# COM(2020) 823 final

**ASSEMBLÉE NATIONALE**

**QUINZIÈME LÉGISLATURE**

**SÉNAT**

**SESSION ORDINAIRE DE 2020/2021**

**Reçu à la Présidence de l'Assemblée nationale**
**le 19 janvier 2021**

**Enregistré à la Présidence du Sénat**
**le 19 janvier 2021**

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

PAR LE GOUVERNEMENT,

À L'ASSEMBLÉE NATIONALE ET AU SÉNAT

Proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148

E 15447

Conseil de
l'Union européenne

**Bruxelles, le 17 décembre 2020**
**(OR. en)**

**14150/20**

**Dossier interinstitutionnel:**
**2020/0359 (COD)**

**CYBER 281**
**JAI 1119**
**DATAPROTECT 155**
**TELECOM 270**
**MI 581**
**CSC 368**
**CSCI 97**

**NOTE DE TRANSMISSION**

| | |
|---|---|
| Origine: | Pour la secrétaire générale de la Commission européenne, Madame Martine DEPREZ, directrice |
| Date de réception: | 16 décembre 2020 |
| Destinataire: | Monsieur Jeppe TRANHOLM-MIKKELSEN, secrétaire général du Conseil de l'Union européenne |
| N° doc. Cion: | COM(2020) 823 final |
| Objet: | Proposition de DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148 |

Les délégations trouveront ci-joint le document COM(2020) 823 final.

p.j.: COM(2020) 823 final

COMMISSION
EUROPÉENNE

Bruxelles, le 16.12.2020
COM(2020) 823 final

2020/0359 (COD)

Proposition de

# DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL

## concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148

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

{SEC(2020) 430 final} - {SWD(2020) 344 final} - {SWD(2020) 345 final}

# EXPOSÉ DES MOTIFS

## 1. CONTEXTE DE LA PROPOSITION

### • Justification et objectifs de la proposition

La présente proposition fait partie d'un ensemble de mesures destinées à améliorer la résilience et les capacités de réaction aux incidents des entités publiques et privées, des autorités compétentes et de l'Union dans son ensemble dans le domaine de la cybersécurité et de la protection des infrastructures critiques. Elle est conforme aux priorités de la Commission consistant à adapter l'Europe à l'ère du numérique et bâtir une économie au service des personnes et parée pour l'avenir. La cybersécurité est l'une des priorités de la réponse de la Commission à la crise de la COVID-19. Cet ensemble de mesures comprend une nouvelle stratégie de cybersécurité, dans le but de renforcer l'autonomie stratégique de l'Union afin d'améliorer sa résilience et la réaction collective et de construire un internet ouvert et mondial. Enfin, l'ensemble de mesures contient une proposition de directive concernant la résilience des opérateurs critiques de services essentiels, qui a pour objectif d'atténuer les menaces physiques qui pèsent sur eux.

La présente proposition capitalise sur la directive (UE) 2016/1148 relative à la sécurité des réseaux et des systèmes d'information (ci-après la «directive SRI»), qu'elle annule, et qui était le premier acte législatif adopté à l'échelle de l'Union européenne dans le domaine de la cybersécurité et prévoyait des mesures juridiques pour renforcer le niveau général de cybersécurité dans l'Union. La directive SRI 1) a contribué à améliorer les capacités nationales en matière de cybersécurité en exigeant des États membres qu'ils adoptent une stratégie de cybersécurité nationale et qu'ils désignent les autorités compétentes; 2) a accru la coopération entre les États membres au niveau de l'Union en créant différents forums facilitant l'échange d'informations stratégiques et opérationnelles; et 3) a amélioré la cyber-résilience des entités publiques et privées de sept secteurs spécifiques (l'énergie, les transports, la banque, les infrastructures des marchés financiers, les soins de santé, la fourniture et la distribution d'eau potable et les infrastructures numériques) et/ou qui fournissent trois types de services numériques (les places de marché en ligne, les moteurs de recherche en ligne et les services d'informatique en nuage) en exigeant des États membres qu'ils veillent à ce que les opérateurs de services essentiels et les fournisseurs de services numériques mettent en place des exigences en matière de cybersécurité et signalent les incidents.

La présente proposition modernise le cadre juridique existant en tenant compte de l'utilisation croissante de supports et formats numériques dans le marché intérieur ces dernières années et de l'évolution du paysage des menaces qui pèsent sur la cybersécurité, deux tendances qui se sont encore amplifiées depuis le début de la pandémie de COVID-19. Elle comble également plusieurs lacunes qui empêchaient d'exploiter pleinement le potentiel de la directive SRI.

Malgré ses accomplissements notables, la directive SRI, qui a ouvert la voie à une évolution importante des mentalités en ce qui concerne l'approche institutionnelle et réglementaire de la cybersécurité dans de nombreux États membres, a également montré ses limites. La transformation numérique de la société (intensifiée par la crise de la COVID-19) a étendu le paysage des menaces et fait naître de nouveaux défis qui nécessitent des réponses adaptées et novatrices. Le nombre de cyberattaques continue d'augmenter, les attaques, toujours plus sophistiquées, provenant d'un large éventail de sources à l'intérieur et à l'extérieur de l'Union.

L'évaluation du fonctionnement de la directive SRI, réalisée aux fins de l'analyse d'impact, a relevé les problèmes suivants: 1) le faible niveau de cyber-résilience des entreprises établies

dans l'Union; 2) un degré de résilience variable en fonction des États membres et des secteurs concernés; et 3) le faible niveau de prise de conscience conjointe de la situation et l'absence de réponse conjointe à la crise. Par exemple, dans un État membre, certains grands hôpitaux ne relèvent pas du champ d'application de la directive SRI et ne sont donc pas tenus de mettre en œuvre les mesures de sécurité qui en découlent, tandis que dans un autre État membre, la quasi-totalité des fournisseurs de soins de santé du pays sont couverts par les exigences en matière de sécurité des réseaux et des systèmes d'information.

Puisqu'il s'agit d'une initiative relevant du programme pour une réglementation affûtée et performante (REFIT), cette proposition a pour objectif de réduire la charge réglementaire pesant sur les autorités compétentes ainsi que les coûts de mise en conformité pour les entités publiques et privées. Plus particulièrement, il convient pour ce faire de supprimer l'obligation faite aux autorités compétentes d'identifier les opérateurs de services essentiels, et de relever le niveau d'harmonisation des exigences en matière de sécurité et de signalement afin de faciliter aux entités qui fournissent des services transfrontières la tâche de mise en conformité réglementaire. Dans le même temps, un certain nombre de nouvelles tâches seront confiées aux autorités compétentes, notamment la supervision d'entités de secteurs qui ne sont pas encore couverts par la directive SRI.

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

La présente proposition fait partie d'un ensemble plus large d'instruments juridiques existants et d'initiatives imminentes à l'échelle de l'Union ayant pour objectif d'accroître la résilience des entités publiques et privées face aux menaces.

Dans le domaine de la cybersécurité, il s'agit notamment de la directive (UE) 2018/1972 établissant le code des communications électroniques européen (dont les dispositions en matière de sécurité seront remplacées par les dispositions de la présente proposition) et de la proposition de règlement sur la résilience opérationnelle numérique du secteur financier [COM(2020) 595 final], ce dernier règlement constituant la lex specialis de la directive proposée une fois les deux actes entrés en vigueur.

Dans le domaine de la sécurité physique, la proposition complète la proposition de directive sur la résilience des entités critiques, qui révise la directive 2008/114/CE du Conseil concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection (ci-après la «directive sur les ICE»), qui créée un processus à l'échelle de l'Union pour recenser et désigner les infrastructures critiques européennes et définit une approche pour l'amélioration de leur protection. En juillet 2020, la Commission a adopté la stratégie de l'UE pour l'union de la sécurité[1], qui reconnaissait l'interconnexion et l'interdépendance croissantes entre les infrastructures physiques et les infrastructures numériques. Elle soulignait la nécessité d'une approche visant à améliorer la cohérence et la concordance entre la directive sur les ICE et 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.

Cette proposition s'aligne donc étroitement sur la proposition de directive sur la résilience des entités critiques, qui a pour objectif d'améliorer la résilience des entités critiques face aux menaces physiques dans un grand nombre de secteurs. Elle vise à garantir que les autorités compétentes en vertu des deux actes adoptent des mesures complémentaires et échangent des

[1] COM(2020) 605 final.

informations autant que de besoin concernant la cyber-résilience et la résilience en dehors du cyberespace et que les opérateurs particulièrement critiques dans les secteurs considérés comme «essentiels» au titre de la présente proposition sont également soumis à des obligations d'amélioration de la résilience plus générales, axées sur les risques non liés au cyberespace.

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

Comme indiqué dans la communication intitulée «Façonner l'avenir numérique de l'Europe»[2], il est essentiel que l'Europe exploite pleinement les avantages de l'ère numérique et renforce son industrie et sa capacité d'innovation dans des limites sûres et éthiques. La stratégie européenne pour les données définit quatre piliers – la protection des données, les droits fondamentaux, la sûreté et la cybersécurité – comme des conditions préalables essentielles pour une société à laquelle les données confèrent les moyens dont elle a besoin.

Dans une résolution en date du 12 mars 2019, le Parlement européen a invité «*[…] la Commission à étudier la nécessité d'élargir le champ d'application de la directive SRI à de nouveaux secteurs et services d'importance critique qui ne sont pas couverts par une législation spécifique*»[3]. Le Conseil, dans ses conclusions du 9 juin 2020, a salué «*[…] les projets de la Commission visant à garantir des règles cohérentes pour les opérateurs du marché et à faciliter un échange d'informations sécurisé, fiable et approprié sur les menaces ainsi que sur les incidents, y compris grâce au réexamen de la directive sur la sécurité des réseaux et des systèmes d'information (directive SRI), afin de rechercher des solutions permettant d'améliorer la cyberrésilience et de réagir plus efficacement aux cyberattaques, en particulier celles ciblant des activités essentielles pour l'économie et la société, tout en respectant les compétences des États membres, y compris la responsabilité qui est la leur en matière de sécurité nationale*»[4]. De plus, l'acte juridique proposé est sans préjudice de l'application des règles de concurrence prévues par le traité sur le fonctionnement de l'Union européenne (TFUE).

Puisqu'une partie significative des menaces qui pèsent sur la cybersécurité trouvent leur origine en dehors de l'Union, une approche cohérente de la coopération internationale s'impose. Cette directive constitue un modèle de référence à promouvoir dans le cadre de la coopération de l'Union avec des pays tiers, notamment lors de la fourniture d'une assistance technique externe.

## 2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

- **Base juridique**

La base juridique de la directive SRI est l'article 114 du traité sur le fonctionnement de l'Union européenne, dont l'objectif est la création et le fonctionnement du marché intérieur en renforçant les mesures relatives au rapprochement des règles nationales. Comme l'a jugé la Cour de justice de l'Union européenne dans son arrêt dans l'affaire C-58/08, Vodafone e.a., il est justifié de recourir à l'article 114 TFUE en cas de divergences entre les réglementations nationales qui ont une incidence directe sur le fonctionnement du marché intérieur. De même,

[2] COM(2020) 67 final.
[3] https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_FR.html
[4] https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/fr/pdf

la Cour a estimé que lorsqu'un acte fondé sur l'article 114 TFUE avait déjà éliminé tout obstacle aux échanges dans le domaine qu'il harmonise, le législateur de l'Union ne saurait être privé de la possibilité d'adapter cet acte à toute modification des circonstances ou à toute évolution des connaissances eu égard à la tâche qui lui incombe de veiller à la protection des intérêts généraux reconnus par le traité. Enfin, la Cour a jugé que les mesures relatives au rapprochement visées par l'article 114 TFUE étaient conçues pour laisser, en fonction du contexte général et des circonstances spécifiques de la matière à harmoniser, une marge d'appréciation quant à la technique de rapprochement la plus appropriée afin d'aboutir au résultat souhaité. L'acte juridique proposé éliminerait les obstacles au marché intérieur et améliorerait la création et le fonctionnement de celui-ci pour les entités essentielles et importantes, en créant des règles claires d'application générale relatives au champ d'application de la directive SRI et en harmonisant les règles applicables dans le domaine de la gestion des risques et du signalement des incidents de cybersécurité. Les disparités actuelles dans ce domaine, tant au niveau législatif qu'au niveau de la surveillance, à l'échelle nationale comme à l'échelle de l'Union sont des obstacles au marché intérieur car les entités qui exercent une activité transfrontalière sont confrontées à des exigences réglementaires différentes et pouvant se chevaucher (ou à une application de ces exigences qui diffère ou se chevauche), au détriment de l'exercice de leur liberté d'établissement et de prestation des services. Des règles différentes ont également une incidence négative sur les conditions de concurrence sur le marché intérieur lorsqu'il s'agit d'entités du même type de différents États membres.

- **Subsidiarité (en cas de compétence non exclusive)**

La résilience en matière de cybersécurité dans l'ensemble de l'Union ne peut être effective si elle est appréhendée de manière disparate sous l'effet de cloisonnements nationaux ou régionaux. La directive SRI a partiellement comblé cette lacune en établissant un cadre pour la sécurité des réseaux et des systèmes d'information au niveau national et au niveau de l'Union. Cependant, ses transpositions et mise en œuvre ont également mis en lumière les insuffisances intrinsèques et les limites de certaines dispositions ou approches, comme la délimitation peu claire du champ d'application de la directive, qui a entraîné d'importantes différences en ce qui concerne le degré et l'ampleur de l'intervention de l'Union, de fait, au niveau des États membres. De plus, avec la crise de la COVID-19, l'économie européenne dépend plus que jamais des réseaux et systèmes d'information et les secteurs et les services sont de plus en plus interconnectés. Une intervention de l'UE allant au-delà des mesures actuelles de la directive SRI se justifie principalement par: i) la nature de plus en plus transfrontalière des menaces et défis pour les SRI; ii) le potentiel de l'action de l'Union d'amélioration et de facilitation des politiques nationales efficaces et coordonnées; et iii) la contribution de mesures stratégiques concertées et collaboratives à la protection efficace des données et de la vie privée.

- **Proportionnalité**

Les règles proposées dans la présente directive ne vont pas au-delà de ce qui est nécessaire pour réaliser les objectifs spécifiques de manière satisfaisante. L'alignement et la rationalisation envisagés des mesures de sécurité et des obligations de signalement sont liés aux demandes d'amélioration du cadre actuel formulées par les États membres et les entreprises.

La présente proposition tient compte des pratiques qui existent déjà dans les États membres. Un niveau de protection amélioré obtenu grâce à des mesures et obligations rationalisées et

coordonnées est proportionné aux risques de plus en plus élevés rencontrés, notamment ceux comportant un élément transfrontalier; ces mesures et obligations sont raisonnables et correspondent de manière générale à l'intérêt des entités concernées consistant à assurer la continuité et la qualité de leurs services. Les coûts permettant d'assurer la coopération systématique entre les États membres sont peu élevés si on les compare aux pertes et dommages économiques et sociaux causés par les incidents de cybersécurité. De plus, les consultations des parties intéressées organisées dans le cadre de la révision de la directive SRI, y compris les résultats de la consultation publique ouverte et des enquêtes ciblées, ont montré que la révision de la directive SRI de la manière envisagée ci-dessus était favorablement perçue.

- **Choix de l'instrument**

Cette proposition renforcera la rationalisation des obligations incombant aux entreprises et garantira un niveau plus élevé d'harmonisation de ces obligations. Dans le même temps, elle a pour objectif de donner aux États membres la flexibilité nécessaire pour tenir compte des spécificités nationales (comme la possibilité de recenser des entités essentielles ou importantes supplémentaires, allant au-delà du niveau de référence défini par l'acte juridique). Le futur instrument juridique devrait donc prendre la forme d'une directive puisque cet instrument juridique permet de réaliser une harmonisation améliorée ciblée et laisse un certain degré de flexibilité aux autorités compétentes.

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

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

La Commission a réalisé une évaluation du fonctionnement de la directive SRI[5]. Elle en a analysé la pertinence, la valeur ajoutée pour l'Union européenne, la cohérence, l'efficacité et l'efficience. Les principales conclusions de cette analyse sont les suivantes:

- Le champ d'application de la directive SRI est trop limité en ce qui concerne les secteurs couverts, principalement en raison: i) de l'adoption croissante, ces dernières années, du format numérique et d'un degré accru d'interconnexion, ii) du fait que le champ d'application de la directive SRI ne reflète plus la totalité des secteurs numériques qui fournissent des services essentiels à l'économie et à la société dans son ensemble.
- La directive SRI n'est pas suffisamment claire en ce qui concerne la latitude des opérateurs de services essentiels et ses dispositions manquent de clarté quant à la compétence nationale sur les fournisseurs de services numériques. Cela a conduit à une situation dans laquelle certains types d'entités n'ont pas été recensés dans tous les États membres et n'ont donc pas été tenus de mettre en place des mesures de sécurité ni de signaler les incidents.
- La directive SRI laissait un large pouvoir d'appréciation aux États membres dans leur définition des exigences en matière de sécurité et de signalement des incidents applicables aux opérateurs de services essentiels (ci-après les «OSE»). L'évaluation montre que, dans certains cas, les États membres ont mis en place ces exigences de

[5] [Annexe 5 de l'analyse d'impact].

manières considérablement différentes, créant ainsi une charge supplémentaire pour les entreprises actives dans plusieurs États membres.

- Le système de surveillance et d'application de la directive SRI n'est pas efficace: par exemple, les États membres se sont montrés très réticents à appliquer des sanctions aux entités qui n'avaient pas mis en place les exigences en matière de sécurité ou qui n'ont pas signalé les incidents. Cela peut avoir des conséquences négatives pour la cyber-résilience des entités à titre individuel.
- Les ressources humaines et financières que les États membres ont affectées à l'accomplissement de leurs tâches (comme le recensement ou la surveillance des OSE) et, par conséquent, les différents niveaux de maturité du traitement des risques liés à la cybersécurité varient considérablement; des variations qui exacerbent encore les différences en matière de cyber-résilience entre les États membres.
- Les États membres ne partagent pas de manière systématique les informations entre eux, ce qui a des conséquences négatives sur, notamment, l'efficacité des mesures de cybersécurité et le niveau de prise de conscience conjointe de la situation au niveau de l'Union. Il en va de même pour le partage d'informations entre entités privées, ainsi que pour les liens entre les structures de coopération au niveau de l'Union et les entités privées.

- **Consultations des parties intéressées**

La Commission a consulté un large éventail de parties intéressées. Les États membres et les parties intéressées ont été invités à participer à la consultation publique ouverte ainsi qu'aux enquêtes et aux ateliers organisés par le cabinet Wavestone, le think tank CEPS et l'organisme de recherche politique ICF, auxquels la Commission avait commandé une étude visant à étayer le processus de révision de la directive SRI. Les parties intéressées consultées incluaient les autorités compétentes, les organismes de l'Union chargés de la cybersécurité, les opérateurs de services essentiels, les fournisseurs de service numérique, les entités fournissant des services ne relevant pas de la directive SRI actuelle, les associations professionnelles, les associations de consommateurs et les citoyens.

De plus, la Commission est restée en permanence en contact avec les autorités compétentes chargées de la mise en œuvre de la directive SRI. Le groupe de coopération a largement couvert les différents aspects transversaux et sectoriels de la mise en œuvre. Enfin, au cours de ses «visites SRI» dans les pays en 2019 et en 2020, la Commission a interrogé 154 entités publiques et privées ainsi que 117 autorités compétentes.

- **Obtention et utilisation d'expertise**

La Commission a confié à un consortium formé du cabinet Wavestone, du think tank CEPS et de l'organisme de recherche politique ICF la mission de l'aider dans son processus de révision de la directive SRI[6]. Le consortium missionné ne s'est pas contenté de se rapprocher des parties intéressées directement touchées par la directive SRI à l'aide d'enquêtes ciblées et d'ateliers: il a également consulté un large éventail d'experts dans le domaine de la cybersécurité, comme des chercheurs en cybersécurité et des professionnels du secteur de la cybersécurité.

[6] Étude visant à étayer la révision de 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 (directive SRI) - nº 2020-665. Wavestone, CEPS et ICF.

- **Analyse d'impact**

La présente proposition s'accompagne d'une analyse d'impact[7], qui a été soumise au comité d'examen de la réglementation (CER) le 23 octobre 2020, qui a rendu un avis positif assorti de commentaires le 20 novembre 2020. Le CER a recommandé que des améliorations soient apportées dans certains domaines, et ce afin de: 1) mieux tenir compte du rôle joué par les retombées transfrontières dans l'analyse des problèmes; 2) mieux expliquer ce en quoi consisterait une réussite pour cette initiative si elle aboutissait; 3) davantage justifier la liste des options stratégiques; 4) donner davantage de détails concernant les coûts des mesures proposées. L'analyse d'impact a été corrigée pour tenir compte de ces points ainsi que des commentaires plus détaillés formulés par le CER. Elle comprend désormais des explications plus détaillées sur le rôle joué par les retombées transfrontières dans le domaine de la cybersécurité, un aperçu plus clair de la manière dont la réussite peut être mesurée, une explication plus détaillée de la conception et de la logique sous-tendant les différentes options stratégiques et les actions envisagées dans le cadre de ces options, une explication plus détaillée des aspects analysés en lien avec la portée sectorielle de la directive SRI et davantage de précisions concernant les coûts.

La Commission a envisagé un certain nombre d'options stratégiques pour améliorer le cadre juridique dans le domaine de la cyber-résilience et de la réaction aux incidents:

- «Ne rien changer»: la directive SRI ne serait pas modifiée et aucune autre mesure de nature non législative ne serait adoptée afin de résoudre les problèmes constatés lors de l'évaluation de la directive SRI.
- Option nº 1: il n'y aurait aucun changement au niveau législatif. La Commission formulerait des recommandations et des lignes directrices (par exemple concernant le recensement des opérateurs de services essentiels, les exigences en matière de sécurité, les procédures de notification des incidents et la surveillance), après avoir consulté le groupe de coopération, l'agence de l'Union européenne pour la cybersécurité (agence européenne chargée de la sécurité des réseaux et de l'information, ENISA) et, le cas échéant, le réseau des équipes d'intervention en cas d'urgence informatique (CSIRT).
- Option nº 2: cette option comprend des modifications ciblées de la directive SRI, notamment une extension de son champ d'application et plusieurs autres modifications qui auraient pour objectif de garantir des solutions immédiates aux problèmes constatés, d'apporter plus de clarté et de renforcer l'harmonisation (par exemple des dispositions visant à harmoniser les seuils de recensement). La directive SRI conserverait cependant ses principaux piliers, son approche et sa motivation.
- Option nº 3: ce scénario implique des modifications systémiques et structurelles de la directive SRI (au moyen d'une nouvelle directive) et prévoit un changement d'approche plus fondamental, consistant à couvrir un segment plus large des économies de l'Union, à l'aide d'une surveillance plus ciblée visant les acteurs clés et essentiels. Il rationaliserait également les obligations imposées aux entreprises et garantirait un niveau plus élevé d'harmonisation de ces obligations, créerait un cadre plus efficace pour les aspects opérationnels et établirait une base claire pour renforcer

[7] **[Liens vers le document final et la fiche de synthèse à ajouter].**

le partage des responsabilités et la reddition de compte des différentes parties intéressées concernant les mesures de cybersécurité.

L'analyse d'impact a conclu que l'option privilégiée était l'option 3 (c'est-à-dire les modifications systémiques et structurelles du cadre des SRI). En matière d'efficacité, l'option privilégiée déterminerait clairement le champ d'application de la directive SRI, étendu à une fraction plus représentative des économies et des sociétés de l'Union, ainsi que la rationalisation des exigences, assorti d'un cadre plus défini pour la surveillance et l'application qui aurait pour objectif d'accroître le niveau de conformité. Elle impliquerait également des mesures visant à améliorer les approches de conceptions des politiques au niveau des États membres et à en modifier le paradigme, à promouvoir de nouveaux cadres pour la gestion des risques liés aux relations avec les fournisseurs et la divulgation coordonnée des vulnérabilités. Dans le même temps, l'option stratégique privilégiée créée une base claire pour les responsabilités et les obligations de rendre compte partagées et envisage des mécanismes dont l'objectif est de renforcer la confiance entre les États membres, tant au niveau des autorités qu'au niveau du secteur, de favoriser le partage d'informations et de garantir une approche plus opérationnelle, comme les mécanismes d'assistance mutuelle et d'évaluation par les pairs. Cette option créerait également un cadre de gestion de crise au niveau de l'Union, tirant parti du réseau opérationnel de l'Union récemment lancé, et garantirait un dialogue renforcé avec l'ENISA dans le cadre de son mandat actuel, permettant ainsi d'avoir une vue d'ensemble précise de l'état de la cybersécurité dans l'Union.

En ce qui concerne l'efficience, même si l'option privilégiée entraînait des coûts de conformité et d'application supplémentaires pour les entreprises et les États membres, elle conduirait également à des compromis et des synergies efficaces, le meilleur potentiel de toutes les options stratégiques étant analysé pour garantir un niveau accru et cohérent de cyber-résilience des entités clés dans l'ensemble de l'Union, ce qui engendrerait à terme des économies tant pour les entreprises que pour la société. Cette option stratégique entraînerait une certaine charge administrative supplémentaire et des coûts de mise en conformité supplémentaires pour les autorités des États membres. Cependant, en définitive, sur le moyen et le long terme, elle donnerait également lieu à des bénéfices considérables grâce à l'amélioration de la coopération entre les États membres, notamment au niveau opérationnel, et facilitant, grâce aux mécanismes d'assistance mutuelle et d'évaluation par les pairs, une meilleure vue d'ensemble des entreprises clés et de meilleures interactions avec celles-ci, et une amélioration générale des capacités de cybersécurité au niveau national et régional. L'option stratégique privilégiée garantirait également dans une large mesure la cohérence avec d'autres actes législatifs, initiatives ou mesures politiques, notamment une lex specialis sectorielle.

Les lacunes qui persistent actuellement en ce qui concerne la préparation des États membres comme des entreprises et des autres organisations en matière de cybersécurité seraient comblées, produisant des gains d'efficacité ainsi qu'une réduction des coûts supplémentaires générés par les incidents de cybersécurité.

- Pour les entités essentielles et importantes, le relèvement du niveau de préparation à la cybersécurité pourrait aboutir à une atténuation des éventuelles pertes de revenu dues aux perturbations, notamment à l'espionnage industriel, et pourrait réduire les dépenses considérables résultant de l'atténuation ad hoc des menaces. Il est probable que ces bénéfices l'emportent sur les coûts d'investissement nécessaires. La réduction de la fragmentation du marché intérieur égaliserait les conditions de concurrence entre les opérateurs.

- En ce qui concerne les États membres, cette option pourrait réduire encore le risque d'une augmentation des dépenses budgétaires consacrées à l'atténuation ad hoc des risques et des coûts supplémentaires entraînés par les cas d'urgence liés aux incidents de cybersécurité.
- En ce qui concerne les citoyens, la réponse aux incidents de cybersécurité devrait entraîner une réduction des pertes de revenus dues aux perturbations économiques.

Les niveaux renforcés de cybersécurité dans les États membres et de la capacité des entreprises et des autorités à réagir rapidement à un incident et à en mitiger les conséquences conduiront très probablement à accroître la confiance généralement accordée par les citoyens à l'économie numérique, ce qui pourrait avoir une incidence positive sur la croissance et sur les investissements.

L'amélioration du niveau global de cybersécurité devrait mener à une meilleure sécurité générale et à un fonctionnement harmonieux et ininterrompu des services essentiels, qui sont cruciaux pour la société. Cette initiative pourrait également contribuer à d'autres incidences sociales, comme la baisse du niveau de cybercriminalité et du terrorisme et une meilleure protection civile. Le relèvement du niveau de préparation des entreprises et des autres organisations face aux défis posés par le cyberespace pourrait permettre d'éviter d'éventuelles pertes financières dues à des cyberattaques, et empêcher ainsi de devoir licencier des salariés.

Le relèvement du niveau global de cybersécurité pourrait aussi conduire à la prévention de risques ou dommages environnementaux en cas d'attaque visant un service essentiel. Cela serait tout particulièrement valable pour les secteurs de l'énergie, de la fourniture et de la distribution d'eau et des transports. En renforçant les capacités en matière de cybersécurité, cette initiative pourrait conduire à un recours accru aux infrastructures et services de technologies de l'information et de la communication (TIC) de dernière génération, qui sont également plus durables d'un point de vue environnemental, et au remplacement d'anciennes infrastructures inefficaces et moins sûres. Cette option vise également à contribuer à la réduction du nombre de cyber-incidents coûteux, libérant ainsi des ressources pour réaliser des investissements durables.

- **Réglementation affûtée et simplification**

Cette proposition prévoit une exclusion générale des microentités et des entités de petite taille du champ d'application de la directive SRI et l'application d'un régime de surveillance ex post allégé à un grand nombre des nouvelles entités visées par le champ d'application révisé (dites «entités importantes»). Ces mesures ont pour objectif de minimiser et d'équilibrer la charge pesant sur les entreprises et les administrations publiques. De plus, cette proposition remplace le système complexe de recensement des opérateurs de services essentiels par une obligation d'application générale, et introduit un niveau plus élevé d'harmonisation des obligations de sécurité et de signalement, ce qui permettrait de réduire la charge de mise en conformité, notamment pour les entités fournissant des services transfrontaliers.

Elle réduit au minimum les coûts de mise en conformité pour les PME puisque les entités sont tenues d'adopter uniquement les mesures nécessaires pour garantir un niveau de sécurité des réseaux et des systèmes d'information adapté au risque existant.

- **Droits fondamentaux**

L'Union européenne a la volonté de respecter des normes élevées de protection des droits fondamentaux. Tous les accords de partage volontaire d'informations entre les visées par la

présente directive devraient être exécutés dans des environnements de confiance, dans le strict respect des règles de l'Union en matière de protection des données, notamment le règlement (UE) 2016/679 du Parlement européen et du Conseil[8].

## 4. INCIDENCE BUDGÉTAIRE

*Voir la fiche financière*

## 5. AUTRES ÉLÉMENTS

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

La présente proposition prévoit un plan général de suivi et d'évaluation des incidences sur les objectifs spécifiques. La Commission sera ainsi tenue de procéder à un réexamen au minimum [54 mois] après la date d'entrée en vigueur, et de rendre compte de ses principales conclusions au Parlement européen et au Conseil.

Ce réexamen sera réalisé conformément aux lignes directrices de la Commission pour une meilleure réglementation.

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

Cette proposition s'articule autour de plusieurs grands domaines d'action, qui sont interconnectés et ont pour objet de relever le niveau de cybersécurité dans l'Union.

Objet et champ d'application (article 1er et article 2)

Plus particulièrement, cette directive: a) fait obligation aux États membres d'adopter une stratégie nationale de cybersécurité, de désigner des autorités nationales compétentes, des points de contact uniques et des équipes de réponse aux incidents de sécurité informatique (CSIRT); b) dispose que les États membres définissent les obligations en matière de gestion et de signalement des risques de cybersécurité qui incombent aux entités appelées «entités essentielles» à l'annexe I et «entités importantes» à l'annexe II; c) dispose que les États membres définissent les obligations relatives au partage d'informations en matière de cybersécurité.

Elle s'applique à certaines entités essentielles publiques ou privées actives dans les secteurs énumérés à l'annexe I (énergie; transports; secteur bancaire; infrastructures des marchés financiers; santé; eau potable; eaux usées; infrastructure numérique; administration publique et espace) et à certaines entités importantes actives dans les secteurs énumérés à l'annexe II (services postaux et de courrier; gestion des déchets; fabrication, production et distribution de produits chimiques; production, transformation et distribution des denrées alimentaires; fabrication et fournisseurs numériques). Les microentités et les entités de petite taille au sens de la recommandation 2003/361/CE de la Commission du 6 mai 2003 sont exclues du champ d'application de la directive, à l'exception des fournisseurs de réseaux de communications électroniques ou de services de communications électroniques accessibles au public, des prestataires de services de confiance, des registres des noms de domaines de premier niveau (*top level domain(s)*, TLD) et de l'administration publique de ces types de domaines, ainsi

[8] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

que de certaines autres entités, comme le fournisseur exclusif d'un service dans un État membre.

Cadres nationaux de cybersécurité (articles 5 à 11)

Les États membres sont tenus d'adopter une stratégie nationale en matière de cybersécurité qui définit les objectifs stratégiques et les mesures politiques et réglementaires appropriées, en vue de parvenir à un niveau élevé de cybersécurité et de le maintenir.

La directive créé également un cadre pour la divulgation coordonnée des vulnérabilités et impose aux États membres de désigner des CSIRT qui agiront en tant qu'intermédiaires de confiance et faciliteront les interactions entre les entités effectuant le signalement et les fabricants ou les fournisseurs de produits TIC et de services TIC. L'ENISA est tenue de produire et de tenir à jour un registre européen des vulnérabilités recensant les vulnérabilités constatées.

Les États membres sont tenus de mettre en place des cadres nationaux de gestion de crise dans le domaine de la cybersécurité, notamment en désignant les autorités nationales compétentes chargées de gérer les incidents et crises de grande ampleur en matière de cybersécurité.

Les États membres sont également tenus de désigner une ou plusieurs autorités nationales compétentes en matière de cybersécurité, auxquelles seront confiées des missions de surveillance au titre de la présente directive ainsi qu'un point de contact national unique pour toutes les questions de cybersécurité, qui exercera une fonction de liaison pour assurer la coopération transfrontalière entre les autorités compétentes des États membres. Les États membres sont également tenus de désigner des CSIRT.

Coopération (articles 12 à 16)

La directive crée un groupe de coopération afin de soutenir et faciliter la coopération stratégique et l'échange d'informations entre les États membres et de renforcer la confiance. Elle établit également un réseau des CSIRT afin de contribuer au renforcement de la confiance entre les États membres et de promouvoir une coopération opérationnelle rapide et effective.

Un réseau européen pour la préparation et la gestion des crises cyber par les États membres (UE-CyCLONe – *Cyber Crises Liaison Organisation Network*) est institué afin de contribuer à la gestion coordonnée des incidents et crises de grande ampleur en matière de cybersécurité, et de garantir l'échange régulier d'informations entre les États membres et les institutions, organes et agences de l'Union.

L'ENISA est tenue de produire, en coopération avec la Commission, un rapport bisannuel sur l'état de la cybersécurité dans l'Union.

La Commission est tenue de mettre en place un système d'évaluation par les pairs, permettant de soumettre les politiques de cybersécurité des États membres à un examen collégial périodique pour en contrôler l'efficacité.

Obligations en matière de gestion et de signalement des risques de cybersécurité (articles 17 à 23)

La directive impose aux États membres de s'assurer que les organes de direction de toutes les entités relevant de son champ d'application approuvent les mesures de gestion des risques en matière de cybersécurité adoptées respectivement par ces entités, et qu'ils suivent une formation aux questions de cybersécurité spécifiquement.

Les États membres sont tenus de veiller à ce que les entités relevant du champ d'application de la directive prennent les mesures techniques et organisationnelles nécessaires et proportionnées pour gérer les risques de cybersécurité qui menacent la sécurité des réseaux et des systèmes d'information. Ils sont également tenus de veiller à ce que les entités notifient aux autorités nationales compétentes ou aux CSIRT les incidents de cybersécurité qui ont des effets significatifs sur la prestation des services qu'ils fournissent.

Les registres des noms de domaines de premier niveau ainsi que les entités qui fournissent des services d'enregistrement de noms de domaines de premier niveau collectent et conservent des données d'enregistrement de noms de domaines exactes et complètes. De plus, ces entités sont tenues de donner un accès efficace aux données d'enregistrement de noms de domaines aux demandeurs d'accès légitimes.

Compétence et enregistrement (articles 24 et 25)

De manière générale, les entités essentielles et importantes sont réputées relever de la compétence de l'État membre dans lequel elles fournissent leurs services. Cependant, certains types d'entités (fournisseurs de services DNS, registres de noms de domaines de premier niveau, fournisseurs de services d'informatique en nuage, fournisseurs de services de centres de données et fournisseurs de réseaux de diffusion de contenu, ainsi que certains fournisseurs numériques) sont réputés relever la compétence de l'État membre dans lequel se trouve leur établissement principal dans l'Union. Cela permet de garantir que ces entités ne se retrouvent pas confrontées à une multitude d'exigences juridiques différentes alors qu'elles fournissent des services transfrontières dans une mesure particulièrement importante. L'ENISA est tenue de créer et de tenir à jour un registre de ces entités.

Partage d'informations (articles 26 et 27)

Les États membres adoptent des règles permettant aux entités de partager des informations en matière de cybersécurité dans le cadre d'accords spécifiques de partage d'informations en matière de cybersécurité, conformément à l'article 101 TFUE. De plus, les États membres permettent aux entités ne relevant pas du champ d'application de la présente directive de signaler, à titre volontaire, les incidents importants, les cybermenaces ou les incidents évités.

Surveillance et exécution (articles 28 à 34)

Les autorités compétentes sont tenues de surveiller les entités qui relèvent du champ d'application de la directive, et notamment de s'assurer qu'elles respectent les exigences en matière de sécurité et de notification des incidents. La directive établit une distinction entre un régime de surveillance ex ante pour les entités essentielles et un régime de surveillance ex post pour les entités importantes, le second nécessitant que les autorités compétentes adoptent des mesures lorsque, selon les éléments de preuve ou les indications qui leur sont communiqués, une entité importante ne respecte pas les exigences en matière de sécurité et de notification des incidents.

Elle demande également aux États membres d'imposer des amendes administratives aux entités essentielles et importantes et définit le montant maximal de certaines amendes.

Les États membres sont tenus de coopérer et de se prêter mutuellement assistance si nécessaire lorsque des entités fournissent des services dans plusieurs États membres ou lorsque l'établissement principal ou le représentant d'une entité se trouve dans un certain État membre alors que ses réseaux et systèmes d'information sont situés dans un ou plusieurs autres États membres.

2020/0359 (COD)

Proposition de

**DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL**

**concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148**

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

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 114, considérant ce qui suit:

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen[9],

vu l'avis du Comité des régions[10],

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(1) la directive (UE) 2016/1148 du Parlement européen et du Conseil[11] avait pour objectif de créer des capacités en matière de cybersécurité dans toute l'Union, d'atténuer les menaces pesant sur les réseaux et les systèmes d'information servant à fournir des services essentiels dans des secteurs clés et d'assurer la continuité de ces services en cas d'incidents de cybersécurité, contribuant ainsi au fonctionnement efficace de l'économie et de la société de l'Union.

(2) Depuis l'entrée en vigueur de la directive (UE) 2016/1148, des progrès significatifs ont été réalisés concernant l'amélioration du niveau de cyber-résilience de l'Union. Le réexamen de cette directive a montré qu'elle avait joué le rôle de catalyseur dans l'approche institutionnelle et réglementaire de la cybersécurité dans l'Union, ouvrant la voie à une évolution importante des mentalités. Cette directive a veillé à ce que les cadres nationaux soient achevés en définissant des stratégies nationales en matière de cybersécurité, en créant des capacités nationales et en mettant en œuvre des mesures réglementaires couvrant les infrastructures et les acteurs essentiels recensés par chacun des États membres. Elle a également contribué à la coopération au niveau de l'Union par la création du groupe de coopération[12] et du réseau des centres de réponse aux

---

9 JO C du , p. .

10 JO C du , p. .

11 Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (JO L 194/1 du 19.7.2016, p. 1).

12 Article 11 de la directive (UE) 2016/1148.

incidents de sécurité informatique (ci-après le «réseau des CSIRT»)[13]. En dépit de ces accomplissements, le réexamen de la directive (UE) 2016/1148 a montré que certaines insuffisances intrinsèques l'empêchaient de répondre efficacement aux défis actuels et émergents liés à la cybersécurité.

(3) Les réseaux et systèmes d'information sont devenus une caractéristique essentielle de la vie quotidienne en raison de la transformation numérique rapide et de l'interconnexion de la société, notamment dans le cadre des échanges transfrontières. Cette évolution a conduit à une expansion du paysage des menaces qui pèsent sur la cybersécurité et à l'émergence de nouveaux défis, qui nécessitent des réponses adaptées, coordonnées et novatrices dans tous les États membres. Le nombre, l'ampleur, la sophistication, la fréquence et les effets des incidents de cybersécurité ne cessent de croître et représentent une menace considérable pour le fonctionnement des réseaux et des systèmes d'information. En conséquence, les incidents de cybersécurité peuvent nuire à la poursuite des activités économiques sur le marché intérieur, entraîner des pertes financières importantes, entamer la confiance des utilisateurs et causer un préjudice majeur à l'économie et la société de l'Union. La préparation à la cybersécurité et l'effectivité de la cybersécurité sont dès lors plus importantes que jamais pour le bon fonctionnement du marché intérieur.

(4) La base juridique de la directive (UE) 2016/1148 était l'article 114 du traité sur le fonctionnement de l'Union européenne (TFUE), dont l'objectif est la création et le fonctionnement du marché intérieur par l'amélioration de mesures pour le rapprochement des règles nationales. Les exigences en matière de cybersécurité imposées aux entités fournissant des services ou des activités pertinentes d'un point de vue économique varient grandement d'un État membre à l'autre en ce qui concerne le type d'exigence, le niveau de précision et la méthode de surveillance: ces disparités entraînent des coûts supplémentaires et créent des difficultés pour les entreprises qui fournissent des biens ou des services en mode transfrontière. Les exigences imposées par un État membre et qui diffèrent des exigences imposées par un autre État membre, voire qui les contredisent, peuvent avoir une incidence considérable sur ces activités transfrontières. De surcroît, il est probable qu'une conception ou une mise en œuvre sous-optimales des normes de cybersécurité dans un État membre ait des répercussions sur le niveau de cybersécurité d'un autre État membre, notamment en raison des échanges transfrontières intenses. Le réexamen de la directive (UE) 2016/1148 a montré l'existence de fortes divergences dans sa mise en œuvre par les États membres, notamment eu égard à son champ d'application, dont la délimitation a dans une grande mesure été laissée à l'appréciation des États membres. La directive (UE) 2016/1148 laissait également un large pouvoir d'appréciation aux États membres en ce qui concerne la mise en œuvre des obligations qu'elle prévoyait en matière de sécurité et de signalement des incidents: partant, ces obligations ont été mises en œuvre de manières considérablement différentes au niveau national. Des divergences de mise en œuvre similaires ont été constatées s'agissant des dispositions de cette directive relatives à la surveillance et à l'application.

(5) L'ensemble de ces divergences donnent lieu à une fragmentation du marché intérieur et sont susceptibles de produire un effet nuisible sur le fonctionnement de celui-ci, affectant plus particulièrement la fourniture transfrontière de services et le niveau de cyber-résilience en raison de l'adoption de normes différentes. La présente directive a

[13] Article 12 de la directive (UE) 2016/1148.

pour objectif de supprimer ces divergences importantes entre les États membres, notamment en définissant des règles minimales concernant le fonctionnement d'un cadre réglementaire coordonné, en établissant des mécanismes permettant une coopération efficace entre les autorités compétentes de chaque État membre, en mettant à jour la liste des secteurs et activités soumis à des obligations en matière de cybersécurité, et en prévoyant des recours et des sanctions effectifs qui sont essentiels à l'application effective de ces obligations. Il convient, par conséquent, que la directive (UE) 2016/1148 soit abrogée et remplacée par la présente directive.

(6) La présente directive ne modifie pas la possibilité donnée à chaque État membre d'adopter les mesures nécessaires pour garantir la protection des intérêts essentiels de sa sécurité, assurer l'action publique et la sécurité publique et permettre la détection d'infractions pénales et les enquêtes et poursuites en la matière, dans le respect du droit de l'Union. Conformément à l'article 346 du TFUE, aucun État membre n'est tenu de fournir des renseignements dont la divulgation serait contraire aux intérêts essentiels de sa sécurité intérieure. À cet égard, les règles nationales et de l'Union visant à protéger les informations classifiées, les accords de non-divulgation et les accords informels de non-divulgation, tels que le protocole d'échange d'information «Traffic Light Protocol»[14], sont pertinentes.

(7) Avec l'abrogation de la directive (UE) 2016/1148, le champ d'application par secteur devrait être étendu à une plus grande partie de l'économie au regard des considérations exposées aux considérants 4 à 6. Les secteurs couverts par la directive (UE) 2016/1148 devraient dès lors être étendus pour assurer une couverture complète des secteurs et des services revêtant une importance cruciale pour les activités économiques et sociales essentielles au sein du marché intérieur. Les règles ne devraient pas être différentes selon que les entités sont des opérateurs de services essentiels ou des fournisseurs de services numériques: cette différenciation s'est avérée obsolète puisqu'elle ne reflète pas l'importance réelle des secteurs ou des services pour les activités économiques et sociales sur le marché intérieur.

(8) Conformément à la directive (UE) 2016/1148, les États membres étaient chargés de déterminer quelles entités remplissaient les critères établis pour être qualifiées d'opérateurs de services essentiels (ci-après le «processus d'identification»). Afin d'éliminer les divergences importantes entre les États membres à cet égard et de garantir la sécurité juridique concernant les exigences de gestion des risques et les obligations de signalement pour toutes les entités concernées, il convient d'établir un critère uniforme déterminant les entités qui relèvent du champ d'application de la présente directive. Ce critère devrait consister en l'application de la règle du plafond, en vertu de laquelle toutes les entreprises de taille moyenne et de grande taille, au sens de la recommandation 2003/361/CE de la Commission[15], actives dans les secteurs ou fournissant le type de services couverts par la présente directive relèvent de son champ d'application. Les États membres ne devraient pas être tenus de dresser la liste des entités qui remplissent ce critère d'application générale portant sur la taille.

---

14 Le protocole «Traffic Light Protocol» permet à une personne partageant des informations d'indiquer à son public des limitations applicables à la diffusion plus large de ces informations: il est utilisé par la quasi-totalité des communautés des CSIRT et par certains centres d'échange et d'analyse d'informations (ISAC).

15 Recommandation 2003/361/EC de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises (JO L 124 du 20.5.2003, p. 36).

(9) Toutefois, les microentités ou les entités de petite taille qui remplissent certains critères indiquant qu'elles jouent un rôle essentiel pour les économies ou les sociétés des États membres ou pour des secteurs ou des types de services particuliers devraient également être couvertes par la présente directive, et les États membres devraient être chargés d'établir une liste de ces entités, et de la transmettre à la Commission.

(10) La Commission, en coopération avec le groupe de coopération, peut publier des lignes directrices concernant la mise en œuvre des critères applicables aux microentreprises et aux entreprises de petite taille.

(11) En fonction du secteur dans lequel elles sont actives ou du type de services qu'elles fournissent, les entités qui relèvent du champ d'application de la présente directive devraient être classées en deux catégories: entités essentielles et entités importantes. Cette catégorisation devrait tenir compte du niveau de criticité du secteur ou du type de services, ainsi que du niveau de dépendance des autres secteurs ou types de services. Les entités tant essentielles qu'importantes devraient être soumises aux mêmes exigences en matière de gestion des risques et obligations de signalement. Les régimes de surveillance et de sanction applicables à ces deux catégories d'entités devraient être différenciés afin de garantir un juste équilibre entre les exigences et les obligations, d'une part, et la charge administrative qui découle du contrôle de la conformité, d'autre part.

(12) La législation et les instruments sectoriels peuvent contribuer à garantir des niveaux élevés de cybersécurité tout en tenant pleinement compte du caractère spécifique et complexe de ces secteurs. Lorsqu'un acte juridique sectoriel de l'Union impose aux entités essentielles ou importantes d'adopter des mesures de gestion des risques en matière de cybersécurité ou de notifier des incidents ou des cybermenaces importantes et que cette obligation produit un effet au moins équivalent à celui des obligations prévues par la présente directive, il convient d'appliquer ces dispositions sectorielles, y compris en matière de surveillance et d'application. La Commission peut publier des lignes directrices relatives à la mise en œuvre de la lex specialis. La présente directive n'empêche pas l'adoption d'actes sectoriels de l'Union supplémentaires prévoyant des mesures de gestion des risques en matière de cybersécurité et la notification des incidents. La présente directive est sans préjudice des compétences de mise en œuvre existantes qui ont été conférées à la Commission dans un certain nombre de secteurs, notamment les transports et l'énergie.

(13) Le règlement XXXX/XXXX du Parlement européen et du Conseil[16] devrait être considéré comme un acte juridique sectoriel de l'Union en lien avec la présente directive en ce qui concerne les entités du secteur financier. Les dispositions du règlement XXXX/XXXX portant sur les mesures de gestion des risques concernant les technologies de l'information et de la communication (TIC), la gestion des risques liés aux TIC et notamment le signalement des incidents, ainsi que sur le test de la résilience opérationnelle numérique, les accords de partage d'informations et les risques liés aux tiers en matière de TIC devraient s'appliquer au lieu de celles prévues par la présente directive. Les États membres ne devraient par conséquent pas appliquer les dispositions de la présente directive concernant la gestion des risques de cybersécurité et les obligations de signalement, le partage d'informations et la surveillance et l'application aux entités financières couvertes par le règlement XXXX/XXXX. Dans le même temps, il est important de conserver une relation forte

[16] *[insérer le titre complet et la référence de la publication au JO lorsqu'elle est connue]*

et de maintenir le partage d'informations avec le secteur financier dans le cadre de la présente directive. À cet effet, le règlement XXXX/XXXX permet à l'ensemble des autorités de surveillance financière, des autorités européennes de surveillance (AES) pour le secteur financier et des autorités nationales compétentes au titre du règlement XXXX/XXXX de participer aux discussions sur les politiques stratégiques et aux travaux techniques du groupe de coopération, ainsi que d'échanger des informations et de coopérer avec les points de contact uniques désignés en vertu de la présente directive et avec les CSIRT nationaux. Les autorités compétentes en vertu du règlement XXXX/XXXX devraient également communiquer les détails des incidents importants liés aux TIC aux points de contact uniques désignés en vertu de la présente directive. De plus, les États membres devraient continuer de couvrir le secteur financier dans leurs stratégies de cybersécurité et les CSIRT nationaux peuvent inclure le secteur financier dans leurs activités.

(14) Vu les liens qui existent entre la cybersécurité et la sécurité physique des entités, il convient d'assurer la cohérence des approches entre la directive (UE) XXXX/XXXX du Parlement européen et du Conseil[17] et la présente directive. À cet effet, les États membres devraient veiller à ce que les entités critiques et les entités équivalentes, au titre de la directive (UE) XXXX/XXXX, soient considérées comme des entités essentielles en vertu de la présente directive. Les États membres devraient également veiller à ce que leurs stratégies de cybersécurité prévoient un cadre politique pour une coordination renforcée entre l'autorité compétente en vertu de la présente directive et l'autorité compétente en vertu de la directive (UE) XXXX/XXXX dans le cadre du partage d'informations relatives aux incidents et aux cybermenaces ainsi que de l'exercice des tâches de surveillance. Les autorités en vertu des deux directives devraient coopérer et échanger des informations, notamment en ce qui concerne le recensement des entités critiques, les cybermenaces, les risques en matière de cybersécurité, les incidents affectant les entités critiques ainsi que les mesures de cybersécurité adoptées par les entités critiques. Sur demande des autorités compétentes au titre de la directive (UE) XXX/XXX, les autorités compétentes au titre de la présente directive devraient être autorisées à exercer leurs pouvoirs de surveillance et d'exécution sur une entité essentielle définie comme critique. Les deux autorités devraient coopérer et échanger des informations à cette fin.

(15) Le fait de maintenir et préserver un système de noms de domaines (DNS) fiable, résilient et sécurisé constitue un facteur crucial pour la protection de l'intégrité d'internet et est essentiel à son fonctionnement continu et stable, dont dépendent l'économie numérique et la société. Par conséquent, la présente directive devrait s'appliquer à tous les fournisseurs de services DNS, y compris les opérateurs de serveurs racines de noms de domaines, aux serveurs de noms de domaines de premier niveau (TLD), aux serveurs d'autorité pour les noms de domaines et aux résolveurs récursifs.

(16) Les services d'informatique en nuage devraient couvrir les services qui permettent l'accès sur demande et l'accès large à distance à un ensemble modulable et variable de ressources informatiques distribuées et pouvant être partagées. Ces ressources informatiques comprennent des ressources telles que les réseaux, les serveurs ou les autres infrastructures, les systèmes d'exploitation, les logiciels, le stockage, les applications et les services. Les modèles de déploiement de l'informatique en nuage

[17] *[insérer le titre complet et la référence de la publication au JO lorsqu'elle est connue]*

devraient inclure les modèles privés, communautaires, publics et hybrides en nuage. Les services et modèles de déploiement susmentionnés revêtent le même sens que celui des conditions de service et des modèles de déploiement défini dans la norme ISO/CEI 17788:2014. La capacité des utilisateurs de l'informatique en nuage de s'autofournir unilatéralement des capacités informatiques, comme du temps de serveur ou du stockage en réseau, sans aucune intervention humaine de la part du fournisseur de service d'informatique en nuage pourrait être décrite comme une gestion sur demande. Le terme «accès large à distance» est utilisé pour décrire le fait que les capacités en nuage sont fournies sur le réseau et que l'accès à celles-ci se fait par des mécanismes encourageant le recours à des plateformes clients légères ou lourdes disparates (y compris les téléphones mobiles, les tablettes, les ordinateurs portables et les postes de travail). Le terme «modulable» renvoie aux ressources informatiques qui sont attribuées d'une manière souple par le fournisseur de services en nuage, indépendamment de la localisation géographique de ces ressources, pour gérer les fluctuations de la demande. Les termes «ensemble variable» sont utilisés pour décrire les ressources informatiques qui sont mobilisées et libérées en fonction de la demande pour pouvoir augmenter ou réduire rapidement les ressources disponibles en fonction de la charge de travail. Les termes «pouvant être partagées» sont utilisés pour décrire les ressources informatiques qui sont mises à disposition de nombreux utilisateurs qui partagent un accès commun au service, le traitement étant effectué séparément pour chaque utilisateur bien que le service soit fourni à partir du même équipement électronique. Le terme «distribué» est utilisé pour décrire les ressources informatiques qui se trouvent sur des ordinateurs ou des appareils en réseau différents, qui communiquent et se coordonnent par transmission de messages.

(17) Vu l'émergence de technologies innovantes et de nouveaux modèles commerciaux, de nouveaux modèles de déploiement et de service d'informatique en nuage devraient apparaître sur le marché en cause en réaction aux besoins changeants des clients. Dans un tel contexte, les services d'informatique en nuage peuvent être fournis sous une forme extrêmement distribuée, toujours plus près de l'endroit où les données sont générées ou collectées, entraînant ainsi une transition du modèle traditionnel vers un modèle très distribué (le traitement des données à la périphérie, ou «edge computing»).

(18) Les services proposés par les fournisseurs de services de centre de données ne sont pas toujours fournis sous la forme de service d'informatique en nuage. En conséquence, les centres de données ne font pas toujours partie d'une infrastructure d'informatique en nuage. Afin de gérer l'ensemble des risques qui menacent la sécurité des réseaux et des systèmes d'information, la présente directive devrait également couvrir les fournisseurs de services de centres de données qui ne sont pas des services d'informatique en nuage. Aux fins de la présente directive, le terme «service de centre de données» devrait couvrir la fourniture d'un service qui englobe les structures, ou les groupes de structures, dédiées à l'hébergement, l'interconnexion et l'exploitation centralisés des équipements de traitement de l'information et de réseau fournissant des services de stockage, de traitement et de transport des données, ainsi que l'ensemble des installations et des infrastructures de distribution d'électricité et de contrôle environnemental. Le terme «service de centre de données» ne s'applique pas aux centres de données internes propres à une entreprise et exploités pour les besoins de l'entité concernée.

(19) Les fournisseurs de services postaux au sens de la directive 97/67/CE du Parlement européen et du Conseil[18], ainsi que les fournisseurs de services de livraison express ou de messagerie, devraient être soumis à la présente directive s'ils fournissent au moins l'une des étapes de la chaîne postale de livraison, notamment la levée, le tri ou la distribution, y compris les services d'enlèvement. Les services de transport qui ne sont pas réalisés en lien avec l'une de ces étapes devraient sortir de la portée des services postaux.

(20) Ces interdépendances croissantes découlent d'un réseau de fourniture de services de plus en plus transfrontière et interdépendant, qui utilise des infrastructures essentielles dans toute l'Union dans les secteurs de l'énergie, des transports, des infrastructures numériques, de l'eau potable, des eaux usées, de la santé, de certains aspects de l'administration publique et de l'espace, dans la mesure où la fourniture de certains services dépendant de structures terrestres détenues, gérées et exploitées par des États membres ou par des parties privées est concernée, ce qui ne couvre donc pas les infrastructures détenues, gérées ou exploitées par ou au nom de l'Union dans le cadre de ses programmes spatiaux. Ces interdépendances signifient que toute perturbation, même initialement limitée à une entité ou un secteur, peut produire des effets en cascade plus larges, entraînant éventuellement des incidences négatives durables et de grande ampleur pour la fourniture de services dans l'ensemble du marché intérieur. La pandémie de COVID-19 a mis en évidence la vulnérabilité de nos sociétés de plus en plus interdépendantes face à des risques peu probables.

(21) Compte tenu des divergences entre les structures de gouvernance nationales et en vue de sauvegarder les accords existants au niveau sectoriel ou les autorités de surveillance et de régulation de l'Union, les États membres devraient pouvoir désigner plusieurs autorités nationales compétentes chargées d'accomplir les tâches liées à la sécurité des réseaux et des systèmes d'information des entités essentielles et importantes dans le cadre de la présente directive. Les États membres devraient pouvoir attribuer cette mission à une autorité existante.

(22) Afin de faciliter la coopération et la communication transfrontalières entre les autorités et pour permettre la mise en œuvre effective de la présente directive, il est nécessaire que chaque État membre désigne un point de contact national unique chargé de coordonner les tâches liées à la sécurité des réseaux et des systèmes d'information et de la coopération transfrontalière au niveau de l'Union.

(23) Les autorités compétentes ou les CSIRT devraient recevoir les notifications d'incidents provenant des entités de manière efficace et efficiente. Les points de contact uniques devraient être chargés de transmettre les notifications d'incidents aux points de contact uniques des autres États membres touchés. Au niveau des autorités des États membres, afin de garantir l'existence d'un seul point d'entrée dans chaque État membre, les points de contact uniques devraient également être les destinataires des informations pertinentes portant sur les incidents concernant les entités du secteur financier fournies par les autorités compétentes au titre du règlement XXXX/XXXX, qu'ils devraient pouvoir transmettre, le cas échéant, aux autorités nationales compétentes ou aux CSIRT en vertu de la présente directive.

---

[18] Directive 97/67/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant des règles communes pour le développement du marché intérieur des services postaux de la Communauté et l'amélioration de la qualité du service (JO L 15 du 21.1.1998, p. 14).

(24) Les États membres devraient disposer de moyens suffisants, sur les plans technique et organisationnel, pour prévenir et détecter les incidents et risques liés aux réseaux et systèmes d'information et prendre les mesures d'intervention et d'atténuation nécessaires. Les États membres devraient dès lors veiller à disposer de CSIRT, également connus sous la dénomination de centres de réponse aux urgences informatiques (CERT), opérationnels et conformes aux exigences essentielles afin de garantir l'existence de moyens effectifs et compatibles pour gérer les incidents et les risques et d'assurer une coopération efficace au niveau de l'Union. Afin d'améliorer la relation de confiance entre les entités et les CSIRT, dans les cas où un CSIRT fait partie de l'autorité compétente, les États membres devraient envisager de mettre en place une séparation fonctionnelle entre d'une part les tâches opérationnelles assurées par les CSIRT, notamment en lien avec le partage d'informations et l'assistance aux entités, et d'autre part les activités de surveillance des autorités compétentes.

(25) En ce qui concerne les données à caractère personnel, les CSIRT devraient être en mesure de réaliser, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil[19] relatif aux données à caractère personnel, au nom et sur demande d'une entité en vertu de la présente directive, une analyse des réseaux et des systèmes d'information utilisés pour la fourniture de leurs services. Les États membres devraient avoir pour but d'assurer l'égalité du niveau des capacités techniques de tous les CSIRT sectoriels. Les États membres peuvent solliciter l'assistance de l'agence européenne pour la cybersécurité (ENISA) pour la mise en place des CSIRT nationaux.

(26) Compte tenu de l'importance de la coopération internationale en matière de cybersécurité, les CSIRT devraient pouvoir participer à des réseaux de coopération internationaux en plus du réseau des CSIRT institué par la présente directive.

(27) Conformément à l'annexe de la recommandation (UE) 2017/1584 de la Commission sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs («plan d'action»)[20], un incident majeur signifie un incident qui frappe plusieurs États membres ou qui provoque des perturbations dépassant les capacités d'action du seul État membre concerné. En fonction de leur cause et de leurs conséquences, les incidents majeurs peuvent dégénérer et se transformer en crises à part entière, empêchant le bon fonctionnement du marché intérieur. Vu la large portée et, dans la plupart des cas, la nature transfrontalière de ces incidents, les États membres et les institutions, organes et agences compétents de l'Union devraient coopérer au niveau technique, opérationnel et politique afin de coordonner correctement la réaction dans toute l'Union.

(28) Puisque l'exploitation des vulnérabilités dans les réseaux et les systèmes d'information peut causer des perturbations et des dommages considérables, l'identification et la correction rapide de ces vulnérabilités est un facteur important de la réduction du risque en matière de cybersécurité. Les entités qui mettent au point de tels systèmes devraient dont établir des procédures appropriées pour gérer les vulnérabilités découvertes. Puisque les vulnérabilités sont souvent découvertes et signalées

---

19 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

20 Recommandation (UE) 2017/1584 de la Commission du 13 septembre 2017 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs (JO L 239 du 19.9.2017, p. 36).

(divulguées) par des tiers (les entités effectuant le signalement), le fabricant de produits ou le fournisseur de services TIC devraient également mettre en place les procédures nécessaires pour recevoir les informations relatives aux vulnérabilités communiquées par les tiers. À cet égard, les normes internationales ISO/CEI 30111 et ISO/CEI 29417 fournissent des orientations sur la gestion des vulnérabilités et la divulgation des vulnérabilités respectivement. En ce qui concerne la divulgation des vulnérabilités, la coordination entre les entités effectuant le signalement et les fabricants ou les fournisseurs de produits ou de services TIC est particulièrement importante. La divulgation coordonnée des vulnérabilités consiste en un processus structuré dans lequel les vulnérabilités sont signalées aux organisations de manière à leur donner la possibilité de diagnostiquer la vulnérabilité et d'y remédier avant que des informations détaillées à ce sujet soient divulguées à des tiers ou au public. La divulgation coordonnée des vulnérabilités devrait également comprendre la coordination entre l'entité effectuant le signalement et l'organisation en ce qui concerne le calendrier des corrections et la publication des vulnérabilités.

(29) Les États membres devraient par conséquent adopter des mesures destinées à faciliter la divulgation coordonnée des vulnérabilités en créant une politique nationale pertinente. À cet égard, les États membres devraient désigner un CSIRT pour jouer le rôle de «coordinateur» et agir comme un intermédiaire entre les entités effectuant le signalement et les fabricants ou les fournisseurs de produits ou de services TIC lorsque cela est nécessaire. Les missions du CSIRT agissant en tant que coordinateur devraient notamment impliquer d'identifier et de contacter les entités concernées, d'apporter une assistance aux entités effectuant le signalement, de négocier des délais de divulgation et de gérer les vulnérabilités qui touchent plusieurs organisations (divulgation de vulnérabilité multipartite). Lorsque les vulnérabilités touchent plusieurs fabricants ou fournisseurs de produits ou services TIC établis dans plusieurs États membres, les CSIRT désignés par chaque État membre touché devraient coopérer au sein du réseau des CSIRT.

(30) L'accès en temps utile à des informations correctes relatives aux vulnérabilités touchant les produits et services TIC contribue à une meilleure gestion des risques en matière de cybersécurité. À cet égard, les sources d'informations publiquement accessibles concernant les vulnérabilités sont des outils importants pour les entités et leurs utilisateurs, mais également pour les autorités nationales compétentes et les CSIRT. C'est pour cette raison que l'ENISA devrait mettre en place un registre des vulnérabilités dans lequel les entités essentielles et importantes et leurs fournisseurs, ainsi que les entités qui ne relèvent pas du champ d'application de la présente directive, peuvent, à titre volontaire, divulguer les vulnérabilités et fournir des informations à cet égard afin de permettre aux utilisateurs de prendre les mesures d'atténuation appropriées.

(31) Bien que des registres ou des bases de données similaires sur les vulnérabilités existent, ils sont hébergés et gérés par des entités qui ne sont pas établies dans l'Union. Un registre européen des vulnérabilités géré par l'ENISA améliorerait la transparence du processus de publication avant la divulgation officielle d'une vulnérabilité et la résilience en cas de perturbation ou d'interruption de la fourniture de services similaires. Afin d'éviter la duplication des efforts déployés et de viser la complémentarité dans la mesure du possible, l'ENISA devrait étudier la possibilité de conclure des accords de coopération structurés avec les registres existants sur le territoire de pays tiers.

(32) Tous les deux ans, le groupe de coopération devrait élaborer un programme de travail qui inclurait les actions qu'il doit réaliser afin de mettre en œuvre ses objectifs et ses tâches. Le calendrier du premier programme adopté au titre de la présente directive devrait être aligné sur le calendrier du dernier programme adopté au titre de la directive (UE) 2016/1148 afin d'éviter de perturber les travaux du groupe.

(33) Lorsqu'il met au point les documents d'orientation, le groupe de coopération devrait toujours: dresser l'état des lieux des solutions et des expériences nationales, évaluer les effets produits par les éléments livrables du groupe de coopération sur les approches nationales, discuter des défis en matière de mise en œuvre et formuler des recommandations spécifiques auxquelles il convient de répondre par une meilleure application des règles existantes.

(34) Le groupe de coopération devrait conserver sa forme de forum flexible et continuer d'être en mesure de réagir aux priorités politiques et aux difficultés nouvelles et en évolution, tout en tenant compte de la disponibilité des ressources. Il devrait régulièrement organiser des réunions conjointes avec les parties intéressées privées de toute l'Union en vue de discuter des activités menées par le groupe et de recueillir des informations sur les nouveaux défis politiques. Afin d'améliorer la coopération au niveau de l'Union, le groupe devrait envisager d'inviter les organes et agences de l'Union participant à la politique de cybersécurité, comme le Centre européen de lutte contre la cybercriminalité (EC3), l'Agence de l'Union européenne pour la sécurité aérienne (AESA) et l'Agence de l'Union européenne pour le programme spatial (EUSPA), à participer à ses travaux.

(35) Les autorités compétentes et les CSIRT devraient pouvoir participer aux programmes d'échange d'agents provenant d'autres États membres afin d'améliorer la coopération. Elles devraient prendre les mesures nécessaires pour que les agents d'autres États membres puissent jouer un rôle effectif dans les activités de l'autorité compétente hôte.

(36) L'Union devrait, conformément à l'article 218 du traité sur le fonctionnement de l'Union européenne et lorsque cela est pertinent, conclure, avec des pays tiers ou des organisations internationales, des accords internationaux qui permettent et organisent leur participation à certaines activités du groupe de coopération et du réseau des CSIRT. De tels accords devraient assurer un niveau suffisant de protection des données.

(37) Les États membres devraient contribuer à la création du cadre de l'Union européenne pour la réaction aux crises de cybersécurité défini dans la recommandation (UE) 2017/1584 via les réseaux de coopération existants, notamment le réseau européen d'organisations de liaison en cas de crises de cybersécurité (UE - CyCLONe), le réseau des CSIRT et le groupe de coopération. EU-CyCLONe et le réseau des CSIRT devraient coopérer sur la base de modalités de procédure définissant les conditions de cette coopération. Le règlement intérieur d'UE-CyCLONe devrait préciser plus en détail les modalités selon lesquelles le réseau devrait fonctionner, y compris, mais sans s'y limiter, les rôles, les modes de coopération, les interactions avec les autres acteurs pertinents et les modèles de partage d'informations, ainsi que les moyens de communication. Pour la gestion des crises au niveau de l'Union, les parties concernées devraient s'appuyer sur le dispositif intégré pour une réaction au niveau politique dans les situations de crise (IPCR). La Commission devrait avoir recours au processus intersectoriel de premier niveau ARGUS pour la coordination en cas de crise. Si la crise comporte d'importantes implications liées à la politique extérieure ou à la

politique de sécurité et de défense commune (PSDC), le système de réponse aux crises (SRC) du Service européen pour l'action extérieure (SEAE) devrait être activé.

(38) Aux fins de la présente directive, le terme «risque» devrait faire référence au potentiel de perte ou de perturbation causé par un incident de cybersécurité et devrait être exprimé comme la combinaison de l'ampleur de cette perte ou de cette perturbation et de la probabilité qu'un tel incident se produise.

(39) Aux fins de la présente directive, le terme «incidents évités» devrait faire référence à un événement qui aurait potentiellement pu causer des dommages, mais dont la réalisation totale a pu être empêchée.

(40) Parmi les mesures de gestion des risques devraient figurer celles permettant de déterminer tous les risques d'incidents, de prévenir, de repérer et de gérer les incidents et d'en atténuer les effets. La sécurité des réseaux et des systèmes d'information devrait inclure la sécurité des données stockées, transmises et traitées.

(41) Pour éviter que la charge financière et administrative imposée aux entités essentielles et importantes ne soit excessive, il convient que les exigences en matière de gestion des risques de cybersécurité soient proportionnées aux risques que présentent le réseau et le système d'information concernés, compte tenu de l'état le plus avancé de la technique en ce qui concerne ces mesures.

(42) Les entités essentielles et importantes devraient garantir la sécurité des réseaux et des systèmes d'information qu'elles utilisent dans le cadre de leurs activités. Il s'agit principalement de réseaux et de systèmes d'information privés qui sont gérés par leurs propres services informatiques ou dont la gestion de la sécurité a été sous-traitée. Les exigences en matière de gestion des risques de cybersécurité et de signalement prévues par la présente directive devraient s'appliquer aux entités essentielles et importantes que la maintenance de leurs réseaux et systèmes d'information soit assurée en interne ou qu'elle soit sous-traitée.

(43) Il est tout particulièrement important de répondre aux risques de cybersécurité découlant de la chaîne d'approvisionnement d'une entité et de ses relations avec ses fournisseurs vu la prévalence d'incidents dans le cadre desquels les entités ont été victimes de cyberattaques et des acteurs malveillants ont réussi à compromettre la sécurité des réseaux et systèmes d'information d'une entité en exploitant les vulnérabilités touchant les produits et les services de tiers. Les entités devraient donc évaluer et prendre en compte la qualité globale des produits et des pratiques de cybersécurité de leurs fournisseurs et fournisseurs de services, y compris de leurs procédures de développement sécurisées.

(44) Parmi tous les fournisseurs de services, les fournisseurs de services gérés de sécurité dans des domaines comme la réaction aux incidents, les tests de pénétration, les audits de sécurité et le conseil jouent un rôle particulièrement important s'agissant de soutenir les efforts mis en œuvre par les entités pour détecter les incidents et y réagir. Ces fournisseurs de services gérés de sécurité ont également été eux-mêmes la cible de cyberattaques et, du fait de leur grande intégration dans les activités des opérateurs, ils représentent un risque considérable en matière de cybersécurité. Les entités doivent donc faire preuve d'une diligence renforcée lorsqu'elles sélectionnent leurs fournisseurs de services gérés de sécurité.

(45) Les entités devraient également répondre aux risques de cybersécurité découlant de leurs interactions et de leurs relations avec d'autres parties intéressées dans le cadre d'un écosystème plus large. Plus particulièrement, les entités devraient prendre des

mesures appropriées pour veiller à ce que leur coopération avec les institutions universitaires et de recherche se déroule dans le respect de leurs politiques en matière de cybersécurité et des bonnes pratiques concernant l'accès et la diffusion d'informations en toute sécurité de manière générale et la protection des droits de propriété intellectuelle de manière spécifique. De même, vu l'importance et la valeur que représentent les données pour leurs activités, les entités devraient prendre toutes les mesures de cybersécurité appropriées lorsqu'elles ont recours à des services de transformation et d'analyse des données fournis par des tiers.

(46) Afin de mieux répondre aux risques principaux liés aux chaînes d'approvisionnement et d'aider les entités actives dans les secteurs couverts par la présente directive à bien gérer les risques de cybersécurité liés aux chaînes d'approvisionnement et aux fournisseurs, le groupe de coopération impliquant les autorités nationales compétentes, en collaboration avec la Commission et l'ENISA, devrait réaliser des évaluations coordonnées sectorielles des risques liés aux chaînes d'approvisionnement, comme cela a été le cas pour les réseaux 5G suite à la recommandation (UE) 2019/534 sur la cybersécurité des réseaux 5G[21], dans le but de déterminer, secteur par secteur, les services, systèmes ou produits TIC critiques, les menaces pertinentes et les vulnérabilités.

(47) Les évaluations des risques liés aux chaînes d'approvisionnement, à la lumière des caractéristiques du secteur concerné, devraient tenir compte des facteurs techniques et, le cas échéant, non techniques, y compris ceux définis dans la recommandation (UE) 2019/534, dans l'évaluation coordonnée à l'échelle de l'Union des risques concernant la sécurité des réseaux 5G et dans la boîte à outils de l'UE pour la cybersécurité 5G convenue par le groupe de coopération. Afin de déterminer quelles chaînes d'approvisionnement devraient être soumises à une évaluation coordonnée des risques, il convient de tenir compte des critères suivants: i) la mesure dans laquelle les entités essentielles et importantes utilisent des services, systèmes ou produits TIC critiques spécifiques et en dépendent; ii) la pertinence des services, systèmes ou produits TIC critiques spécifiques pour la réalisation des fonctions sensibles ou critiques, notamment le traitement de données à caractère personnel; iii) la disponibilité d'autres services, systèmes ou produits TIC; iv) la résilience de la chaîne d'approvisionnement générale des services, systèmes ou produits TIC face aux événements perturbateurs et v) concernant les services, systèmes ou produits TIC émergents, leur potentielle importance à l'avenir pour les activités des entités.

(48) Afin de rationaliser les obligations juridiques imposées aux fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public et aux prestataires de services de confiance en lien avec la sécurité de leurs réseaux et systèmes d'information, ainsi que de permettre à ces entités et à leurs autorités compétentes respectives de bénéficier du cadre juridique établi par la présente directive (y compris la désignation du CSIRT chargé de la gestion des risques et des incidents, la participation des autorités et organes compétents aux travaux du groupe de coopération et le réseau des CSIRT), il convient de les inclure dans le champ d'application de la présente directive. Il convient donc d'abroger les dispositions correspondantes prévues par le règlement (UE) nº 910/2014

[21] Recommandation (UE) 2019/534 de la Commission du 26 mars 2019 Cybersécurité des réseaux 5G (JO L 88 du 29.3.2019, p. 42).

du Parlement européen et du Conseil[22] et par la directive (UE) 2018/1972 du Parlement européen et du Conseil[23] portant sur l'imposition d'exigences en matière de sécurité et de notification à ce type d'entités. Les règles relatives aux obligations de signalement devraient être sans préjudice du règlement (UE) 2016/679 et de la directive 2002/58/CE du Parlement européen et du Conseil[24].

(49) Lorsque cela est approprié et afin d'éviter toute perturbation inutile, les autorités compétentes chargées de la surveillance et de l'application aux fins de la présente directive devraient continuer d'utiliser les lignes directrices nationales et les législations nationales existantes adoptées en vue de la transposition des règles portant sur les mesures de sécurité prévues par l'article 40, paragraphe 1, de la directive (UE) 2018/1972 ainsi que des exigences prévues par l'article 40, paragraphe 2, de cette directive concernant les paramètres liés à l'importance d'un incident.

(50) Étant donné l'importance croissante des services de communications interpersonnelles non fondés sur la numérotation, il convient de veiller à ce que ceux-ci soient également soumis à des exigences de sécurité appropriées au regard de leur nature spécifique et de leur importance économique. Les fournisseurs de tels services devraient par conséquent également garantir un niveau de sécurité des réseaux et des systèmes d'information correspondant au risque encouru. Étant donné que les fournisseurs de services de communications interpersonnelles non fondés sur la numérotation n'exercent normalement pas de contrôle effectif sur la transmission de signaux sur les réseaux, le degré de risque pour ces services peut être considéré, à certains égards, comme étant inférieur à ce qu'il est pour les services de communications électroniques traditionnels. Il en va de même pour les services de communications interpersonnelles fondés sur la numérotation et qui n'exercent aucun contrôle effectif sur la transmission de signaux.

(51) Le marché intérieur dépend plus que jamais du fonctionnement d'internet. Les services de la quasi-totalité des entités essentielles et importantes dépendent de services fournis sur internet. Afin d'assurer la prestation harmonieuse des services fournis par les entités essentielles et importantes, il est important que les réseaux de communications électroniques publics, comme les dorsales internet ou les câbles de communication sous-marins, disposent de mesures de cybersécurité appropriées et signalent les incidents qui les concernent.

(52) Lorsque cela est approprié, les entités devraient informer les destinataires de leurs services des menaces importantes et considérables, ainsi que des mesures qu'ils peuvent prendre pour atténuer le risque qui en résulte pour eux. L'obligation qui est faite aux entités d'informer les destinataires de ces menaces ne devrait pas les dispenser de l'obligation de prendre immédiatement, à leurs frais, les mesures appropriées pour prévenir ou remédier à toute cybermenace pour la sécurité et pour

---

22 Règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (JO L 257 du 28.8.2014, p. 73).

23 Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen (JO L 321 du 17.12.2018, p. 36).

24 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37).

rétablir le niveau normal de sécurité du service. Informer les destinataires au sujet des menaces pour la sécurité devrait être gratuit.

(53) Plus particulièrement, il convient que les fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public informent les destinataires des services des cybermenaces particulières et importantes pour la sécurité et des mesures qu'ils peuvent prendre pour sécuriser leurs communications, par exemple en recourant à des types spécifiques de logiciels ou de techniques de chiffrement.

(54) Afin de préserver la sécurité des réseaux et services de communications électroniques, il convient d'encourager l'utilisation du chiffrement, notamment du chiffrement de bout en bout, voire si nécessaire de l'imposer, pour les fournisseurs de ces services et réseaux, conformément aux principes de sécurité et de respect de la vie privée par défaut et dès la conception aux fins de l'article 18. Il convient de concilier l'utilisation du chiffrement de bout en bout avec les pouvoirs dont disposent les États membres pour garantir la protection de leurs intérêts essentiels de sécurité et de la sécurité publique et pour permettre la détection d'infractions pénales et les enquêtes et poursuites en la matière, dans le respect du droit de l'Union. Les solutions pour un accès légal aux informations contenues dans les communications chiffrées de bout en bout devraient préserver l'efficacité du cryptage pour ce qui est de la protection de la vie privée et de la sécurité des communications, tout en apportant une réponse efficace à la criminalité.

(55) La présente directive établit une approche en deux étapes du signalement des incidents afin de trouver le juste équilibre entre, d'une part, le signalement rapide qui aide à atténuer la propagation potentielle des incidents et permet aux entités de chercher de l'aide et, d'autre part, le signalement approfondi qui permet de tirer des leçons précieuses des incidents individuels et d'améliorer au fil du temps la résilience des entreprises individuelles et de secteurs tout entiers face aux cybermenaces. Lorsque les entités prennent connaissance d'un incident, elles devraient être tenues de présenter une notification initiale dans les 24 heures, suivie d'un rapport final un mois après au plus tard. La notification initiale ne devrait inclure que les informations strictement nécessaires pour porter l'incident à la connaissance des autorités compétentes et permettre à l'entité de demander une assistance, le cas échéant. Cette notification, le cas échéant, devrait indiquer si l'incident semble être causé par des actions illégales ou malveillantes. Les États membres devraient veiller à ce que l'obligation de présenter cette notification initiale ne détourne pas les ressources de l'entité effectuant le signalement des activités liées à la gestion de l'incident, qui doivent être prioritaires. Afin d'évider que les obligations de signalement des incidents détournent les ressources des activités de gestion des incidents ou compromettent de quelque manière que ce soit les efforts déployés par les entités à cet égard, les États membres devraient également prévoir que, dans des cas dûment justifiés et en accord avec les autorités compétentes ou avec le CSIRT, l'entité concernée peut ne pas respecter les délais de 24 heures pour la notification initiale et de un mois pour le rapport final.

(56) Les entités essentielles et importantes se retrouvent souvent dans une situation dans laquelle un incident en particulier, en raison de ses caractéristiques, doit être signalé à différentes autorités en raison d'obligations de notification incluses dans différents instruments juridiques. De tels cas créent des charges supplémentaires et peuvent également conduire à des incertitudes en ce qui concerne le format et les procédures de ces notifications. C'est pourquoi, afin de simplifier le signalement des incidents de sécurité, les États membres devraient mettre en place un *point d'entrée unique* pour

toutes les notifications requises en vertu de la présente directive et d'autres actes législatifs de l'Union, comme le règlement (UE) 2016/679 et la directive 2002/58/CE. L'ENISA, en collaboration avec le groupe de coopération, devrait mettre au point des formulaires de notification communs au moyen de lignes directrices qui permettraient de simplifier et de rationaliser les informations de signalement exigées par le droit de l'Union et de réduire les charges pesant sur les entreprises.

(57) Lorsqu'il y a lieu de suspecter qu'un incident est lié à des activités criminelles graves au regard du droit de l'Union ou du droit national, les États membres devraient encourager les entités essentielles et importantes, sur la base de leurs procédures pénales applicables conformément au droit de l'Union, à signaler aux autorités répressives compétentes tout incident de ce type. Le cas échéant, et sans préjudice des règles de protection des données à caractère personnel applicables à Europol, il est souhaitable que la coordination entre les autorités compétentes et les autorités répressives de différents États membres soit facilitée par le CE3 et l'ENISA.

(58) Dans de nombreux cas, des données à caractère personnel sont compromises à la suite d'incidents. Dans de telles circonstances, les autorités compétentes devraient coopérer et échanger des informations sur tous les aspects pertinents avec les autorités chargées de la protection des données et les autorités de contrôle conformément à la directive 2002/58/CE.

(59) Le maintien à jour des bases de données précises et complètes de noms de domaines et de données d'enregistrement (appelées «données WHOIS») ainsi que la fourniture d'un accès licite à ces données sont essentiels pour garantir la sécurité, la stabilité et la résilience du système de noms de domaines (DNS), lequel contribue en retour à assurer un niveau élevé commun de cybersécurité dans l'Union. Lorsque le traitement comprend des données à caractère personnel, ce traitement doit s'effectuer conformément au droit de l'Union en matière de protection des données.

(60) La disponibilité de ces données, et leur accessibilité, en temps opportun, pour les autorités publiques, y compris les autorités compétentes en vertu du droit de l'Union ou du droit national en matière de prévention d'infractions pénales, d'enquêtes et de poursuites en la matière, les CERT (ou CSIRT) et, en ce qui concerne les données de leurs clients, pour les fournisseurs de réseaux et de services de communications électroniques et les fournisseurs de technologies et de services de cybersécurité agissant pour le compte de ces clients, sont essentielles pour prévenir et à combattre l'utilisation abusive des noms de domaines, en particulier pour prévenir, détecter et répondre aux incidents de cybersécurité. Cet accès doit être conforme au droit de l'Union en matière de protection des données dans la mesure où il concerne des données à caractère personnel.

(61) Afin d'assurer la disponibilité de données exactes et complètes sur l'enregistrement des noms de domaines, les registres des noms de domaines de premier niveau ainsi que les entités qui fournissent des services d'enregistrement de noms de domaines pour le registre de noms de domaines de premier niveau (appelées «bureaux d'enregistrement») doivent collecter et garantir l'intégrité et la disponibilité des données relatives à l'enregistrement des noms de domaines. En particulier, les registres de noms domaines de premier niveau ainsi que les entités fournissant des services d'enregistrement de noms de domaines pour le registre de noms de domaines de premier niveau devraient établir des politiques et des procédures aux fins de collecter et maintenir des données d'enregistrement exactes et complètes, ainsi que

pour prévenir et corriger les données d'enregistrement inexactes, conformément aux règles de l'Union en matière de protection des données.

(62) Les registres des noms de domaines de premier niveau ainsi que les entités leur fournissant des services d'enregistrement de noms de domaines devraient rendre publiques les données relatives à l'enregistrement de noms de domaines qui ne relèvent pas du champ d'application des règles de l'Union en matière de protection des données, telles que les données concernant les personnes morales[25]. Les registres des noms de domaines de premier niveau ainsi que les entités fournissant des services d'enregistrement de noms de domaines pour le registre de noms de domaines de premier niveau devraient également permettre aux demandeurs d'accès légitimes d'accéder légalement à des données spécifiques d'enregistrement de noms de domaines concernant des personnes physiques, conformément à la législation de l'Union sur la protection des données. Les États membres devraient veiller à ce que les registres des noms de domaines de premier niveau ainsi que les entités qui leur fournissent des services d'enregistrement de noms de domaines répondent dans les meilleurs délais aux demandes de divulgation de données d'enregistrement de noms de domaines émanant de demandeurs d'accès légitimes. Les registres des noms de domaines de premier niveau ainsi que les entités qui leur fournissent des services d'enregistrement de noms de domaines devraient établir des politiques et des procédures entourant la publication et la divulgation des données d'enregistrement, y compris des accords de niveau de service régissant la gestion des demandes d'accès des demandeurs d'accès légitimes. La procédure d'accès peut également inclure l'utilisation d'une interface, d'un portail ou d'un autre outil technique afin de fournir un système efficace de demande et d'accès aux données d'enregistrement. En vue de promouvoir des pratiques harmonisées dans l'ensemble du marché intérieur, la Commission peut adopter des lignes directrices eu égard à ces procédures sans préjudice des compétences du comité européen de la protection des données.

(63) Toutes les entités essentielles et importantes au sens de la présente directive devraient relever de la juridiction de l'État membre dans lequel elles fournissent leurs services. Si l'entité fournit des services dans plus d'un État membre, elle doit dès lors relever de la juridiction distincte et concurrente de chacun de ces États membres. Les autorités compétentes de ces États membres devraient coopérer, se prêter mutuellement assistance et, le cas échéant, mener des actions communes de surveillance.

(64) Afin de tenir compte de la nature transfrontalière des services et des opérations des fournisseurs de services DNS, des registres des noms de domaines de premier niveau, des fournisseurs de réseaux de diffusion de contenu, des fournisseurs de services d'informatique en nuage, des fournisseurs de services de centres de données et des fournisseurs de service numérique, un seul État membre devrait avoir compétence eu égard à ces entités. La compétence devrait être attribuée à l'État membre dans lequel l'entité concernée a son principal établissement dans l'Union. Le critère d'établissement aux fins de la présente directive suppose l'exercice effectif d'une activité au moyen d'une installation stable. La forme juridique retenue pour un tel dispositif, qu'il s'agisse d'une succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard. Le respect de ce critère ne devrait pas

[25] RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL, considérant 14, aux termes duquel «Le présent règlement ne couvre pas le traitement des données à caractère personnel qui concernent les personnes morales, et en particulier des entreprises dotées de la personnalité juridique, y compris le nom, la forme juridique et les coordonnées de la personne morale».

dépendre de la localisation physique du réseau et des systèmes d'information dans un lieu donné; la présence et l'utilisation de tels systèmes ne constituent pas en soi l'établissement principal et ne sont donc pas des critères déterminants permettant de déterminer l'établissement principal. L'établissement principal devrait être le lieu où sont prises les décisions relatives aux mesures de gestion des risques en matière de cybersécurité dans l'Union. Cela correspondra généralement au lieu d'administration centrale des entreprises dans l'Union. Si ces décisions ne sont pas prises dans l'Union, l'établissement principal doit être considéré comme se trouvant dans les États membres où l'entité possède un établissement avec le plus grand nombre de salariés dans l'Union. Lorsque les services sont effectués par un groupe d'entreprises, l'établissement principal de l'entreprise qui exerce le contrôle devrait être considéré comme étant l'établissement principal du groupe d'entreprises.

(65) Dans les cas où un fournisseur de services DNS, un registre de noms de domaines de premier niveau, un fournisseur de réseau de diffusion de contenu, un fournisseur de services d'informatique en nuage, un fournisseur de services de centre de données ou un fournisseur de service numérique non établi dans l'Union propose des services à l'intérieur de l'Union, il devrait désigner un représentant. Afin de déterminer si une telle entité propose des services dans l'Union, il convient d'examiner s'il apparaît qu'elle envisage d'offrir des services à des personnes dans un ou plusieurs États membres. La seule accessibilité, dans l'Union, du site internet de l'entité ou d'un intermédiaire ou d'une adresse électronique et d'autres coordonnées ou encore l'utilisation d'une langue généralement utilisée dans le pays tiers où l'entité est établie ne suffisent pas pour établir une telle intention. Cependant, des facteurs tels que l'utilisation d'une langue ou d'une monnaie généralement utilisée dans un ou plusieurs États membres avec la possibilité de commander des services dans cette autre langue ou la mention de clients ou d'utilisateurs qui se trouvent dans l'Union peuvent indiquer que l'entité envisage d'offrir des services dans l'Union. Le représentant devrait agir pour le compte de l'entité et devrait pouvoir être contacté par les autorités compétentes ou les CSIRT. Le représentant devrait être expressément désigné par un mandat écrit de l'entité le chargeant d'agir en son nom pour remplir les obligations, y compris la notification des incidents, qui lui incombent en vertu de la présente directive.

(66) Lorsque des informations considérées comme classifiées en vertu du droit national ou du droit de l'Union sont échangées, communiquées ou partagées d'une autre manière en vertu des dispositions de la présente directive, les règles spécifiques correspondantes relatives au traitement des informations classifiées doivent être appliquées.

(67) Face à la complexité et la sophistication croissantes des cybermenaces, l'efficacité des mesures de détection et de prévention dépend dans une large mesure de l'échange régulier de renseignements sur les menaces et les vulnérabilités entre les entités. Le partage d'informations contribue à accroître la sensibilisation aux cybermenaces, laquelle renforce à son tour la capacité des entités à empêcher les menaces de se concrétiser en incidents réels et leur permet de mieux contenir les effets des incidents et de se rétablir plus efficacement. En l'absence d'orientations au niveau de l'Union, plusieurs facteurs semblent avoir entravé ce partage de renseignements, notamment l'incertitude quant à la compatibilité avec les règles en matière de concurrence et de responsabilité.

(68) Les entités devraient être encouragées à exploiter collectivement leurs connaissances individuelles et leur expérience pratique aux niveaux stratégique, tactique et

opérationnel en vue d'améliorer leurs capacités à évaluer, surveiller, se défendre et répondre de manière adéquate aux cybermenaces. Il est donc nécessaire de permettre l'émergence, au niveau de l'Union, d'accords de partage volontaire d'informations. À cette fin, les États membres devraient activement soutenir et encourager également les entités concernées qui ne relèvent pas du champ d'application de la présente directive à participer à ces mécanismes d'échange d'informations. Ces mécanismes devraient être opérés dans le plein respect des règles de concurrence de l'Union ainsi que des règles du droit de l'Union en matière de protection des données.

(69) Le traitement de données à caractère personnel, dans la mesure strictement nécessaire et proportionnée aux fins de garantir la sécurité du réseau et des informations par des entités, des autorités publiques, des CERT, des CSIRT et des fournisseurs de technologies et de services de sécurité devrait constituer un intérêt légitime du responsable du traitement concerné, tel que visé dans le règlement (UE) 2016/679. Cela devrait comprendre des mesures liées à la prévention, à la détection, à l'analyse et à la réaction aux incidents, des mesures de sensibilisation à des cybermenaces spécifiques, l'échange d'informations dans le cadre de la correction des vulnérabilités et de la divulgation coordonnée, ainsi que l'échange volontaire d'informations sur ces incidents, les cybermenaces et les vulnérabilités, de même que les indicateurs de compromis, les tactiques, techniques et procédures, les alertes de cybersécurité et les outils de configuration. Ces mesures peuvent nécessiter le traitement des types de données à caractère personnel suivants: Adresses IP, localisateurs de ressources uniformes (URL), noms de domaines et adresses électroniques.

(70) Afin de renforcer les pouvoirs et actions de surveillance qui contribuent à assurer un respect effectif des règles, la présente directive devrait prévoir une liste minimale d'actions et de moyens de surveillance par lesquels les autorités compétentes peuvent contrôler les entités essentielles et importantes. En outre, la présente directive devrait établir une différenciation du régime de surveillance entre les entités essentielles et les entités importantes en vue de garantir un juste équilibre des obligations tant pour les entités que pour les autorités compétentes. Ainsi, les entités essentielles devraient être soumises à un régime de surveillance à part entière *(ex ante* et *ex post*), tandis que les entités importantes devraient pour leur part être soumises à un régime de surveillance léger, uniquement *ex post*. Pour ces dernières, cela signifie que les entités importantes ne sont pas tenues de documenter systématiquement le respect des exigences en matière de gestion des risques de cybersécurité, tandis que les autorités compétentes sont quant à elles invitées à mettre en œuvre une approche réactive de la surveillance *ex post* et, par conséquent, ne pas être assujetties à une obligation générale de surveillance de ces entités.

(71) Afin de rendre l'application effective, il convient d'établir une liste minimale de sanctions administratives pour violation des obligations de gestion des risques et de notification en matière de cybersécurité prévues par la présente directive, en établissant un cadre clair et cohérent pour ces sanctions dans toute l'Union. Il convient de tenir dûment compte de la nature, de la gravité et de la durée de la violation, des dommages ou pertes réels causés ou des dommages ou pertes potentiels qui auraient pu être provoqués, du caractère intentionnel ou négligent de la violation, des mesures prises pour prévenir ou atténuer les dommages et/ou pertes subis, du degré de responsabilité ou de toute violation antérieure pertinente, du degré de coopération avec l'autorité compétente et de toute autre circonstance aggravante ou atténuante. L'imposition de sanctions y compris d'amendes administratives devrait faire l'objet de garanties procédurales appropriées conformément aux principes généraux du droit de

l'Union et de la charte des droits fondamentaux de l'Union européenne, y compris le droit à une protection juridictionnelle effective et à une procédure régulière.

(72) Afin de garantir une application efficace des obligations prévues par la présente directive, chaque autorité compétente devrait avoir le pouvoir d'imposer ou de demander l'imposition d'amendes administratives.

(73) Lorsque des amendes administratives sont imposées à une entreprise, ce terme doit, à cette fin, être compris comme une entreprise conformément aux articles 101 et 102 du traité sur le fonctionnement de l'Union européenne. Lorsque des amendes administratives sont imposées à des personnes qui ne sont pas une entreprise, l'autorité de contrôle devrait tenir compte, lorsqu'elle examine quel serait le montant approprié de l'amende, du niveau général des revenus dans l'État membre ainsi que de la situation économique de la personne en cause. Il devrait appartenir aux États membres de déterminer si et dans quelle mesure les autorités publiques devraient faire l'objet d'amendes administratives. L'imposition d'une amende administrative n'affecte pas l'exercice d'autres pouvoirs par les autorités compétentes ou l'imposition d'autres sanctions prévues dans les dispositions nationales transposant la présente directive.

(74) Les États membres devraient pouvoir déterminer le régime des sanctions pénales applicables en cas de violations des dispositions nationales transposant la présente directive. Toutefois, l'imposition de sanctions pénales en cas de violation de ces dispositions nationales et l'imposition de sanctions administratives connexes ne devraient pas entraîner la violation du principe *ne bis in idem* tel qu'il a été interprété par la Cour de justice.

(75) Lorsque la présente directive n'harmonise pas les sanctions administratives ou, si nécessaire dans d'autres circonstances, par exemple en cas de violation grave des obligations prévues par la présente directive, les États membres devraient mettre en œuvre un système qui prévoit des sanctions effectives, proportionnées et dissuasives. La nature de ces sanctions, pénales ou administratives devrait être déterminée par le droit des États membres.

(76) Afin de renforcer encore l'efficacité et le caractère dissuasif des sanctions applicables aux violations des obligations prévues en vertu de la présente directive, les autorités compétentes devraient être habilitées à imposer des sanctions consistant en la suspension d'une certification ou d'une autorisation concernant tout ou partie des services fournis par une entité essentielle et en l'interdiction temporaire de l'exercice de fonctions de direction par une personne physique. Compte tenu de leur gravité et de leur incidence sur les activités des entités et, en définitive, sur leurs consommateurs, ces sanctions ne devraient être appliquées que proportionnellement à la gravité de la violation et en tenant compte des circonstances spécifiques de chaque cas, notamment le caractère intentionnel ou négligent de la violation, les mesures prises pour prévenir ou atténuer les dommages et/ou les pertes subis. Ces sanctions ne devraient être appliquées qu'à titre d'*ultima ratio*, c'est-à-dire uniquement après que les autres mesures d'exécution pertinentes prévues par la présente directive ont été épuisées, et seulement pendant la période durant laquelle les entités auxquelles elles s'appliquent prennent les mesures nécessaires pour remédier aux manquements ou se conformer aux exigences de l'autorité compétente pour laquelle ces sanctions ont été appliquées. L'imposition de ces sanctions est soumise à des garanties procédurales appropriées conformément aux principes généraux du droit de l'Union et à la charte des droits fondamentaux de l'Union européenne, y compris le droit à une protection

juridictionnelle effective, une procédure régulière, la présomption d'innocence et les droits de la défense.

(77) La présente directive devrait établir des règles de coopération entre les autorités compétentes et les autorités de contrôle conformément au règlement (UE) 2016/679 pour traiter les violations relatives aux données à caractère personnel.

(78) La présente directive devrait viser à assurer un niveau de responsabilité important pour les mesures de gestion des risques en matière de cybersécurité et les obligations de notification au niveau des organisations. Pour ces raisons, les organes de direction des entités entrant dans le champ d'application de la présente directive devraient approuver les mesures relatives aux risques en matière de cybersécurité et superviser leur mise en œuvre.

(79) Un mécanisme d'évaluation par les pairs devrait être mis en place, permettant l'évaluation par des experts désignés par les États membres de la mise en œuvre des politiques de cybersécurité, y compris le niveau des capacités et des ressources disponibles des États membres.

(80) Afin de tenir compte des nouvelles cybermenaces, de l'évolution technologique ou des spécificités sectorielles, 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 les éléments en rapport avec les mesures de gestion des risques requis en vertu de la présente directive. La Commission devrait également être habilitée à adopter des actes délégués établissant quelles catégories d'entités essentielles sont tenues d'obtenir un certificat et dans le cadre de quels régimes européens de certification de cybersécurité spécifiques. 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 du 13 avril 2016 «Mieux légiférer»[26]. 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 la préparation des actes délégués.

(81) Afin d'assurer des conditions uniformes de mise en œuvre des dispositions pertinentes de la présente directive concernant les modalités de procédure nécessaires au fonctionnement du groupe de coopération, les éléments techniques des mesures de gestion des risques ou le type d'informations, le format et la procédure de notification des incidents, il convient de conférer des compétences d'exécution à la Commission. Ces compétences devraient être exercées en conformité avec le règlement (UE) nº 182/2011 du Parlement européen et du Conseil.[27]

(82) La présente directive devrait être réexaminée périodiquement par la Commission, en consultation avec les parties intéressées, notamment en vue de déterminer s'il est nécessaire de la modifier pour tenir compte de l'évolution de la société, de la situation politique, des technologies ou de la situation des marchés.

---

26 JO L 123 du 12.5.2016, p. 1.

27 Règlement (UE) nº 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

(83) Étant donné que l'objectif de la présente directive, qui vise à atteindre un niveau élevé commun de cybersécurité dans l'Union, ne peut pas être atteint de manière suffisante par les États membres mais peut, en raison des effets de l'action, l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures, conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité tel qu'énoncé audit article, la présente directive n'excède pas ce qui est nécessaire pour atteindre cet objectif.

(84) La présente directive respecte les droits fondamentaux et observe les principes reconnus par la charte des droits fondamentaux de l'Union européenne et, en particulier, le droit au respect de la vie privée et des communications, le droit à la protection des données à caractère personnel, le droit à la liberté d'entreprise, le droit de propriété ainsi que le droit à un recours effectif et à un procès équitable. La présente directive devrait être mise en œuvre conformément à ces droits et principes,

ONT ARRÊTÉ LA PRÉSENTE DIRECTIVE:

## CHAPITRE I

*Dispositions générales*

*Article premier*

***Objet***

1. La présente directive établit des mesures visant à assurer un niveau commun élevé de cybersécurité dans l'Union.

2. À cette fin, la présente directive:

(a) fixe des obligations aux États membres en ce qui concerne l'adoption de stratégies nationales de cybersécurité, la désignation d'autorités nationales compétentes, de points de contact uniques et d'équipes de réponse aux incidents de sécurité informatique (CSIRT);

b) définit les obligations en matière de gestion et de notification des risques de cybersécurité pour les entités d'un type appelé «entités essentielles» à l'annexe I et «entités importantes» à l'annexe II;

(c) fixe des obligations pour le partage d'informations en matière de cybersécurité.

*Article 2*

***Champ d'application***

1. La présente directive s'applique aux entités publiques et privées d'un type appelé «entités essentielles» à l'annexe I et «entités importantes» à l'annexe II. La présente directive ne s'applique pas aux entités qui peuvent être qualifiées de microentreprises

et de petites entreprises au sens de la recommandation 2003/361/CE de la Commission.[28]

2. Toutefois, quelle que soit leur taille, la présente directive s'applique également aux entités visées aux annexes I et II, dans les cas suivants:

(a) les services sont fournis par l'une des entités suivantes:

i) des réseaux de communications électroniques publics ou des services de communications électroniques accessibles au public visés à l'annexe I, point 8;

ii) des prestataires de services de confiance visés à l'annexe I, point 8;

iii) des registres des noms de domaines de premier niveau et des prestataires de services du système de noms de domaines (DNS) visés à l'annexe I, point 8;

b) l'entité est une entité d'administration publique telle que définie à l'article 4, point 23;

c) l'entité est le seul prestataire de services dans un État membre;

d) une éventuelle interruption du service fourni par l'entité pourrait avoir une incidence sur la sécurité publique, la sûreté publique ou la santé publique;

e) une éventuelle perturbation du service fourni par l'entité pourrait induire des risques systémiques, en particulier pour les secteurs où cette perturbation pourrait avoir une incidence transfrontalière;

f) l'entité est critique en raison de son importance spécifique au niveau régional ou national pour le secteur ou le type de service en question, ou pour d'autres secteurs interdépendants dans l'État membre;

g) l'entité est identifiée comme une entité critique conformément à la directive (UE) XXXX/XXXX du Parlement européen et du Conseil[29] [directive sur la résilience des entités critiques], ou comme une entité équivalente à une entité critique conformément à l'article 7 de cette directive.

Les États membres établissent une liste des entités identifiées conformément aux points b) à f) et la soumettent à la Commission au plus tard [6 mois après la date limite de transposition]. Les États membres réexaminent la liste régulièrement, puis au moins tous les deux ans, et, le cas échéant, la mettent à jour.

3. La présente directive est sans préjudice des compétences des États membres concernant la préservation de la sécurité publique, de la défense et de la sécurité nationale dans le respect du droit de l'Union.

4. La présente directive est sans préjudice de la directive 2008/114/CE du Conseil[30] et des directives du Parlement européen et du Conseil 2011/93/UE[31] et 2013/40/UE[32].

---

28 Recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises (JO L 124 du 20.5.2003, p. 36).

29 *[insérer le titre complet et la référence de la publication au JO lorsqu'elle est connue]*

30 Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection (JO L 345 du 23.12.2008, p. 75).

5. Sans préjudice de l'article 346 du traité sur le fonctionnement de l'Union européenne, les informations considérées comme confidentielles en application de la réglementation nationale et de l'Union, telle que les règles applicables au secret des affaires, ne peuvent faire l'objet d'un échange avec la Commission et d'autres autorités concernées que si cet échange est nécessaire à l'application de la présente directive. Les informations échangées se limitent au minimum nécessaire et sont proportionnées à l'objectif de cet échange. L'échange d'informations préserve la confidentialité des informations concernées et protège la sécurité et les intérêts commerciaux des entités essentielles ou importantes.

6. Lorsque des dispositions de réglementations sectorielles du droit de l'Union imposent à des entités essentielles ou importantes soit d'adopter des mesures de gestion des risques en matière de cybersécurité, soit de notifier des incidents ou des cybermenaces importantes, et lorsque ces exigences sont au moins équivalentes dans leurs effets aux obligations prévues par la présente directive, les dispositions pertinentes de la présente directive, y compris la disposition relative à la surveillance et à l'exécution prévue au chapitre VI, ne sont pas applicables.

*Article 3*

***Harmonisation minimale***

Sans préjudice des autres obligations qui leur incombent en vertu du droit de l'Union, les États membres peuvent, conformément à la présente directive, adopter ou maintenir des dispositions assurant un niveau plus élevé de cybersécurité.

*Article 4*

***Définitions***

Aux fins de la présente directive, on entend par:

(1) «réseau et système d'information»,

a) un réseau de communications électroniques au sens de l'article 2, point 1), du règlement (UE) 2018/1972;

b) tout dispositif ou tout ensemble de dispositifs interconnectés ou apparentés, dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques;

c) les données numériques stockées, traitées, récupérées ou transmises par les éléments visés aux points a) et b) en vue de leur fonctionnement, utilisation, protection et maintenance;

---

31 Directive 2011/93/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil (JO L 335 du 17.12.2011, p. 1).

32 Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil (JO L 218 du 14.8.2013, p. 8).

(2) «sécurité des réseaux et des systèmes d'information», la capacité des réseaux et des systèmes d'information de résister, à un niveau de confiance donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles;

(3) «cybersécurité», la cybersécurité au sens de l'article 2, point 1, du règlement (UE) 2019/881 du Parlement européen et du Conseil[33];

(4) «stratégie nationale en matière de cybersécurité», le cadre cohérent d'un État membre fournissant des objectifs et des priorités stratégiques en matière de sécurité des réseaux et des systèmes d'information dans cet État membre;

(5) «incident», tout événement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement ou des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles;

(6) «traitement des incidents», toutes les actions et procédures visant à détecter, analyser et contenir un incident et à y répondre;

(7) «cybermenance», une cybermenace au sens de l'article 2, point 8), du règlement (UE) 2019/881;

(8) «vulnérabilité», une faiblesse, une susceptibilité ou la faille d'un bien, d'un système, d'un processus ou d'un contrôle qui peut être exploitée par une cybermenace;

(9) «représentant», toute personne physique ou morale établie dans l'Union qui est expressément désignée pour agir pour le compte i) d'un fournisseur de services DNS, d'un registre de noms de domaines de premier niveau, d'un fournisseur d'informatique en nuage, d'un fournisseur de services de centre de données, d'un fournisseur de réseau de diffusion de contenu tel que désigné au point 8 de l'Annexe I ou ii) d'entités visées au point 6 de l'Annexe II non établies dans l'Union, qui peut être contactée par une autorité nationale compétente ou un CSIRT à la place de l'entité concernant les obligations incombant à ladite entité en vertu de la présente directive;

(10) «norme», une norme au sens de l'article 2, point 1, du règlement (UE) 1025/2012 du Parlement européen et du Conseil[34];

(11) «spécification technique», une spécification technique au sens de l'article 2, point 4), du règlement (UE) nº 1025/2012;

(12) «point d'échange internet (IXP)» une structure de réseau qui permet l'interconnexion de plus de deux réseaux indépendants (systèmes autonomes), essentiellement aux fins de faciliter l'échange de trafic internet; un IXP n'assure l'interconnexion que pour des systèmes autonomes; un IXP n'exige pas que le trafic internet passant entre

---

33 Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) nº 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15).

34 Règlement (UE) nº 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision nº 1673/2006/CE du Parlement européen et du Conseil (JO L 316 du 14.11.2012, p. 12).

une paire quelconque de systèmes autonomes participants transite par un système autonome tiers, pas plus qu'il ne modifie ou n'altère par ailleurs un tel trafic;

(13) «système de noms de domaines (DNS)», un système hiérarchique et distribué d'affectation de noms qui permet aux utilisateurs finaux d'accéder à des services et à des ressources sur l'internet;

(14) «fournisseur de services DNS» une entité qui fournit des services de résolution de noms de domaines récursifs ou faisant autorité aux utilisateurs finaux de l'internet et à d'autres fournisseurs de services DNS;

(15) «registre de noms de domaines de premier niveau», une entité à laquelle un registre de noms de domaines de premier niveau spécifique a été délégué et qui est responsable de l'administration du registre de noms de domaines de premier niveau, y compris de l'enregistrement des noms de domaines sous le registre de noms de domaines de premier niveau et du fonctionnement technique du registre de noms de domaines de premier niveau, notamment l'exploitation de ses serveurs de noms, la maintenance de ses bases de données et la distribution des fichiers de zone du registre de noms de domaines de premier niveau sur les serveurs de noms;

(16) «service numérique», un service au sens de l'article 1er, paragraphe 1, point b), de la directive (UE) 2015/1535 du Parlement européen et du Conseil[35];

(17) «place de marché en ligne», un service numérique au sens de l'article 2, point n), de la directive 2005/29/CE du Parlement européen et du Conseil[36];

(18) «moteur de recherche en ligne», un service numérique au sens de l'article 2, point 5, du règlement (UE) 2019/1150 du Parlement européen et du Conseil[37];

(19) «service d'informatique en nuage», un service numérique qui permet l'administration à la demande et l'accès à distance à un ensemble modulable et variable de ressources informatiques distribuées et pouvant être partagées;

(20) «service de centre de données», un service qui englobe les structures, ou groupes de structures, dédiées à l'hébergement, l'interconnexion et l'exploitation centralisées des équipements de traitement de l'information et de réseau fournissant des services de stockage, de traitement et de transport des données, ainsi que l'ensemble des installations et infrastructures de distribution d'électricité et de contrôle environnemental;

(21) «réseau de diffusion de contenu», un réseau de serveurs géographiquement répartis visant à assurer la haute disponibilité, l'accessibilité ou la fourniture rapide de contenu et de services numériques aux utilisateurs d'internet pour le compte de fournisseurs de contenu et de services;

---

35 Directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information (JO L 241 du 17.9.2015, p. 1).

36 Directive 2005/29/CE du Parlement européen et du Conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur et modifiant la directive 84/450/CEE du Conseil et les directives 97/7/CE, 98/27/CE et 2002/65/CE du Parlement européen et du Conseil et le règlement (CE) nº 2006/2004 du Parlement européen et du Conseil (JO L 149 du 11.6.2005, p. 22).

37 Règlement (UE) 2019/1150 du Parlement européen et du Conseil du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne (JO L 186 du 11.7.2019, p. 57).

(22) «plateforme de services de réseaux sociaux», une plateforme qui permet aux utilisateurs finaux de se connecter, de partager, de découvrir et de communiquer entre eux sur plusieurs terminaux, notamment par conversations en ligne, publications, vidéos et recommandations);

(23) «entité de l'administration publique», une entité d'un État membre qui satisfait aux critères suivants:

(a) elle a été créée pour satisfaire des besoins d'intérêt général et n'a pas de caractère industriel ou commercial;

(b) elle est dotée de la personnalité juridique;

(c) elle est financée majoritairement par l'État, les collectivités régionales ou d'autres organismes de droit public; ou leur gestion est soumise à un contrôle de la part de ces autorités ou organes; ou leur organe d'administration, de direction ou de surveillance est composé de membres dont plus de la moitié sont désignés par l'État, les autorités régionales ou d'autres organismes de droit public;

(d) elle a le pouvoir de signifier aux personnes physiques ou morales des décisions administratives ou réglementaires affectant leurs droits en matière de mouvements transfrontaliers des personnes, des biens, des services ou des capitaux.

Les entités de l'administration publique qui exercent des activités dans les domaines de la sécurité publique, de l'application de la loi, de la défense ou de la sécurité nationale sont exclues.

(24) «entité», toute personne physique ou morale constituée et reconnue comme telle en vertu du droit national de son lieu de constitution, et ayant, en son nom propre, la capacité d'être titulaire de droits et d'obligations;

(25) «entité essentielle», toute entité d'un type appelé «entité essentielle» à l'annexe I;

(26) «entité importante», toute entité d'un type appelé «entité importante» à l'annexe II.

## CHAPITRE II

Cadres réglementaires coordonnés en matière de cybersécurité

*Article 5*

***Stratégie nationale en matière de cybersécurité***

1. Chaque État membre adopte une stratégie nationale en matière de cybersécurité qui définit les objectifs stratégiques et les mesures politiques et réglementaires appropriées, en vue de parvenir à un niveau élevé de cybersécurité et de le maintenir. La stratégie nationale en matière de cybersécurité comprend notamment les éléments suivants:

(a) une définition des objectifs et des priorités de la stratégie des États membres en matière de cybersécurité;

(b) un cadre de gouvernance visant à atteindre ces objectifs et priorités, y compris les politiques visées au paragraphe 2 ainsi que les rôles et responsabilités des organismes et entités publics ainsi que des autres acteurs concernés;

(c) une évaluation visant à déterminer les actifs pertinents et les risques de cybersécurité dans cet État membre;

(d) un inventaire des mesures garantissant la préparation, la réaction et la récupération des services après incident, y compris la coopération entre les secteurs public et privé;

(e) une liste des différents acteurs et autorités concernés par la mise en œuvre de la stratégie nationale en matière de cybersécurité;

(f) un cadre politique visant une coordination renforcée entre les autorités compétentes en vertu de la présente directive et de la directive (UE) XXXX/XXXX du Parlement européen et du Conseil[38] [directive sur la résilience des entités critiques] aux fins du partage d'informations sur les incidents et les cybermenaces et de l'exercice des tâches de contrôle.

2. Dans le cadre de la stratégie nationale en matière de cybersécurité, les États membres adoptent notamment les politiques suivantes:

a) une politique traitant de la cybersécurité dans le cadre de la chaîne d'approvisionnement des produits et services TIC utilisés par des entités essentielles et importantes pour la fourniture de leurs services;

b) des lignes directrices concernant l'inclusion et la spécification d'exigences liées à la cybersécurité pour les produits et services TIC dans les marchés publics;

c) une politique visant à promouvoir et à faciliter la divulgation coordonnée des vulnérabilités au sens de l'article 6;

d) une politique liée au maintien de la disponibilité générale et de l'intégrité du noyau public de l'internet ouvert;

e) une politique de promotion et de développement des compétences en matière de cybersécurité, de sensibilisation et d'initiatives de recherche et développement;

f) une politique de soutien aux institutions universitaires et de recherche visant à développer des outils de cybersécurité et à sécuriser les infrastructures de réseau;

g) une politique, des procédures pertinentes et des outils de partage d'informations appropriés visant à soutenir le partage volontaire d'informations sur la cybersécurité entre les entreprises dans le respect du droit de l'Union;

h) une politique répondant aux besoins spécifiques des PME, en particulier de celles qui sont exclues du champ d'application de la présente directive, en matière d'orientation et de soutien visant à améliorer leur résilience aux menaces de cybersécurité.

3. Les États membres notifient leurs stratégies nationales en matière de cybersécurité à la Commission dans les trois mois suivant leur adoption. Les États membres peuvent

[38] *[insérer le titre complet et la référence de la publication au JO lorsqu'elle est connue]*

exclure certaines informations de la notification lorsque et dans la mesure où cela est strictement nécessaire pour préserver la sécurité nationale.

4. Les États membres évaluent leurs stratégies nationales de cybersécurité au moins tous les quatre ans sur la base d'indicateurs clés de performance et, le cas échéant, les modifient. L'Agence de l'Union européenne pour la cybersécurité (ENISA) aide les États membres, sur demande, à élaborer une stratégie nationale et des indicateurs clés de performance aux fins de l'évaluation de la stratégie.

*Article 6*

***Divulgation coordonnée des vulnérabilités et registre européen des vulnérabilités***

1. Chaque État membre désigne l'un de ses CSIRT visés à l'article 9 comme coordinateur aux fins de la divulgation coordonnée des vulnérabilités. Le CSIRT désigné doit agir comme intermédiaire de confiance, en facilitant, si nécessaire, les interactions entre l'entité effectuant le signalement et le fabricant ou le fournisseur de produits ou de services TIC. Lorsque la vulnérabilité signalée concerne plusieurs fabricants ou fournisseurs de produits ou services TIC dans l'Union, le CSIRT désigné de chaque État membre concerné coopère avec le réseau CSIRT.

2. L'ENISA élabore et tient à jour un registre européen des vulnérabilités. À cette fin, l'ENISA établit et maintient les systèmes d'information, les politiques et les procédures appropriés en vue notamment de permettre aux entités importantes et essentielles et à leurs fournisseurs de réseaux et de systèmes d'information de divulguer et d'enregistrer les vulnérabilités présentes dans les produits TIC ou les services TIC, ainsi que de donner accès à toutes les parties intéressées aux informations sur les vulnérabilités contenues dans le registre. Le registre comprend notamment des informations décrivant la vulnérabilité, le produit TIC ou les services TIC affectés ainsi que la gravité de la vulnérabilité en termes de circonstances dans lesquelles elle peut être exploitée, la disponibilité des correctifs correspondants et, en l'absence de correctifs disponibles, des orientations adressées aux utilisateurs de produits et services vulnérables sur la manière dont les risques résultant des vulnérabilités divulguées peuvent être atténués.

*Article 7*

***Cadres nationaux de gestion de crise dans le domaine de la cybersécurité***

1. Chaque État membre désigne une ou plusieurs autorités compétentes qui sont chargées de la gestion des crises et incidents majeurs. Les États membres veillent à ce que les autorités compétentes disposent de ressources suffisantes pour s'acquitter, de manière effective et efficace, des tâches qui leur sont dévolues.

2. Chaque État membre recense les capacités, les moyens et les procédures qui peuvent être déployés en cas de crise aux fins de la présente directive.

3. Chaque État membre adopte un plan national de réaction aux incidents et aux crises de cybersécurité dans lequel sont définis les objectifs et les modalités de gestion des incidents et crises de cybersécurité majeurs. Le plan doit, notamment, prévoir les éléments suivants:

a) les objectifs des mesures et activités nationales de préparation;

b) les tâches et responsabilités des autorités compétentes nationales;

c) les procédures de gestion de crise et les canaux d'échange d'informations;

d) les mesures de préparation, y compris des exercices et des activités de formation;

e) les parties intéressées publiques et privées et les infrastructures concernées;

f) les procédures et arrangements nationaux entre les autorités et les organismes nationaux compétents visant à garantir la participation et le soutien effectifs de l'État membre à la gestion coordonnée des incidents et des crises de cybersécurité majeurs au niveau de l'Union.

4. Les États membres communiquent à la Commission la désignation de leurs autorités compétentes visées au paragraphe 1 et soumettent leurs plans nationaux d'intervention en cas d'incident et de crise de cybersécurité visés au paragraphe 3 dans les trois mois suivant cette désignation et l'adoption de ces plans. Les États membres peuvent exclure certaines informations du plan lorsque et dans la mesure où cela est strictement nécessaire pour préserver la sécurité nationale.

*Article 8*

***Autorités nationales compétentes et points de contact uniques***

1. Chaque État membre désigne une ou plusieurs autorités compétentes chargées de la cybersécurité et des tâches de contrôle visées au chapitre VI de la présente directive. Les États membres peuvent désigner à cet effet une ou des autorités existantes.

2. Les autorités compétentes visées au paragraphe 1 contrôlent l'application de la présente directive au niveau national.

3. Chaque État membre désigne un point de contact national unique en matière de sécurité (ci-après dénommé «point de contact unique»). Lorsqu'un État membre désigne une seule autorité compétente, cette dernière fait aussi fonction de point de contact unique dudit État membre.

4. Chaque point de contact unique exerce une fonction de liaison visant à assurer la coopération transfrontalière des autorités de son État membre avec les autorités compétentes des autres États membres, ainsi que pour garantir la coopération intersectorielle avec les autres autorités nationales compétentes de son État membre.

5. Les États membres veillent à ce que les autorités compétentes visées au paragraphe 1 et les points de contact uniques disposent de ressources suffisantes pour pouvoir s'acquitter de leurs tâches de manière effective et efficace et atteindre ainsi les objectifs de la présente directive. Les États membres font en sorte que les représentants désignés pour siéger au sein du groupe de coopération visé à l'article 12 puissent coopérer de manière effective, efficace et sécurisée.

6. Chaque État membre notifie dans les meilleurs délais à la Commission la désignation de l'autorité compétente visée au paragraphe 1 et du point de contact unique visé au paragraphe 3, les tâches qui leur sont confiées et toute modification ultérieure dans ce cadre. Chaque État membre rend leur désignation publique. La Commission publie la liste des points de contact uniques désignés.

*Article 9*

***Centres de réponse aux incidents de sécurité informatique (CSIRT)***

1. Chaque État membre désigne un ou plusieurs CSIRT, se conformant aux exigences énumérées à l'article 10, paragraphe 1, couvrant au moins les secteurs, les sous-secteurs ou les entités visés aux annexes I et II, et chargés de la gestion des incidents selon un processus bien défini. Un CSIRT peut être établi au sein d'une autorité compétente visée à l'article 8.
2. Les États membres veillent à ce que chaque CSIRT dispose de ressources suffisantes pour pouvoir s'acquitter efficacement de ses tâches énumérées à l'article 10, paragraphe 2.
3. Les États membres veillent à ce que chaque CSIRT dispose d'une infrastructure de communication et d'information adaptée, sécurisée et résiliente pour échanger des informations avec les entités essentielles et importantes et les autres parties intéressées concernées. À cette fin, les États membres veillent à ce que les CSIRT contribuent au déploiement d'outils sécurisés de partage d'informations.
4. Les CSIRT coopèrent et, le cas échéant, échangent des informations pertinentes conformément à l'article 26 avec des communautés sectorielles ou intersectorielles de confiance d'entités essentielles et importantes.
5. Les CSIRT participent aux évaluations par les pairs organisées conformément à l'article 16.
6. Les États membres veillent à ce que leurs CSIRT coopèrent de manière effective, efficace et sécurisée au sein du réseau des CSIRT visé à l'article 13.
7. Les États membres communiquent dans les meilleurs délais à la Commission les CSIRT désignés conformément au paragraphe 1, le coordinateur des CSIRT désigné conformément à l'article 6, paragraphe 1, et leurs tâches respectives prévues en ce qui concerne les entités visées aux annexes I et II.
8. Les États membres peuvent solliciter l'assistance de l'ENISA pour la mise en place des CSIRT nationaux.

*Article 10*

***Obligations et tâches des CSIRT***

1. Les CSIRT satisfont aux exigences suivantes:
   a) les CSIRT doivent veiller à un niveau élevé de disponibilité de leurs services de communication en évitant les points uniques de défaillance et ils doivent disposer de plusieurs moyens pour être contactés et contacter autrui à tout moment. Les CSIRT doivent clairement spécifier les canaux de communication et les faire connaître aux partenaires et collaborateurs;
   b) les locaux des CSIRT et les systèmes d'information utilisés doivent se trouver sur des sites sécurisés;
   c) les CSIRT sont dotés d'un système approprié de gestion et de routage des demandes afin, notamment, de faciliter les transferts effectifs et efficaces;

d) les CSIRT sont dotés des effectifs adéquats afin de pouvoir garantir une disponibilité permanente;

e) les CSIRT doivent être dotés de systèmes redondants et d'un espace de travail de secours pour assurer la continuité de leurs services;

f) les CSIRT ont la possibilité de participer aux réseaux de coopération internationale.

2. Les CSIRT assument les tâches suivantes:

a) la surveillance des cybermenaces, des vulnérabilités et des incidents au niveau national;

b) l'activation du mécanisme d'alerte précoce, la diffusion de messages d'alerte, les annonces et la diffusion d'informations sur les cybermenaces, les vulnérabilités et les incidents auprès des entités essentielles et importantes ainsi qu'auprès des autres parties intéressées;

c) la réaction aux incidents;

d) l'analyse dynamique des risques et incidents et la conscience situationnelle en matière de cybersécurité;

e) la réalisation, à la demande d'une entité, d'un scannage proactif du réseau et des systèmes d'information utilisés pour la fourniture de leurs services;

f) la participation au réseau des CSIRT ainsi que la fourniture d'une assistance mutuelle aux autres membres du réseau à leur demande.

3. Les CSIRT établissent des relations de coopération avec les acteurs concernés du secteur privé, en vue de mieux atteindre les objectifs de la directive.

4. Afin de faciliter la coopération, les CSIRT encouragent l'adoption et l'utilisation de pratiques, de systèmes de classification et de taxonomies communs ou normalisés en ce qui concerne

a) les procédures de gestion des incidents;

b) la gestion des crises de cybersécurité;

c) la divulgation coordonnée des vulnérabilités.

*Article 11*

***Coopération au niveau national***

1. Lorsqu'ils sont distincts, les autorités compétentes visées à l'article 8, le point de contact unique et le(s) CSIRT d'un même État membre coopèrent les uns avec les autres aux fins du respect des obligations énoncées dans la présente directive.

2. Les États membres veillent à ce que leurs autorités compétentes ou leurs CSIRT reçoivent des notifications relatives aux incidents, aux cybermenaces importantes et quasi-accidents, soumises en application de la présente directive. Lorsqu'un État membre décide que ses CSIRT ne reçoivent pas ces notifications, ils se voient accorder, dans la mesure nécessaire à l'accomplissement de leurs tâches, un accès aux données relatives aux incidents notifiés par les entités essentielles ou importantes conformément à l'article 20.

3. Chaque État membre veille à ce que ses autorités compétentes ou CSIRT informent son point de contact unique des notifications d'incidents, de cybermenaces importantes et de quasi-accidents soumises en application de la présente directive.

4. Dans la mesure nécessaire pour s'acquitter efficacement des tâches et obligations prévues par la présente directive, les États membres assurent une coopération appropriée entre les autorités compétentes et les points de contact uniques et les services répressifs, les autorités chargées de la protection des données et les autorités responsables des infrastructures critiques en vertu de la directive (UE) XXXX/XXXX [directive sur la résilience des entités critiques] et les autorités financières nationales désignées conformément au règlement (UE) XXXX/XXXX du Parlement européen et du Conseil[39] [le règlement sur la résilience opérationnelle numérique du secteur financier] dans cet État membre.

5. Les États membres veillent à ce que leurs autorités compétentes fournissent régulièrement des informations aux autorités compétentes désignées en vertu de la directive (UE) XXXX/XXXX [directive sur la résilience des entités critiques] eu égard aux risques en matière de cybersécurité, aux cybermenaces et aux incidents affectant les entités essentielles identifiées comme critiques, ou comme entités équivalentes aux entités critiques, en vertu de la directive (UE) XXXX/XXXX [directive sur la résilience des entités critiques], ainsi qu'eu égard aux mesures prises par les autorités compétentes en réponse à ces risques et incidents.

## CHAPITRE III

*Coopération*

### *Article 12*
### ***Groupe de coopération***

1. Afin de soutenir et de faciliter la coopération stratégique et l'échange d'informations entre les États membres dans le domaine de l'application de la directive, un groupe de coopération est créé.

2. Le groupe de coopération exécute ses tâches en s'appuyant sur les programmes de travail bisannuels visés au paragraphe 6.

3. Le groupe de coopération est composé de représentants des États membres, de la Commission et de l'ENISA. Le service européen pour l'action extérieure participe aux activités du groupe de coopération en qualité d'observateur. Les autorités européennes de surveillance (AES), conformément à l'article 17, paragraphe 5, point c), du règlement (UE) XXXX/XXXX [le règlement sur la résilience opérationnelle numérique du secteur financier], peuvent participer aux activités du groupe de coopération.

   Si besoin est, le groupe de coopération peut inviter des représentants des acteurs concernés à participer à ses travaux.

[39] *[insérer le titre complet et la référence de la publication au JO lorsqu'elle est connue]*

Le secrétariat est assuré par la Commission.

4. Le groupe de coopération est chargé des tâches suivantes:

   a) la fourniture d'orientations aux autorités compétentes en rapport avec la transposition et la mise en œuvre de la présente directive;

   b) l'échange des meilleures pratiques et d'informations relatives à la mise en œuvre de la présente directive, notamment en ce qui concerne les cybermenaces, les incidents, les vulnérabilités, les quasi-accidents, les initiatives de sensibilisation, les formations, les exercices et les compétences, le renforcement des capacités ainsi que les normes et les spécifications techniques;

   c) l'échange de conseils et la coopération avec la Commission sur les initiatives politiques émergentes en matière de cybersécurité;

   d) l'échange de conseils et la coopération avec la Commission sur les projets d'actes d'exécution ou d'actes délégués de la Commission adoptés en vertu de la présente directive;

   e) l'échange de bonnes pratiques et d'informations avec les institutions, organes et organismes compétents de l'Union;

   f) la discussion portant sur les rapports relatifs à l'évaluation par les pairs visés à l'article 16, paragraphe 7;

   g) la discussion portant sur les résultats des activités de contrôle conjoint dans les affaires transfrontalières visées à l'article 34;

   h) l'indication d'une orientation stratégique au réseau des CSIRT sur des questions nouvelles spécifiques;

   i) la contribution aux capacités en matière de cybersécurité dans l'ensemble de l'Union via la facilitation de l'échange de fonctionnaires nationaux grâce à un programme de renforcement des capacités impliquant le personnel des autorités compétentes des États membres ou des CSIRT;

   j) l'organisation régulière de réunions conjointes avec les parties privées intéressées de toute l'Union en vue de discuter des activités menées par le groupe et de recueillir des informations sur les nouveaux défis politiques;

   k) la discussion portant sur les travaux entrepris en relation avec les exercices de cybersécurité, y compris les travaux effectués par l'ENISA.

5. Le groupe de coopération peut demander au réseau CSIRT d'élaborer un rapport technique sur des sujets choisis.

6. Au plus tard le ... [ 24 mois après la date d'entrée en vigueur de la présente directive] et ensuite tous les deux ans, le groupe de coopération établit un programme de travail concernant les actions à entreprendre pour mettre en œuvre ses objectifs et ses tâches. Le calendrier du premier programme adopté au titre de la présente directive est aligné sur le calendrier du dernier programme adopté au titre de la directive (UE) 2016/1148.

7. La Commission peut adopter des actes d'exécution fixant les modalités de procédure nécessaires au fonctionnement du groupe de coopération. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 37, paragraphe 2.

8. Le groupe de coopération se réunit régulièrement et au moins une fois par an avec le groupe sur la résilience des entités critiques instauré en vertu de la directive (UE) XXXX/XXXX [directive sur la résilience des entités critiques] afin de promouvoir la coopération stratégique et l'échange d'informations.

*Article 13*
***Réseau des CSIRT***

1. Afin de contribuer au renforcement de la confiance et de promouvoir une coopération opérationnelle rapide et effective entre les États membres, un réseau des CSIRT nationaux est établi.
2. Le réseau des CSIRT est composé de représentants des CSIRT des États membres et du CERT-UE. La Commission participe au réseau des CSIRT en qualité d'observateur. L'ENISA assure le secrétariat et soutient activement la coopération entre les CSIRT.
3. Le réseau des CSIRT est chargé des tâches suivantes:
   (a) l'échange d'informations sur les capacités des CSIRT;
   (b) l'échange d'informations pertinentes sur les incidents, les quasi-accidents, les cybermenaces, les risques et les vulnérabilités;
   (c) à la demande d'un représentant du réseau CSIRT potentiellement affecté par un incident, l'échange et la discussion portant sur les informations en rapport avec cet incident et les cybermenaces, risques et vulnérabilités connexes;
   (d) à la demande du représentant d'un CSIRT d'un État membre, la discussion et, si possible, la mise en œuvre d'une réponse coordonnée à un incident déterminé qui relève de la juridiction de cet État membre;
   (e) la fourniture aux États membres d'une assistance face aux incidents transfrontaliers en application de la présente directive;
   (f) la coopération et la fourniture d'une assistance aux CSIRT désignés visés à l'article 6 en ce qui concerne la gestion de la divulgation coordonnée multipartite des vulnérabilités affectant plusieurs fabricants ou fournisseurs de produits TIC, de services TIC et processus TIC établis dans différents États membres;
   (g) la discussion et l'identification d'autres formes de coopération opérationnelle, notamment en rapport avec:
      i) les catégories de cybermenaces et d'incidents;
      ii) les alertes précoces;
      iii) l'assistance mutuelle;
      iv) les principes et modalités d'une coordination en réponse à des risques et incidents transfrontaliers;
      v) la contribution au plan national de réaction aux incidents et aux crises de cybersécurité visé à l'article 7, paragraphe 3;

(h) l'information du groupe de coopération de ses activités et des autres formes de coopération opérationnelle débattues en application du point g), et lorsque cela s'avère nécessaire, la demande de fourniture d'orientations à cet égard;

(i) l'examen des exercices de cybersécurité, y compris ceux organisés par l'ENISA;

(j) à la demande d'un CSIRT donné, l'étude des capacités et de l'état de préparation dudit CSIRT;

(k) la coopération et l'échange d'informations avec les centres d'opérations de sécurité (COS) régionaux et au niveau de l'Union afin d'améliorer la connaissance commune de la situation concernant les incidents et les menaces dans toute l'Union;

(l) l'examen des rapports de l'évaluation par les pairs visés à l'article 16, paragraphe 7;

(m) la publication de lignes directrices afin de faciliter la convergence des pratiques opérationnelles en ce qui concerne l'application des dispositions du présent article relatives à la coopération opérationnelle.

4. Aux fins du réexamen visé à l'article 35 et d'ici le [24 mois après la date d'entrée en vigueur de la présente directive], puis tous les deux ans, le réseau des CSIRT évalue les progrès réalisés dans le cadre de la coopération opérationnelle et produit un rapport. Le rapport tire notamment des conclusions sur les résultats des évaluations par les pairs visées à l'article 16, effectuées en rapport avec les CSIRT nationaux, y compris des conclusions et des recommandations, conformément au présent article. Ce rapport est aussi transmis au groupe de coopération.

5. Le réseau des CSIRT adopte son propre règlement intérieur.

*Article 14*

***Le réseau européen Cyber Crisis Liaison Organisation Network (UE-CyCLONe)***

1. Afin de contribuer à la gestion coordonnée, au niveau opérationnel, des incidents et crises de grande ampleur en matière de cybersécurité, et de garantir l'échange régulier d'informations entre les États membres et les institutions, organes et agences de l'Union, le réseau européen pour la préparation et la gestion des crises cyber par les États membres (UE-CyCLONe – *Cyber Crisis Liaison Organisation Network*) est institué.

2. Le réseau UE-CyCLONe est composé des représentants de la Commission, de l'ENISA et des autorités des États membres chargées de la gestion des crises désignées conformément à l'article 7. L'ENISA assure le secrétariat du réseau et soutient l'échange sécurisé d'informations.

3. Le réseau UE-CyCLONe a pour mission:

a) de renforcer le niveau de préparation à la gestion des crises et incidents majeurs;

b) de développer une connaissance situationnelle partagée des événements pertinents en matière de cybersécurité;

c) de coordonner la gestion des crises et incidents majeurs et de soutenir la prise de décision au niveau politique en ce qui concerne ces incidents et ces crises;

d) d'examiner les incidents de cybersécurité nationaux et les plans d'intervention visés à l'article 7, paragraphe 2.

4. UE-CyCLONe adopte son règlement intérieur.

5. UE-CyCLONe rend régulièrement compte au groupe de coopération des cybermenaces ainsi que des incidents et tendances en matière de cybersécurité, en mettant notamment l'accent sur leur incidence sur les entités essentielles et importantes.

6. EU-CyCLONe coopère avec le réseau des CSIRT sur la base des modalités procédurales convenues.

*Article 15*

***Rapport sur l'état de la cybersécurité dans l'Union***

1. L'ENISA publie, en coopération avec la Commission, un rapport bisannuel sur l'état de la cybersécurité dans l'Union. Le rapport comporte notamment une évaluation des éléments suivants:

(a) le développement des capacités de cybersécurité dans l'ensemble de l'Union;

(b) les ressources techniques, financières et humaines dont disposent les autorités compétentes et les politiques en matière de cybersécurité, ainsi que la mise en œuvre des mesures de contrôle et des mesures d'exécution à la lumière des résultats des évaluations par les pairs visées à l'article 16;

(c) un indice de cybersécurité permettant une évaluation globale du niveau de maturité des capacités de cybersécurité.

2. Le rapport comprend des recommandations politiques spécifiques visant à accroître le niveau de cybersécurité dans l'Union ainsi qu'un résumé des conclusions pour la période concernée des rapports de situation technique de l'Agence de l'UE sur la cybersécurité, publiés par l'ENISA conformément à l'article 7, paragraphe 6, du règlement (UE) 2019/881.

*Article 16*

**Évaluations par les pairs**

1. La Commission établit, après consultation du groupe de coopération et de l'ENISA, et au plus tard 18 mois après l'entrée en vigueur de la présente directive, la méthodologie et le contenu d'un système d'évaluation par les pairs pour apprécier l'efficacité des politiques en matière de cybersécurité des États membres. Les évaluations sont effectuées par des experts techniques en cybersécurité provenant d'États membres différents de celui qui fait l'objet de l'évaluation et portent au moins sur les points suivants:

i) l'efficacité de la mise en œuvre des exigences en matière de gestion des risques liés à la cybersécurité et des obligations de notification visées aux articles 18 et 20;

ii) le niveau des capacités, y compris les ressources financières, techniques et humaines disponibles, et l'efficacité de l'exercice des tâches des autorités nationales compétentes;

iii) les capacités opérationnelles et l'efficacité des CSIRT;

iv) l'efficacité de l'assistance mutuelle visée à l'article 34;

v) l'efficacité du cadre de partage des informations, visé à l'article 26 de la présente directive.

2. La méthodologie comprend des critères objectifs, non discriminatoires, équitables et transparents sur la base desquels les États membres désignent les experts habilités à effectuer les évaluations par les pairs. L'ENISA et la Commission désignent des experts pour participer en tant qu'observateurs aux évaluations par les pairs. La Commission, soutenue par l'ENISA, établit, dans le cadre de la méthodologie visée au paragraphe 1, un système objectif, non discriminatoire, équitable et transparent aux fins de la sélection et de la répartition aléatoire des experts pour chaque évaluation par les pairs.

3. Les aspects organisationnels des évaluations par les pairs sont décidés par la Commission, avec le soutien de l'ENISA, et, après consultation du groupe de coopération, sont fondés sur les critères définis dans la méthodologie visée au paragraphe 1. Les évaluations par les pairs portent sur les aspects visés au paragraphe 1 pour tous les États membres et secteurs, y compris sur des questions ciblées propres à un ou plusieurs États membres ou à un ou plusieurs secteurs.

4. Les évaluations par les pairs comportent des visites sur place physiques ou virtuelles et des échanges hors site. Compte tenu du principe de bonne coopération, les États membres faisant l'objet de l'évaluation fournissent aux experts désignés les informations demandées qui sont nécessaires à l'évaluation des aspects examinés. Toute information obtenue durant le processus d'évaluation par les pairs n'est utilisée qu'à cet effet. Les experts participant à l'évaluation par les pairs ne divulguent à aucun tiers les informations sensibles ou confidentielles obtenues au cours de cette évaluation.

5. Une fois examinés dans un État membre, les mêmes aspects ne font pas l'objet d'une nouvelle évaluation par les pairs dans cet État membre au cours des deux années suivant la conclusion d'une évaluation par les pairs, sauf décision contraire de la Commission, après consultation de l'ENISA et du groupe de coopération.

6. L'État membre veille à ce que tout risque de conflit d'intérêts concernant les experts désignés soit révélé aux autres États membres, à la Commission et à l'ENISA dans les meilleurs délais.

7. Les experts participant aux évaluations par les pairs rédigent des rapports sur les résultats et les conclusions des évaluations. Les rapports sont soumis à la Commission, au groupe de coopération, au réseau des CSIRT et à l'ENISA. Les rapports sont débattus au sein du groupe de coopération et du réseau des CSIRT. Ces rapports peuvent être publiés sur le site internet dédié du groupe de coopération.

## CHAPITRE IV

### *Gestion et signalement des risques de cybersécurité*

SECTION I

*Gestion et signalement des risques de cybersécurité*

*Article 17*

***Gouvernance***

1. Les États membres veillent à ce que les organes de direction des entités essentielles et importantes approuvent les mesures de gestion des risques en matière de cybersécurité prises par ces entités afin de se conformer à l'article 18, supervisent sa mise en œuvre et soient tenus responsables du non-respect par ces entités des obligations découlant du présent article.

2. Les États membres veillent à ce que les membres de l'organe de direction suivent régulièrement des formations spécifiques afin d'acquérir des connaissances et des compétences suffisantes pour appréhender et évaluer les risques et les pratiques de gestion en matière de cybersécurité et leur incidence sur les activités de l'entité.

*Article 18*

***Mesures de gestion des risques en matière de cybersécurité***

1. Les États membres veillent à ce que les entités essentielles et importantes prennent les mesures techniques et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information que ces entités utilisent dans le cadre de la fourniture de leurs services. Ces mesures garantissent, pour les réseaux et les systèmes d'information, un niveau de sécurité adapté au risque existant, compte tenu de l'état des connaissances.

2. Les mesures visées au paragraphe 1 comprennent au minimum:

   (a) l'analyse des risques et les politiques de sécurité des systèmes d'information;

   (b) la gestion des incidents (prévention, détection et réaction aux incidents);

   (c) la continuité des activités et la gestion des crises;

   (d) la sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services tels que les fournisseurs de services de stockage et de traitement des données ou de services de sécurité gérés;

   (e) la sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information, y compris le traitement et la divulgation des vulnérabilités;

(f) des politiques et des procédures (tests et audits) pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité;

(g) l'utilisation de la cryptographie et du cryptage.

3. Les États membres veillent à ce que, lorsqu'elles envisagent de prendre les mesures appropriées visées au paragraphe 2, point d), les entités tiennent compte des vulnérabilités propres à chaque fournisseur et prestataire de services et de la qualité globale des produits et des pratiques de cybersécurité de leurs fournisseurs et prestataires de services, y compris de leurs procédures de développement sécurisé.

4. Les États membres veillent à ce que, lorsqu'une entité constate que ses services ou tâches respectifs ne sont pas conformes aux exigences énoncées au paragraphe 2, elle prenne dans les meilleurs délais toutes les mesures correctives nécessaires pour mettre le service concerné en conformité.

5. La Commission peut adopter des actes d'exécution afin d'établir les spécifications techniques et méthodologiques des éléments visés au paragraphe 2. Lorsqu'elle prépare ces actes, la Commission procède conformément à la procédure d'examen visée à l'article 37, paragraphe 2, et suit, dans toute la mesure du possible, les normes internationales et européennes, ainsi que les spécifications techniques pertinentes.

6. La Commission est habilitée à adopter des actes délégués conformément à l'article 36 pour compléter les éléments prévus au paragraphe 2 afin de tenir compte des nouvelles cybermenaces, des évolutions technologiques ou des spécificités sectorielles.

*Article 19*

***Évaluations coordonnées au niveau de l'UE des risques liés aux chaînes d'approvisionnement critiques***

1. Le groupe de coopération, en coopération avec la Commission et l'ENISA, peut procéder à des évaluations coordonnées des risques de sécurité inhérents à des chaînes d'approvisionnement de services, de systèmes ou de produits TIC critiques spécifiques, en tenant compte des facteurs de risque techniques et, le cas échéant, non techniques.

2. La Commission, après avoir consulté le groupe de coopération et l'ENISA, détermine les services, systèmes ou produits TIC critiques spécifiques qui peuvent faire l'objet de l'évaluation coordonnée des risques visée au paragraphe 1.

*Article 20*

***Obligations en matière de communication d'informations***

1. Les États membres veillent à ce que les entités essentielles et importantes notifient dans les meilleurs délais aux autorités compétentes ou au CSIRT conformément aux paragraphes 3 et 4 tout incident ayant une incidence significative sur la fourniture de leurs services. Le cas échéant, ces entités notifient dans les meilleurs délais aux destinataires de leurs services les incidents susceptibles de nuire à la fourniture de ces services. Les États membres veillent à ce que ces entités signalent, entre autres,

toute information permettant aux autorités compétentes ou au CSIRT de déterminer si l'incident a une incidence au niveau transfrontalier.

2. Les États membres veillent à ce que les entités essentielles et importantes notifient dans les meilleurs délais aux autorités compétentes ou au CSIRT toute cybermenace importante que ces entités décèlent et qui aurait pu entraîner un incident significatif.

Le cas échéant, ces entités notifient dans les meilleurs délais aux destinataires de leurs services qui sont potentiellement affectés par une cybermenace importante toutes les mesures ou corrections que ces destinataires peuvent appliquer en réponse à cette menace. Le cas échéant, les entités informent également leurs destinataires de la menace elle-même. La notification n'accroît pas la responsabilité de l'entité qui en est à l'origine.

3. Un incident est considéré comme «significatif» si:

(a) l'incident a causé ou est susceptible de causer une perturbation opérationnelle importante ou des pertes financières substantielles pour l'entité concernée;

(b) l'incident a affecté ou est susceptible d'affecter d'autres personnes physiques ou morales en causant des pertes matérielles ou non matérielles considérables.

4. Les États membres veillent à ce que, aux fins de la notification visée au paragraphe 1, les entités concernées soumettent aux autorités compétentes ou au CSIRT:

(a) sans retard injustifié et en tout cas dans les 24 heures après avoir eu connaissance de l'incident, une première notification qui, le cas échéant, indique si l'incident est vraisemblablement causé par une action illicite ou malveillante;

(b) à la demande d'une autorité compétente ou d'un CSIRT, un rapport intermédiaire sur les mises à jour pertinentes de la situation;

(c) un rapport final au plus tard un mois après la présentation du rapport visé au point a), comprenant au moins les éléments suivants:

i) une description détaillée de l'incident, de sa gravité et de son incidence;

ii) le type de menace ou la cause profonde qui a probablement déclenché l'incident;

iii) les mesures d'atténuation appliquées et en cours.

Les États membres prévoient que, dans des cas dûment justifiés et en accord avec les autorités compétentes ou le CSIRT, l'entité concernée peut déroger aux délais fixés aux points a) et c).

5. Les autorités nationales compétentes ou le CSIRT fournissent, dans les 24 heures suivant la réception de la notification initiale visée au paragraphe 4, point a), une réponse à l'entité émettrice de la notification, y compris un retour d'information initial sur l'incident et, à la demande de l'entité, des orientations sur la mise en œuvre d'éventuelles mesures d'atténuation. Lorsque le CSIRT n'a pas reçu la notification visée au paragraphe 1, l'orientation est émise par l'autorité compétente en collaboration avec le CSIRT. Le CSIRT fournit un soutien technique supplémentaire si l'entité concernée le demande. Lorsqu'il y a lieu de suspecter que l'incident est de nature criminelle, les autorités nationales compétentes ou le CSIRT fournissent

également des orientations sur les modalités de signalement de l'incident aux autorités répressives.

6. Lorsque c'est approprié, et notamment si l'incident visé au paragraphe 1 concerne deux États membres ou plus, l'autorité compétente ou le CSIRT informe les autres États membres touchés et l'ENISA de l'incident. Ce faisant, les autorités compétentes, les CSIRT et les points de contact uniques doivent, dans le respect du droit de l'Union ou de la législation nationale conforme au droit de l'Union, préserver la sécurité et les intérêts commerciaux de l'entité ainsi que la confidentialité des informations communiquées.

7. Lorsque la sensibilisation du public est nécessaire pour prévenir un incident ou pour faire face à un incident en cours, ou lorsque la divulgation de l'incident est par ailleurs dans l'intérêt public, l'autorité compétente ou le CSIRT et, le cas échéant, les autorités ou les CSIRT des autres États membres concernés peuvent, après avoir consulté l'entité concernée, informer le public de l'incident ou exiger de l'entité qu'elle le fasse.

8. À la demande de l'autorité compétente ou du CSIRT, le point de contact unique transmet les notifications reçues en vertu des paragraphes 1 et 2 aux points de contact uniques des autres États membres touchés.

9. Le point de contact unique soumet mensuellement à l'ENISA un rapport de synthèse comprenant des données anonymisées et agrégées sur les incidents, les cybermenaces majeures et les quasi-accidents notifiés conformément aux paragraphes 1 et 2 et conformément à l'article 27. Afin de contribuer à la fourniture d'informations comparables, l'ENISA peut émettre des orientations techniques sur les paramètres des informations incluses dans le rapport de synthèse.

10. Les autorités compétentes fournissent aux autorités compétentes désignées en vertu de la directive (UE) XXXX/XXXX [directive sur la résilience des entités critiques] des informations sur les incidents et les cybermenaces notifiés conformément aux paragraphes 1 et 2 par les entités essentielles identifiées comme des entités critiques, ou comme des entités équivalentes aux entités critiques, en vertu de la directive (UE) XXXX/XXXX [directive sur la résilience des entités critiques].

11. La Commission peut adopter des actes d'exécution précisant plus en détail le type d'informations, le format et la procédure d'une notification présentée en vertu des paragraphes 1 et 2. La Commission peut également adopter des actes d'exécution pour préciser plus en détail les cas dans lesquels un incident est considéré comme significatif au sens du paragraphe 3. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 37, paragraphe 2.

*Article 21*

***Recours aux schémas européens de certification de cybersécurité***

1. Afin de démontrer la conformité à certaines exigences visées à l'article 18, les États membres peuvent exiger que des entités essentielles et importantes certifient certains produits TIC, services TIC et processus TIC dans le cadre de schémas européens de certification en matière de cybersécurité spécifiques adoptés conformément à l'article 49 du règlement (UE) 2019/881. Les produits, services et processus soumis à

la certification peuvent être développés par une entité essentielle ou importante ou achetés à des tiers.

2. La Commission est habilitée à adopter des actes délégués précisant quelles catégories d'entités essentielles sont tenues d'obtenir un certificat et dans le cadre de quels régimes européens de certification de cybersécurité spécifiques en application du paragraphe 1. Les actes délégués sont adoptés conformément à l'article 36.

3. La Commission peut demander à l'ENISA de préparer un schéma candidat conformément à l'article 48, paragraphe 2, du règlement (UE) 2019/881 dans les cas où il n'existe pas de schéma européen de certification de cybersécurité approprié aux fins du paragraphe 2.

*Article 22*

***Normalisation***

1. Afin de favoriser la convergence de la mise en œuvre de l'article 18, paragraphes 1 et 2, les États membres encouragent, sans imposer l'utilisation d'un type particulier de technologies ni créer de discrimination en faveur d'un tel type particulier de technologies, le recours à des normes et des spécifications européennes ou internationalement reconnues pour la sécurité des réseaux et des systèmes d'information.

2. L'ENISA, en collaboration avec les États membres, formule des avis et des lignes directrices concernant les domaines techniques qui doivent être pris en considération en lien avec le paragraphe 1, et concernant les normes existantes, y compris les normes nationales des États membres, qui permettraient de couvrir ces domaines.

*Article 23*

***Bases de données des noms de domaines et des données d'enregistrement***

1. Afin de contribuer à la sécurité, à la stabilité et à la résilience du DNS, les États membres veillent à ce que les registres des noms de domaines de premier niveau et les entités fournissant des services d'enregistrement de noms de domaines pour le registre de noms de domaines de premier niveau collectent et maintiennent les données d'enregistrement de noms de domaines exactes et complètes au sein d'une base de données dédiée avec la diligence requise, sous réserve du droit de l'Union en matière de protection des données à caractère personnel.

2. Les États membres veillent à ce que les bases de données relatives à l'enregistrement des noms de domaines visées au paragraphe 1 contiennent des informations pertinentes pour identifier et contacter les titulaires des noms de domaines et les points de contact qui gèrent les noms de domaines dans les registres des noms de domaines de premier niveau.

3. Les États membres veillent à ce que les registres des noms de domaines de premier niveau et les entités fournissant des services d'enregistrement de noms de domaines pour le registre de noms de domaines de premier niveau aient mis en place des politiques et des procédures visant à garantir que les bases de données contiennent des informations exactes et complètes. Les États membres veillent à ce que ces politiques et procédures soient mises à la disposition du public.

4. Les États membres veillent à ce que les registres des noms de domaines de premier niveau et les entités fournissant des services d'enregistrement de noms de domaines pour le registre de noms de domaines de premier niveau publient, dans les meilleurs délais après l'enregistrement d'un nom de domaine, des données d'enregistrement de domaine qui ne sont pas des données personnelles.

5. Les États membres veillent à ce que les registres des noms de domaines de premier niveau et les entités fournissant des services d'enregistrement de noms de domaines pour le registre de noms de domaines de premier niveau donnent accès aux données spécifiques d'enregistrement de noms de domaines sur demande légitime et dûment justifiée des demandeurs d'accès légitimes, dans le respect du droit de l'Union en matière de protection des données. Les États membres veillent à ce que les registres des noms de domaines de premier niveau et les entités fournissant des services d'enregistrement de noms de domaines pour le registre de noms de domaines de premier niveau répondent dans les meilleurs délais à toutes les demandes d'accès. Les États membres veillent à ce que les politiques et procédures de divulgation de ces données soient rendues publiques.

Partie II

## Compétence et enregistrement

*Article 24*

### *Compétence et territorialité*

1. Les fournisseurs de services DNS, les registres des noms de domaines de premier niveau, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données et les fournisseurs de réseaux de diffusion de contenu visés à l'annexe I, point 8, ainsi que les fournisseurs de services numériques visés à l'annexe II, point 6, sont réputés relever de la juridiction de l'État membre dans lequel ils ont leur établissement principal dans l'Union.

2. Aux fins de la présente directive, les entités visées au paragraphe 1 sont réputées avoir leur établissement principal dans l'Union dans l'État membre où sont prises les décisions relatives aux mesures de gestion des risques en matière de cybersécurité. Si ces décisions ne sont pas prises dans un quelconque établissement de l'Union, l'établissement principal doit être considéré comme se trouvant dans les États membres où les entités possèdent un établissement comptant le plus grand nombre de salariés dans l'Union.

3. Si une entité visée au paragraphe 1 n'est pas établie dans l'Union, mais offre des services dans l'Union, elle désigne un représentant dans l'Union. Le représentant est établi dans l'un des États membres dans lesquels les services sont fournis. Ladite entité est considérée comme relevant de la compétence de l'État membre dans lequel le représentant est établi. En l'absence d'un représentant désigné au sein de l'Union en vertu du présent article, tout État membre dans lequel l'entité fournit des services peut intenter une action en justice contre l'entité pour non-respect des obligations découlant de la présente directive.

4. La désignation d'un représentant par une entité visée au paragraphe 1 est sans préjudice d'actions en justice qui pourraient être intentées contre l'entité elle-même.

*Article 25*

***Registre des entités essentielles et importantes***

1. L'ENISA crée et tient un registre des entités essentielles et importantes visées à l'article 24, paragraphe 1. Les entités doivent soumettre les informations suivantes à l'ENISA au plus tard [12 mois après l'entrée en vigueur de la directive]:

   (a) le nom de l'entité;

   (b) l'adresse de son établissement principal et de ses autres établissements légaux dans l'Union ou, si elle n'est pas établie dans l'Union, de son représentant désigné conformément à l'article 24, paragraphe 3;

   (c) les coordonnées actualisées, y compris les adresses de courrier électronique et les numéros de téléphone des entités.

2. Les entités visées au paragraphe 1 notifient à l'ENISA toute modification des informations qu'elles ont communiquées en vertu du paragraphe 1 dans les meilleurs délais et, en tout état de cause, dans un délai de trois mois à compter de la date à laquelle la modification a pris effet.

3. Dès réception des informations visées au paragraphe 1, l'ENISA les transmet aux points de contact uniques en fonction de la localisation indiquée de l'établissement principal de chaque entité ou, si elle n'est pas établie dans l'Union, de son représentant désigné. Lorsqu'une entité visée au paragraphe 1 possède, outre son établissement principal dans l'Union, d'autres établissements dans d'autres États membres, l'ENISA en informe également les points de contact uniques de ces États membres.

4. Lorsqu'une entité n'enregistre pas son activité ou ne fournit pas les informations pertinentes dans le délai fixé au paragraphe 1, tout État membre dans lequel l'entité fournit des services est compétent pour veiller au respect par cette entité des obligations énoncées dans la présente directive.

## CHAPITRE V

## *Partage d'informations*

*Article 26*

***Dispositions relatives à l'échange d'informations en matière de cybersécurité***

1. Sans préjudice du règlement (UE) 2016/679, les États membres veillent à ce que les entités essentielles et importantes puissent échanger entre elles des informations pertinentes en matière de cybersécurité, y compris des informations relatives aux cybermenaces, aux vulnérabilités, aux indicateurs de compromission, aux tactiques, techniques et procédures, aux alertes de cybersécurité et aux outils de configuration, lorsque ce partage d'informations:

   (a) vise à prévenir, détecter, répondre ou atténuer les incidents;

   (b) renforce le niveau de cybersécurité, notamment en sensibilisant aux cybermenaces, en limitant ou en empêchant leur «capacité de se propager», en

soutenant une série de capacités de défense, en remédiant aux vulnérabilités et en les révélant, en mettant en œuvre des techniques de détection des menaces, des stratégies d'atténuation ou des étapes de réaction et de rétablissement.

2. Les États membres veillent à ce que l'échange d'informations ait lieu au sein de communautés de confiance d'entités essentielles et importantes. Cet échange est mis en œuvre au moyen d'accords de partage d'informations, compte tenu de la nature potentiellement sensible des informations partagées et dans le respect des règles du droit de l'Union visées au paragraphe 1.

3. Les États membres établissent des règles précisant la procédure, les éléments opérationnels (y compris l'utilisation de plateformes TIC dédiées), le contenu et les conditions des accords de partage d'informations visés au paragraphe 2. Ces règles fixent également les détails de la participation des autorités publiques à ces accords, ainsi que les éléments opérationnels, y compris l'utilisation de plateformes informatiques dédiées. Les États membres offrent un soutien à l'application de ces accords conformément à leurs politiques visées à l'article 5, paragraphe 2, point g).

4. Les entités essentielles et importantes notifient aux autorités compétentes leur participation aux mécanismes de partage d'informations visés au paragraphe 2, lorsqu'elles commencent à participer à de tels mécanismes ou, le cas échéant, lorsqu'elles se retirent de ces mécanismes, une fois que le retrait prend effet.

5. Conformément au droit de l'Union, l'ENISA soutient la mise en place des mécanismes de partage d'informations en matière de cybersécurité visés au paragraphe 2 par la fourniture de bonnes pratiques et d'orientations.

*Article 27*

***Notification volontaire d'informations pertinentes***

Sans préjudice de l'article 3, les États membres veillent à ce que les entités qui ne relèvent pas du champ d'application de la présente directive puissent, à titre volontaire, transmettre des notifications relatives aux incidents importants, aux cybermenaces ou aux incidents évités. Lorsqu'ils traitent des notifications, les États membres agissent conformément à la procédure énoncée à l'article 20. Les États membres peuvent traiter les notifications obligatoires en leur donnant la priorité par rapport aux notifications volontaires. Un signalement volontaire n'a pas pour effet d'imposer à l'entité qui est à l'origine du signalement des obligations supplémentaires auxquelles elle n'aurait pas été soumise si elle n'avait pas transmis ladite notification.

## CHAPITRE VI

*Surveillance et exécution*

*Article 28*

***Aspects généraux concernant la surveillance et l'exécution***

1. Les États membres veillent à ce que les autorités compétentes procèdent à une surveillance efficace et prennent les mesures nécessaires pour assurer le respect de la présente directive, et notamment des obligations énoncées aux articles 18 et 20.

2. Pour traiter des incidents donnant lieu à des violations de données à caractère personnel, les autorités compétentes coopèrent étroitement avec les autorités chargées de la protection des données.

*Article 29*

**Surveillance et exécution pour les entités essentielles**

1. Les États membres veillent à ce que les mesures de surveillance ou d'exécution imposées aux entités essentielles au titre des obligations énoncées dans la présente directive soient effectives, proportionnées et dissuasives, compte tenu des circonstances de chaque cas.

2. Les États membres veillent à ce que les autorités compétentes, lorsqu'elles accomplissent leurs missions de surveillance à l'égard d'entités essentielles, aient le pouvoir de soumettre ces entités à:

   a) des inspections sur place et une surveillance à distance, y compris des contrôles aléatoires;

   b) des audits réguliers;

   c) des audits de sécurité ciblés fondés sur des évaluations des risques ou sur des informations disponibles ayant trait aux risques;

   d) des scans de sécurité fondés sur des critères d'évaluation des risques objectifs, non discriminatoires, équitables et transparents;

   e) des demandes d'informations nécessaires à l'évaluation des mesures de cybersécurité adoptées par l'entité, notamment les politiques de cybersécurité consignées par écrit, ainsi que du respect de l'obligation de notifier l'ENISA conformément à l'article 25, paragraphes 1 et 2;

   f) des demandes d'accès à des données, à des documents ou à toutes informations nécessaires à l'accomplissement de leurs missions de surveillance;

   g) des demandes de preuves de la mise en œuvre de politiques de cybersécurité, telles que les résultats des audits de sécurité effectués par un auditeur qualifié et les éléments de preuve sous-jacents correspondants.

3. Lorsqu'elles exercent leurs pouvoirs en vertu du paragraphe 2, points e) à g), les autorités compétentes mentionnent la finalité de la demande et précisent quelles sont les informations exigées.

4. Les États membres veillent à ce que les autorités compétentes, lorsqu'elles exercent leurs pouvoirs d'exécution à l'égard d'entités essentielles, aient le pouvoir:

   (a) d'émettre des avertissements concernant le non-respect par les entités des obligations énoncées dans la présente directive;

   (b) d'émettre des instructions contraignantes ou une injonction exigeant de ces entités qu'elles remédient aux insuffisances constatées ou aux violations des obligations énoncées dans la présente directive;

   (c) d'ordonner à ces entités de mettre un terme à un comportement qui ne respecte pas les obligations énoncées dans la présente directive et de ne pas le réitérer;

(d) d’ordonner à ces entités de mettre leurs mesures de gestion des risques et/ou leurs obligations de signalement en conformité avec les obligations énoncées aux articles 18 et 20 de manière spécifique et dans un délai déterminé;

(e) d’ordonner à ces entités d’informer la ou les personnes physiques ou morales à qui elles fournissent des services ou des activités susceptibles d’être affectées par une cybermenace importante de toutes mesures préventives ou réparatrices que ces personnes physiques ou morales pourraient prendre en réponse à cette menace;

(f) d’ordonner à ces entités de mettre en œuvre les recommandations formulées à la suite d’un audit de sécurité dans un délai raisonnable;

(g) de désigner, pour une période déterminée, un responsable du contrôle ayant des tâches bien définies pour superviser le respect de leurs obligations en vertu des articles 18 et 20;

(h) d’ordonner à ces entités de rendre publics les aspects de non-respect des obligations énoncées dans la présente directive de manière spécifique;

(i) de faire une déclaration publique désignant la ou les personnes physiques et morales responsables de la violation d’une obligation énoncée dans la présente directive et la nature de cette violation;

(j) d’imposer ou de demander aux juridictions ou organes compétents d'imposer, conformément à la législation nationale, une amende administrative en vertu de l’article 31 en plus ou en lieu et place des mesures visées aux points a) à i) du présent paragraphe, en fonction des circonstances propres à chaque cas.

5. Lorsque les mesures d’exécution adoptées en vertu du paragraphe 4, points a) à d) et point f), se révèlent inefficaces, les États membres veillent à ce que les autorités compétentes aient le pouvoir de fixer un délai dans lequel l’entité essentielle est invitée à prendre les mesures nécessaires pour remédier aux insuffisances ou satisfaire aux exigences de ces autorités. Si la mesure demandée n’est pas prise dans le délai imparti, les États membres veillent à ce que les autorités compétentes aient le pouvoir:

(a) de suspendre ou de demander à un organisme de certification ou d’autorisation de suspendre une certification ou une autorisation concernant tout ou partie des services ou activités fournis par une entité essentielle;

(b) d’imposer ou de demander aux juridictions ou organes compétents d'imposer, conformément à la législation nationale, une interdiction temporaire interdisant à toute personne exerçant des responsabilités dirigeantes à un niveau de directeur général ou de représentant légal dans cette entité essentielle, ainsi qu’à toute autre personne physique tenue pour responsable de la violation, d’exercer des responsabilités dirigeantes dans cette entité.

Ces sanctions sont appliquées jusqu’à ce que l’entité prenne les mesures nécessaires pour remédier aux insuffisances ou se conformer aux exigences de l’autorité compétente à l'origine de l'application de ces sanctions.

6. Les États membres veillent à ce que toute personne physique responsable d’une entité essentielle ou agissant en qualité de représentant d’une entité essentielle sur la base du pouvoir de la représenter, de prendre des décisions en son nom ou d’exercer son contrôle ait le pouvoir de veiller au respect, par l’entité, des obligations énoncées dans la présente directive. Les États membres veillent à ce que ces personnes

physiques puissent être tenues responsables des manquements à leur devoir de veiller au respect des obligations énoncées dans la présente directive.

7. Lorsqu'elles prennent des mesures d'exécution ou appliquent des sanctions en vertu des paragraphes 4 et 5, les autorités compétentes respectent les droits de la défense et tiennent compte des circonstances propres à chaque cas et, au minimum, tiennent dûment compte:

   (a) de la gravité de la violation et de l'importance des dispositions enfreintes. Parmi les violations devant être considérées comme graves, figurent: les violations répétées, le fait de ne pas notifier des incidents ayant des effets perturbateurs importants ou de ne pas y remédier, le fait de ne pas remédier aux insuffisances à la suite d'instructions contraignantes des autorités compétentes, le fait d'entraver des audits ou des activités de contrôle ordonnées par les autorités compétentes à la suite de la constatation d'une violation, la fourniture d'informations fausses ou manifestement inexactes relatives aux exigences en matière de gestion des risques ou aux obligations de signalement énoncées aux articles 18 et 20;

   (b) de la durée de la violation, y compris du caractère répété des violations;

   (c) des dommages effectifs causés, des pertes subies, des dommages potentiels ou des pertes qui auraient pu être engendrées, dans la mesure où il est possible de les déterminer. Lors de l'évaluation de cet aspect, il est tenu compte, entre autres, des pertes financières ou économiques effectives ou potentielles, des incidences sur d'autres services, du nombre d'utilisateurs touchés ou potentiellement touchés;

   (d) du fait que la violation a été commise délibérément ou par négligence;

   (e) des mesures prises par l'entité pour prévenir ou atténuer les dommages et/ou les pertes;

   (f) de l'application de codes de conduite approuvés ou de mécanismes de certification approuvés;

   (g) du degré de coopération de la ou des personnes physiques ou morales tenues pour responsables avec les autorités compétentes.

8. Les autorités compétentes exposent en détail les motifs de leurs décisions d'exécution. Avant de prendre de telles décisions, les autorités compétentes informent les entités concernées de leurs conclusions préliminaires et laissent à ces entités un délai raisonnable pour communiquer leurs observations.

9. Les États membres veillent à ce que leurs autorités compétentes informent les autorités compétentes de l'État membre concerné désignées conformément à la directive (UE) XXXX/XXXX [directive relative à la résilience des entités critiques] lorsqu'ils exercent leurs pouvoirs de surveillance et d'exécution dans le but de garantir qu'une entité définie comme critique ou une entité équivalente à une entité critique en vertu de la directive (UE) XXXX/XXXX [directive relative à la résilience des entités critiques] respecte ses obligations au titre de la présente directive. Sur demande des autorités compétentes au titre de la directive (UE) XXXX/XXXX [directive relative à la résilience des entités critiques], les autorités compétentes peuvent exercer leurs pouvoirs de surveillance et d'exécution sur une entité essentielle définie comme critique ou équivalente.

*Article 30*

**Surveillance et exécution pour les entités importantes**

1. Lorsque, selon les éléments de preuve ou les indications communiquées, une entité importante ne respecte pas les obligations énoncées dans la présente directive, et notamment aux articles 18 et 20, les États membres veillent à ce que les autorités compétentes prennent des mesures, le cas échéant, dans le cadre de mesures de contrôle ex post.

2. Les États membres veillent à ce que les autorités compétentes, lorsqu'elles accomplissent leurs missions de surveillance à l'égard d'entités importantes, aient le pouvoir de soumettre ces entités à:

   (a) des inspections sur place et une surveillance à distance ex post;

   (b) des audits de sécurité ciblés fondés sur des évaluations des risques ou sur des informations disponibles ayant trait aux risques;

   (c) des scans de sécurité fondés sur des critères d'évaluation des risques objectifs, équitables et transparents;

   (d) des demandes de toutes informations nécessaires à l'évaluation ex post des mesures de cybersécurité, notamment les politiques de cybersécurité consignées par écrit, ainsi que du respect de l'obligation de notifier l'ENISA conformément à l'article 25, paragraphes 1 et 2;

   (e) des demandes d'accès à des données, à des documents et/ou à des informations nécessaires à l'accomplissement de leurs missions de surveillance.

3. Lorsqu'elles exercent leurs pouvoirs en vertu du paragraphe 2, points d) ou e), les autorités compétentes mentionnent la finalité de la demande et précisent quelles sont les informations exigées.

4. Les États membres veillent à ce que les autorités compétentes, lorsqu'elles exercent leurs pouvoirs d'exécution à l'égard d'entités importantes, aient le pouvoir:

   (a) d'émettre des avertissements concernant le non-respect par les entités des obligations énoncées dans la présente directive;

   (b) d'émettre des instructions contraignantes ou une injonction exigeant de ces entités qu'elles remédient aux insuffisances constatées ou aux violations des obligations énoncées dans la présente directive;

   (c) d'ordonner à ces entités de mettre un terme à un comportement qui ne respecte pas les obligations énoncées dans la présente directive et de ne pas le réitérer;

   (d) d'ordonner à ces entités de mettre leurs mesures de gestion des risques ou leurs obligations de signalement en conformité avec les obligations énoncées aux articles 18 et 20 de manière spécifique et dans un délai déterminé;

   (e) d'ordonner à ces entités d'informer la ou les personnes physiques ou morales à qui elles fournissent des services ou des activités susceptibles d'être affectées par une cybermenace importante de toutes mesures préventives ou réparatrices que ces personnes physiques ou morales pourraient prendre en réponse à cette menace;

   (f) d'ordonner à ces entités de mettre en œuvre les recommandations formulées à la suite d'un audit de sécurité dans un délai raisonnable;

(g) d'ordonner à ces entités de rendre publics les aspects de non-respect de leurs obligations énoncées dans la présente directive de manière spécifique;

(h) de faire une déclaration publique désignant la ou les personnes physiques et morales responsables de la violation d'une obligation énoncée dans la présente directive et la nature de cette violation;

(i) d'imposer ou de demander l'imposition par les juridictions ou organes compétents, conformément à la législation nationale, d'une amende administrative en vertu de l'article 31 en plus ou en lieu et place des mesures visées aux points a) à h) du présent paragraphe, en fonction des circonstances propres à chaque cas.

5. L'article 29, paragraphes 6 à 8, s'applique également aux mesures de surveillance et d'exécution prévues au présent article pour les entités importantes énumérées à l'annexe II.

*Article 31*

***Conditions générales pour imposer des amendes administratives à des entités essentielles et importantes***

1. Les États membres veillent à ce que les amendes administratives imposées aux entités essentielles et importantes en vertu du présent article pour des violations des obligations énoncées dans la présente directive soient, dans chaque cas d'espèce, effectives, proportionnées et dissuasives.

2. En fonction des circonstances propres à chaque cas, les amendes administratives sont imposées en complément ou à la place des mesures visées à l'article 29, paragraphe 4, points a) à i), à l'article 29, paragraphe 5, et à l'article 30, paragraphe 4, points a) à h).

3. Pour décider s'il y a lieu d'imposer une amende administrative et pour décider de son montant, dans chaque cas d'espèce, il est dûment tenu compte, au minimum, des éléments prévus à l'article 29, paragraphe 7.

4. Les États membres veillent à ce que les violations des obligations énoncées à l'article 18 ou à l'article 20, conformément aux paragraphes 2 et 3 du présent article, soient soumises à des amendes administratives d'un montant maximum s'élevant à au moins 10 000 000 EUR ou à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle l'entité essentielle ou importante appartient, le montant le plus élevé étant retenu.

5. Les États membres peuvent prévoir le pouvoir d'imposer des astreintes pour contraindre une entité essentielle ou importante à mettre un terme à une violation conformément à une décision préalable de l'autorité compétente.

6. Sans préjudice des pouvoirs dont les autorités de contrôle disposent en vertu des articles 29 et 30, chaque État membre peut établir les règles déterminant si et dans quelle mesure des amendes administratives peuvent être imposées à des entités de l'administration publique au sens de l'article 4, paragraphe 23, sous réserve des obligations prévues dans la présente directive.

*Article 32*

***Infractions donnant lieu à une violation de données à caractère personnel***

1. Lorsque les autorités compétentes disposent d'indications selon lesquelles l'infraction commise par une entité essentielle ou importante à l'égard des obligations énoncées aux articles 18 et 20 donne lieu à une violation de données à caractère personnel au sens de l'article 4, paragraphe 12, du règlement (UE) 2016/679, devant être notifiée en vertu de l'article 33 dudit règlement, elles en informent les autorités de contrôle compétentes en vertu des articles 55 et 56 dudit règlement dans un délai raisonnable.

2. Lorsque les autorités de contrôle compétentes conformément aux articles 55 et 56 du règlement (UE) 2016/679 décident d'exercer leurs pouvoirs en vertu de l'article 58, point i), dudit règlement et d'imposer une amende administrative, les autorités compétentes n'imposent pas d'amende administrative pour la même violation au titre de l'article 31 de la présente directive. Les autorités compétentes peuvent toutefois appliquer les mesures d'exécution ou exercer les pouvoirs de sanction prévus à l'article 29, paragraphe 4, points a) à i), et à l'article 30, paragraphe 4, points a) à h), de la présente directive.

3. Lorsque l'autorité de contrôle compétente en vertu du règlement (UE) 2016/679 est établie dans un autre État membre que l'autorité compétente, l'autorité compétente informe l'autorité de contrôle établie dans le même État membre.

*Article 33*

**Sanctions**

1. Les États membres fixent des règles relatives aux sanctions applicables en cas d'infraction aux dispositions nationales adoptées en vertu de la présente directive et prennent toutes les mesures nécessaires pour que ces règles soient appliquées. Les sanctions prévues sont effectives, proportionnées et dissuasives.

2. Les États membres informent la Commission, au plus tard [deux] ans après la date d'entrée en vigueur de la présente directive, des règles et mesures adoptées à cet égard, ainsi que, sans retard indu, de toute modification qui y serait apportée ultérieurement.

*Article 34*

**Assistance mutuelle**

1. Si une entité essentielle ou importante fournit des services dans plusieurs États membres, ou a son établissement principal ou un représentant dans un État membre alors que ses réseaux et systèmes d'information sont situés dans un ou plusieurs autres États membres, l'autorité compétente de l'État membre de l'établissement principal, de l'autre établissement ou du représentant et les autorités compétentes de ces autres États membres coopèrent et se prêtent mutuellement assistance si nécessaire. Cette coopération suppose, au minimum:

   (a) que les autorités compétentes appliquant des mesures de surveillance ou d'exécution dans un État membre informent et consultent, par l'intermédiaire du point de contact unique, les autorités compétentes des autres États membres

concernés en ce qui concerne les mesures de surveillance et d'exécution prises et leur suivi, conformément aux articles 29 et 30;

(b) qu'une autorité compétente puisse demander à une autre autorité compétente de prendre les mesures de surveillance ou d'exécution visées aux articles 29 et 30;

(c) qu'une autorité compétente, dès réception d'une demande justifiée d'une autre autorité compétente, fournisse à l'autre autorité compétente une assistance afin que les mesures de surveillance ou d'exécution visées aux articles 29 et 30 puissent être mises en œuvre de manière efficace, efficiente et cohérente. Cette assistance mutuelle peut porter sur des demandes d'informations et des mesures de contrôle, y compris des demandes de procéder à des inspections sur place, à une surveillance à distance ou à des audits de sécurité ciblés. Une autorité compétente à laquelle une demande d'assistance est adressée ne peut refuser cette demande que si, après un échange avec les autres autorités concernées, l'ENISA et la Commission, il est établi que l'autorité n'est pas compétente pour fournir l'assistance demandée ou que l'assistance demandée n'est pas proportionnée aux missions de surveillance de l'autorité compétente exercées conformément à l'article 29 ou à l'article 30.

2. Le cas échéant et d'un commun accord, les autorités compétentes de différents États membres peuvent mener à bien les actions communes de surveillance visées aux articles 29 et 30.

## CHAPITRE VII

*Dispositions transitoires et finales*

### *Article 35*

### ***Révision***

La Commission réexamine périodiquement le fonctionnement de la présente directive et en rend compte au Parlement européen et au Conseil. Le compte rendu évalue notamment la pertinence des secteurs, des sous-secteurs, de la taille et du type des entités visées aux annexes I et II pour le fonctionnement de l'économie et de la société en ce qui concerne la cybersécurité. À cette fin et en vue de faire progresser la coopération stratégique et opérationnelle, la Commission tient compte des rapports du groupe de coopération et du réseau des CSIRT sur l'expérience acquise au niveau tant stratégique qu'opérationnel. Le premier rapport est présenté au plus tard le… [54 mois après la date d'entrée en vigueur de la présente directive].

### *Article 36*

### ***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 à l'article 18, paragraphe 6, et à l'article 21, paragraphe 2, est conféré à la Commission pour une période de cinq ans à compter du […].

3. La délégation de pouvoir visée à l'article 18, paragraphe 6, et à l'article 21, paragraphe 2, 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 l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer».

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

6. Un acte délégué adopté en vertu de l'article 18, paragraphe 6, et de l'article 21, paragraphe 2, 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 de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de deux mois à l'initiative du Parlement européen ou du Conseil.

*Article 37*

***Procédure de comité***

1. La Commission est assistée par un comité. Ledit comité est un comité au sens du règlement (UE) nº 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) nº 182/2011 s'applique.

3. Lorsque l'avis du comité doit être obtenu par procédure écrite, ladite procédure est close sans résultat lorsque, dans le délai prévu pour émettre un avis, le président du comité le décide ou un membre du comité le demande.

*Article 38*

***Transposition***

1. Les États membres adoptent et publient, au plus tard le… [18 mois après l'entrée en vigueur de la présente directive], les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive. Ils en informent immédiatement la Commission. Ils appliquent ces dispositions à partir du… [un jour après la date visée au premier alinéa].

2. Lorsque les États membres adoptent ces dispositions, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de

leur publication officielle. Les modalités de cette référence sont arrêtées par les États membres.

*Article 39*

***Modification du règlement (UE) nº 910/2014***

L'article 19 du règlement (UE) nº 910/2014 est supprimé.

*Article 40*

***Modification de la directive (UE) 2018/1972***

Les articles 40 et 41 de la directive (UE) 2018/1972 sont supprimés.

*Article 41*

***Abrogation***

La directive (UE) 2016/1148 est abrogée avec effet au… [date limite de transposition de la directive].

Les références à la directive (UE) 2016/1148 s'entendent comme faites à la présente directive et sont à lire selon le tableau de correspondance figurant à l'annexe III.

*Article 42*

***Entrée en vigueur***

La présente directive entre en vigueur le vingtième jour suivant celui de sa publication au Journal officiel de l'Union européenne.

*Article 43*

***Destinataires***

Les États membres sont destinataires de la présente directive.

Fait à Bruxelles, le

*Par le Parlement européen*
*Le président*

*Par le Conseil*
*Le président*

**FICHE FINANCIÈRE LÉGISLATIVE**

# Contenu

## 1. CADRE DE LA PROPOSITION/DE L'INITIATIVE

### 1.1. Dénomination de la proposition/de l'initiative

Proposition de directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148

### 1.2. Domaine(s) politique(s) concerné(s) *(groupe de programmes)*

Réseaux de communication, contenu et technologies

### 1.3. La proposition/l'initiative porte sur:

☐ **une action nouvelle**

☐ **une action nouvelle suite à un projet pilote/une action préparatoire**[40]

☒ **la prolongation d'une action existante**

☐ **une fusion ou une réorientation d'une ou de plusieurs actions vers une autre action/une action nouvelle**

### 1.4. Justification(s) de la proposition/de l'initiative

*1.4.1. Besoin(s) à satisfaire à court ou à long terme, assorti(s) d'un calendrier détaillé pour la mise en œuvre de l'initiative*

L'objectif de la révision est d'accroître le niveau de cyber-résilience d'un ensemble exhaustif d'entreprises opérant dans l'Union européenne dans tous les secteurs concernés, de réduire les incohérences en matière de résilience dans l'ensemble du marché intérieur dans les secteurs déjà couverts par la directive et d'améliorer le niveau de prise de conscience conjointe de la situation et la capacité collective à se préparer et à réagir.

*1.4.2. Valeur ajoutée de l'intervention de l'Union (celle-ci peut résulter de différents facteurs: gains de coordination, sécurité juridique, efficacité accrue, complémentarités, etc.). Aux fins du présent point, on entend par «valeur ajoutée de l'intervention de l'Union» la valeur découlant de l'intervention de l'Union qui vient s'ajouter à la valeur qui, sans cela, aurait été générée par la seule action des États membres.*

La résilience en matière de cybersécurité dans l'ensemble de l'Union ne peut être effective si elle est appréhendée de manière disparate sous l'effet de cloisonnements nationaux ou régionaux. La directive SRI est venue combler cette lacune en établissant un cadre pour la sécurité des réseaux et des systèmes d'information au niveau national et au niveau de l'Union. Toutefois, le premier réexamen périodique de la directive SRI a mis en évidence un certain nombre de défauts inhérents qui ont fini par donner lieu à des disparités considérables entre les États membres en termes de capacités, de planification et de niveau de protection, ce qui porte en même temps atteinte à l'égalité des conditions de concurrence pour des entreprises similaires sur le marché intérieur.

Une intervention de l'Union allant au-delà des mesures actuelles de la directive SRI se justifie principalement par: i) la nature transfrontière du problème; ii) le potentiel

[40] Tel(le) que visé(e) à l'article 58, paragraphe 2, point a) ou b), du règlement financier.

de l'action de l'Union pour améliorer et permettre des politiques nationales efficaces; iii) la contribution de mesures stratégiques concertées et collaboratives en matière de SRI à la protection efficace des données et de la vie privée.

Les objectifs énoncés peuvent donc être plus aisément atteints par une action au niveau de l'Union que par les États membres seuls.

*1.4.3. Leçons tirées d'expériences similaires*

La directive SRI est le premier instrument horizontal du marché intérieur visant à améliorer la résilience des réseaux et des systèmes dans l'Union face aux risques liés à la cybersécurité. Elle a déjà grandement contribué à accroître le niveau commun de cybersécurité parmi les États membres. Cependant, le réexamen du fonctionnement et de la mise en œuvre de la directive a mis en évidence un certain nombre de lacunes qui, outre la numérisation croissante et la nécessité d'apporter une réponse plus actualisée, doivent être comblées dans un acte juridique révisé.

*1.4.4. Compatibilité et synergie éventuelle avec d'autres instruments appropriés*

La nouvelle proposition est pleinement cohérente avec d'autres initiatives connexes telles que la proposition de règlement sur la résilience opérationnelle numérique du secteur financier et la proposition de directive sur la résilience des opérateurs critiques de services essentiels. Elle est également cohérente avec le code des communications électroniques européen, le règlement général sur la protection des données et le règlement eIDAS.

La proposition est un élément essentiel de la stratégie de l'UE pour l'union de la sécurité.

## 1.5. Durée et incidence financière

☐ **durée limitée**

– ☐ en vigueur à partir de/du [JJ/MM]AAAA jusqu'en/au [JJ/MM]AAAA

– ☐ incidence financière de AAAA jusqu'en AAAA pour les crédits d'engagement et de AAAA jusqu'en AAAA pour les crédits de paiement.

☒ **durée illimitée**

– Mise en œuvre avec une période de montée en puissance de 2022 jusqu'en 2025,

– puis un fonctionnement à un rythme de croisière au-delà.

## 1.6. Mode(s) de gestion prévu(s)[41]

**Gestion directe** par la Commission

– ☒ dans ses services, y compris par l'intermédiaire de son personnel dans les délégations de l'Union;

– ☐ par les agences exécutives.

☐ **Gestion partagée** avec les États membres

☐ **Gestion indirecte** en confiant des tâches d'exécution budgétaire:

– ☐ à des pays tiers ou aux organismes qu'ils ont désignés;

– ☐ à des organisations internationales et à leurs agences (à préciser);

– ☐ à la BEI et au Fonds européen d'investissement;

– X☐ aux organismes visés aux articles 70 et 71 du règlement financier;

– ☐ à des organismes de droit public;

– ☐ à des organismes de droit privé investis d'une mission de service public, pour autant qu'ils présentent les garanties financières suffisantes;

– ☐ à des organismes de droit privé d'un État membre qui sont chargés de la mise en œuvre d'un partenariat public-privé et présentent les garanties financières suffisantes;

– ☐ à des personnes chargées de l'exécution d'actions spécifiques relevant de la PESC, en vertu du titre V du traité sur l'Union européenne, identifiées dans l'acte de base concerné.

– *Si plusieurs modes de gestion sont indiqués, veuillez donner des précisions dans la partie «Remarques».*

Remarques

L'Agence de l'Union européenne pour la cybersécurité, l'ENISA, à laquelle le règlement sur la cybersécurité a octroyé un nouveau mandat permanent, aidera les États membres et la Commission dans la mise en œuvre de la directive SRI révisée.

Du fait de la révision de la directive SRI, à compter de 2022/2023, l'ENISA aura des domaines d'action supplémentaires. Bien que ces domaines d'action relèvent des missions générales de l'ENISA conformément à son mandat, ils entraîneront une charge de travail

[41] Les explications sur les modes de gestion ainsi que les références au règlement financier sont disponibles sur le site BudgWeb: https://myintracomm.ec.europa.eu/budgweb/FR/man/budgmanag/Pages/budgmanag.aspx

supplémentaire pour l'agence. Plus précisément, outre ses domaines d'action actuels, en vertu de la proposition de la Commission relative à une directive SRI révisée, l'ENISA devra également intégrer spécifiquement dans son programme de travail, entre autres, les actions suivantes: i) élaborer et gérer un registre européen des vulnérabilités (article 6, paragraphe 2, de la proposition), ii) assurer le secrétariat du réseau européen d'organisations de liaison en cas de crises de cybersécurité (réseau CyCLONe) (article 14 de la proposition) et publier un rapport annuel sur l'état de la cybersécurité dans l'UE (article 15 de la proposition), iii) soutenir l'organisation d'évaluations par les pairs entre les États membres (article 16 de la proposition), iv) recueillir des données agrégées sur les incidents auprès des États membres et émettre des orientations techniques (article 20, paragraphe 9, de la proposition), v) créer et maintenir un registre des entités qui fournissent des services transfrontières (article 25 de la proposition).

Par conséquent, une demande de 5 ETP supplémentaires sera présentée à partir de 2022, accompagnée d'un budget correspondant d'environ 610 000 EUR par an pour couvrir ces nouveaux postes (voir la fiche financière séparée «agences»).

## 2. MESURES DE GESTION

### 2.1. Dispositions en matière de suivi et de compte rendu

*Préciser la fréquence et les conditions de ces dispositions.*

La Commission réexaminera périodiquement le fonctionnement de la directive et en rendra compte au Parlement européen et au Conseil, la première fois trois ans après son entrée en vigueur.

La Commission établira également si les États membres transposent correctement la directive.

### 2.2. Système(s) de gestion et de contrôle

*2.2.1. Justification du (des) mode(s) de gestion, du (des) mécanisme(s) de mise en œuvre du financement, des modalités de paiement et de la stratégie de contrôle proposée*

L'unité au sein de la DG CNECT chargée de ce domaine politique assurera la mise en œuvre de la directive.

*2.2.2. Informations sur les risques recensés et sur le(s) système(s) de contrôle interne mis en place pour les atténuer*

Risque très faible, étant donné que l'écosystème de la directive SRI est déjà en place.

*2.2.3. Estimation et justification du rapport coût/efficacité des contrôles (rapport «coûts du contrôle ÷ valeur des fonds gérés concernés»), et évaluation du niveau attendu de risque d'erreur (lors du paiement et lors de la clôture)*

Sans objet. Seul le budget administratif («enveloppe globale») sera utilisé.

### 2.3. Mesures de prévention des fraudes et irrégularités

*Préciser les mesures de prévention et de protection existantes ou envisagées, au titre de la stratégie antifraude par exemple.*

Sans objet. Seul le budget administratif («enveloppe globale») sera utilisé.

## 3. INCIDENCE FINANCIÈRE ESTIMÉE DE LA PROPOSITION/DE L'INITIATIVE

### 3.1. Rubrique du cadre financier pluriannuel et nouvelle(s) ligne(s) budgétaire(s) de dépenses proposée(s)

| Rubrique du cadre financier pluriannuel | Ligne budgétaire | Nature de la dépense | Participation | | | |
|---|---|---|---|---|---|---|
| | Numéro [Rubrique 7……...……] | CD/CND[42] | de pays AELE[43] | de pays candidats[44] | de pays tiers | au sens de l'article 21, paragraphe 2, point b), du règlement financier |
| | 20 02 06 dépenses de gestion<br><br>20 02 06 | CND | NON | NON | NON | NON |

42 CD = crédits dissociés / CND = crédits non dissociés.

43 AELE: Association européenne de libre-échange.

44 Pays candidats et, le cas échéant, pays candidats potentiels des Balkans occidentaux.

## 3.2. Incidence estimée sur les dépenses

### *3.2.1. Synthèse de l'incidence estimée sur les dépenses*

En Mio EUR (à la 3e décimale)

| **Rubrique du cadre financier pluriannuel** | **<…>** | [Rubrique……...……] |
|---|---|---|

| | | | **2021** | **2022** | **2023** | **2024** | **2025** | **2026** | **2027** | ***Après 2027*** | **TOTAL** |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Crédits opérationnels (répartis en fonction des lignes budgétaires énumérées au point 3.1) | Engagements | (1) | | | | | | | | | |
| | Paiements | (2) | | | | | | | | | |
| Crédits de nature administrative financés par l'enveloppe du programme[45] | Engagements = Paiements | (3) | | | | | | | | | |
| **TOTAL des crédits pour l'enveloppe du programme** | Engagements | =1+3 | | | | | | | | | |
| | Paiements | =2+3 | | | | | | | | | |

| | | |
|---|---|---|
| **Rubrique du cadre financier pluriannuel** | 7 | «Dépenses administratives»<br>Réunions: les réunions plénières du groupe de coopération SRI se tiennent généralement quatre fois par an. La Commission couvre les frais de restauration et les frais de déplacement des représentants des 27 États membres (un représentant par État membre). Les coûts d'une réunion peuvent s'élever jusqu'à 15 000 EUR.<br>Missions: Les missions ont trait au suivi de la mise en œuvre de la directive SRI. Exemple: Au cours d'une année (mai 2019 - juillet 2020), il était prévu que nous organisions des «visites SRI» dans les pays et que nous nous rendions dans les 27 États membres pour discuter de la mise en œuvre de la directive SRI dans |

[45] Assistance technique et/ou administrative et dépenses d'appui à la mise en œuvre de programmes et/ou d'actions de l'UE (anciennes lignes «BA»), recherche indirecte, recherche directe.

| | | |
|---|---|---|
| | | l'ensemble de l'UE. |

Cette partie est à compléter en utilisant les «données budgétaires de nature administrative», à introduire d'abord dans l'annexe de la fiche financière législative, à charger dans DECIDE pour les besoins de la consultation interservices.

En Mio EUR (à la 3e décimale)

| | | 2021 | 2022 | 2023 | 2024 | 2025 | 2026 | 2027 | *Après 2027* | TOTAL |
|---|---|---|---|---|---|---|---|---|---|---|
| Ressources humaines | | 1,14 | 1,14 | 1,14 | 1,14 | 1,14 | 1,14 | **1,14** | | **7,98** |
| Autres dépenses administratives | | **0,09** | **0,09** | **0,09** | **0,09** | **0,09** | **0,09** | **0,09** | | **0,63** |
| **TOTAL des crédits pour la RUBRIQUE 7 du cadre financier pluriannuel** | (Total engagements = Total paiements) | **1,23** | **1,23** | **1,23** | **1,23** | **1,23** | **1,23** | **1,23** | | **8,61** |

En Mio EUR (à la 3e décimale)

| | | 2021 | 2022 | 2023 | 2024 | 2025 | 2026 | 2027 | *Après 2027* | TOTAL |
|---|---|---|---|---|---|---|---|---|---|---|
| **TOTAL des crédits des diverses RUBRIQUES** du cadre financier pluriannuel | Engagements | | | | | | | | | |
| | Paiements | | | | | | | | | |

*3.2.2. Synthèse de l'incidence estimée sur les crédits de nature administrative*

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits de nature administrative.

– ☐X La proposition/l'initiative engendre l'utilisation de crédits de nature administrative, comme expliqué ci-après:

En Mio EUR (à la 3e décimale)

| Années | 2021 | 2022 | 2023 | 2024 | 2025 | 2026 | 2027 | TOTAL |
|---|---|---|---|---|---|---|---|---|
| **RUBRIQUE 7 du cadre financier pluriannuel** | | | | | | | | |
| Ressources humaines | 1,14 | 1,14 | 1,14 | 1,14 | 1,14 | 1,14 | **1,14** | **7,98** |
| Autres dépenses administratives | 0,09 | 0,09 | 0,09 | 0,09 | 0,09 | 0,09 | **0,09** | **0,63** |
| **Sous-Total RUBRIQUE 7 du cadre financier pluriannuel** | 1,23 | 1,23 | 1,23 | 1,23 | 1,23 | 1,23 | **1,23** | **8,61** |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Hors RUBRIQUE 7[46] du cadre financier pluriannuel** | | | | | | | | |
| Ressources humaines | | | | | | | | |
| Autres dépenses de nature administrative | | | | | | | | |
| **Sous-total hors RUBRIQUE 7 du cadre financier pluriannuel** | | | | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **TOTAL** | **1,23** | **1,23** | **1,23** | **1,23** | **1,23** | **1,23** | **1,23** | **8,61** |

Les besoins en crédits pour les ressources humaines et les autres dépenses de nature administrative seront couverts par les crédits de la DG déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés le cas échéant par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes.

46 Assistance technique et/ou administrative et dépenses d'appui à la mise en œuvre de programmes et/ou d'actions de l'UE (anciennes lignes «BA»), recherche indirecte, recherche directe.

3.2.2.1. Besoins estimés en ressources humaines

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de ressources humaines.

– X☐ La proposition/l'initiative engendre l'utilisation de ressources humaines, comme expliqué ci-après:

*Estimation à exprimer en équivalents temps plein*

| **Années** | | **2021** | **2022** | **2023** | **2024** | **2025** | **2026** | **2027** |
|---|---|---|---|---|---|---|---|---|
| • **Emplois du tableau des effectifs (fonctionnaires et agents temporaires)** | | | | | | | | |
| Siège et bureaux de représentation de la Commission | | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| Délégations | | | | | | | | |
| Recherche | | | | | | | | |
| • **Personnel externe (en équivalents temps plein: ETP) — AC, AL, END, INT et JED** [47] Rubrique 7 | | | | | | | | |
| Financés au titre de la RUBRIQUE 7 du cadre financier pluriannuel | - au siège | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| | - en délégation | | | | | | | |
| Financés par l'enveloppe du programme [48] | - au siège | | | | | | | |
| | - en délégation | | | | | | | |
| Recherche | | | | | | | | |
| Autre (préciser) | | | | | | | | |
| **TOTAL** | | **9** | **9** | **9** | **9** | **9** | **9** | **9** |

Les besoins en ressources humaines seront couverts par les effectifs de la DG déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés si nécessaire par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes.

Description des tâches à effectuer:

| | |
|---|---|
| Fonctionnaires et agents temporaires | • préparation d'actes délégués conformément à l'article 18, paragraphe 6, à l'article 21, paragraphe 2, et à l'article 36;<br>• préparation d'actes d'exécution conformément à l'article 12, paragraphe 8, à l'article 18, paragraphe 5, et à l'article 20, paragraphe 11;<br>• mise à disposition d'un secrétariat au groupe de coopération SRI;<br>• organisation des réunions plénières et des réunions des volets de travail du groupe de coopération SRI;<br>• coordination du travail des États membres sur différents documents (orientations, boîte à outils, etc.);<br>• liaison avec d'autres services de la Commission, l'ENISA et les autorités nationales en vue de mettre en œuvre la directive SRI;<br>• analyse des méthodes et des bonnes pratiques nationales relatives à la mise en œuvre de la directive SRI. |
| Personnel externe | Participation aux tâches ci-dessus en fonction des besoins |

47 AC = agent contractuel; AL = agent local; END = expert national détaché; INT = intérimaire; JPD = jeune professionnel en délégation.

48 Sous-plafonds de personnel externe financés sur crédits opérationnels (anciennes lignes «BA»).

*3.2.3. Participation de tiers au financement*

La proposition/l'initiative

– X☐ ne prévoit pas de cofinancement par des tiers

– ☐ prévoit le cofinancement par des tiers estimé ci- après:

Crédits en Mio EUR (à la 3e décimale)

| Années | 2021 | 2022 | 2023 | 2024 | 2025 | 2026 | 2027 | TOTAL |
|---|---|---|---|---|---|---|---|---|
| Préciser l'organisme de cofinancement | | | | | | | | |
| TOTAL des crédits cofinancés | | | | | | | | |

## 3.3. Incidence estimée sur les recettes

– ☐X La proposition/l'initiative est sans incidence financière sur les recettes.

– ☐ La proposition/l'initiative a une incidence financière décrite ci-après:

☐ sur les ressources propres

☐ sur les autres recettes

veuillez indiquer si les recettes sont affectées à des lignes de dépenses ☐

En Mio EUR (à la 3e décimale)

| Ligne budgétaire de recettes: | Incidence de la proposition/de l'initiative[49] | | | | | | |
|---|---|---|---|---|---|---|---|
| | 2021 | 2022 | 2023 | 2024 | 2025 | 2026 | 2027 |
| Article ……. | | | | | | | |

Pour les recettes qui seront «affectées», préciser la (les) ligne(s) budgétaire(s) de dépenses concernée(s).

Autres remarques (relatives par exemple à la méthode/formule utilisée pour le calcul de l'incidence sur les recettes ou toute autre information).

[49] En ce qui concerne les ressources propres traditionnelles (droits de douane, cotisations sur le sucre), les montants indiqués doivent être des montants nets, c'est-à-dire des montants bruts après déduction de 20 % de frais de perception.

# ANNEXE
# de la FICHE FINANCIÈRE LÉGISLATIVE

Dénomination de la proposition/l'initiative:

Proposition de directive modifiant la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union

……
……

**1. NOMBRE et COÛT des RESSOURCES HUMAINES ESTIMÉES NÉCESSAIRES**

**2. COÛT des AUTRES DÉPENSES de NATURE ADMINISTRATIVE**

**3. MÉTHODES de CALCUL UTILISÉES pour l'ESTIMATION des COÛTS**

**3.1 Ressources humaines**

**3.2 Autres dépenses administratives**

*La présente annexe, **à compléter par chaque DG/service prenant part à la proposition/l'initiative**, accompagne la fiche financière législative lors du lancement de la consultation interservices.*

*Les tableaux de données servent à alimenter les tableaux contenus dans la fiche financière législative. Ils restent un document strictement interne à la Commission.*

1. Coût des ressources humaines estimées nécessaires

☐ La proposition/l'initiative n'engendre pas l'utilisation de ressources humaines.

X☐ La proposition/l'initiative engendre l'utilisation de ressources humaines, comme expliqué ci-après:

En Mio EUR (à la 3e décimale)

| **RUBRIQUE 7** du cadre financier pluriannuel | | **2021** | | **2022** | | **2023** | | **2024** | | **2025** | | **2026** | | **2027** | | **TOTAL** | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | ETP | Crédits | ETP | Crédits | ETP | Crédits | ETP | Crédits | ETP | Crédits | ETP | Crédits | ETP | Crédits | ETP | Crédits |
| **• Emplois du tableau des effectifs (fonctionnaires et agents temporaires)** | | | | | | | | | | | | | | | | | |
| Siège et bureaux de représentation de la Commission | AD | 6 | 0,9 | 6 | 0,9 | 6 | 0,9 | 6 | 0,9 | 6 | 0,9 | 6 | 0,9 | 6 | 0,9 | 42 | 6,3 |
| | TSA | | | | | | | | | | | | | | | | |
| en délégation: | AD | | | | | | | | | | | | | | | | |
| | TSA | | | | | | | | | | | | | | | | |
| **• Personnel externe [50] 0,24** | | | | | | | | | | | | | | | | | |
| Enveloppe globale | AC | 3 | 0,24 | 3 | 0,24 | 3 | 0,24 | 3 | 0,24 | 3 | 0,24 | 3 | 0,24 | 3 | 0,24 | 21 | 1,68 |
| | FIN | | | | | | | | | | | | | | | | |
| | INT | | | | | | | | | | | | | | | | |
| en délégation: | AC | | | | | | | | | | | | | | | | |
| | AL | | | | | | | | | | | | | | | | |
| | FIN | | | | | | | | | | | | | | | | |

[50] AC = agent contractuel; AL = agent local; END = expert national détaché; INT = intérimaire; JPD = jeune professionnel en délégation.

| | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | INT | | | | | | | | | | | | | | | | |
| | JPD | | | | | | | | | | | | | | | | |
| Autres lignes budgétaires (*à préciser*) | | | | | | | | | | | | | | | | | |
| **Sous-total – RUBRIQUE 7** du cadre financier pluriannuel | | 9 | 1,14 | 9 | 1,14 | 9 | 1,14 | 9 | 1,14 | 9 | 1,14 | 9 | 1,14 | 9 | 1,14 | 63 | 7,98 |

Les besoins en ressources humaines seront couverts par les effectifs de la DG déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés si nécessaire par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes.

| Hors RUBRIQUE 7 du cadre financier pluriannuel | | 2021 | | 2022 | | 2023 | | 2024 | | 2025 | | 2025 | | 2025 | | TOTAL | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | ETP | Crédits | ETP | Crédits | ETP | Crédits | ETP | Crédits | ETP | Crédits | ETP | Crédits | ETP | Crédits | ETP | Crédits |
| **• Emplois du tableau des effectifs (fonctionnaires et agents temporaires)** | | | | | | | | | | | | | | | | | |
| Recherche | AD | | | | | | | | | | | | | | | | |
| | TSA | | | | | | | | | | | | | | | | |
| **• Personnel externe [51]** | | | | | | | | | | | | | | | | | |
| Personnel externe financé sur crédits opérationnels (anciennes lignes «BA») | - au siège AC | | | | | | | | | | | | | | | | |
| | - au siège FIN | | | | | | | | | | | | | | | | |
| | - au siège INT | | | | | | | | | | | | | | | | |
| | - en délégation AC | | | | | | | | | | | | | | | | |
| | - en délégation AL | | | | | | | | | | | | | | | | |
| | - en délégation FIN | | | | | | | | | | | | | | | | |
| | - en délégation INT | | | | | | | | | | | | | | | | |
| | - en délégation JPD | | | | | | | | | | | | | | | | |
| Recherche | AC | | | | | | | | | | | | | | | | |
| | FIN | | | | | | | | | | | | | | | | |
| | INT | | | | | | | | | | | | | | | | |
| Autres lignes budgétaires (*à* | | | | | | | | | | | | | | | | | |

[51] AC = agent contractuel; AL = agent local; END = expert national détaché; INT = intérimaire; JPD = jeune professionnel en délégation.

| | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *préciser*) | | | | | | | | | | | | | | | | | |
| **Sous-total - Hors RUBRIQUE 7**<br>du cadre financier pluriannuel | | | | | | | | | | | | | | | | | |

Les besoins en ressources humaines seront couverts par les effectifs de la DG déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés si nécessaire par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes.

*Incidence estimée sur les ressources humaines de l'ENISA*

L'Agence de l'Union européenne pour la cybersécurité, l'ENISA, à laquelle le règlement sur la cybersécurité a octroyé un nouveau mandat permanent, aidera les États membres et la Commission dans la mise en œuvre de la directive SRI révisée.

Du fait de la révision de la directive SRI, à compter de 2022/2023, l'ENISA aura des domaines d'action supplémentaires. Bien que ces domaines d'action relèvent des missions générales de l'ENISA conformément à son mandat, ils entraîneront une charge de travail supplémentaire pour l'agence. Plus précisément, outre ses domaines d'action actuels, en vertu de la proposition de la Commission relative à une directive SRI révisée, l'ENISA devra également intégrer spécifiquement dans son programme de travail, entre autres, les actions suivantes: i) élaborer et gérer un registre européen des vulnérabilités (article 6, paragraphe 2, de la proposition), ii) assurer le secrétariat du réseau européen d'organisations de liaison en cas de crises de cybersécurité (réseau CyCLONe) (article 14 de la proposition) et publier un rapport annuel sur l'état de la cybersécurité dans l'UE (article 15 de la proposition), iii) soutenir l'organisation d'évaluations par les pairs entre les États membres (article 16 de la proposition), iv) recueillir des données agrégées sur les incidents auprès des États membres et émettre des orientations techniques (article 20, paragraphe 9, de la proposition), v) créer et maintenir un registre des entités qui fournissent des services transfrontières (article 25 de la proposition).

Par conséquent, une demande de 5 ETP supplémentaires sera présentée à partir de 2022, accompagnée d'un budget correspondant d'environ 610 000 EUR par an pour couvrir ces nouveaux postes (voir la fiche financière séparée «agences»).

Par conséquent, une demande de 5 ETP supplémentaires sera présentée à partir de 2022, accompagnée du budget correspondant pour couvrir ces nouveaux postes.

☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits de nature administrative.

☐X La proposition/l'initiative engendre l'utilisation de crédits de nature administrative, comme expliqué ci-après:

En Mio EUR (à la 3e décimale)

| | Année **N** [52] **2022** | Année **N+1** **2023** | Année **N+2** **2024** | Année **N+3** **2025** | Indiquer le nombre d'années correspondant à la durée de l'incidence (cf. point 1.6) | **TOTAL** |
|---|---|---|---|---|---|---|

[52] L'année N est l'année du début de la mise en œuvre de la proposition/de l'initiative. Veuillez remplacer «N» par la première année de mise en œuvre prévue (par exemple: 2021). Procédez de la même façon pour les années suivantes.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Agents temporaires (grades AD) | 0,450 | 0,450 | 0,450 | 0,450 | 0,450 | 0,450 | | **2,7** |
| Agents temporaires (grades AST) | | | | | | | | |
| Agents contractuels | 0,160 | 0,160 | 0,160 | 0,160 | 0,160 | 0,160 | | |
| Experts nationaux détachés | | | | | | | | **0,96** |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **TOTAL** | **0,61** | **0,61** | **0,61** | **0,61** | **0,61** | **0,61** | | **3,66** |

Besoins en personnel (ETP):

| | Année **N** [53] **2022** | Année **N+1** **2023** | Année **N+2** **2024** | Année **N+3** **2025** | Indiquer le nombre d'années correspondant à la durée de l'incidence (cf. point 1.6) | | | **TOTAL** |
|---|---|---|---|---|---|---|---|---|
| Agents temporaires (grades AD) | 3 | 3 | 3 | 3 | 3 | 3 | | **18** |
| Agents temporaires (grades AST) | | | | | | | | |
| Agents contractuels | 2 | 2 | 2 | 2 | 2 | 2 | | **12** |

[53] L'année N est l'année du début de la mise en œuvre de la proposition/de l'initiative. Veuillez remplacer «N» par la première année de mise en œuvre prévue (par exemple: 2021). Procédez de la même façon pour les années suivantes.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Experts nationaux détachés | | | | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **TOTAL** | **5** | **5** | **5** | **5** | **5** | **5** | | **30** |

2. Coût des autres dépenses de nature administrative

☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits de nature administrative

X☐ La proposition/l'initiative engendre l'utilisation de crédits de nature administrative, comme expliqué ci-après:

*En Mio EUR (à la 3e décimale)*

| **RUBRIQUE 7** du cadre financier pluriannuel | **2021** | **2022** | **2023** | **2024** | **2025** | **2026** | **2027** | **Total** |
|---|---|---|---|---|---|---|---|---|
| **Au siège:** | | | | | | | | |
| Frais de missions et de représentation | 0,03 | 0,03 | 0,03 | 0,03 | 0,03 | 0,03 | 0,03 | **0,21** |
| Frais de conférences et de réunions | 0,06 | 0,06 | 0,06 | 0,06 | 0,06 | 0,06 | 0,06 | **0,42** |
| Comités[54] | | | | | | | | |
| Études et consultations | | | | | | | | |

[54] Préciser le type de comité, ainsi que le groupe auquel il appartient.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Systèmes d'information et de gestion | | | | | | | | |
| Équipements et services liés aux TIC[55] | | | | | | | | |
| Autres lignes budgétaires (*à préciser le cas échéant*) | | | | | | | | |
| **En délégation:** | | | | | | | | |
| Frais de mission, de conférence et de représentation | | | | | | | | |
| Perfectionnement professionnel | | | | | | | | |
| Frais d'acquisition et de location et frais connexes | | | | | | | | |
| Équipement, mobilier, fournitures et prestations de services | | | | | | | | |
| **Sous-Total RUBRIQUE 7** du cadre financier pluriannuel | 0,09 | 0,09 | 0,09 | 0,09 | 0,09 | 0,09 | 0,09 | **0,63** |

[55] TIC: technologies de l'information et des communications: la DG DIGIT doit être consultée.

*En Mio EUR (à la 3e décimale)*

| **Hors RUBRIQUE 7**<br>du cadre financier pluriannuel | **2021** | **2022** | **2023** | **2024** | **2025** | **2026** | **2027** | **Total** |
|---|---|---|---|---|---|---|---|---|
| Dépenses d'assistance technique et administrative (hors personnel externe), sur crédits opérationnels (anciennes lignes «BA») | | | | | | | | |
| - au siège | | | | | | | | |
| - en délégation | | | | | | | | |
| Autres dépenses de gestion pour la recherche | | | | | | | | |
| Autres lignes budgétaires (*à préciser le cas échéant*) | | | | | | | | |
| **Sous-total – Hors RUBRIQUE 7**<br>du cadre financier pluriannuel | | | | | | | | |

| **TOTAL**<br>**RUBRIQUE 7 et Hors RUBRIQUE 7**<br>du cadre financier pluriannuel | 1,23 | 1,23 | 1,23 | 1,23 | 1,23 | 1,23 | 1,23 | **8,61** |
|---|---|---|---|---|---|---|---|---|

Les besoins en crédits de nature administrative seront couverts par les crédits déjà affectés à la gestion de l'action et/ou réaffectés, complétés le cas échéant par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes.

3. Méthodes de calcul utilisées pour l'estimation des coûts

3.1 Ressources humaines

*Cette partie explicite la méthode de calcul retenue pour l'estimation des ressources humaines jugées nécessaires [hypothèses concernant la charge de travail, y inclus les métiers spécifiques (profils de postes Sysper 2), les catégories de personnel et les coûts moyens correspondants].*

| **RUBRIQUE 7** du cadre financier pluriannuel |
|---|
| Note: les coûts moyens par catégorie de personnel au siège sont disponibles sur BudgWeb, à l'adresse suivante: https://myintracomm.ec.europa.eu/budgweb/FR/pre/legalbasis/Pages/pre-040-020_preparation.aspx |
| • Fonctionnaires et agents temporaires<br>6 fonctionnaires ETP (coût moyen 0,150) = 0,9 par an<br>- préparation d'actes délégués conformément à l'article 18, paragraphe 6, à l'article 21, paragraphe 2, et à l'article 36;<br>- préparation d'actes d'exécution conformément à l'article 12, paragraphe 8, à l'article 18, paragraphe 5, et à l'article 20, paragraphe 11;<br>- mise à disposition d'un secrétariat au groupe de coopération SRI;<br>- organisation des réunions plénières et des réunions des volets de travail du groupe de coopération SRI;<br>- coordination du travail des États membres sur différents documents (orientations, boîte à outils, etc.);<br>- liaison avec d'autres services de la Commission, l'ENISA et les autorités nationales en vue de mettre en œuvre la directive SRI;<br>- analyse des méthodes et des bonnes pratiques nationales relatives à la mise en œuvre de la directive SRI. |
| • Personnel externe<br>3 AC (coût moyen 0,08) = 0,24 par an<br>- Participation aux tâches ci-dessus en fonction des besoins |

| **Hors RUBRIQUE 7** du cadre financier pluriannuel |
|---|
| • Seulement postes financés à charge du budget de la recherche |
| • Personnel externe |

3.2 Autres dépenses administratives

*Détailler par ligne budgétaire la méthode de calcul utilisée,*

*en particulier les hypothèses sous-jacentes (par exemple nombre de réunions par an, coûts moyens, etc.)*

**RUBRIQUE 7** du cadre financier pluriannuel

Réunions: Les réunions plénières du groupe de coopération SRI se tiennent généralement quatre fois par an. La Commission couvre les frais de restauration et les frais de déplacement des représentants des 27 États membres (un représentant par État membre). Les coûts d'une réunion peuvent s'élever jusqu'à 15 000 EUR, soit 60 000 EUR par an.

Missions: Les missions ont trait au suivi de la mise en œuvre de la directive SRI. Exemple: Au cours d'une année (mai 2019 - juillet 2020), il était prévu que nous organisions des «visites SRI» dans les pays et que nous nous rendions dans les 27 États membres pour discuter

de la mise en œuvre de la directive SRI dans l'ensemble de l'UE.

**Hors RUBRIQUE 7** du cadre financier pluriannuel

**ANNEXE 7**

**de la**
**DÉCISION DE LA COMMISSION**

**relative aux règles internes sur l'exécution du budget général de l'Union européenne (section Commission européenne) à l'attention des services de la Commission**

## FICHE FINANCIÈRE LÉGISLATIVE «AGENCES»

**La présente fiche financière législative porte sur la demande d'augmentation des effectifs de l'ENISA de 5 ETP à compter de 2022 pour réaliser des activités supplémentaires liées à la mise en œuvre de la directive SRI. Ces activités sont déjà couvertes par le mandat de l'ENISA.**

Table des matières

## 1. CADRE DE LA PROPOSITION/DE L'INITIATIVE

### 1.1. Dénomination de la proposition/de l'initiative

Proposition de directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148.

### 1.2. Domaine(s) politique(s) concerné(s)

Réseaux de communication, contenu et technologies

### 1.3. La proposition porte sur:

☐ **une action nouvelle**

☐ **une action nouvelle suite à un projet pilote/une action préparatoire**[56]

☒ **la prolongation d'une action existante**

☐ **la fusion d'une ou plusieurs actions pour créer une action supplémentaire ou une action nouvelle**

## 1.4. Objectif(s)

### *1.4.1. Objectif général/objectifs généraux*

L'objectif de la révision est d'accroître le niveau de cyber-résilience d'un ensemble exhaustif d'entreprises opérant dans l'Union européenne dans tous les secteurs concernés, de réduire les incohérences en matière de résilience dans l'ensemble du marché intérieur dans les secteurs déjà couverts par la directive et d'améliorer le niveau de prise de conscience conjointe de la situation et la capacité collective à se préparer et à réagir.

### *1.4.2. Objectif(s) spécifique(s)*

Pour remédier au problème du faible niveau de cyber-résilience des entreprises actives dans l'Union européenne, l'objectif spécifique consiste à faire en sorte que les entités dans tous les secteurs qui dépendent des réseaux et des systèmes d'information et qui fournissent des services essentiels à l'économie et à la société dans son ensemble soient tenues de prendre des mesures de cybersécurité et de signaler les incidents en vue d'accroître le niveau global de cyber-résilience dans l'ensemble du marché intérieur.

Pour remédier au problème de la résilience inégale en fonction des États membres et des secteurs, l'objectif spécifique consiste à faire en sorte que toutes les entités qui sont actives dans des secteurs couverts par le cadre juridique SRI, et qui sont de taille semblable et ont un rôle comparable soient soumises au même régime réglementaire (soit elles sont incluses dans le champ d'application, soit elles en sont exclues), quelle que soit la juridiction dont elles relèvent au sein de l'Union.

Pour veiller à ce que toutes les entités qui sont actives dans des secteurs couverts par le cadre juridique SRI soient tenues de respecter les mêmes obligations fondées sur le concept de gestion des risques pour ce qui est des mesures de sécurité et de signaler tous les incidents en fonction d'un ensemble uniforme de critères, les objectifs spécifiques consistent à faire en sorte que les autorités compétentes appliquent les règles établies par l'instrument juridique de manière plus efficace grâce à des mesures de surveillance et d'exécution harmonisées et à garantir qu'un niveau comparable de ressources dans l'ensemble des États membres est attribué aux autorités compétentes pour leur permettre de s'acquitter des missions essentielles établies par le cadre SRI.

Pour remédier au problème de la prise de conscience conjointe de la situation et de l'absence de réponse conjointe à la crise, l'objectif spécifique consiste à faire en sorte que les informations essentielles soient échangées entre les États membres par l'introduction d'obligations claires faites aux autorités compétentes de partager des informations et de coopérer en matière de cybermenaces et d'incidents et par la mise en place d'une capacité de réaction conjointe opérationnelle de l'Union aux crises.

[56] Tel(le) que visé(e) à l'article 58, paragraphe 2, point a) ou b), du règlement financier.

*1.4.3. Résultat(s) et incidence(s) attendus*

*Préciser les effets que la proposition/l'initiative devrait avoir sur les bénéficiaires/la population visée.*

La proposition devrait apporter des avantages significatifs: selon les estimations, elle pourrait entraîner une diminution du coût des incidents de cybersécurité de 11,3 milliards d'EUR. Le champ d'application sectoriel serait considérablement élargi en vertu du cadre SRI, mais à côté des avantages susmentionnés, la charge que les exigences en matière de SRI pourraient créer, notamment du point de vue de la surveillance, serait également équilibrée tant pour les nouvelles entités qui seront couvertes que pour les autorités compétentes. En effet, le nouveau cadre SRI établirait une approche à deux niveaux, mettant l'accent sur les grandes entités et les entités clés, et une différenciation du régime de contrôle qui ne permettrait qu'une surveillance ex post pour un grand nombre de ces entités, notamment celles considérées comme «importantes», mais non «essentielles».

Dans l'ensemble, la proposition entraînerait des arbitrages et des synergies efficaces, le potentiel de toutes les options stratégiques étant analysé pour garantir un niveau accru et cohérent de cyber-résilience des entités clés dans l'ensemble de l'Union, ce qui engendrerait à terme des économies tant pour les entreprises que pour la société.

La proposition entraînerait également certains coûts de mise en conformité et d'exécution pour les autorités compétentes des États membres (une augmentation globale d'environ 20 à 30 % des ressources a été estimée). Cependant, le nouveau cadre apporterait également des avantages substantiels grâce à une meilleure vue d'ensemble des entreprises clés et à une meilleure interaction avec celles-ci, à un renforcement de la coopération opérationnelle transfrontière, ainsi qu'à des mécanismes d'assistance mutuelle et d'évaluation par les pairs. Cela entraînerait une augmentation globale des capacités dans le domaine de la cybersécurité dans l'ensemble des États membres.

Selon les estimations, les entreprises qui relèveraient du cadre SRI devraient augmenter leurs dépenses actuelles consacrées à la sécurité des TIC de 22 % maximum au cours des premières années suivant l'introduction du nouveau cadre SRI (12 % pour les entreprises qui relèvent déjà du champ d'application de la directive SRI actuelle). Cependant, cette augmentation moyenne des dépenses consacrées à la sécurité des TIC donnerait lieu à des avantages proportionnels liés à ces investissements, en raison notamment d'une réduction considérable des coûts des incidents de cybersécurité (estimée à 118 milliards d'EUR sur dix ans).

Les micro et petites entreprises seraient exclues du champ d'application du cadre SRI. Pour les moyennes entreprises, on peut s'attendre à une augmentation des dépenses consacrées à la sécurité des TIC au cours des premières années suivant l'introduction du nouveau cadre SRI. En parallèle, le relèvement du niveau d'exigences de sécurité pour ces entités encouragerait également le renforcement de leurs capacités dans le domaine de la cybersécurité et contribuerait à améliorer leur gestion des risques liés aux TIC.

Il y aurait une incidence sur les budgets nationaux et les administrations nationales: une augmentation des ressources d'environ 20 à 30 % est prévue à court et moyen terme.

Aucune autre incidence négative significative n'est attendue. La proposition devrait entraîner un renforcement des capacités dans le domaine de la cybersécurité et, par conséquent, elle devrait permettre d'atténuer davantage le nombre et la gravité des incidents, y compris des violations de données. Elle est également susceptible d'avoir une incidence positive sur la mise en place de conditions de concurrence équitables dans l'ensemble des États membres

pour toutes les entités relevant du champ d'application du cadre SRI et de réduire les disparités en matière d'information sur la cybersécurité.

### *1.4.4. Indicateurs de performance*

*Préciser les indicateurs permettant de suivre l'avancement et les réalisations.*

L'évaluation des indicateurs sera effectuée par la Commission, avec le soutien de l'ENISA et du groupe de coopération, et commencera trois ans après l'entrée en vigueur du nouvel acte juridique SRI. Voici quelques-uns des indicateurs de suivi sur lesquels reposera l'évaluation du succès du réexamen du cadre SRI:

- Amélioration de la gestion des incidents: en prenant des mesures de cybersécurité, les entreprises améliorent non seulement leur capacité à éviter complètement certains incidents, mais aussi leur capacité de réaction en cas d'incident. Les indicateurs de succès sont donc i) la réduction du temps moyen nécessaire pour détecter un incident, ii) le temps moyen nécessaire aux organisations pour se remettre d'un incident et iii) le coût moyen des dommages causés par un incident.

- Amélioration de la sensibilisation des dirigeants d'entreprises aux risques liés à la cybersécurité: en imposant aux entreprises de prendre des mesures, une directive SRI révisée contribuerait à sensibiliser les dirigeants aux risques liés à la cybersécurité. Ce point peut être mesuré en étudiant dans quelle mesure les entreprises qui relèvent du champ d'application du cadre SRI accordent la priorité à la cybersécurité dans leurs politiques et processus internes, comme en témoignent les documents internes, les programmes de formation pertinents et les activités de sensibilisation à l'intention des employés, et accordent la priorité aux investissements liés à la sécurité dans le domaine des TIC. Les dirigeants de toutes les entités essentielles et importantes devraient également connaître les règles énoncées dans la directive SRI.

- Nivellement des dépenses sectorielles: les dépenses consacrées à la sécurité des TIC varient considérablement d'un secteur à l'autre dans l'UE. En imposant aux entreprises dans davantage de secteurs de prendre des mesures, les écarts par rapport à la moyenne des dépenses sectorielles consacrées à la sécurité des TIC en pourcentage de l'ensemble des dépenses consacrées aux TIC devraient diminuer entre les secteurs et dans les différents États membres.

- Renforcement des autorités compétentes et coopération accrue: une directive SRI révisée pourrait conférer des missions supplémentaires aux autorités compétentes. Cela aurait une incidence mesurable sur les ressources financières et humaines allouées aux agences de cybersécurité au niveau national et devrait également avoir un effet positif sur la capacité des autorités compétentes à coopérer de manière proactive et, partant, à augmenter le nombre de cas dans lesquels les autorités compétentes travaillent ensemble pour traiter des incidents transfrontières ou mener des activités de surveillance conjointes.

- Partage d'informations accru: la directive SRI révisée améliorerait également le partage d'informations parmi les entreprises et avec les autorités compétentes. L'un des objectifs du réexamen pourrait consister à accroître le nombre d'entités participant aux diverses formes de partage d'informations.

## 1.5. Justification(s) de la proposition/de l'initiative

*1.5.1. Besoin(s) à satisfaire à court ou à long terme, assorti(s) d'un calendrier détaillé pour la mise en œuvre de l'initiative*

La proposition vise à accroître le niveau de cyber-résilience d'un ensemble exhaustif d'entreprises opérant dans l'Union européenne dans tous les secteurs concernés, à réduire les incohérences en matière de résilience dans l'ensemble du marché intérieur dans les secteurs déjà couverts par la directive et à améliorer le niveau de prise de conscience conjointe de la situation et la capacité collective à se préparer et à réagir. Elle s'appuiera sur les réalisations obtenues grâce à la mise en œuvre de la directive (UE) 2016/1148 au cours des quatre dernières années.

*1.5.2. Valeur ajoutée de l'intervention de l'Union (celle-ci peut résulter de différents facteurs: gains de coordination, sécurité juridique, efficacité accrue, complémentarités, etc.). Aux fins du présent point, on entend par «valeur ajoutée de l'intervention de l'Union» la valeur découlant de l'intervention de l'Union qui vient s'ajouter à la valeur qui, sans cela, aurait été générée par la seule action des États membres.*

La résilience en matière de cybersécurité dans l'ensemble de l'Union ne peut être effective si elle est appréhendée de manière disparate sous l'effet de cloisonnements nationaux ou régionaux. La directive SRI est venue combler cette lacune en établissant un cadre pour la sécurité des réseaux et des systèmes d'information au niveau national et au niveau de l'Union. Toutefois, le premier réexamen périodique de la directive SRI a mis en évidence un certain nombre de défauts inhérents qui ont fini par donner lieu à des disparités considérables entre les États membres en termes de capacités, de planification et de niveau de protection, ce qui porte en même temps atteinte à l'égalité des conditions de concurrence pour des entreprises similaires sur le marché intérieur.

Une intervention de l'Union allant au-delà des mesures actuelles de la directive SRI se justifie principalement par: i) la nature transfrontière du problème; ii) le potentiel de l'action de l'Union pour améliorer et permettre des politiques nationales efficaces; iii) la contribution de mesures stratégiques concertées et collaboratives en matière de SRI à la protection efficace des données et de la vie privée.

Les objectifs énoncés peuvent donc être plus aisément atteints par une action au niveau de l'Union que par les États membres seuls.

*1.5.3. Leçons tirées d'expériences similaires*

La directive SRI est le premier instrument horizontal du marché intérieur visant à améliorer la résilience des réseaux et des systèmes dans l'Union face aux risques liés à la cybersécurité. Depuis son entrée en vigueur en 2016, elle a déjà grandement contribué à accroître le niveau commun de cybersécurité parmi les États membres. Cependant, le réexamen du fonctionnement et de la mise en œuvre de la directive a mis en évidence un certain nombre de lacunes qui, outre la numérisation croissante et la nécessité d'apporter une réponse plus actualisée, doivent être comblées dans un acte juridique révisé.

*1.5.4. Compatibilité avec le cadre financier pluriannuel et synergies éventuelles avec d'autres instruments appropriés*

La nouvelle proposition est pleinement cohérente avec d'autres initiatives connexes telles que la proposition de règlement sur la résilience opérationnelle numérique du secteur financier et la proposition de directive sur la résilience des opérateurs critiques de services essentiels. Elle est également cohérente avec le code des communications électroniques européen, le règlement général sur la protection des données et le règlement eIDAS.

La proposition est un élément essentiel de la stratégie de l'UE pour l'union de la sécurité.

*1.5.5. Évaluation des différentes possibilités de financement disponibles, y compris des possibilités de redéploiement*

La gestion de ces tâches par l'ENISA requiert des profils spécifiques et une charge de travail supplémentaire qui ne peut pas être absorbée sans une augmentation des ressources humaines.

## 1.6. Durée et incidence financière de la proposition/de l'initiative

☐ **durée limitée**

– ☐ Proposition/initiative en vigueur à partir de/du [JJ/MM]AAAA jusqu'en/au [JJ/MM]AAAA

– ☐ Incidence financière de AAAA jusqu'en AAAA

☒ **durée illimitée**

– Mise en œuvre avec une période de montée en puissance de 2022 jusqu'en 2025,

– puis un fonctionnement à un rythme de croisière au-delà.

## 1.7. Mode(s) de gestion prévu(s)[57]

☒ **Gestion directe** par la Commission

par

– ☐ des agences exécutives

☐ **Gestion partagée** avec les États membres

☐X **Gestion indirecte** en confiant des tâches d'exécution budgétaire:

☐ à des organisations internationales et à leurs agences (à préciser);

☐ à la BEI et au Fonds européen d'investissement;

☒ aux organismes visés aux articles 70 et 71;

☐ à des organismes de droit public;

☐ à des organismes de droit privé investis d'une mission de service public, pour autant qu'ils présentent les garanties financières suffisantes;

☐ à des organismes de droit privé d'un État membre qui sont chargés de la mise en œuvre d'un partenariat public-privé et présentent les garanties financières suffisantes;

☐ à des personnes chargées de l'exécution d'actions spécifiques relevant de la PESC, en vertu du titre V du traité sur l'Union européenne, identifiées dans l'acte de base concerné.

Remarques

L'Agence de l'Union européenne pour la cybersécurité, l'ENISA, à laquelle le règlement sur la cybersécurité a octroyé un nouveau mandat permanent, aidera les États membres et la Commission dans la mise en œuvre de la directive SRI révisée.

Du fait de la révision de la directive SRI, à compter de 2022/2023, l'ENISA aura des domaines d'action supplémentaires. Bien que ces domaines d'action relèvent des missions générales de l'ENISA conformément à son mandat, ils entraîneront une charge de travail supplémentaire pour l'agence. Plus précisément, outre ses domaines d'action actuels, en vertu de la proposition de la Commission relative à une directive SRI révisée, l'ENISA devra également intégrer spécifiquement dans son programme de travail, entre autres, les actions suivantes: i) élaborer et gérer un registre européen des vulnérabilités (article 6, paragraphe 2, de la proposition), ii) assurer le secrétariat du réseau européen d'organisations

[57] Les explications sur les modes de gestion ainsi que les références au règlement financier sont disponibles sur le site BudgWeb: https://myintracomm.ec.europa.eu/budgweb/FR/man/budgmanag/Pages/budgmanag.aspx.

de liaison en cas de crises de cybersécurité (réseau CyCLONe) (article 14 de la proposition) et publier un rapport annuel sur l'état de la cybersécurité dans l'UE (article 15 de la proposition), iii) soutenir l'organisation d'évaluations par les pairs entre les États membres (article 16 de la proposition), iv) recueillir des données agrégées sur les incidents auprès des États membres et émettre des orientations techniques (article 20, paragraphe 9, de la proposition), v) créer et maintenir un registre des entités qui fournissent des services transfrontières (article 25 de la proposition).

Par conséquent, une demande de 5 ETP supplémentaires sera présentée à partir de 2022, accompagnée d'un budget correspondant d'environ 610 000 EUR par an pour couvrir ces nouveaux postes.

## 2. MESURES DE GESTION

### 2.1. Dispositions en matière de suivi et de compte rendu

*Préciser la fréquence et les conditions de ces dispositions.*

La Commission réexaminera périodiquement le fonctionnement de la directive et en rendra compte au Parlement européen et au Conseil, la première fois trois ans après son entrée en vigueur.

La Commission établira également si les États membres transposent correctement la directive.

Le suivi et le compte rendu de la proposition respecteront les principes énoncés dans le mandat permanent de l'ENISA en vertu du règlement (UE) 2019/881 (règlement sur la cybersécurité).

Les sources de données utilisées pour le suivi prévu proviendraient principalement de l'ENISA, du groupe de coopération, du réseau des CSIRT et des autorités des États membres. Outre les données recueillies dans les rapports (y compris les rapports d'activité annuels) de l'ENISA, du groupe de coopération et du réseau des CSIRT, des outils de collecte de données spécifiques pourraient être utilisés en cas de besoin (par exemple, des enquêtes auprès des autorités nationales, des sondages Eurobaromètre ainsi que les rapports découlant de la campagne du «mois de la cybersécurité» et des exercices paneuropéens).

### 2.2. Système(s) de gestion et de contrôle

*2.2.1. Justification du (des) mode(s) de gestion, du (des) mécanisme(s) de mise en œuvre du financement, des modalités de paiement et de la stratégie de contrôle proposée*

L'unité au sein de la DG CNECT chargée de ce domaine politique assurera la mise en œuvre de la directive.

En ce qui concerne la gestion de l'ENISA, l'article 15 du règlement sur la cybersécurité fournit une liste détaillée des fonctions de contrôle du conseil d'administration de l'ENISA.

En vertu de l'article 31 du règlement sur la cybersécurité, le directeur exécutif de l'ENISA est responsable de l'exécution du budget de l'ENISA et l'auditeur interne de la Commission exerce à l'égard de l'ENISA les mêmes pouvoirs que ceux qui lui sont attribués à l'égard des services de la Commission. Le conseil d'administration de l'ENISA rend un avis sur les comptes définitifs de l'ENISA.

*2.2.2. Informations sur les risques recensés et sur le(s) système(s) de contrôle interne mis en place pour les atténuer*

Risque très faible, étant donné que l'écosystème de la directive SRI est déjà en place et couvre déjà l'ENISA, qui dispose d'un mandat permanent à la suite de l'entrée en vigueur du règlement sur la cybersécurité en 2019.

*2.2.3. Estimation et justification du rapport coût/efficacité des contrôles (rapport «coûts du contrôle ÷ valeur des fonds gérés concernés»), et évaluation du niveau attendu de risque d'erreur (lors du paiement et lors de la clôture)*

L'augmentation budgétaire demandée s'applique au titre 1 et est destinée à financer les salaires. Le risque d'erreur au niveau des paiements est donc très faible.

## 2.3. Mesures de prévention des fraudes et irrégularités

*Préciser les mesures de prévention et de protection existantes ou envisagées, au titre de la stratégie antifraude par exemple.*

Les mesures de prévention et de protection de l'ENISA s'appliqueraient, et notamment:

- Le contrôle du paiement de tout service ou étude nécessaire est effectué par le personnel de l'Agence avant le paiement, compte tenu de toute obligation contractuelle, des principes économiques et des bonnes pratiques financières ou de gestion. Des dispositions antifraude (surveillance, exigences en matière de rapports) seront introduites dans tous les accords et contrats conclus entre l'Agence et les bénéficiaires de tous paiements.

- Aux fins de la lutte contre la fraude, la corruption et les autres actes illégaux, les dispositions du règlement (UE, Euratom) nº 883/2013 du Parlement européen et du Conseil du 25 mai 1999 relatif aux enquêtes effectuées par l'Office européen de lutte antifraude (OLAF) s'appliquent sans restriction.

- En vertu de l'article 33 du règlement sur la cybersécurité, l'ENISA a adhéré, le 28 décembre 2019 à l'accord interinstitutionnel du 25 mai 1999 entre le Parlement européen, le Conseil de l'Union européenne et la Commission des Communautés européennes relatif aux enquêtes internes effectuées par l'OLAF. L'ENISA arrête sans tarder les dispositions appropriées applicables à tous les membres du personnel de l'agence.

# 3. INCIDENCE FINANCIÈRE ESTIMÉE DE LA PROPOSITION/DE L'INITIATIVE

## 3.1. Rubrique(s) du cadre financier pluriannuel et ligne(s) budgétaire(s) de dépenses concernée(s)

- Lignes budgétaires existantes

Dans l'ordre des rubriques du cadre financier pluriannuel et des lignes budgétaires.

| Rubrique du cadre financier pluriannuel | Ligne budgétaire | Nature de la dépense | Participation | | | |
|---|---|---|---|---|---|---|
| | Numéro | CD/CND[58] | de pays AELE[59] | de pays candidats[60] | de pays tiers | au sens de l'article 21, paragraphe 2, point b), du règlement financier |
| 2 | 02 10 04 | /CND | OUI | NON | NON | NON |

- Nouvelles lignes budgétaires, dont la création est demandée

Dans l'ordre des rubriques du cadre financier pluriannuel et des lignes budgétaires.

| Rubrique | Ligne budgétaire | Nature de | Participation |
|---|---|---|---|

[58] CD = crédits dissociés / CND = crédits non dissociés.

[59] AELE: Association européenne de libre-échange.

[60] Pays candidats et, le cas échéant, pays candidats potentiels des Balkans occidentaux.

| du cadre financier pluriannuel | | la dépense | | | | |
|---|---|---|---|---|---|---|
| | Numéro | CD/CND | de pays AELE | de pays candidats | de pays tiers | au sens de l'article 21, paragraphe 2, point b), du règlement financier |
| | [XX.YY.YY.YY] | | OUI/NON | OUI/NON | OUI/NON | OUI/NON |

### 3.2. Incidence estimée sur les dépenses

*3.2.1. Synthèse de l'incidence estimée sur les dépenses*

En Mio EUR (à la 3e décimale)

| **Rubrique du cadre financier pluriannuel** | Numéro | [Rubrique…2 Marché unique, innovation et numérique……..……] |
|---|---|---|

| [Organisme]: <…ENISA….> | | | Année **N**[61] **2022** | Année **N+1** **2023** | Année **N+2** **2024** | Année **N+3** **2025** | Indiquer le nombre d'années correspondant à la durée de l'incidence (cf. point 1.6) **2026** | **2027** | | **TOTAL** |
|---|---|---|---|---|---|---|---|---|---|---|
| Titre 1: | Engagements | (1) | 0,61 | 0,61 | 0,61 | 0,61 | 0,61 | 0,61 | | **3,66** |
| | Paiements | (2) | 0,61 | 0,61 | 0,61 | 0,61 | 0,61 | 0,61 | | **3,66** |
| Titre 2: | Engagements | (1a) | | | | | | | | |
| | Paiements | (2a) | | | | | | | | |
| Titre 3: | Engagements | (3a) | | | | | | | | |
| | Paiements | (3b) | | | | | | | | |
| **TOTAL des crédits pour [organisme]** <ENISA…….> | Engagements | =1+1a +3a | 0,61 | 0,61 | 0,61 | 0,61 | 0,61 | 0,61 | | **3,66** |
| | Paiements | =2+2a +3b | 0,61 | 0,61 | 0,61 | 0,61 | 0,61 | 0,61 | | **3,66** |

61 L'année N est l'année du début de la mise en œuvre de la proposition/de l'initiative. Veuillez remplacer «N» par la première année de mise en œuvre prévue (par exemple: 2021). Procédez de la même façon pour les années suivantes.

| Rubrique du cadre financier pluriannuel | 5 | «Dépenses administratives» |
|---|---|---|

En Mio EUR (à la 3e décimale)

| | | Année N | Année N+1 | Année N+2 | Année N+3 | Indiquer le nombre d'années correspondant à la durée de l'incidence (cf. point 1.6) | | | TOTAL |
|---|---|---|---|---|---|---|---|---|---|
| DG: <…….> | | | | | | | | | |
| • Ressources humaines | | | | | | | | | |
| • Autres dépenses administratives | | | | | | | | | |
| **TOTAL DG** <…….> | Crédits | | | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **TOTAL des crédits pour la RUBRIQUE 5** du cadre financier pluriannuel | (Total engagements = Total paiements) | | | | | | | | |

En Mio EUR (à la 3e décimale)

| | | Année N[62] 2022 | Année N+1 2023 | Année N+2 2024 | Année N+3 2025 | Indiquer le nombre d'années correspondant à la durée de l'incidence (cf. point 1.6) 2026 | 2027 | | TOTAL |
|---|---|---|---|---|---|---|---|---|---|
| **TOTAL des crédits pour les RUBRIQUES 1 à 5** du cadre financier pluriannuel | Engagements | 0,61 | 0,61 | 0,61 | 0,61 | 0,61 | 0,61 | | **3,66** |
| | Paiements | 0,61 | 0,61 | 0,61 | 0,61 | 0,61 | 0,61 | | **3,66** |

62 L'année N est l'année du début de la mise en œuvre de la proposition/de l'initiative. Veuillez remplacer «N» par la première année de mise en œuvre prévue (par exemple: 2021). Procédez de la même façon pour les années suivantes.

*3.2.2. Incidence estimée sur les crédits [de l'organisme]*

– ☐x La proposition/l'initiative n'engendre pas l'utilisation de crédits opérationnels

– ☐ La proposition/l'initiative engendre l'utilisation de crédits opérationnels, comme expliqué ci-après:

Crédits d'engagement en Mio EUR (à la 3e décimale)

| **Indiquer les objectifs et les réalisations** ⇩ | | | Année **N** | | Année **N+1** | | Année **N+2** | | Année **N+3** | | Indiquer le nombre d'années correspondant à la durée de l'incidence (cf. point 1.6) | | | | | | **TOTAL** | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **RÉALISATIONS (outputs)** | | | | | | | | | | | | | | | | | |
| | Type[63] | Coût moyen | Nbre | Coût | Nbre | Coût | Nbre | Coût | Nbre | Coût | Nbre | Coût | Nbre | Coût | Nbre | Coût | Nbre total | Coût total |
| OBJECTIF SPÉCIFIQUE nº 1[64]... | | | | | | | | | | | | | | | | | | |
| - Réalisation | | | | | | | | | | | | | | | | | | |
| - Réalisation | | | | | | | | | | | | | | | | | | |
| - Réalisation | | | | | | | | | | | | | | | | | | |
| Sous-total objectif spécifique nº 1 | | | | | | | | | | | | | | | | | | |
| OBJECTIF SPÉCIFIQUE nº 2… | | | | | | | | | | | | | | | | | | |
| - Réalisation | | | | | | | | | | | | | | | | | | |
| Sous-total objectif spécifique nº 2 | | | | | | | | | | | | | | | | | | |
| **COÛT TOTAL** | | | | | | | | | | | | | | | | | | |

63 Les réalisations se réfèrent aux produits et services qui seront fournis (par exemple: nombre d'échanges d'étudiants financés, nombre de km de routes construites, etc.).

64 Tel que décrit dans la partie 1.4.2. «Objectif(s) spécifique(s)…».

### *3.2.3. Incidence estimée sur les ressources humaines de l'ENISA*

#### 3.2.3.1. Synthèse

Du fait de la révision de la directive SRI, à compter de 2022/2023, l'ENISA aura des missions supplémentaires. Bien que ces missions relèvent du mandat de l'ENISA, elles entraîneront une charge de travail supplémentaire pour l'agence. Plus précisément, en plus de ses missions actuelles, dans le cadre d'une directive SRI révisée, l'ENISA sera chargée entre autres i) d'élaborer et gérer un registre européen des vulnérabilités (article 6, paragraphe 2), ii) d'assurer le secrétariat du réseau européen d'organisations de liaison en cas de crises de cybersécurité (réseau CyCLONe) (article 14) et publier un rapport annuel sur l'état de la cybersécurité dans l'UE (article 15), iii) de soutenir l'organisation d'évaluations par les pairs entre les États membres (article 16), iv) de recueillir des données agrégées sur les incidents auprès des États membres et émettre des orientations techniques (article 20, paragraphe 9), et v) de créer et maintenir un registre des entités qui fournissent des services transfrontières (article 25).

Par conséquent, une demande de 5 ETP supplémentaires sera présentée à partir de 2022, accompagnée du budget correspondant pour couvrir ces nouveaux postes.

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits de nature administrative.

– ☐X La proposition/l'initiative engendre l'utilisation de crédits de nature administrative, comme expliqué ci-après:

En Mio EUR (à la 3e décimale)

| | Année **N** [65] **2022** | Année **N+1** **2023** | Année **N+2** **2024** | Année **N+3** **2025** | Indiquer le nombre d'années correspondant à la durée de l'incidence (cf. point 1.6) **2026** **2027** | | | **TOTAL** |
|---|---|---|---|---|---|---|---|---|
| Agents temporaires (grades AD) | 0,450 | 0,450 | 0,450 | 0,450 | 0,450 | 0,450 | | **2,7** |
| Agents temporaires (grades AST) | | | | | | | | |
| Agents contractuels | 0,160 | 0,160 | 0,160 | 0,160 | 0,160 | 0,160 | | **0,96** |
| Experts nationaux détachés | | | | | | | | |

[65] L'année N est l'année du début de la mise en œuvre de la proposition/de l'initiative. Veuillez remplacer «N» par la première année de mise en œuvre prévue (par exemple: 2021). Procédez de la même façon pour les années suivantes.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **TOTAL** | **0,61** | **0,61** | **0,61** | **0,61** | **0,61** | **0,61** | | **3,66** |

Besoins en personnel (ETP):

| | Année **N** [66] **2022** | Année **N+1** **2023** | Année **N+2** **2024** | Année **N+3** **2025** | Indiquer le nombre d'années correspondant à la durée de l'incidence (cf. point 1.6) **2026** **2027** | | | **TOTAL** |
|---|---|---|---|---|---|---|---|---|
| Agents temporaires (grades AD) | 3 | 3 | 3 | 3 | 3 | 3 | | **18** |
| Agents temporaires (grades AST) | | | | | | | | |
| Agents contractuels | 2 | 2 | 2 | 2 | 2 | 2 | | **12** |
| Experts nationaux détachés | | | | | | | | |
| **TOTAL** | **5** | **5** | **5** | **5** | **5** | **5** | | **30** |

3.2.3.2. Besoins estimés en ressources humaines pour la DG de tutelle

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de ressources humaines.

– ☐ La proposition/l'initiative engendre l'utilisation de ressources humaines, comme expliqué ci-après:

*Estimation à exprimer en valeur entière (ou au plus avec une décimale)*

| | Année **N** | Année **N+1** | Année **N+2** | Année **N +3** | Indiquer le nombre d'années correspondant à la durée de l'incidence (cf. point 1.6) | | |
|---|---|---|---|---|---|---|---|
| • **Emplois du tableau des effectifs (fonctionnaires et d'agents temporaires)** | | | | | | | |
| XX 01 01 01 (au siège et dans les bureaux de représentation de la Commission) | | | | | | | |
| XX 01 01 02 (en délégation) | | | | | | | |

[66] L'année N est l'année du début de la mise en œuvre de la proposition/de l'initiative. Veuillez remplacer «N» par la première année de mise en œuvre prévue (par exemple: 2021). Procédez de la même façon pour les années suivantes.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| XX 01 05 01 (recherche indirecte) | | | | | | | | |
| 10 01 05 01 (recherche directe) | | | | | | | | |
| | | | | | | | | |
| **• Personnel externe (en équivalent temps plein: ETP[67]** | | | | | | | | |
| XX 01 02 01 (AC, END, INT de l'enveloppe globale) | | | | | | | | |
| XX 01 02 02 (AC, AL, END, INT et JPD dans les délégations) | | | | | | | | |
| **XX** 01 04 ***yy***[68] | - au siège[69] | | | | | | | |
| | - en délégation | | | | | | | |
| **XX** 01 05 02 (AC, END, INT – Recherche indirecte) | | | | | | | | |
| 10 01 05 02 (AC, END, INT sur recherche directe) | | | | | | | | |
| Autres lignes budgétaires (à préciser) | | | | | | | | |
| **TOTAL** | | | | | | | | |

**XX** est le domaine d'action ou le titre concerné.

Les besoins en ressources humaines seront couverts par les effectifs de la DG déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés si nécessaire par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes.

Description des tâches à effectuer:

| | |
|---|---|
| Fonctionnaires et agents temporaires | |
| Personnel externe | |

Il convient de faire figurer à l'annexe V, section 3, la description du calcul des coûts pour les équivalents temps plein.

67 AC = agent contractuel; AL = agent local; END = expert national détaché; INT = intérimaire; JPD = jeune professionnel en délégation.

68 Sous-plafonds de personnel externe financés sur crédits opérationnels (anciennes lignes «BA»).

69 Essentiellement pour les Fonds structurels, le Fonds européen agricole pour le développement rural (FEADER) et le Fonds européen pour la pêche (FEP).

*3.2.4. Compatibilité avec le cadre financier pluriannuel actuel*

– ☐X La proposition/l'initiative est compatible avec le cadre financier pluriannuel actuel.

– ☐ La proposition/l'initiative nécessite une reprogrammation de la rubrique concernée du cadre financier pluriannuel.

| |
|---|
| Expliquez la reprogrammation requise, en précisant les lignes budgétaires concernées et les montants correspondants.<br>La proposition est compatible avec le CFP 2021-2027.<br>Le budget demandé pour couvrir l'augmentation des ressources humaines de l'ENISA sera compensé par une réduction du même montant du budget du programme pour une Europe numérique, à la même rubrique. |

– ☐ La proposition/l'initiative nécessite le recours à l'instrument de flexibilité ou la révision du cadre financier pluriannuel[70].

| |
|---|
| Expliquez le besoin, en précisant les rubriques et lignes budgétaires concernées et les montants correspondants. |

*3.2.5. Participation de tiers au financement*

– La proposition/l'initiative ne prévoit pas de cofinancement par des tiers.

– La proposition/l'initiative prévoit un cofinancement estimé ci-après:

En Mio EUR (à la 3e décimale)

| | Année **N** | Année **N+1** | Année **N+2** | Année **N+3** | Indiquer le nombre d'années correspondant à la durée de l'incidence (cf. point 1.6) | | | Total |
|---|---|---|---|---|---|---|---|---|
| Préciser l'organisme de cofinancement | | | | | | | | |
| TOTAL des crédits cofinancés | | | | | | | | |

[70] Voir les articles 11 et 17 du règlement (UE, Euratom) nº 1311/2013 du Conseil fixant le cadre financier pluriannuel pour la période 2014-2020.

### 3.3. Incidence estimée sur les recettes

– ☐ La proposition/l'initiative est sans incidence financière sur les recettes.

– ☐ La proposition/l'initiative a une incidence financière décrite ci-après:

☐ sur les ressources propres

☐ sur les autres recettes

☐ veuillez indiquer si les recettes sont affectées à des lignes de dépenses

En Mio EUR (à la 3e décimale)

| Ligne budgétaire de recettes: | Montants inscrits pour l'exercice en cours | Incidence de la proposition/de l'initiative[71] | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Année **N** | Année **N+1** | Année **N+2** | Année **N+3** | Indiquer le nombre d'années correspondant à la durée de l'incidence (cf. point 1.6) | | |
| Article ……. | | | | | | | | |

Pour les recettes diverses qui seront «affectées», préciser la (les) ligne(s) budgétaire(s) de dépenses concernée(s).

Préciser la méthode de calcul de l'incidence sur les recettes.

[71] En ce qui concerne les ressources propres traditionnelles (droits de douane, cotisations sur le sucre), les montants indiqués doivent être des montants nets, c'est-à-dire des montants bruts après déduction de 20 % de frais de perception.