisme accrédité en tant qu'organisme d'évaluation de la conformité conformément à l'article 51, paragraphe 1, du présent règlement. La personne physique ou morale qui soumet ses 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 toutes les informations nécessaires pour mener la procédure de certification.***

Amendement 205

Proposition de règlement
Article 48 – paragraphe 5

Texte proposé par la Commission	*Amendement*
5. La personne physique ou morale qui soumet ses produits ou services TIC au mécanisme de certification fournit à l'organisme d'évaluation de la conformité visé à l'article 51 toutes les informations nécessaires pour mener la procédure de certification.	5. La personne physique ou morale qui soumet ses produits***,*** services ou ***processus*** TIC au mécanisme de certification fournit à l'organisme d'évaluation de la conformité visé à l'article 51 toutes les informations nécessaires pour mener la procédure de certification***, notamment les informations sur toute vulnérabilité connue en matière de sécurité. La soumission peut être effectuée auprès de tout organisme d'évaluation de la conformité visé à l'article 51.***

Amendement 206

Proposition de règlement
Article 48 – paragraphe 6

Texte proposé par la Commission	*Amendement*
6. Les certificats sont délivrés pour une durée maximale de ***trois*** ans et peuvent être renouvelés ***dans les mêmes conditions*** pourvu que les exigences applicables continuent d'être satisfaites.	6. Les certificats sont délivrés pour une durée maximale ***fixée au cas par cas pour chaque système, compte étant tenu d'un cycle*** de ***vie raisonnable, mais ne dépassant en tout état de cause pas cinq*** ans**,** et peuvent être renouvelés pourvu que les exigences applicables continuent d'être satisfaites.

Justification

Cela garantit une flexibilité pour ajuster la période de validité à l'utilisation prévue.

Amendement 207

Proposition de règlement
Article 48 – paragraphe 7

Texte proposé par la Commission	*Amendement*
7. Un certificat européen de cybersécurité délivré au titre du présent article est reconnu dans tous les États membres.	7. Un certificat européen de cybersécurité délivré au titre du présent article est reconnu dans tous les États membres ***comme répondant aux exigences locales en matière de cybersécurité pour les produits et processus TIC ainsi que les dispositifs électroniques grand public couverts par ledit certificat, compte tenu du niveau d'assurance précisé visé à l'article 46, et aucune distinction n'est opérée entre ces certificats sur la base de l'État membre d'origine ou de l'organisme d'évaluation de la conformité de délivrance visé à l'article 51***.

Justification

Afin d'éviter la fragmentation de la reconnaissance et/ou de la conformité des systèmes européens de certification de cybersécurité, cet article doit insister sur le fait que le lieu de délivrance d'un certificat ne doit pas donner lieu à une discrimination.

Amendement 208

Proposition de règlement
Article 48 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	Article 48 bis
	Systèmes de certification pour les opérateurs de services essentiels
	1. Lorsque des système européens de certification de cybersécurité ont été adoptés conformément au paragraphe 2 du présent article, les opérateurs de services essentiels utilisent, afin de se conformer aux exigences de sécurité visées à l'article 14 de la directive (UE) 2016/1148, des produits, processus et services couverts par ces systèmes.
	2. Au plus tard [un an après l'entrée en vigueur du présent règlement], la Commission, après consultation du groupe de coopération visé à l'article 11 de la directive (UE) 2016/1148, adopte des actes délégués conformément à l'article 55 bis pour compléter le présent règlement en énumérant les catégories de produits, processus et services qui répondent simultanément aux deux critères suivants:
	a) ils sont destinés à être utilisés par des opérateurs de services essentiels; et
	b) leur dysfonctionnement aurait des effets perturbateurs non négligeables sur la fourniture du service essentiel concerné.
	3. La Commission adopte des actes délégués conformément à l'article 55 bis pour modifier le présent règlement en mettant à jour, si besoin est, la liste des catégories de produits, processus et services visée au paragraphe 2 du présent article.
	4. La Commission demande à l'Agence d'élaborer un système européen de certification de cybersécurité candidat conformément à l'article 44, paragraphe -1, du présent règlement, pour la liste des catégories de produits, processus et services visée aux paragraphes 2 et 3 du présent article dès que cette liste est

adoptée ou mise à jour. Le niveau d'assurance des certificats délivrés au titre d'un tel système européen de certification de cybersécurité est le niveau élevé.

Amendement 209

Proposition de règlement
Article 48 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	Article 48 ter
	Objections formelles aux systèmes européens de certification de cybersécurité
	1. Lorsqu'un État membre considère qu'un système de certification de cybersécurité européen ne satisfait pas entièrement aux exigences qu'il a pour objet de respecter, définies dans la législation d'harmonisation pertinente de l'Union, il en informe la Commission et lui fournit une explication détaillée. La Commission, après consultation du comité institué conformément à la législation d'harmonisation pertinente de l'Union, le cas échéant, ou après d'autres formes de consultation d'experts sectoriels, décide:
	a) de publier, de ne pas publier ou de publier partiellement les références au système de cybersécurité européen concerné au Journal officiel de l'Union européenne;
	b) de maintenir intégralement ou partiellement les références au système de cybersécurité européen concerné au Journal officiel de l'Union européenne ou de les en retirer.
	2. La Commission publie sur son site internet des informations sur les systèmes de cybersécurité européens ayant fait l'objet de la décision visée au paragraphe 1 du présent article.

	3. La Commission informe l'Agence de la décision visée au paragraphe 1 du présent article et, si nécessaire, demande la révision du système européen de cybersécurité concerné.
	4. La décision visée au paragraphe 1, point a), du présent article est adoptée en conformité avec la procédure consultative visée à l'article 55, paragraphe 2, du présent règlement.
	5. La décision visée au paragraphe 1, point b), du présent article est adoptée en conformité avec la procédure d'examen visée à l'article 55, paragraphe 2 bis, du présent règlement.

Amendement 210

Proposition de règlement
Article 49 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Sans préjudice du paragraphe 3, les systèmes nationaux de certification de cybersécurité et les procédures connexes pour les 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 existants et les procédures connexes pour les produits et services TIC qui ne sont pas couverts par un système européen de certification de cybersécurité continuent à exister.	1. Sans préjudice du paragraphe 3, les systèmes nationaux de certification de cybersécurité et les procédures connexes pour les produits***, processus*** 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 existants et les procédures connexes pour les produits***, processus*** et services TIC qui ne sont pas couverts par un système européen de certification de cybersécurité continuent à exister.

Amendement 211

Proposition de règlement
Article 49 – paragraphe 2

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

Amendement 212

Proposition de règlement
Article 49 – paragraphe 3 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	3 bis. Les États membres communiquent à la Commission toutes les demandes d'élaboration de systèmes nationaux de certification de cybersécurité et indiquent les motifs de leur adoption.

Amendement 213

Proposition de règlement
Article 49 – paragraphe 3 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	3 ter. Sur demande, les États membres envoient au moins sous forme électronique tout projet de système national de certification de cybersécurité aux autres États membres, à l'Agence ou à la Commission.

Amendement 214

Proposition de règlement
Article 49 – paragraphe 3 quater (nouveau)

Texte proposé par la Commission	*Amendement*
	3 quater. Sans préjudice des dispositions de la directive (UE) 2015/1535, chaque

	État membre, dans un délai de trois mois, répond aux observations reçues de tout autre État membre, de l'Agence ou de la Commission, et en tient dûment compte, pour tout projet visé au paragraphe 3 ter du présent article.

Amendement 215

Proposition de règlement
Article 49 – paragraphe 3 quinquies (nouveau)

Texte proposé par la Commission	*Amendement*
	3 quinquies. Lorsque des observations reçues au titre du paragraphe 3 quater du présent article indiquent qu'un projet de système national de certification de cybersécurité est susceptible d'avoir des retombées négatives sur le bon fonctionnement du marché intérieur, l'État membre auquel sont adressées les observations consulte l'Agence et la Commission et tient dûment compte de leurs observations avant d'adopter ledit projet.

Amendement 216

Proposition de règlement
Article 50 – paragraphe 5

Texte proposé par la Commission	*Amendement*
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.	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 ***des États membres pour la certification*** institué en vertu de l'article 53.

Amendement 217

Proposition de règlement
Article 50 – paragraphe 6 – point a

Texte proposé par la Commission	*Amendement*
(a) contrôlent et assurent l'application des dispositions du présent titre au niveau national et ***supervisent*** la conformité ***des certificats qui ont été délivrés*** par ***les organismes d'évaluation*** de ***la conformité établis sur leur territoire aux exigences énoncées dans le présent titre et dans le système européen de certification de cybersécurité correspondant;***	a) contrôlent et assurent l'application des dispositions du présent titre au niveau national et ***vérifient, dans le respect des règles adoptées*** par ***le groupe européen*** de ***certification de cybersécurité conformément à l'article 53, paragraphe 3, point d bis):***
	i) la conformité des certificats délivrés par les organismes d'évaluation de la conformité établis sur leur territoire avec les exigences énoncées dans le présent titre et dans le système européen de certification de cybersécurité correspondant; et
	ii) la conformité des auto-déclarations de conformité d'un processus, produit ou service TIC effectuées dans le cadre d'un système;

Amendement 218

Proposition de règlement
Article 50 – paragraphe 6 – point b

Texte proposé par la Commission	*Amendement*
(b) contrôlent et supervisent les activités des organismes d'évaluation de la conformité aux fins du présent règlement, notamment en ce qui concerne la notification des organismes d'évaluation de la conformité et des missions connexes énoncées à l'article 52 du présent règlement;	b) contrôlent***,*** supervisent et***, au moins tous les deux ans, évaluent*** les activités des organismes d'évaluation de la conformité aux fins du présent règlement, notamment en ce qui concerne la notification des organismes d'évaluation de la conformité et des missions connexes énoncées à l'article 52 du présent règlement;

Amendement 219

Proposition de règlement
Article 50 – paragraphe 6 – point b bis (nouveau)

Texte proposé par la Commission	*Amendement*
	b bis) effectuent des audits pour s'assurer que des normes équivalentes s'appliquent dans l'Union et rendent compte des résultats à l'Agence et au groupe;

Justification

Cela contribue à garantir l'application d'un niveau de service et de qualité uniforme dans l'ensemble de l'UE et à empêcher la recherche de la juridiction la plus favorable pour la certification.

Amendement 220

Proposition de règlement
Article 50 – paragraphe 6 – point c

Texte proposé par la Commission	*Amendement*
(c) traitent les réclamations introduites par une personne physique ou morale en rapport avec les certificats délivrés par des organismes d'évaluation de la conformité établis sur leur territoire, 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;	c) traitent les réclamations introduites par une personne physique ou morale en rapport avec les certificats délivrés par des organismes d'évaluation de la conformité établis sur leur territoire ***ou avec les auto-évaluations de conformité effectuées***, 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;

Amendement 221

Proposition de règlement
Article 50 – paragraphe 6 – point c bis (nouveau)

Texte proposé par la Commission	*Amendement*
	c bis) transmettent à l'Agence et au groupe européen de certification de cybersécurité les résultats des vérifications visées au point a) et les évaluations visées au point b);

Amendement 222

Proposition de règlement
Article 50 – paragraphe 6 – point d

Texte proposé par la Commission	*Amendement*
(d) coopèrent avec les autres autorités nationales de contrôle de la certification ou d'autres autorités publiques, notamment en partageant 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;	d) coopèrent avec les autres autorités nationales de contrôle de la certification ou d'autres autorités publiques, ***telles que les autorités nationales de contrôle de la protection des données,*** notamment en partageant des informations sur l'éventuelle non-conformité de produits***,*** ***processus*** et services TIC ***avec les*** exigences du présent règlement ou à celles de systèmes de certification de cybersécurité spécifiques;

Amendement 223

Proposition de règlement
Article 50 – paragraphe 6 – point d

Texte proposé par la Commission	*Amendement*
(d) coopèrent avec les autres autorités nationales de contrôle de la certification ou d'autres autorités publiques, notamment en partageant 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;	d) coopèrent avec les autres autorités nationales de contrôle de la certification ou d'autres autorités publiques, ***telles que les autorités nationales de contrôle de la protection des données,*** notamment en partageant des informations sur l'éventuelle non-conformité de produits et services TIC ***avec les*** exigences du présent règlement ou ***avec*** celles de systèmes ***européens*** de certification de ***sécurité informatique*** spécifiques;

Justification

Suivant l'avis du CEPD.

Amendement 224

Proposition de règlement
Article 50 – paragraphe 7 – point c bis (nouveau)

Texte proposé par la Commission	*Amendement*
	c bis) retirer l'accréditation des organismes nationaux de conformité qui ne respectent pas le présent règlement;

Amendement 225

Proposition de règlement
Article 50 – paragraphe 7 – point e

Texte proposé par la Commission	*Amendement*
(e) retirer, conformément au droit national, les certificats qui ne sont pas conformes au présent règlement ou à un système européen de certification de cybersécurité;	e) retirer, conformément au droit national, les certificats qui ne sont pas conformes au présent règlement ou à un système européen de certification de cybersécurité ***et informer les organismes nationaux d'accréditation en conséquence***;

Amendement 226

Proposition de règlement
Article 50 – paragraphe 8

Texte proposé par la Commission	*Amendement*
8. Les autorités nationales de contrôle de la certification coopèrent entre elles et avec la Commission et échangent notamment des informations, expériences et bonnes pratiques en ce qui concerne la certification de cybersécurité et les questions techniques relatives à la cybersécurité des produits et services TIC.	8. Les autorités nationales de contrôle de la certification coopèrent entre elles et avec la Commission et échangent notamment des informations, expériences et bonnes pratiques en ce qui concerne la certification de cybersécurité et les questions techniques relatives à la cybersécurité des produits***, processus*** et services TIC.

Amendement 227

Proposition de règlement
Article 50 – paragraphe 8 bis (nouveau)

Texte proposé par la Commission	*Amendement*

	8 bis. Chaque autorité nationale de contrôle de la certification ainsi que tous les membres du personnel de chaque autorité nationale de contrôle de la certification sont soumis, conformément à la législation de l'Union ou de l'État membre concerné, a une obligation de secret professionnel à l'égard de toute information confidentielle dont ils ont eu connaissance dans l'exercice de leurs fonctions ou de leurs compétences et ce, que ce soit au cours de leur mandat ou par la suite.

Amendement 228

Proposition de règlement
Article 50 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	Article 50 bis
	Examen par les pairs
	1. Les autorités nationales de contrôle de la certification font l'objet d'un examen par les pairs en ce qui concerne toute activité organisée par l'Agence qu'elles exercent au titre de l'article 50.
	2. L'évaluation par les pairs est effectuée selon des critères et des procédures d'évaluation cohérents et transparents, en particulier en ce qui concerne les exigences organisationnelles, celles relatives aux ressources humaines et aux processus, ainsi que la confidentialité et les plaintes. Des procédures de recours appropriées à l'encontre de décisions prises à la suite de cette évaluation sont prévues.
	3. L'examen par les pairs couvre les évaluations des procédures mises en place par les autorités nationales de contrôle de la certification, notamment les procédures de contrôle de la conformité des certificats, les procédures de suivi et de contrôle des activités des organes d'évaluation de la conformité, la

compétence du personnel, la régularité des contrôles et la méthode d'inspection, ainsi que l'exactitude des résultats. L'examen par les pairs détermine également si les autorités nationales de contrôle de la certification en question disposent de ressources suffisantes pour la bonne exécution de leurs tâches, comme l'exige l'article 50, paragraphe 4.

4. L'examen par les pairs d'une autorité nationale de contrôle de la certification est effectué par deux autorités nationales de contrôle de la certification d'autres États membres et la Commission, au minimum une fois tous les cinq ans. L'Agence peut participer à l'examen par les pairs et décide de sa participation sur la base d'une analyse des risques.

5. La Commission peut adopter des actes délégués, conformément à l'article 55 bis, pour compléter le présent règlement en établissant un plan pour l'examen par les pairs couvrant une période d'au moins cinq ans, définissant des critères concernant la composition de l'équipe chargée de l'examen par les pairs, la méthode utilisée pour mener cet examen, le programme, la périodicité et les autres tâches y relatives. Lors de l'adoption de ces actes délégués, la Commission tient dûment compte des observations formulées par le groupe des États membres pour la certification.

6. Le groupe des États membres pour la certification examine les conclusions de l'examen par les pairs. L'Agence rédige un résumé des conclusions et, le cas échéant, des documents d'orientation et de bonnes pratiques, qu'elle rend publics.

Amendement 229

Proposition de règlement
Article 51 – paragraphe 1 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	1 bis. En ce qui concerne le niveau d'assurance élevé, l'organisme d'évaluation de la conformité doit, outre son accréditation, être notifié par l'autorité nationale de contrôle de la certification au regard de leur compétence et expertise en matière d'évaluation de la cybersécurité. L'autorité nationale de contrôle de la certification doit procéder à des audits réguliers de l'expertise et des compétences des organismes d'évaluation de la conformité notifiés.

Justification

Les niveaux d'assurance élevés requièrent des tests d'efficacité. L'expertise et les compétences des organismes d'évaluation de la conformité procédant à des tests d'efficacité doivent être régulièrement auditées pour s'assurer notamment de la qualité des tests.

Amendement 230

Proposition de règlement
Article 51 – paragraphe 2 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	2 bis. Des audits sont réalisés afin de s'assurer que des normes équivalentes s'appliquent dans l'Union, et les résultats de ces audits sont communiqués à l'Agence et au groupe.

Amendement 231

Proposition de règlement
Article 51 – paragraphe 2 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	2 ter. Lorsque les fabricants optent pour l'auto-déclaration de conformité visée à l'article 48, paragraphe 3, les organismes d'évaluation de la conformité prennent des mesures supplémentaires, afin de vérifier les procédures internes qu'a engagées le fabricant à l'effet de s'assurer

	que ses produits ou services satisfont aux exigences du système européen de certification de cybersécurité.

Amendement 232

Proposition de règlement
Article 52 – paragraphe 5

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

Amendement 233

Proposition de règlement
Article 53 – titre

Texte proposé par la Commission	*Amendement*
Systèmes européens de certification de cybersécurité	***Groupe des États membres pour la certification*** *(Cette modification s'applique à l'ensemble du texte législatif à l'examen; son adoption impose des adaptations techniques dans tout le texte.)*

Amendement 234

Proposition de règlement
Article 53 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Le Groupe ***européen de certification de cybersécurité (ci-après le «Groupe»)*** est institué.	1. Le groupe ***des États membres pour la certification*** est institué.

Amendement 235

Proposition de règlement
Article 53 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Le Groupe est composé d'autorités nationales de contrôle de la certification. Les autorités sont représentées par leur dirigeant ou par d'autres représentants de haut niveau.	2. Le groupe ***des États membres pour la certification*** est composé d'autorités nationales de contrôle de la certification ***de tous les États membres***. Les autorités sont représentées par leur dirigeant ou par d'autres représentants de haut niveau. ***Les membres du groupe des parties prenantes pour la certification peuvent être invités aux réunions du groupe des États membres pour la certification et à participer à ses travaux.***

Amendement 236

Proposition de règlement
Article 53 – paragraphe 3 – partie introductive

Texte proposé par la Commission	*Amendement*
3. Le Groupe a pour mission:	3. Le groupe ***des États membres pour la certification*** a pour mission:

Amendement 237

Proposition de règlement
Article 53 – paragraphe 3 – point b

Texte proposé par la Commission	*Amendement*
(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) d'assister, de conseiller et de coopérer avec ***l'Agence*** en ce qui concerne l'élaboration d'un système candidat conformément à l'article 44 du présent règlement;

Amendement 238

Proposition de règlement
Article 53 – paragraphe 3 – point d bis (nouveau)

Texte proposé par la Commission	*Amendement*
	d bis) d'adopter des recommandations précisant les intervalles auxquels les autorités nationales de contrôle de la certification doivent procéder à des vérifications des certificats et des auto-évaluations de conformité ainsi que les critères, l'ampleur et la portée de ces vérifications, et d'arrêter des règles et normes communes en ce qui concerne la transmission des résultats prévue à l'article 50, paragraphe 6;

Amendement 239

Proposition de règlement
Article 53 – paragraphe 3 – point e

Texte proposé par la Commission	*Amendement*
(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;	e) d'examiner les évolutions pertinentes dans le domaine de la certification de cybersécurité et de l'échange ***d'informations et*** de bonnes pratiques sur les systèmes de certification de cybersécurité;

Amendement 240

Proposition de règlement
Article 53 – paragraphe 3 – point f bis (nouveau)

Texte proposé par la Commission	*Amendement*
	f bis) de faciliter l'alignement des systèmes européens de certification de cybersécurité sur les normes internationalement reconnues, y compris en examinant les systèmes européens de certification de cybersécurité existants et, s'il y a lieu, en recommandant à l'Agence de nouer le dialogue avec les organisations internationales de normalisation compétentes dans le but de remédier à des insuffisances ou à des

lacunes affectant les normes internationalement reconnues en vigueur;

Amendement 241

Proposition de règlement
Article 53 – paragraphe 3 – point f ter (nouveau)

Texte proposé par la Commission	*Amendement*
	f ter) de mettre en place un processus d'examen par les pairs. Celui-ci concerne en particulier l'expertise technique requise par les autorités nationales de contrôle de la certification dans l'accomplissement de leurs missions, tel que décrit aux articles 48 et 50, et comprend, si nécessaire, l'élaboration de documents d'orientation et de bonnes pratiques visant à améliorer le respect du présent règlement par les autorités nationales de contrôle de la certification;

Amendement 242

Proposition de règlement
Article 53 – paragraphe 3 – point f quater (new)

Texte proposé par la Commission	*Amendement*
	f quater) de superviser le contrôle et le maintien des certificats;

Amendement 243

Proposition de règlement
Article 53 – paragraphe 3 – point f quinquies (nouveau)

Texte proposé par la Commission	*Amendement*
	f quinquies) de tenir compte des résultats de la consultation des parties prenantes réalisée lors de la préparation d'un système candidat conformément à l'article 44;

Amendement 244

Proposition de règlement
Article 53 – paragraphe 4

Texte proposé par la Commission	*Amendement*
4. La Commission préside le Groupe et en assure le secrétariat, avec l'aide de ***l'ENISA conformément*** à l'article 8, point a).	4. La Commission préside le groupe ***des États membres pour la certification*** et en assure le secrétariat, avec l'aide de ***l'Agence comme prévu*** à l'article 8, point a).

Amendement 245

Proposition de règlement
Article 53 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	Article 53 bis
	Droit à un recours juridictionnel effectif contre une autorité de contrôle ou un organisme d'évaluation de la conformité
	1. Sans préjudice de tout autre recours administratif ou non juridictionnel, toute personne physique ou morale dispose d'un droit de recours juridictionnel effectif:
	a) contre une décision prise par un organisme d'évaluation de la conformité ou une autorité nationale de contrôle de la certification la concernant, y compris, le cas échéant, en ce qui concerne la délivrance, la non-délivrance ou la reconnaissance d'un certificat européen de cybersécurité détenu par ladite personne; et
	b) dans les cas où une autorité nationale de contrôle de la certification ne traite pas une réclamation pour laquelle elle est compétente.
	2. Les actions contre un organisme d'évaluation de la conformité ou une

autorité nationale de contrôle de la certification sont intentées devant les juridictions de l'État membre sur le territoire duquel l'autorité nationale de contrôle de la certification ou l'organisme d'évaluation de la conformité est établi.

Amendement 246

Proposition de règlement
Article 55 – paragraphe 2 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	2 bis. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) n° 182/2011 s'applique.

Amendement 247

Proposition de règlement
Article 55 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	Article 55 bis
	Exercice de la délégation
	1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.
	2. Le pouvoir d'adopter des actes délégués visé aux articles 44 et 48 bis est conféré à la Commission pour une durée indéterminée à compter du ... [date d'entrée en vigueur du présent acte législatif de base].
	3. La délégation de pouvoir visée aux articles 44 et 48 bis peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au Journal officiel de l'Union

européenne ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Avant d'adopter un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel «Mieux légiférer» du 13 avril 2016.

5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie au Parlement européen et au Conseil simultanément.

6. Un acte délégué adopté conformément aux articles 44 ou 48 bis n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de deux mois à compter de la notification dudit acte au Parlement européen et au Conseil ou si, avant l'expiration dudit délai, le Parlement européen et le Conseil ont tous deux informé la Commission qu'ils ne comptaient pas exprimer d'objection. Ce délai est prolongé de deux mois à l'initiative du Parlement européen ou du Conseil.

Amendement 248

Proposition de règlement
Article 56 – paragraphe 1

Texte proposé par la Commission	*Amendement*
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.	1. Au plus tard ***deux*** ans après la date visée à l'article 58, et ensuite tous les ***deux*** 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.	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.

Amendement 249

Proposition de règlement
Article 56 – paragraphe 2

Texte proposé par la Commission	*Amendement*
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.	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***,*** ***processus*** et services TIC dans l'Union et à améliorer le fonctionnement du marché intérieur.

Amendement 250

Proposition de règlement
Article 56 – paragraphe 2 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	2 bis. L'évaluation examine s'il est nécessaire de fixer des exigences essentielles en matière de cybersécurité comme condition d'accès au marché intérieur pour empêcher que des produits, services et processus qui ne satisfont pas aux exigences de base en matière de cybersécurité entrent sur le marché de l'Union.

Amendement 251

Proposition de règlement
Annexe -I (nouvelle)

Texte proposé par la Commission	*Amendement*
	ANNEXE -I
	Lors du lancement du cadre européen de certification de cybersécurité, il est probable qu'une attention particulière soit prêtée aux domaines présentant un intérêt imminent pour relever le défi posé par les technologies émergentes. L'internet des objets présente un intérêt particulier dans la mesure où il touche aux exigences des consommateurs comme de l'industrie. La liste de priorités suivantes est proposée en vue de leur adoption dans le cadre de certification:
	1) certification des services d'informatique en nuage;
	2) certification des appareils connectés à l'internet des objets, y compris:
	a. les dispositifs individuels, comme les accessoires vestimentaires intelligents,
	b. les dispositifs communautaires, comme les voitures intelligentes, les maisons intelligentes et les dispositifs de santé,
	c. les dispositifs au niveau de la société, comme les villes et réseaux intelligents;
	3) l'industrie 4.0 avec des systèmes cyberphysiques intelligents et interconnectés qui automatisent toutes les phases des opérations industrielles, depuis la conception et la fabrication jusqu'à l'exploitation, à la chaîne d'approvisionnement et à la maintenance des services;
	4) la certification des technologies et produits utilisés dans la vie de tous les jours. Ce pourrait par exemple être le cas des dispositifs de réseau comme les routeurs internet dans les habitations.

Amendement 252

Proposition de règlement
Annexe I – alinéa 1 – point 5 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	5 bis. Si un organisme d'évaluation de la conformité appartient à une entité ou à une institution publique, ou est géré par une telle entité ou institution, l'indépendance et l'absence de conflit d'intérêts entre l'autorité de contrôle de la certification, d'une part, et l'organisme d'évaluation de la conformité, d'autre part, sont garanties et documentées.

Amendement 253

Proposition de règlement
Annexe I – alinéa 1 – point 8

Texte proposé par la Commission	*Amendement*
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.	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. ***Toute sous-traitance ou consultation de personnes externes est documentée de manière appropriée, ne fait intervenir aucun intermédiaire et fait l'objet d'un accord écrit concernant, entre autres, la confidentialité et les conflits d'intérêts. L'organisme d'évaluation de la conformité en question assume l'entière responsabilité des tâches accomplies.***

Amendement 254

Proposition de règlement
Annexe I – alinéa 1 – point 12

Texte proposé par la Commission	*Amendement*
12) L'impartialité des organismes d'évaluation de la conformité, de leurs cadres supérieurs et de leur personnel	12) L'impartialité des organismes d'évaluation de la conformité, de leurs cadres supérieurs et de leur personnel ***et de***

effectuant l'évaluation est garantie.	***leurs sous-traitants*** effectuant l'évaluation est garantie.

Amendement 255

Proposition de règlement
Annexe I – alinéa 1 – point 15

Texte proposé par la Commission	*Amendement*
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.	15) ***L'organisme d'évaluation de la conformité et son personnel, ses comités, ses filiales, ses sous-traitants et tout organisme associé ainsi que le*** personnel ***des organes externes*** d'un organisme d'évaluation de la conformité ***assurent le respect de la confidentialité et sont liés*** par le secret professionnel pour toutes les informations obtenues dans l'exercice de ses fonctions au titre du présent règlement ou de toute disposition de droit national lui donnant effet, sauf ***dans les cas où la communication de ces informations est requise par le droit de l'Union ou de l'État membre auquel ces personnes sont soumises, sauf*** à l'égard des autorités compétentes de l'État membre où il exerce ses activités. ***Les droits de propriété sont protégés. L'organisme d'évaluation de la conformité possède des procédures documentées concernant les exigences de la présente section 15.***

Amendement 256

Proposition de règlement
Annexe I – alinéa 1 – point 15 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	15 bis) À l'exception de la section 15, les exigences de la présente annexe n'empêchent en rien les échanges d'informations techniques et d'orientations réglementaires entre un organisme d'évaluation de la conformité et une personne qui introduit ou envisage

d'introduire une demande de certification.

Amendement 257

Proposition de règlement
Annexe I – alinéa 1 – point 15 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	15 ter) Les organismes d'évaluation de la conformité agissent conformément à un ensemble de conditions cohérentes, justes et raisonnables, en tenant compte des intérêts des petites et moyennes entreprises au sens de la recommandation 2003/361/CE pour ce qui est des redevances.