Journal officiel de l'Union européenne

L 151

Édition de langue française

Législation

62e année

7 juin 2019

Sommaire

[1] Texte présentant de l'intérêt pour l'EEE.

FR

Les actes dont les titres sont imprimés en caractères maigres sont des actes de gestion courante pris dans le cadre de la politique agricole et ayant généralement une durée de validité limitée.

Les actes dont les titres sont imprimés en caractères gras et précédés d'un astérisque sont tous les autres actes.

I

(Actes législatifs)

RÈGLEMENTS

RÈGLEMENT (UE) 2019/880 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 17 avril 2019

concernant l'introduction et l'importation de biens culturels

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

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 207, paragraphe 2,

vu la proposition de la Commission européenne,

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

statuant conformément à la procédure législative ordinaire [1],

considérant ce qui suit:

(1) À la lumière des conclusions du Conseil du 12 février 2016 sur la lutte contre le financement du terrorisme, de la communication de la Commission au Parlement européen et au Conseil du 2 février 2016 relative à un plan d'action destiné à renforcer la lutte contre le financement du terrorisme et de la directive (UE) 2017/541 du Parlement européen et du Conseil [2], il convient d'adopter des règles communes sur le commerce avec les pays tiers de manière à assurer une protection efficace contre le commerce illicite de biens culturels et leur perte ou destruction, à préserver le patrimoine culturel de l'humanité et à empêcher le financement du terrorisme et le blanchiment de capitaux par la vente de biens culturels pillés à des acheteurs dans l'Union.

(2) L'exploitation de peuples et de territoires peut être à l'origine du commerce illicite de biens culturels, en particulier lorsque ce commerce illicite survient à la faveur d'une situation de conflit armé. À cet égard, il convient que le présent règlement tienne compte des caractéristiques régionales et locales des peuples et des territoires, plutôt que de la valeur marchande des biens culturels.

(3) Les biens culturels font partie du patrimoine culturel et revêtent souvent une importance culturelle, artistique, historique et scientifique majeure. Le patrimoine culturel constitue l'un des éléments fondamentaux de la civilisation, comportant notamment une valeur symbolique et constituant la mémoire culturelle de l'humanité. Il enrichit la vie culturelle de tous les peuples et unit les personnes autour d'une mémoire partagée, de la connaissance et du développement de la civilisation. Il devrait dès lors être protégé de l'appropriation illicite et du pillage. Le pillage des sites archéologiques a toujours existé, mais se produit désormais à une échelle industrielle et constitue, avec le commerce de biens culturels exhumés de manière illicite, une forme grave de criminalité qui entraîne un préjudice considérable pour les personnes touchées directement ou indirectement. Le commerce illicite de biens culturels contribue dans de nombreux cas à l'imposition par la force d'une homogénéisation culturelle ou d'une perte d'identité culturelle, tandis que le pillage des biens culturels entraîne, entre autres, la désintégration des cultures. Tant qu'il sera possible de prendre part au commerce lucratif de biens culturels exhumés de manière illicite et d'en tirer profit sans risque notable, ces fouilles et ces pillages continueront. La valeur économique et artistique des biens culturels suscite une forte demande sur le marché international. L'absence de mesures législatives internationales solides et l'application inefficace des mesures qui existent ont pour conséquence que ces biens passent dans l'économie souterraine. Il convient par conséquent que l'Union interdise l'introduction sur son territoire douanier

[1] Position du Parlement européen du 12 mars 2019 (non encore parue au Journal officiel) et décision du Conseil du 9 avril 2019.
[2] Directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil (JO L 88 du 31.3.2017, p. 6).

de biens culturels exportés illicitement depuis des pays tiers, en accordant une attention particulière aux biens culturels provenant de pays tiers touchés par des conflits armés, en particulier lorsque ces biens culturels ont été commercialisés illicitement par des organisations terroristes ou d'autres organisations criminelles. Bien que cette interdiction générale ne devrait pas entraîner des contrôles systématiques, les États membres devraient être autorisés à intervenir lorsqu'ils reçoivent des renseignements concernant des cargaisons suspectes et à prendre toutes les mesures appropriées pour intercepter les biens culturels exportés illicitement.

(4) Étant donné que des règles différentes s'appliquent dans les États membres en ce qui concerne l'importation de biens culturels sur le territoire douanier de l'Union, il y a lieu d'adopter des mesures, en particulier pour veiller à ce que certaines importations de biens culturels soient soumises à des contrôles uniformes lors de leur entrée sur le territoire douanier de l'Union, sur la base des processus, procédures et outils administratifs existants visant à parvenir à une application uniforme du règlement (UE) n° 952/2013 du Parlement européen et du Conseil ([3]).

(5) La protection des biens culturels considérés comme des trésors nationaux des États membres est déjà régie par le règlement (CE) n° 116/2009 du Conseil ([4]) et la directive 2014/60/UE du Parlement européen et du Conseil ([5]). Par conséquent, le présent règlement ne devrait pas s'appliquer aux biens culturels qui ont été créés ou découverts sur le territoire douanier de l'Union. Les règles communes introduites par le présent règlement devraient couvrir le traitement douanier des biens culturels non Union qui entrent sur le territoire douanier de l'Union. Aux fins du présent règlement, le territoire douanier pertinent devrait être le territoire douanier de l'Union au moment de l'importation.

(6) Les mesures de contrôle à mettre en place au sujet des zones franches et des dénommés «ports francs» devraient avoir un champ d'application aussi vaste que possible pour ce qui est des régimes douaniers concernés, afin d'empêcher le contournement du présent règlement par l'exploitation de ces zones franches, qui peuvent être utilisées pour une prolifération constante du commerce illicite. Ces mesures devraient dès lors porter non seulement sur les biens culturels mis en libre pratique mais aussi sur les biens culturels placés sous un régime douanier particulier. Le champ d'application ne devrait toutefois pas aller au-delà de l'objectif consistant à empêcher l'entrée sur le territoire douanier de l'Union de biens culturels exportés illicitement. En conséquence, tout en intégrant la mise en libre pratique et certains régimes douaniers particuliers sous lesquels des biens entrant sur le territoire douanier de l'Union peuvent être placés, il y a lieu d'exclure le transit des mesures de contrôle systématique.

(7) De nombreux pays tiers et la majorité des États membres sont familiarisés avec les définitions utilisées dans la convention de l'Unesco concernant les mesures à prendre pour interdire et empêcher l'importation, l'exportation et le transfert de propriété illicites des biens culturels, signée à Paris le 14 novembre 1970 (ci-après dénommée «convention de l'Unesco de 1970») à laquelle un grand nombre d'État membres sont parties, et dans la convention d'Unidroit sur les biens culturels volés ou illicitement exportés, signée à Rome le 24 juin 1995. Pour cette raison, les définitions utilisées dans le présent règlement se fondent sur ces définitions.

(8) Il y a lieu d'examiner principalement la licéité des exportations de biens culturels au regard des dispositions législatives et réglementaires du pays où ces biens culturels ont été créés ou découverts. Toutefois, afin de ne pas entraver déraisonnablement le commerce légitime, une personne qui tente d'importer des biens culturels sur le territoire douanier de l'Union devrait, dans certains cas, être exceptionnellement autorisée à prouver plutôt l'exportation licite depuis un autre pays tiers dans lequel les biens culturels se situaient avant leur expédition vers l'Union. Cette exception devrait s'appliquer dans les cas où le pays dans lequel les biens culturels ont été créés ou découverts ne peut pas être déterminé de manière fiable ou lorsque l'exportation des biens culturels en question a eu lieu avant l'entrée en vigueur de la convention de l'Unesco de 1970, à savoir le 24 avril 1972. Afin d'empêcher que le présent règlement puisse être contourné par le simple envoi de biens culturels exportés illicitement dans un autre pays tiers avant leur importation dans l'Union, les exceptions devraient être applicables lorsque les biens culturels ont été situés dans un pays tiers pendant une période de plus de cinq ans à des fins autres que l'utilisation temporaire, le transit, la réexportation ou le transbordement. Lorsque ces conditions sont remplies pour plus d'un pays, le pays pertinent devrait être le dernier de ces pays dans lequel les biens culturels se sont trouvés avant d'être introduits sur le territoire douanier de l'Union.

(9) L'article 5 de la convention de l'Unesco de 1970 demande aux États parties d'instituer un ou plusieurs services nationaux de protection des biens culturels contre l'importation, l'exportation et le transfert de propriété illicites. Ces services nationaux devraient être dotés d'un personnel qualifié et en nombre suffisant, afin d'assurer cette protection conformément à cette convention et devraient également permettre la collaboration active nécessaire entre les autorités compétentes des États membres qui sont parties à cette convention dans le domaine de la sécurité et de la lutte contre les importations illicites de biens culturels, en particulier des régions touchées par un conflit armé.

([3]) Règlement (UE) n° 952/2013 du Parlement européen et du Conseil du 9 octobre 2013 établissant le code des douanes de l'Union (JO L 269 du 10.10.2013, p. 1).

([4]) Règlement (CE) n° 116/2009 du Conseil du 18 décembre 2008 concernant l'exportation de biens culturels (JO L 39 du 10.2.2009, p. 1).

([5]) Directive 2014/60/UE du Parlement européen et du Conseil du 15 mai 2014 relative à la restitution de biens culturels ayant quitté illicitement le territoire d'un État membre et modifiant le règlement (UE) n° 1024/2012 (JO L 159 du 28.5.2014, p. 1).

(10) Afin de ne pas entraver de manière disproportionnée le commerce de biens culturels aux frontières extérieures de l'Union, il convient que le présent règlement s'applique uniquement aux biens culturels satisfaisant à un critère d'ancienneté donné, fixé par le présent règlement. En outre, il semble approprié de fixer un seuil financier afin d'exclure les biens culturels de moindre valeur de l'application de ces conditions et procédures à leur importation sur le territoire douanier de l'Union. Ces seuils garantiront que les mesures prévues dans le présent règlement se concentrent sur les biens culturels les plus susceptibles d'être convoités par les pilleurs dans les zones de conflits, sans pour autant exclure d'autres biens dont le contrôle est nécessaire en vue de protéger le patrimoine culturel.

(11) Le commerce illicite de biens culturels pillés a été recensé comme une source possible des activités de financement du terrorisme et de blanchiment de capitaux dans le cadre d'une évaluation supranationale des risques de blanchiment de capitaux et de financement du terrorisme qui ont une incidence sur le marché intérieur.

(12) Étant donné que certaines catégories de biens culturels, à savoir les objets archéologiques et éléments de monuments, sont particulièrement vulnérables face au pillage et à la destruction, il semble nécessaire de prévoir un système de contrôle renforcé avant que ces biens soient autorisés à entrer sur le territoire douanier de l'Union. Un tel système devrait exiger la présentation d'une licence d'importation délivrée par l'autorité compétente d'un État membre avant la mise en libre pratique de ces biens culturels dans l'Union ou leur placement sous un régime douanier particulier autre que le transit. Les personnes qui cherchent à obtenir un telle licence devraient être en mesure de prouver l'exportation licite depuis le pays dans lequel les biens culturels ont été créés ou découverts à l'aide des pièces justificatives et preuves appropriées, notamment des certificats d'exportation des titres de propriété, des factures, des contrats de vente, des documents d'assurance, des documents de transport et des expertises. Sur la base de demandes complètes et exactes, les autorités compétentes des États membres devraient décider de délivrer ou non une licence sans retard injustifié. Il y a lieu de conserver l'ensemble des licences d'importation dans un système électronique.

(13) Le terme «icône» désigne une représentation d'une figure religieuse ou d'une manifestation religieuse. Elle peut être produite sur différents supports et en différentes tailles, tant monumentale que portable. Si une icône se trouvait auparavant, par exemple, à l'intérieur d'une église, d'un monastère, d'une chapelle, soit en tant qu'élément isolé, soit en tant que pièce constitutive d'un mobilier architectural, par exemple une iconostase ou un porte-icône, il s'agit d'un élément indispensable et inséparable du culte divin et de la vie liturgique et cette icône devrait être considérée comme faisant partie intégrante du monument religieux qui a été démembré. Même dans les cas où le monument spécifique auquel appartenait l'icône est inconnu, mais s'il existe des éléments de preuve indiquant que celle-ci faisait autrefois partie intégrante d'un monument, en particulier lorsqu'il y a des signes ou des éléments qui indiquent qu'elle faisait auparavant partie d'une iconostase ou d'un porte-icône, l'icône devrait toujours relever de la catégorie «éléments provenant du démembrement de monuments artistiques ou historiques ou de sites archéologiques» énumérée dans l'annexe.

(14) Compte tenu de la nature particulière des biens culturels, le rôle des autorités douanières est extrêmement important, et elles devraient être en mesure, si elles le jugent nécessaire, d'exiger des informations supplémentaires de la part du déclarant et d'analyser les biens culturels en procédant à une expertise physique.

(15) Pour les catégories de biens culturels dont l'importation ne nécessite pas de licence d'importation, les personnes cherchant à les importer sur le territoire douanier de l'Union devraient, au moyen d'une déclaration, certifier l'exportation licite des biens culturels depuis le pays tiers et en assumer la responsabilité, tout en fournissant suffisamment de renseignements pour permettre aux autorités douanières d'identifier ces biens culturels. Afin de faciliter la procédure et dans un souci de sécurité juridique, il convient que les informations relatives aux biens culturels soient transmises au moyen d'un document standardisé. La norme Object ID, recommandée par l'Unesco, pourrait être utilisée pour décrire les biens culturels. Il y a lieu que le détenteur des biens enregistre ces informations dans un système électronique, afin de faciliter l'identification par les autorités douanières, de permettre la réalisation d'une analyse des risques et de contrôles ciblés et de garantir la traçabilité des biens culturels après leur entrée sur le marché intérieur.

(16) Dans le contexte de l'environnement de guichet unique pour les douanes, la Commission devrait être chargée de mettre en place un système électronique centralisé pour l'introduction des demandes de licences d'importation et des déclarations des importateurs, ainsi que pour le stockage et l'échange d'informations entre les autorités des États membres, en particulier pour ce qui est des déclarations des importateurs et des licences d'importation.

(17) Le traitement des données en vertu du présent règlement devrait pouvoir couvrir également les données à caractère personnel et il devrait être effectué conformément au droit de l'Union. Les États membres et la Commission ne devraient traiter les données à caractère personnel qu'aux fins du présent règlement ou dans des circonstances dûment justifiées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique

et la prévention de telles menaces. Toute collecte, divulgation, transmission, communication et autre traitement de données à caractère personnel relevant du champ d'application du présent règlement devraient être soumis aux exigences des règlements (UE) 2016/679 ([6]) et (UE) 2018/1725 ([7]) du Parlement européen et du Conseil. Le traitement de données à caractère personnel aux fins du présent règlement devrait également respecter le droit au respect de la vie privée et familiale, reconnu à l'article 8 de la convention de sauvegarde des droits de l'homme et des libertés fondamentales du Conseil de l'Europe, ainsi que le droit au respect de la vie privée et familiale et le droit à la protection des données à caractère personnel, reconnus respectivement aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne.

(18) Les biens culturels qui n'ont pas été créés ou découverts sur le territoire douanier de l'Union mais qui ont été exportés en tant que marchandises de l'Union ne devraient pas être subordonnés à la présentation d'une licence d'importation ou d'une déclaration de l'importateur lorsqu'ils sont réintroduits sur ce territoire en tant que marchandises en retour au sens du règlement (UE) n° 952/2013.

(19) L'admission temporaire de biens culturels à des fins pédagogiques, scientifiques, de conservation, de restauration, d'exposition ou de numérisation, dans le domaine des arts du spectacle, de recherches menées par des établissements universitaires ou d'une coopération entre musées ou institutions similaires ne devrait pas non plus être subordonnée à la présentation d'une licence d'importation ou d'une déclaration de l'importateur.

(20) Le stockage de biens culturels en provenance de pays touchés par des conflits armés ou une catastrophe naturelle, dans le but exclusif de trouver un lieu sûr pour assurer leur conservation et leur préservation par une autorité publique ou sous la surveillance de celle-ci, ne devrait pas être soumis à la présentation d'une licence d'importation ou d'une déclaration de l'importateur.

(21) Afin de faciliter la présentation de biens culturels lors des foires commerciales d'art, il ne devrait pas être nécessaire de présenter une licence d'importation lorsque les biens culturels en question sont placés sous le régime de l'admission temporaire, au sens de l'article 250 du règlement (UE) n° 952/2013, et qu'une déclaration de l'importateur a été fournie à la place de la licence d'importation. La présentation d'une licence d'importation devrait toutefois être requise lorsque ces biens culturels restent dans l'Union après la foire d'art.

(22) Afin d'assurer des conditions uniformes d'exécution du présent règlement, il convient de conférer des compétences d'exécution à la Commission afin d'adopter des modalités applicables aux biens culturels qui sont des marchandises en retour ou l'admission temporaire des biens culturels sur le territoire douanier de l'Union et leur conservation, les modèles pour les demandes de licences d'importation et les formulaires correspondants, les modèles pour les déclarations des importateurs et les documents qui les accompagnent, et d'autres règles de procédure concernant le dépôt et le traitement de ces pièces. Il convient également de conférer des compétences d'exécution à la Commission afin de prendre des dispositions en vue de la mise en place d'un système électronique pour l'introduction des demandes de licences d'importation et des déclarations des importateurs, ainsi que pour le stockage d'informations et l'échange d'informations entre les États membres. Ces compétences devraient être exercées en conformité avec le règlement (UE) n° 182/2011 du Parlement européen et du Conseil ([8]).

(23) Afin d'assurer une coordination efficace et d'éviter une duplication des efforts lors de l'organisation de formations, d'activités de renforcement des capacités et de campagnes de sensibilisation, ainsi que de demander la réalisation de travaux de recherche pertinents et l'élaboration de normes, le cas échéant, la Commission et les États membres devraient coopérer avec les organisations et instances internationales, telles que l'Unesco, Interpol, Europol, l'Organisation mondiale des douanes, le Centre international d'études pour la conservation et la restauration des biens culturels et le Conseil international des musées (ICOM).

(24) Les informations utiles concernant les flux commerciaux de biens culturels devraient être recueillies et partagées par voie électronique par les États membres et la Commission, aux fins de la mise en œuvre efficace du présent règlement et de la constitution d'une base pour son évaluation future. Dans un souci de transparence et d'examen public, il convient de rendre publiques autant d'informations que possible. Un contrôle efficace des flux commerciaux de biens culturels ne peut reposer uniquement sur la valeur ou le poids des biens. Il est essentiel de collecter des informations par voie électronique sur le nombre d'articles déclarés. Aucune unité de mesure supplémentaire n'étant spécifiée dans la nomenclature combinée pour les biens culturels, il est nécessaire d'exiger que le nombre d'articles soit déclaré.

([6]) 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).

([7]) Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

([8]) Règlement (UE) n° 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).

(25) La stratégie et le plan d'action de l'Union européenne sur la gestion des risques en matière douanière visent, notamment, à renforcer les capacités des autorités douanières en vue d'accroître la capacité de réaction face aux risques dans le domaine des biens culturels. Il convient d'utiliser le cadre commun de gestion des risques établi dans le règlement (UE) n° 952/2013 et de veiller à l'échange d'informations utiles en matière de risques entre les autorités douanières.

(26) Afin de tirer parti de l'expertise des organisations et instances internationales qui jouent un rôle actif dans le domaine culturel ainsi que de leur expérience concernant le commerce illicite de biens culturels, les recommandations et orientations émises par ces organisations et instances devraient être prises en compte dans le cadre commun de gestion des risques lors de l'identification des risques liés aux biens culturels. Il convient en particulier de se référer aux listes rouges publiées par l'ICOM pour identifier les pays tiers dont le patrimoine est le plus menacé et les objets exportés à partir de ces pays qui sont les plus susceptibles de faire l'objet d'un commerce illicite.

(27) Il y a lieu de lancer des campagnes visant à sensibiliser les acheteurs de biens culturels quant au risque de commerce illicite et d'aider les acteurs du marché à comprendre et à appliquer le présent règlement. Les États membres devraient associer les points de contact nationaux et les autres services d'information à la diffusion de ces informations.

(28) Il y a lieu que la Commission s'assure que les micro-, petites et moyennes entreprises (PME) bénéficient d'une assistance technique adéquate et qu'elle facilite la communication d'informations à celles-ci en vue d'une mise en œuvre efficace du présent règlement. Les PME établies dans l'Union qui importent des biens culturels devraient par conséquent bénéficier des programmes actuels et futurs de l'Union qui visent à soutenir la compétitivité des petites et moyennes entreprises.

(29) Afin d'encourager la conformité et d'empêcher tout contournement, il est opportun que les États membres introduisent des sanctions effectives, proportionnées et dissuasives en cas de non-respect des dispositions du présent règlement et qu'ils communiquent ces sanctions à la Commission. Les sanctions instaurées par les États membres quant au non-respect du présent règlement devraient avoir un effet dissuasif équivalent dans toute l'Union.

(30) Les États membres devraient veiller à ce que les autorités douanières et les autorités compétentes s'accordent sur les mesures visées à l'article 198 du règlement (UE) n° 952/2013. Les détails de ces mesures devraient être réglés par le droit national.

(31) La Commission devrait adopter sans retard les modalités d'exécution du présent règlement, en particulier celles relatives aux formulaires électroniques standardisés appropriés à utiliser pour demander une licence d'importation ou établir une déclaration de l'importateur, et elle devrait ensuite mettre en place le système électronique dans les plus brefs délais. L'application des dispositions relatives aux licences d'importation et aux déclarations des importateurs devrait être reportée en conséquence.

(32) Conformément au principe de proportionnalité, il est nécessaire et approprié afin de mettre en œuvre les objectifs fondamentaux du présent règlement de règlementer l'introduction de biens culturels et les conditions et procédures applicables à leur importation sur le territoire douanier de l'Union. Le présent règlement n'excède pas ce qui est nécessaire pour atteindre les objectifs poursuivis, conformément à l'article 5, paragraphe 4, du traité sur l'Union européenne,

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Objet et champ d'application

1. Le présent règlement définit les conditions applicables à l'introduction de biens culturels et les conditions et procédures applicables à leur importation aux fins de la protection du patrimoine culturel de l'humanité et de la prévention du commerce illicite de biens culturels, en particulier lorsque celui-ci est susceptible de contribuer au financement du terrorisme.

2. Le présent règlement ne s'applique pas aux biens culturels qui ont été soit créés soit découverts sur le territoire douanier de l'Union.

Article 2

Définitions

Aux fins du présent règlement, on entend par:

1) «biens culturels»: tout objet présentant de l'importance pour l'archéologie, la préhistoire, l'histoire, la littérature, l'art ou la science, dont la liste figure en annexe;

2) «introduction de biens culturels»: toute entrée sur le territoire douanier de l'Union de biens culturels qui font l'objet d'une surveillance douanière ou d'un contrôle douanier sur le territoire douanier de l'Union conformément au règlement (UE) n° 952/2013;

3) «importation de biens culturels»:

a) la mise en libre pratique de biens culturels visée à l'article 201 du règlement (UE) n° 952/2013; ou

b) le placement de biens culturels sous l'une des catégories suivantes de régimes particuliers visées à l'article 210 du règlement (UE) n° 952/2013:

i) le stockage, qui comprend l'entrepôt douanier et les zones franches;

ii) l'utilisation spécifique, qui comprend l'admission temporaire et la destination particulière;

iii) le perfectionnement actif;

4) «détenteur des biens»: le détenteur des marchandises défini à l'article 5, point 34), du règlement (UE) n° 952/2013;

5) «autorités compétentes»: les autorités publiques désignées par les États membres pour délivrer des licences d'importation.

Article 3

Introduction et importation de biens culturels

1. L'introduction de biens culturels visés à la partie A de l'annexe qui ont été sortis du territoire du pays dans lequel ils ont été créés ou découverts en violation des dispositions législatives et réglementaires de ce pays est interdite.

Les autorités douanières et les autorités compétentes prennent toute mesure appropriée lorsqu'une tentative est entreprise pour introduire les biens culturels visés au premier alinéa.

2. L'importation de biens culturels énumérés aux parties B et C de l'annexe n'est autorisée que sur présentation soit:

a) d'une licence d'importation délivrée conformément à l'article 4; soit

b) d'une déclaration de l'importateur présentée conformément à l'article 5.

3. La licence d'importation ou la déclaration de l'importateur visées au paragraphe 2 du présent article sont fournies aux autorités douanières conformément à l'article 163 du règlement (UE) n° 952/2013. En cas de placement des biens culturels sous le régime des zones franches, le détenteur des biens fournit la licence d'importation ou la déclaration de l'importateur au moment de la présentation des biens conformément à l'article 245, paragraphe 1, points a) et b), du règlement (UE) n° 952/2013.

4. Le paragraphe 2 du présent article ne s'applique pas:

a) aux biens culturels qui sont des marchandises en retour au sens de l'article 203 du règlement (UE) n° 952/2013;

b) à l'importation de biens culturels dans le but exclusif d'assurer leur conservation par une autorité publique ou sous la surveillance de celle-ci, avec l'intention de restituer ces biens culturels, lorsque la situation le permet;

c) à l'admission temporaire de biens culturels, au sens de l'article 250 du règlement (UE) n° 952/2013, sur le territoire douanier de l'Union à des fins pédagogiques, scientifiques, de conservation, de restauration, d'exposition ou de numérisation, dans le domaine des arts du spectacle, de recherches menées par des établissements universitaires ou d'une coopération entre musées ou institutions similaires.

5. Une licence d'importation ne devrait pas être exigée pour les biens culturels placés sous le régime de l'admission temporaire, au sens de l'article 250 du règlement (UE) n° 952/2013, lorsqu'ils sont destinés à être présentés lors de foires commerciales d'art. Dans ce cas, une déclaration de l'importateur est fournie conformément à la procédure de l'article 5 du présent règlement.

Toutefois, lorsque ces biens culturels sont placés ultérieurement sous un autre régime douanier visé à l'article 2, point 3, du présent règlement, une licence d'importation délivrée conformément à l'article 4 du présent règlement est requise.

6. La Commission établit, par voie d'actes d'exécution, les modalités applicables aux biens culturels qui sont des marchandises en retour, à l'importation de biens culturels en vue de leur conservation et à l'admission temporaire visées aux paragraphes 4 et 5 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 13, paragraphe 2.

7. Le paragraphe 2 du présent article est sans préjudice d'autres mesures adoptées par l'Union conformément à l'article 215 du traité sur le fonctionnement de l'Union européenne.

8. Lors de la présentation d'une déclaration en douane pour l'importation de biens culturels énumérés aux parties B et C de l'annexe, le nombre d'articles est indiqué à l'aide de l'unité supplémentaire qui figure à ladite annexe. En cas de placement des biens culturels sous le régime des zones franches, le détenteur des biens indique le nombre d'articles au moment de la présentation des biens conformément à l'article 245, paragraphe 1, points a) et b), du règlement (UE) n° 952/2013.

Article 4

Licence d'importation

1. L'importation des biens culturels énumérés à la partie B de l'annexe, autres que ceux visés à l'article 3, paragraphes 4 et 5, est subordonnée à la présentation d'une licence d'importation. Cette licence d'importation est délivrée par l'autorité compétente de l'État membre dans lequel les biens culturels sont placés pour la première fois sous l'un des régimes douaniers visés à l'article 2, point 3).

2. Les licences d'importation délivrées par les autorités compétentes d'un État membre conformément au présent article sont valides dans l'ensemble de l'Union.

3. Une licence d'importation délivrée conformément au présent article ne saurait être interprétée comme une preuve du caractère licite de la provenance ou de la propriété des biens culturels en question.

4. Le détenteur des biens introduit une demande de licence d'importation auprès de l'autorité compétente de l'État membre visée au paragraphe 1 du présent article par l'intermédiaire du système électronique visé à l'article 8. La demande est accompagnée des pièces justificatives et des informations attestant que les biens culturels en question ont été exportés depuis le pays dans lequel ils ont été créés ou découverts conformément aux dispositions législatives et réglementaires de ce pays ou prouvant l'absence de telles dispositions au moment où ils ont été sortis de son territoire.

Par dérogation au premier alinéa, la demande peut au lieu de cela être accompagnée des pièces justificatives et des informations attestant que les biens culturels en question ont été exportés conformément aux dispositions législatives et réglementaires du dernier pays dans lequel ils ont été situés pendant une période de plus de cinq ans et à des fins autres que l'utilisation temporaire, le transit, la réexportation ou le transbordement, dans les cas suivants:

a) le pays dans lequel les biens culturels ont été créés ou découverts ne peut pas être déterminé de manière fiable; ou

b) les biens culturels ont été sortis du pays dans lequel ils ont été créés ou découverts avant le 24 avril 1972.

5. Les éléments de preuve attestant que les biens culturels en question ont été exportés conformément au paragraphe 4 sont fournis sous la forme de certificats d'exportation ou de licences d'exportation lorsque le pays en question a établi de tels documents pour l'exportation de biens culturels au moment de l'exportation.

6. L'autorité compétente vérifie si la demande est complète. Elle sollicite du demandeur toute information ou tout document manquant ou complémentaire dans un délai de 21 jours à compter de la réception de la demande.

7. Dans un délai de 90 jours à compter de la réception de la demande complète, l'autorité compétente l'examine et décide de délivrer la licence d'importation ou de rejeter la demande.

L'autorité compétente rejette la demande lorsque:

a) elle dispose de renseignements indiquant que les biens culturels ont été sortis du territoire du pays dans lequel ils ont été créés ou découverts en violation des dispositions législatives et réglementaires de ce pays, ou a des motifs raisonnables de le penser;

b) les éléments de preuve requis en vertu du paragraphe 4 n'ont pas été fournis;

c) elle dispose de renseignements indiquant que le détenteur des biens ne les a pas acquis de manière licite, ou a des motifs raisonnables de le penser; ou

d) elle a été informée qu'il existe des demandes de restitution des biens culturels en attente de la part des autorités du pays dans lequel les biens ont été créés ou découverts.

8. En cas de rejet de la demande, la décision administrative visée au paragraphe 7, accompagnée d'un exposé des motifs et des informations relatives à la procédure d'appel, est communiquée sans retard au demandeur.

9. Lorsqu'une demande de licence d'importation concerne des biens culturels pour lesquels une telle demande a précédemment été rejetée, le demandeur informe l'autorité compétente auprès de laquelle la demande est introduite du refus antérieur.

10. Lorsqu'un État membre rejette une demande, ce rejet ainsi que les motifs qui le justifient sont communiqués aux autres États membres et à la Commission par l'intermédiaire du système électronique visé à l'article 8.

11. Les États membres désignent sans retard les autorités compétentes pour délivrer les licences d'importation conformément au présent article. Les États membres communiquent à la Commission les renseignements sur l'identité des autorités compétentes ainsi que tout changement à cet égard.

La Commission publie les renseignements relatifs aux autorités compétentes, ainsi que tout changement les concernant, dans la série C du *Journal officiel de l'Union européenne*.

12. La Commission établit, par voie d'actes d'exécution, le modèle pour la demande de licence d'importation et indique les éventuelles pièces justificatives permettant de prouver la provenance licite des biens culturels en question, ainsi que le format de ces documents et les règles de procédure applicables à l'introduction et au traitement d'une demande de ce type. En élaborant ces éléments, la Commission s'efforce de parvenir à une application uniforme, par les autorités compétentes, des procédures relatives aux licences d'importation. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 13, paragraphe 2.

Article 5

Déclaration de l'importateur

1. L'importation des biens culturels énumérés à la partie C de l'annexe requiert la présentation d'une déclaration de l'importateur que le détenteur des biens présente par l'intermédiaire du système électronique visé à l'article 8.

2. La déclaration de l'importateur comprend:

a) une déclaration signée par le détenteur des biens selon laquelle les biens culturels ont été exportés depuis le pays dans lequel ils ont été créés ou découverts conformément aux dispositions législatives et réglementaires de ce pays au moment où ils ont été sortis de son territoire; et

b) un document standardisé qui décrit les biens culturels en question de manière suffisamment détaillée pour permettre aux autorités de les identifier et de réaliser une analyse des risques et de contrôles ciblés.

Par dérogation au premier alinéa, point a), la déclaration peut au lieu de cela indiquer que les biens culturels en question ont été exportés conformément aux dispositions législatives et réglementaires du dernier pays dans lequel ils ont été situés pendant une période de plus de cinq ans et à des fins autres que l'utilisation temporaire, le transit, la réexportation ou le transbordement, dans les cas suivants:

a) le pays dans lequel les biens culturels ont été créés ou découverts ne peut pas être déterminé de manière fiable; ou

b) les biens culturels ont été sortis du pays dans lequel ils ont été créés ou découverts avant le 24 avril 1972.

3. La Commission établit, par voie d'actes d'exécution, le modèle standardisé pour la déclaration de l'importateur et son format ainsi que les règles de procédure concernant son introduction et indique les éventuelles pièces justificatives permettant de prouver la provenance licite des biens culturels en question que devrait posséder le détenteur des biens et les règles applicables au traitement de ladite déclaration. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 13, paragraphe 2.

Article 6

Bureaux de douane compétents

Les États membres peuvent limiter le nombre de bureaux de douane compétents pour le traitement de l'importation de biens culturels relevant du présent règlement. Lorsqu'ils appliquent une telle limitation, les États membres communiquent à la Commission les renseignements sur l'identité de ces bureaux de douane ainsi que tout changement à cet égard.

La Commission publie les renseignements relatifs aux bureaux de douane compétents, ainsi que tout changement les concernant, dans la série C du *Journal officiel de l'Union européenne*.

Article 7

Coopération administrative

Aux fins de la mise en œuvre du présent règlement, les États membres veillent à la coopération entre leurs autorités douanières et avec les autorités compétentes visées à l'article 4.

Article 8

Utilisation d'un système électronique

1. Le stockage et l'échange d'informations entre les autorités des États membres, en particulier pour ce qui est des licences d'importation et des déclarations des importateurs, sont effectués par l'intermédiaire d'un système électronique centralisé.

En cas de défaillance temporaire du système électronique, d'autres moyens peuvent être utilisés à titre provisoire pour le stockage et l'échange d'informations.

2. La Commission établit, au moyen d'actes d'exécution:

a) les modalités de déploiement, de fonctionnement et de maintenance du système électronique visé au paragraphe 1;

b) les règles détaillées applicables à l'introduction, au traitement, au stockage et à l'échange d'informations entre les autorités des États membres par l'intermédiaire du système électronique ou par les autres moyens visés au paragraphe 1.

Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 13, paragraphe 2, au plus tard le 28 juin 2021.

Article 9

Mise en place d'un système électronique

La Commission met en place le système électronique visé à l'article 8. Le système électronique est opérationnel au plus tard quatre ans après l'entrée en vigueur du premier des actes d'exécution visés à l'article 8, paragraphe 2.

Article 10

Protection des données à caractère personnel et durée de conservation des données

1. Les autorités douanières et les autorités compétentes des États membres agissent en tant que responsables du traitement des données à caractère personnel qu'elles ont obtenues en vertu des articles 4, 5 et 8.

2. Le traitement des données à caractère personnel sur la base du présent règlement a lieu uniquement aux fins définies à l'article 1er, paragraphe 1.

3. Les données à caractère personnel obtenues en vertu des articles 4, 5 et 8 ne sont accessibles qu'au personnel dûment autorisé des autorités et sont protégées de manière adéquate contre l'accès ou la communication non autorisés. Les données ne peuvent être divulguées ou communiquées sans l'autorisation écrite expresse de l'autorité qui a initialement obtenu les informations. Cependant, cette autorisation n'est pas nécessaire lorsque les autorités sont tenues de divulguer ou de communiquer ces informations conformément aux dispositions légales en vigueur dans l'État membre en question, notamment dans le cadre de procédures judiciaires.

4. Les autorités conservent les données à caractère personnel obtenues en vertu des articles 4, 5 et 8 pendant une durée de 20 ans à compter de la date à laquelle ces données ont été obtenues. Ces données à caractère personnel sont effacées à l'expiration de cette période.

Article 11

Sanctions

Les États membres déterminent le régime des sanctions applicables aux violations du présent règlement et prennent toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions. Ces sanctions doivent être effectives, proportionnées et dissuasives.

Au plus tard le 28 décembre 2020, les États membres informent la Commission du régime des sanctions applicables à l'introduction de biens culturels en violation de l'article 3, paragraphe 1, ainsi que des mesures connexes.

Au plus tard le 28 juin 2025, les États membres informent la Commission du régime des sanctions applicables aux autres infractions au présent règlement, notamment en ce qui concerne les fausses déclarations et les informations erronées, ainsi que des mesures connexes.

Les États membres notifient sans retard à la Commission toute modification ultérieure de ce régime.

Article 12

Coopération avec les pays tiers

Pour les questions qui relèvent de ses activités et dans la mesure nécessaire à l'accomplissement de ses tâches en vertu du présent règlement, la Commission peut organiser des activités de formation et de renforcement des capacités destinées aux pays tiers en coopération avec les États membres.

Article 13

Comité

1. La Commission est assistée par le comité institué à l'article 8 du règlement (CE) n° 116/2009 du Conseil. Ledit comité est un comité au sens du règlement (UE) n° 182/2011.

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

Article 14

Rapports et évaluation

1. Les États membres communiquent à la Commission des informations sur la mise en œuvre du présent règlement.

À cette fin, la Commission adresse aux États membres les questionnaires appropriés. Les États membres disposent d'un délai de six mois à compter de la réception du questionnaire pour transmettre à la Commission les informations demandées.

2. Dans un délai de trois ans après la date à laquelle le présent règlement s'applique et tous les cinq ans par la suite, la Commission présente un rapport au Parlement européen et au Conseil sur la mise en œuvre du présent règlement. Ce rapport est rendu public et contient des informations statistiques pertinentes tant au niveau de l'Union qu'au niveau national, telles que le nombre de licences d'importation délivrées, de demandes rejetées et de déclarations des importateurs présentées. Il comprend un examen de la mise en œuvre pratique, y compris l'incidence sur les opérateurs économiques de l'Union, en particulier sur les PME.

3. Au plus tard le 28 juin 2020, et tous les douze mois par la suite jusqu'à ce que le système électronique défini à l'article 9 soit mis en place, la Commission présente un rapport au Parlement européen et au Conseil sur les progrès réalisés concernant l'adoption des actes d'exécution visés à l'article 8, paragraphe 2, et ceux concernant la mise en place du système électronique visé à l'article 9.

Article 15

Entrée en vigueur

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

Article 16

Application

1. Le présent règlement s'applique à partir de la date de son entrée en vigueur.

2. Nonobstant le paragraphe 1:

a) l'article 3, paragraphe 1, s'applique à partir du 28 décembre 2020;

b) l'article 3, paragraphes 2 à 5, l'article 3, paragraphes 7 et 8, l'article 4, paragraphes 1 à 10, l'article 5, paragraphes 1 et 2, et l'article 8, paragraphe 1, s'appliquent à partir de la date à laquelle le système électronique visé à l'article 8 devient opérationnel ou au plus tard à partir du 28 juin 2025. La Commission publie dans la série C du *Journal officiel de l'Union européenne* la date à laquelle les conditions énoncées au présent paragraphe sont remplies.

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

Fait à Strasbourg, le 17 avril 2019.

Par le Parlement européen	*Par le Conseil*
Le président	*Le président*
A. TAJANI	G. CIAMBA

ANNEXE

Partie A. Biens culturels relevant de l'article 3, paragraphe 1

a) collections et spécimens rares de zoologie, de botanique, de minéralogie et d'anatomie, et objets présentant un intérêt paléontologique;

b) biens concernant l'histoire, y compris l'histoire des sciences et des techniques, l'histoire militaire et sociale ainsi que la vie des dirigeants, penseurs, savants et artistes nationaux, et les événements d'importance nationale;

c) produit de fouilles archéologiques (régulières et clandestines) et des découvertes archéologiques terrestres ou sous-marines;

d) éléments provenant du démembrement de monuments artistiques ou historiques et des sites archéologiques ([1]);

e) objets d'antiquité ayant plus de cent ans d'âge, tels qu'inscriptions, monnaies et sceaux gravés;

f) matériel ethnologique;

g) biens d'intérêt artistique, tels que:

  i) tableaux, peintures et dessins faits entièrement à la main sur tout support et en toutes matières (à l'exclusion des dessins industriels et des articles manufacturés décorés à la main);

  ii) productions originales de l'art statuaire et de la sculpture, en toutes matières;

  iii) gravures, estampes et lithographies originales;

  iv) assemblages et montages artistiques originaux, en toutes matières;

h) manuscrits rares et incunables;

i) livres, documents et publications anciens d'intérêt spécial (historique, artistique, scientifique, littéraire, etc.), isolés ou en collections;

j) timbres-poste, timbres fiscaux et analogues, isolés ou en collections;

k) archives, y compris les archives phonographiques, photographiques et cinématographiques;

l) objets d'ameublement ayant plus de cent ans d'âge et instruments de musique anciens.

([1]) Les icônes et statues liturgiques, même en tant qu'éléments isolés, doivent être considérées comme des biens culturels appartenant à cette catégorie.

Partie B. Biens culturels relevant de l'article 4

Catégories de biens culturels conformément à la partie A	Chapitre, position ou sous-position de la nomenclature combinée (NC)	Seuil d'ancienneté minimal	Seuil financier minimal (valeur en douane)	Unités supplémentaires
c) produit de fouilles archéologiques (régulières et clandestines) ou de découvertes archéologiques terrestres ou sous-marines;	ex 9705; ex 9706	ayant plus de 250 ans d'âge	quelle que soit la valeur	nombre de pièces (p/st)
d) éléments provenant du démembrement de monuments artistiques ou historiques et des sites archéologiques [1].	ex 9705; ex 9706	ayant plus de 250 ans d'âge	quelle que soit la valeur	nombre de pièces (p/st)

[1] Les icônes et statues liturgiques, même en tant qu'éléments isolés, doivent être considérées comme des biens culturels appartenant à cette catégorie.

Partie C. Biens culturels relevant de l'article 5

Catégories de biens culturels conformément à la partie A	Chapitre, position ou sous-position de la nomenclature combinée (NC)	Seuil d'ancienneté minimal	Seuil financier minimal (valeur en douane)	Unités supplémentaires
a) collections et spécimens rares de zoologie, de botanique, de minéralogie et d'anatomie, et objets présentant un intérêt paléontologique;	ex 9705	ayant plus de 200 ans d'âge	18 000 EUR ou plus par pièce	nombre de pièces (p/st)
b) biens concernant l'histoire, y compris l'histoire des sciences et des techniques, l'histoire militaire et sociale ainsi que la vie des dirigeants, penseurs, savants et artistes nationaux, et les événements d'importance nationale;	ex 9705	ayant plus de 200 ans d'âge	18 000 EUR ou plus par pièce	nombre de pièces (p/st)
e) objets d'antiquité, tels qu'inscriptions, monnaies et sceaux gravés;	ex 9706	ayant plus de 200 ans d'âge	18 000 EUR ou plus par pièce	nombre de pièces (p/st)
f) matériel ethnologique;	ex 9705	ayant plus de 200 ans d'âge	18 000 EUR ou plus par pièce	nombre de pièces (p/st)
g) biens d'intérêt artistique, tels que:				
i) tableaux, peintures et dessins faits entièrement à la main sur tout support et en toutes matières (à l'exclusion des dessins industriels et des articles manufacturés décorés à la main);	ex 9701	ayant plus de 200 ans d'âge	18 000 EUR ou plus par pièce	nombre de pièces (p/st)

Catégories de biens culturels conformément à la partie A	Chapitre, position ou sous-position de la nomenclature combinée (NC)	Seuil d'ancienneté minimal	Seuil financier minimal (valeur en douane)	Unités supplémentaires
ii) productions originales de l'art statuaire et de la sculpture, en toutes matières;	ex 9703	ayant plus de 200 ans d'âge	18 000 EUR ou plus par pièce	nombre de pièces (p/st)
iii) gravures, estampes et lithographies originales;	ex 9702;	ayant plus de 200 ans d'âge	18 000 EUR ou plus par pièce	nombre de pièces (p/st)
iv) assemblages et montages artistiques originaux, en toutes matières;	ex 9701	ayant plus de 200 ans d'âge	18 000 EUR ou plus par pièce	nombre de pièces (p/st)
h) manuscrits rares et incunables	ex 9702; ex 9706	ayant plus de 200 ans d'âge	18 000 EUR ou plus par pièce	nombre de pièces (p/st)
i) livres, documents et publications anciens d'intérêt spécial (historique, artistique, scientifique, littéraire, etc.), isolés ou en collections.	ex 9705; ex 9706	ayant plus de 200 ans d'âge	18 000 EUR ou plus par pièce	nombre de pièces (p/st)

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)

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

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

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 114,

vu la proposition de la Commission européenne,

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

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

vu l'avis du Comité des régions ([2]),

statuant conformément à la procédure législative ordinaire ([3]),

considérant ce qui suit:

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

(2) L'utilisation des réseaux et des systèmes d'information par les citoyens, les organisations et les entreprises s'est généralisée dans l'Union tout entière. La numérisation et la connectivité deviennent des caractéristiques essentielles d'un nombre toujours croissant de produits et de services et avec l'avènement de l'internet des objets (IdO), un nombre extrêmement élevé de dispositifs numériques connectés devrait être mis en service dans toute l'Union au cours de la prochaine décennie. Alors qu'un nombre croissant de dispositifs sont connectés à l'internet, leur conception n'intègre pas suffisamment la sécurité et la résilience, de sorte que la cybersécurité est insuffisante. Dans ce contexte, le recours limité à la certification conduit les utilisateurs — qu'ils soient des particuliers, des organisations ou des entreprises — à ne pas disposer de suffisamment d'informations sur les caractéristiques en matière de cybersécurité des produits TIC, services TIC et processus TIC, ce qui nuit à la confiance dans les solutions numériques. Les réseaux et systèmes d'information sont à même de nous assister dans tous les aspects de notre vie et constituent le moteur de la croissance économique de l'Union. Ils constituent le pilier de la réalisation du marché unique numérique.

(3) Une numérisation et une connectivité accrues augmentent les risques liés à la cybersécurité, ce qui rend l'ensemble de la société plus vulnérable aux cybermenaces et exacerbe les dangers auxquels sont confrontés les individus, notamment les personnes vulnérables telles que les enfants. Afin d'atténuer ces risques, il convient de prendre toutes les mesures nécessaires pour améliorer la cybersécurité dans l'Union afin que les réseaux et systèmes d'information, les réseaux de communication, les produits, services et appareils numériques utilisés par les citoyens, les organisations et les entreprises — depuis les petites et moyennes entreprises (PME), telles qu'elles sont définies dans la recommandation 2003/361/CE de la Commission ([4]), jusqu'aux opérateurs d'infrastructures critiques — soient mieux protégés contre les cybermenaces.

([1]) JO C 227 du 28.6.2018, p. 86.
([2]) JO C 176 du 23.5.2018, p. 29.
([3]) Position du Parlement européen du 12 mars 2019 (non encore parue au Journal officiel) et décision du Conseil du 9 avril 2019.
([4]) Recommandation 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).

(4) En mettant les informations utiles à la disposition du public, l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA), instituée par le règlement (UE) n° 526/2013 du Parlement européen et du Conseil ([5]), contribue au développement du secteur de la cybersécurité dans l'Union, en particulier les PME et les start-ups. L'ENISA devrait s'efforcer d'établir une coopération plus étroite avec les universités et les entités de recherche afin de contribuer à réduire la dépendance à l'égard des les produits et services de cybersécurité provenant de l'extérieur de l'Union et de renforcer les chaînes d'approvisionnement à l'intérieur de l'Union.

(5) Les cyberattaques sont en augmentation, et une économie et une société connectées qui sont plus vulnérables aux cybermenaces et aux cyberattaques ont besoin de dispositifs de défense renforcés. Cependant, alors que les cyberattaques sont souvent de nature transfrontière, les compétences des autorités chargées de la cybersécurité et des autorités chargées de l'application de la loi ainsi que les réponses politiques qu'elles y apportent sont surtout nationales. Des incidents majeurs pourraient perturber la fourniture de services essentiels dans l'ensemble de l'Union. Cela nécessite de mettre en place des réponses efficaces et coordonnées et une gestion de la crise à l'échelon de l'Union, sur la base de politiques spécifiques et d'instruments élargis aux fins de la solidarité européenne et de l'assistance mutuelle. En outre, il est important pour les décideurs, les entreprises du secteur et les utilisateurs que la situation en matière de cybersécurité et de résilience dans l'Union soit régulièrement évaluée, sur la base de données de l'Union fiables et d'une anticipation systématique des évolutions, défis et menaces futurs au niveau de l'Union et à l'échelle mondiale.

(6) Compte tenu de l'augmentation des enjeux auxquels l'Union est confrontée dans le domaine de la cybersécurité, il est nécessaire de disposer d'un ensemble complet de mesures qui s'appuieraient sur les actions déjà menées par l'Union et favoriseraient des objectifs complémentaires. Ces objectifs comprennent la poursuite du renforcement des capacités et de l'état de préparation des États membres et des entreprises, ainsi qu'une amélioration de la coopération, du partage d'informations et de la coordination entre les États membres et les institutions, organes et organismes de l'Union. En outre, étant donné que les cybermenaces ignorent les frontières, il est nécessaire d'augmenter, au niveau de l'Union, les capacités susceptibles de compléter l'action des États membres, notamment dans les cas d'incidents et de crises transfrontières majeurs, tout en prenant en compte l'importance de préserver et de renforcer les capacités nationales de réaction en cas de cybermenaces de tous types.

(7) Des efforts supplémentaires sont également nécessaires pour sensibiliser davantage les citoyens, les organisations et les entreprises aux questions de cybersécurité. En outre, étant donné que les incidents nuisent à la confiance dans les fournisseurs de services numériques et dans le marché unique numérique lui-même, en particulier chez les consommateurs, cette confiance devrait être encore renforcée par la communication, en toute transparence, d'informations sur le niveau de sécurité qui caractérise les produits TIC, services TIC et processus TIC, qui précisent que la certification de cybersécurité, aussi élevée soit-elle, ne peut garantir qu'un produit TIC, service TIC ou processus TIC soit complètement sécurisé. Un renforcement de la confiance peut être facilité par une certification mise en œuvre à l'échelle de l'Union prévoyant des exigences et des critères d'évaluation communs en matière de cybersécurité dans l'ensemble des marchés nationaux et des secteurs.

(8) La cybersécurité n'est pas qu'une question liée à la technologie, mais une question pour laquelle le comportement humain est tout aussi important. C'est pourquoi il convient d'encourager vivement les citoyens, les organisations et les entreprises à adopter une «hygiène informatique», à savoir des mesures simples, de routine qui, lorsqu'ils les mettent en œuvre et les effectuent régulièrement, réduisent au minimum leur exposition aux risques liés aux cybermenaces.

(9) En vue de renforcer les structures de cybersécurité de l'Union, il est important de préserver et de développer les capacités de réaction globale des États membres en cas de cybermenaces, y compris en cas d'incidents transfrontières.

(10) Les entreprises et les consommateurs individuels devraient disposer d'informations précises sur le niveau d'assurance auquel la sécurité de leurs produits TIC, services TIC et processus TIC a été certifiée. Dans le même temps, aucun produit TIC ou service TIC n'est totalement sécurisé sur le plan de la cybersécurité, et des règles fondamentales d'hygiène informatique doivent être promues et privilégiées. Compte tenu de la disponibilité croissante de dispositifs IdO, le secteur privé peut prendre une série de mesures volontaires dans l'optique de renforcer la sécurité des produits TIC, services TIC et processus TIC.

(11) Souvent, les produits et systèmes TIC modernes intègrent une ou plusieurs technologies et composants tiers et reposent sur ceux-ci, par exemple des modules logiciels, des bibliothèques ou des interfaces de programmation d'applications. Ce rapport dit de «dépendance» pourrait présenter des risques supplémentaires liés à la cybersécurité car les vulnérabilités des composants tiers pourraient aussi affecter la sécurité des produits TIC, services TIC et processus TIC. Dans bon nombre de cas, recenser et documenter ces dépendances permet aux utilisateurs finaux des produits TIC, services TIC et processus TIC d'optimiser leurs activités de gestion des risques liés à la cybersécurité en améliorant, par exemple, les procédures qu'ils mettent en œuvre pour gérer les vulnérabilités liées à la cybersécurité et y remédier.

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

(12) Les organisations, les fabricants ou les fournisseurs impliqués dans la conception et le développement de produits TIC, services TIC ou processus TIC devraient être encouragés à mettre en œuvre, aux stades les plus précoces de la conception et du développement, des mesures permettant de protéger au mieux la sécurité de ces produits, services et processus, de manière que la survenue de cyberattaques soit présumée et que leur incidence soit anticipée et minimisée («sécurité dès le stade de la conception»). La sécurité devrait être prise en charge tout au long du cycle de vie du produit TIC, service TIC ou processus TIC par les processus de conception et de développement qui évoluent constamment pour réduire le risque de préjudice causé par une utilisation malveillante.

(13) Les entreprises, les organisations et le secteur public devraient configurer les produits TIC, services TIC ou processus TIC qu'ils conçoivent de manière à assurer un niveau de sécurité plus élevé, ce qui permettrait au premier utilisateur de recevoir une configuration par défaut avec les paramétrages les plus sûrs possibles (ci-après dénommée «sécurité par défaut»), réduisant ainsi la charge qui pèse sur les utilisateurs de devoir configurer un produit TIC, service TIC ou processus TIC de manière adéquate. Pour fonctionner, la sécurité par défaut ne devrait pas nécessiter une configuration approfondie, ou une compréhension des détails techniques spécifique, ou encore un comportement non intuitif de la part de l'utilisateur, et devrait fonctionner facilement et de façon fiable lorsqu'elle est mise en œuvre. Si, au cas par cas, une analyse des risques et de la facilité d'utilisation aboutit à la conclusion qu'une configuration par défaut n'est pas réalisable, les utilisateurs devraient être incités à choisir le paramétrage le plus sécurisé.

(14) Le règlement (CE) n° 460/2004 du Parlement européen et du Conseil [6] a institué l'ENISA aux fins de contribuer à la réalisation des objectifs visant à assurer un niveau élevé et efficace de sécurité des réseaux et de l'information au sein de l'Union et à favoriser l'émergence d'une culture de la sécurité des réseaux et de l'information dans l'intérêt des citoyens, des consommateurs, des entreprises et des administrations publiques. Le règlement (CE) n° 1007/2008 du Parlement européen et du Conseil [7] a prorogé le mandat de l'ENISA jusqu'en mars 2012. Le règlement (UE) n° 580/2011 du Parlement européen et du Conseil [8] a prorogé le mandat de l'ENISA une nouvelle fois jusqu'au 13 septembre 2013. Le règlement (UE) n° 526/2013 a prorogé le mandat de l'ENISA jusqu'au 19 juin 2020.

(15) L'Union a déjà pris d'importantes mesures pour garantir la cybersécurité et renforcer la confiance dans les technologies numériques. En 2013, la stratégie de cybersécurité de l'Union européenne a été adoptée afin d'orienter la politique que l'Union entendait mener en réaction aux cybermenaces et aux risques liés à la cybersécurité. Dans le but de mieux protéger les citoyens en ligne, l'Union a adopté en 2016 son premier acte juridique dans le domaine de la cybersécurité sous la forme de la directive (UE) 2016/1148 du Parlement européen et du Conseil [9]. La directive (UE) 2016/1148 a instauré des exigences concernant les capacités nationales dans le domaine de la cybersécurité, a établi les premiers mécanismes destinés à améliorer la coopération stratégique et opérationnelle entre les États membres, et a introduit des obligations concernant les mesures de sécurité et la notification des incidents dans différents secteurs qui revêtent une importance vitale pour l'économie et la société tels que l'énergie, les transports, la fourniture et la distribution d'eau potable, les banques, les infrastructures des marchés financiers, les soins de santé, les infrastructures numériques ainsi que les fournisseurs de services numériques fondamentaux (moteurs de recherche, services d'informatique en nuage et places de marché en ligne).

L'ENISA s'est vu attribuer un rôle essentiel d'appui à la mise en œuvre de ladite directive. En outre, lutter efficacement contre la cybercriminalité est une priorité importante du programme européen en matière de sécurité et contribue à l'objectif global consistant à atteindre un niveau élevé de cybersécurité. D'autres actes juridiques tels que le règlement (UE) 2016/679 du Parlement européen et du Conseil [10] et les directives 2002/58/CE [11] et (UE) 2018/1972 [12] du Parlement européen et du Conseil contribuent également à un niveau élevé de cybersécurité dans le marché unique numérique.

---

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

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

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

[9] 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 du 19.7.2016, p. 1).

[10] 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).

[11] 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).

[12] 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).

(16) Depuis l'adoption de la stratégie de cybersécurité de l'Union européenne en 2013 et la dernière révision du mandat de l'ENISA, le cadre d'action général a considérablement évolué en raison d'un environnement mondial devenu plus incertain et moins sécurisé. Dans ce contexte, et compte tenu de l'évolution positive du rôle que l'ENISA joue en tant que point de référence par ses conseils et ses compétences, et en tant que facilitatrice de coopération et de renforcement des capacités, ainsi que dans le cadre de la nouvelle politique de cybersécurité de l'Union, il est nécessaire de réviser le mandat de l'ENISA pour définir son rôle dans le nouvel écosystème de la cybersécurité et faire en sorte qu'elle contribue efficacement à la réponse apportée par l'Union aux défis en matière de cybersécurité qui résultent de la transformation radicale de la situation en ce qui concerne les cybermenaces, à l'égard desquels le mandat actuel de l'ENISA est insuffisant ainsi qu'il est apparu lors de l'évaluation de l'ENISA.

(17) L'ENISA instituée par le présent règlement devrait succéder à l'ENISA instituée par le règlement (UE) n° 526/2013. L'ENISA devrait remplir les tâches qui lui sont confiées par le présent règlement et par les autres actes juridiques de l'Union dans le domaine de la cybersécurité, notamment en fournissant des conseils et en apportant des compétences, ainsi qu'en jouant le rôle de centre d'information et de connaissance de l'Union. Elle devrait promouvoir l'échange de bonnes pratiques entre les États membres et les parties prenantes du secteur privé, proposer des actions politiques à la Commission et aux États membres, agir en tant que point de référence pour les initiatives politiques sectorielles au niveau de l'Union en ce qui concerne les questions de cybersécurité, et favoriser la coopération opérationnelle à la fois entre les États membres et entre ceux-ci et les institutions, organes et organismes de l'Union.

(18) Dans le cadre de la décision 2004/97/CE, Euratom prise d'un commun accord entre les représentants des États membres réunis au niveau des chefs d'État ou de gouvernement ([13]), les représentants des États membres ont décidé que l'ENISA aurait son siège dans une ville en Grèce qui serait désignée par le gouvernement grec. L'État membre d'accueil de l'ENISA devrait offrir les meilleures conditions possibles pour un fonctionnement harmonieux et efficace de l'ENISA. Il est impératif, pour l'exécution correcte et efficace de ses tâches, pour le recrutement et la fidélisation du personnel et pour une plus grande efficacité des activités de mise en réseau, que l'ENISA soit établie dans un lieu approprié, offrant, entre autres, des liaisons de transport et des aménagements appropriés pour les conjoints et enfants accompagnant les membres du personnel de l'ENISA. Les dispositions nécessaires devraient être arrêtées dans un accord conclu entre l'ENISA et l'État membre d'accueil, après approbation du conseil d'administration de l'ENISA.

(19) Compte tenu de l'aggravation des risques et des défis liés à la cybersécurité auxquels l'Union est confrontée, il faudrait augmenter les ressources financières et humaines allouées à l'ENISA pour tenir compte du renforcement de son rôle et de ses tâches, ainsi que de sa position critique parmi les organisations qui défendent l'écosystème numérique de l'Union, pour lui permettre d'exécuter efficacement les tâches qui lui sont confiées en vertu du présent règlement.

(20) L'ENISA devrait acquérir et maintenir un niveau élevé de compétence et servir de point de référence qui instaure la confiance dans le marché intérieur du fait de son indépendance, de la qualité des conseils qu'elle fournit et des informations qu'elle diffuse, de la transparence de ses procédures, de la transparence de ses modes de fonctionnement et de sa diligence à exécuter ses tâches. L'ENISA devrait soutenir activement les efforts déployés au niveau national et devrait contribuer de manière anticipée aux efforts consentis par l'Union, tout en s'acquittant de ses missions en totale coopération avec les institutions, organes et organismes de l'Union et avec les États membres, en évitant les doubles emplois et en favorisant les synergies. De plus, l'ENISA devrait s'appuyer sur les informations fournies par le secteur privé et les autres parties prenantes concernées et travailler en coopération avec ceux-ci. Un ensemble de tâches devrait déterminer la manière dont l'ENISA doit atteindre ses objectifs tout en lui laissant une certaine souplesse de fonctionnement.

(21) Pour être en mesure d'apporter un soutien adéquat à la coopération opérationnelle entre les États membres, l'ENISA devrait renforcer davantage ses capacités et aptitudes techniques et humaines. Elle devrait accroître son savoir-faire et ses capacités. Sur une base volontaire, l'ENISA et les États membres pourraient élaborer des programmes visant à détacher des experts nationaux auprès de l'ENISA, en créant des groupes d'experts et des programmes d'échanges de personnel.

(22) L'ENISA devrait assister la Commission au moyen de conseils, d'avis et d'analyses sur toutes les questions de l'Union liées à l'élaboration, l'actualisation et la révision des politiques et de la législation dans le domaine de la cybersécurité et de ses aspects sectoriels spécifiques, afin d'améliorer la pertinence des politiques et de la législation de l'Union ayant une dimension liée à la cybersécurité et de permettre la mise en œuvre cohérente de ces politiques et législations au niveau national. L'ENISA devrait agir comme point de référence, par ses conseils et ses compétences, pour les initiatives politiques et législatives sectorielles spécifiques au niveau de l'Union lorsque des questions liées à la cybersécurité sont en jeu. L'ENISA devrait tenir le Parlement européen régulièrement informé de ses activités.

([13]) Décision 2004/97/CE, Euratom prise du commun accord des représentants des États membres réunis au niveau des chefs d'État ou de gouvernement du 13 décembre 2003 relative à la fixation des sièges de certains organismes de l'Union européenne (JO L 29 du 3.2.2004, p. 15).

(23) Le noyau public de l'internet ouvert, à savoir ses principaux protocoles et ses principales infrastructures, qui constituent un bien public mondial, joue un rôle essentiel dans la fonction de l'internet en général et soutient son fonctionnement normal. L'ENISA devrait soutenir la sécurité du noyau public de l'internet ouvert et la stabilité de son fonctionnement, y compris, sans s'y limiter, ses protocoles clés (notamment DNS, BGP et IPv6), le fonctionnement du système des noms de domaines (tel que le fonctionnement de tous les domaines de premier niveau) et le fonctionnement de la zone racine.

(24) La principale tâche de l'ENISA consiste à promouvoir la mise en œuvre cohérente du cadre juridique applicable, et notamment la mise en œuvre effective de la directive (UE) 2016/1148 ainsi que des autres instruments juridiques pertinents comportant des aspects liés à la cybersécurité, ce qui est essentiel pour renforcer la cyber-résilience. Compte tenu de l'évolution rapide de la situation en ce qui concerne les cybermenaces, il est clair que les États membres doivent s'appuyer sur une approche plus globale, transsectorielle, du développement de la cyber-résilience.

(25) L'ENISA devrait assister les États membres et les institutions, organes et organismes de l'Union dans leurs efforts pour mettre en place et développer les capacités et la préparation requises aux fins de prévenir et de détecter les cybermenaces et incidents et d'y réagir, et en ce qui concerne la sécurité des réseaux et des systèmes d'information. L'ENISA devrait notamment soutenir le développement et l'amélioration des centres de réponse aux incidents de sécurité informatique (CSIRT) nationaux et de l'Union prévus par la directive (UE) 2016/1148, afin qu'ils atteignent un niveau de maturité commun élevé dans l'ensemble de l'Union. Les activités entreprises par l'ENISA concernant les capacités opérationnelles des États membres devraient soutenir activement les mesures prises par les États membres pour respecter les obligations qui leur incombent au titre de la directive (UE) 2016/1148 et ne devraient donc pas s'y substituer.

(26) L'ENISA devrait également contribuer à l'élaboration et à la mise à jour des stratégies en matière de sécurité des réseaux et systèmes d'information au niveau de l'Union et, sur demande, au niveau des États membres, notamment en matière de cybersécurité, et devrait promouvoir la diffusion de telles stratégies et suivre les progrès de leur mise en œuvre. L'ENISA devrait en outre contribuer à couvrir les besoins en matière de formations et de matériel pédagogique, y compris les besoins des organismes publics et, le cas échéant, dans une large mesure, «former les formateurs» en s'appuyant sur le cadre de compétences numériques pour les citoyens, en vue d'aider les États membres ainsi que les institutions, organes et organismes de l'Union à mettre en place leurs propres capacités de formation.

(27) L'ENISA devrait soutenir les États membres dans le domaine de la sensibilisation et de l'éducation à la cybersécurité en favorisant une coordination plus étroite et l'échange de bonnes pratiques entre les États membres. Un tel soutien pourrait consister à développer un réseau de points de contact nationaux en matière d'éducation ainsi qu'une plateforme de formation à la cybersécurité. Le réseau de points de contact nationaux en matière d'éducation pourrait fonctionner au sein du réseau des agents de liaison nationaux et être un point de départ pour une future coordination au sein des États membres.

(28) L'ENISA devrait aider le groupe de coopération créé par la directive (UE) 2016/1148 à exécuter ses tâches, notamment en le faisant bénéficier de ses conseils et de ses compétences, et en facilitant l'échange de bonnes pratiques en matière de risques et d'incidents, entre autres en ce qui concerne l'identification des opérateurs de services essentiels par les États membres, ainsi que les dépendances transfrontalières.

(29) Afin de stimuler la coopération entre le secteur public et le secteur privé et au sein de ce dernier, notamment pour soutenir la protection des infrastructures critiques, l'ENISA devrait soutenir le partage d'informations au sein des secteurs et entre ceux-ci, en particulier les secteurs énumérés à l'annexe II de la directive (UE) 2016/1148, en proposant des bonnes pratiques et des orientations sur les outils disponibles et sur les procédures, ainsi qu'en proposant des orientations sur la manière de traiter les questions de réglementation liées au partage d'informations, par exemple en facilitant la mise en place de centres de partage et d'analyse d'informations sectoriels.

(30) Comme l'incidence négative potentielle des vulnérabilités des produits TIC, services TIC et processus TIC croît constamment, il importe de détecter ces vulnérabilités et d'y remédier pour réduire le risque global en matière de cybersécurité. Il est prouvé que la coopération entre les organisations, les fabricants de produits TIC vulnérables ou les fournisseurs de services et processus TIC vulnérables ainsi que les acteurs du secteur de la recherche en matière de cybersécurité et les autorités qui détectent les vulnérabilités permet d'améliorer sensiblement le taux de détection et le rythme de l'élimination des vulnérabilités dans les produits TIC, services TIC et processus TIC. La divulgation coordonnée des vulnérabilités consiste en un processus structuré de coopération dans lequel les vulnérabilités sont signalées au propriétaire du système d'information, ce qui donne à l'organisation 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. Ce processus prévoit en outre une coordination entre la partie qui a procédé à la détection et l'organisation en ce qui concerne la publication de ces vulnérabilités. Les politiques coordonnées de divulgation des vulnérabilités pourraient jouer un rôle important dans le cadre des efforts que les États membres déploient pour renforcer la cybersécurité.

(31) L'ENISA devrait agréger et analyser les rapports nationaux partagés volontairement et qui émanent des CSIRT et de l'équipe d'intervention en cas d'urgence informatique pour les institutions, organes et organismes de l'Union interinstitutionnelle instituée en vertu de l'accord entre le Parlement européen, le Conseil européen, le Conseil de l'Union européenne, la Commission européenne, la Cour de justice de l'Union européenne, la Banque centrale européenne, la Cour des comptes européenne, le Service européen pour l'action extérieure, le Comité économique et social européen, le Comité européen des régions et la Banque européenne d'investissement relatif à l'organisation et au fonctionnement d'une équipe d'intervention en cas d'urgence informatique pour les institutions, organes et organismes de l'Union (CERT-UE) ([14]) afin de contribuer à établir des procédures, un langage et une terminologie communs pour l'échange d'informations. Dans ce contexte, l'ENISA devrait impliquer le secteur privé, dans le cadre de la directive (UE) 2016/1148, laquelle fixe les bases de l'échange volontaire d'informations techniques à l'échelon opérationnel au sein du réseau des centres de réponse aux incidents de sécurité informatique (ci-après dénommé «réseau des CSIRT») institué par ladite directive.

(32) L'ENISA devrait contribuer à l'élaboration de réponses au niveau de l'Union en cas d'incidents et de crises transfrontières majeurs liés à la cybersécurité. Cette tâche devrait être effectuée conformément au mandat de l'ENISA en application du présent règlement, ainsi qu'à une approche devant faire l'objet d'un accord des États membres dans le cadre de la recommandation (UE) 2017/1584 de la Commission ([15]) et des conclusions du Conseil du 26 juin 2018 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs de l'Union. Cette tâche pourrait comprendre la collecte d'informations pertinentes et un rôle de facilitateur entre le réseau des CSIRT et la communauté technique, ainsi qu'entre les décideurs chargés de la gestion des crises. En outre, l'ENISA devrait soutenir la coopération opérationnelle entre les États membres si un ou plusieurs États membres le demandent, pour le traitement des incidents sur le plan technique, en facilitant les échanges de solutions techniques pertinents entre les États membres et en contribuant à l'élaboration des communications au public. L'ENISA devrait soutenir la coopération opérationnelle en testant les modalités de cette coopération grâce à des exercices réguliers de cybersécurité.

(33) Pour soutenir la coopération opérationnelle, l'ENISA devrait recourir aux compétences techniques et opérationnelles disponibles de la CERT-UE grâce à une coopération structurée. Une telle coopération structurée pourrait s'appuyer sur les compétences de l'ENISA. Le cas échéant, des accords dédiés entre les deux entités devraient être conclus afin de définir les modalités pratiques de la mise en œuvre de cette coopération et d'éviter la duplication des activités.

(34) En exécutant sa tâche consistant à soutenir la coopération opérationnelle au sein du réseau des CSIRT, l'ENISA devrait être en mesure de fournir un appui aux États membres, à leur demande, par exemple en fournissant des conseils sur la manière d'améliorer leurs capacités de prévention et de détection des incidents et de réaction aux incidents, en facilitant la gestion technique des incidents ayant un impact significatif ou substantiel, ou en assurant l'analyse des cybermenaces et des incidents. L'ENISA devrait faciliter la gestion technique des incidents ayant un impact significatif ou substantiel, en particulier en soutenant le partage volontaire de solutions techniques entre États membres ou en produisant des informations techniques combinées, telles que des solutions techniques partagées volontairement par les États membres. La recommandation (UE) 2017/1584 recommande aux États membres de coopérer de bonne foi et de partager sans retard indu, entre eux et avec l'ENISA, les informations relatives aux incidents et crises de cybersécurité majeurs. Ces informations devraient apporter une aide supplémentaire à l'ENISA dans l'exécution de sa tâche de soutien à la coopération opérationnelle.

(35) Dans le cadre de la coopération régulière sur le plan technique menée pour étayer l'appréciation de la situation au niveau de l'Union, l'ENISA devrait préparer à intervalles réguliers, en coopération étroite avec les États membres, un rapport approfondi de situation technique en matière de cybersécurité sur les incidents et cybermenaces dans l'Union, sur la base d'informations du domaine public, de sa propre analyse et de rapports que lui communiquent les CSIRT des États membres ou les points de contact nationaux uniques en matière de sécurité des réseaux et des systèmes d'information (ci-après dénommés «points de contact uniques») prévus par la directive (UE) 2016/1148, sur une base volontaire dans les deux cas, le Centre européen de lutte contre la cybercriminalité (EC3) au sein d'Europol, la CERT-UE et, le cas échéant, le Centre de l'Union européenne pour l'analyse du renseignement (INTCEN UE) au sein du Service européen pour l'action extérieure. Ce rapport devrait être mis à la disposition du Conseil, de la Commission, du haut représentant de l'Union pour les affaires étrangères et la politique de sécurité et du réseau des CSIRT.

(36) Le soutien apporté par l'ENISA aux enquêtes techniques ex post sur les incidents ayant un impact significatif ou substantiel, effectuées à la demande des États membres concernés, devrait être axé sur la prévention des incidents futurs. Les États membres concernés devraient fournir les informations et l'assistance nécessaires pour permettre à l'ENISA de soutenir efficacement l'enquête technique ex post.

([14]) JO C 12 du 13.1.2018, p. 1.
([15]) 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).

(37) Les États membres peuvent inviter les entreprises concernées par l'incident à coopérer en fournissant les renseignements et l'assistance nécessaires à l'ENISA, sans préjudice de leur droit de protéger les informations commercialement sensibles et les informations pertinentes du point de vue de la sécurité publique.

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

(39) Afin de renforcer la résilience de l'Union, l'ENISA devrait développer des compétences dans le domaine de la cybersécurité des infrastructures, en soutenant en particulier les secteurs énumérés à l'annexe II de la directive (UE) 2016/1148 et ceux utilisés par les fournisseurs des services numériques énumérés à l'annexe III de ladite directive, en fournissant des conseils et des lignes directrices et en échangeant de bonnes pratiques. En vue de faciliter l'accès à des informations mieux structurées sur les risques liés à la cybersécurité et les solutions possibles, l'ENISA devrait mettre sur pied et gérer le «pôle d'information» de l'Union, un portail servant de guichet unique fournissant au public des informations sur la cybersécurité en provenance des institutions, organes et organismes de l'Union et nationaux. Faciliter l'accès à des informations mieux structurées sur les risques liés à la cybersécurité et les solutions possibles pourrait aussi aider les États membres à consolider leurs capacités, à harmoniser leurs pratiques et, partant, à améliorer leur résilience générale face aux cyberattaques.

(40) L'ENISA devrait contribuer à sensibiliser le public aux risques liés à la cybersécurité, y compris en organisant une campagne de sensibilisation à l'échelle de l'Union en favorisant l'éducation, et à fournir, à l'intention des citoyens, des organisations et des entreprises des orientations sur les bonnes pratiques à adopter par les utilisateurs individuels. L'ENISA devrait également contribuer à promouvoir les meilleures pratiques et solutions, y compris en matière d'hygiène informatique et d'habileté numérique au niveau des citoyens, des organisations et des entreprises en collectant et en analysant des informations du domaine public sur les incidents significatifs, et en rédigeant et en publiant des rapports et des orientations à l'intention des citoyens, des organisations et des entreprises en vue d'améliorer leur niveau global de préparation et de résilience. L'ENISA devrait également s'efforcer de fournir aux consommateurs des informations pertinentes concernant les schémas de certification en vigueur, par exemple en fournissant des lignes directrices et des recommandations. L'ENISA devrait en outre organiser, conformément au plan d'action en matière d'éducation numérique établi par la communication de la Commission du 17 janvier 2018 et en coopération avec les États membres et les institutions, organes et organismes de l'Union, des campagnes d'information régulières et des campagnes publiques d'éducation s'adressant aux utilisateurs finaux, en vue de promouvoir une navigation en ligne plus sûre pour les particuliers et l'habileté numérique, de sensibiliser aux cybermenaces potentielles, y compris les activités criminelles en ligne telles que le hameçonnage, les réseaux zombies, les fraudes financières et bancaires, la falsification de données, et de favoriser la fourniture de conseils de base en matière d'authentification multifacteurs, de mises à jour de sécurité, de chiffrement, d'anonymisation et de protection des données.

(41) L'ENISA devrait jouer un rôle central dans l'accélération de la sensibilisation des utilisateurs finaux à la sécurité des appareils et à la sécurité de l'utilisation des services, et devrait promouvoir les concepts de sécurité dès la conception et de protection de la vie privée dès la conception au niveau de l'Union. En poursuivant cet objectif, l'ENISA devrait utiliser les meilleures pratiques et les compétences disponibles, en particulier les meilleures pratiques et les compétences développées par le monde universitaire et par les chercheurs en sécurité informatique.

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

(43) L'ENISA devrait contribuer aux efforts que l'Union déploie en vue de coopérer avec les organisations internationales ainsi qu'au sein des cadres internationaux de coopération concernés dans le domaine de la cybersécurité. En particulier, l'ENISA devrait contribuer, s'il y a lieu, à une coopération avec des organisations telles que l'OCDE, l'OSCE et l'OTAN. Une telle coopération pourrait comprendre des exercices conjoints dans le domaine de la cybersécurité ainsi qu'une coordination conjointe de la réponse à apporter aux incidents. Ces activités doivent se dérouler dans le plein respect des principes d'inclusion, de réciprocité et d'autonomie décisionnelle de l'Union, sans préjudice du caractère particulier de la politique de sécurité et de défense de tout État membre.

(44) Afin de réaliser pleinement ses objectifs, l'ENISA devrait se concerter avec les autorités de contrôle de l'Union compétentes et avec d'autres autorités compétentes de l'Union ainsi qu'avec les institutions, organes et organismes de l'Union, notamment la CERT-UE, l'EC3, l'Agence européenne de défense (AED), l'Agence du système global de navigation par satellite (GNSS — *Global Navigation Satellite Systems*) européen (ci-après dénommée «Agence du GNSS européen»), l'Organe des régulateurs européens des communications électroniques (ORECE), l'Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA), la Banque centrale européenne (BCE), l'Autorité bancaire européenne (ABE), le comité européen de la protection des données, l'Agence de coopération des régulateurs de l'énergie (ACER), l'Agence de l'Union européenne pour la sécurité aérienne (AESA) et toute autre agence de l'Union jouant un rôle dans le domaine de la cybersécurité. L'ENISA devrait aussi se concerter avec les autorités chargées de la protection des données en vue de procéder à des échanges de savoir-faire et de bonnes pratiques et devrait leur fournir des conseils sur les questions liées à la cybersécurité qui sont susceptibles d'avoir une incidence sur leurs travaux. Les représentants des autorités chargées de l'application de la loi et des autorités chargées de la protection des données au niveau national et à l'échelon de l'Union devraient pouvoir être représentés au sein du groupe consultatif de l'ENISA. Dans ses relations avec les autorités chargées de l'application de la loi concernant les questions de sécurité des réseaux et de l'information susceptibles d'avoir une incidence sur leurs travaux, l'ENISA devrait respecter les canaux d'information existants et les réseaux établis.

(45) Des partenariats pourraient être noués avec des établissements universitaires menant des initiatives de recherche dans les domaines en question, et il convient que les organisations de consommateurs et autres disposent de canaux adéquats pour leurs contributions, lesquelles devraient être prises en compte.

(46) L'ENISA, dans son rôle de secrétariat du réseau des CSIRT, devrait soutenir les CSIRT des États membres et la CERT-UE dans le cadre de la coopération opérationnelle en rapport avec les tâches pertinentes du réseau des CSIRT, telles qu'elles sont visées dans la directive (EU) 2016/1148. En outre, l'ENISA devrait promouvoir et soutenir la coopération entre les CSIRT concernés en cas d'incidents, d'attaques ou de perturbations sur les réseaux ou infrastructures dont les CSIRT assurent la gestion ou la protection et impliquant, ou susceptibles d'impliquer, au moins deux CSIRT, tout en tenant dûment compte des procédures opératoires standard du réseau des CSIRT.

(47) Afin que l'Union soit mieux préparée pour réagir aux incidents, l'ENISA devrait organiser régulièrement des exercices de cybersécurité au niveau de l'Union et aider les États membres et les institutions, organes et organismes de l'Union à organiser de tels exercices s'ils en font la demande. Il convient d'organiser tous les deux ans des exercices globaux à grande échelle incluant des éléments techniques, opérationnels ou stratégiques. En outre, l'ENISA devrait pouvoir organiser régulièrement des exercices moins globaux avec le même objectif, à savoir celui de faire en sorte que l'Union soit mieux préparée pour répondre à des incidents.

(48) L'ENISA devrait continuer à développer et maintenir ses compétences en matière de certification de cybersécurité en vue de soutenir la politique de l'Union dans ce domaine. L'ENISA devrait s'appuyer sur les meilleures pratiques existantes et promouvoir l'adoption de la certification de cybersécurité dans l'Union, notamment en contribuant à l'établissement et au maintien d'un cadre de certification de cybersécurité au niveau de l'Union (ci-après dénommé «cadre européen de certification de cybersécurité»), en vue d'accroître la transparence de l'assurance en matière de cybersécurité des produits TIC, services TIC et processus TIC et, partant, de renforcer la confiance dans le marché intérieur numérique ainsi que sa compétitivité.

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

(50) L'ENISA devrait encourager les États membres, les fabricants ou les fournisseurs de produits TIC, services TIC ou processus TIC à renforcer leurs normes de sécurité générales afin que tous les utilisateurs d'internet puissent prendre les mesures nécessaires pour garantir leur propre cybersécurité et devraient inciter à le faire. En particulier, les fabricants et les fournisseurs de produits TIC, services TIC ou processus TIC devraient fournir les mises à jour nécessaires et devraient rappeler, retirer ou recycler les produits TIC, services TIC ou processus TIC qui ne satisfont pas aux normes de cybersécurité, tandis que les importateurs et les distributeurs devraient veiller à ce que les produits TIC, services TIC et processus TIC qu'ils mettent sur le marché de l'Union respectent les exigences applicables et ne présentent pas de risque pour les consommateurs de l'Union.

(51) En coopération avec les autorités compétentes, l'ENISA devrait pouvoir diffuser des informations sur le niveau de cybersécurité des produits TIC, services TIC et processus TIC offerts sur le marché intérieur, et devrait émettre des alertes visant des fabricants ou fournisseurs de produits TIC, services TIC ou processus TIC et les contraignant à améliorer la sécurité de leurs produits TIC, services TIC et processus TIC, y compris la cybersécurité.

(52) L'ENISA devrait prendre pleinement en compte les activités en cours en matière de recherche, de développement et d'évaluation technologique, et plus particulièrement les activités menées dans le cadre des différentes initiatives de recherche de l'Union, pour fournir des conseils aux institutions, organes et organismes de l'Union et, le cas échéant, aux États membres, s'ils en font la demande, sur les besoins et les priorités en matière de recherche dans le domaine de la cybersécurité. Pour recenser les besoins et les priorités en matière de recherche, l'ENISA devrait également consulter les groupes d'utilisateurs concernés. Plus spécifiquement, une coopération pourrait être établie avec le Conseil européen de la recherche, l'Institut européen d'innovation et de technologie et l'Institut d'études de sécurité de l'Union européenne.

(53) L'ENISA devrait consulter régulièrement les organismes de normalisation, en particulier les organismes européens de normalisation, lors de l'élaboration des schémas européens de certification de cybersécurité.

(54) Les cybermenaces constituent un problème mondial. Il est nécessaire de renforcer la coopération internationale pour améliorer les normes de cybersécurité, y compris en ce qui concerne la nécessité de définir des normes de comportement communes, d'adopter des codes de conduite, de recourir à des normes internationales, et de partager des informations, d'encourager une collaboration internationale plus rapide en réponse aux problèmes de sécurité des réseaux et de l'information et de favoriser une approche globale commune de ces problèmes. À cette fin, l'ENISA devrait aider l'Union à poursuivre son engagement et sa coopération avec les pays tiers et les organisations internationales en mettant les compétences et l'analyse nécessaires au service des institutions, organes et organismes de l'Union concernés, le cas échéant.

(55) L'ENISA devrait être en mesure de répondre aux demandes de conseil et d'assistance ad hoc qui sont formulées par les États membres et les institutions, organes et organismes de l'Union sur des questions qui relèvent du mandat de l'ENISA.

(56) Il est raisonnable et recommandé de mettre en œuvre certains principes relatifs à la gouvernance de l'ENISA afin de se conformer à la déclaration commune et à l'approche commune convenues par le groupe de travail interinstitutionnel sur les agences décentralisées de l'Union en juillet 2012, dont l'objectif est de rationaliser les activités des agences décentralisées et d'améliorer leur efficacité. Il convient par ailleurs de tenir compte, s'il y a lieu, des recommandations figurant dans la déclaration commune et de l'approche commune dans les programmes de travail de l'ENISA, les évaluations de l'ENISA ainsi que les pratiques de l'ENISA en matière d'établissement de rapports et ses pratiques administratives.

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

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

(59) Le bon fonctionnement de l'ENISA exige que le directeur exécutif de celle-ci soit nommé sur la base de son mérite et de ses aptitudes attestées dans le domaine de l'administration et de la gestion, ainsi que de ses compétences et de son expérience pertinentes en matière de cybersécurité. Il convient que le directeur exécutif exerce ses fonctions en toute indépendance. Le directeur exécutif devrait élaborer une proposition de programme de travail annuel pour l'ENISA, après consultation préalable de la Commission, et prendre toutes les mesures nécessaires pour garantir la bonne mise en œuvre de ce programme de travail. Le directeur exécutif devrait préparer un rapport annuel à soumettre au conseil d'administration, portant sur la mise en œuvre du programme de travail annuel de l'ENISA, établir un projet d'état prévisionnel des recettes et des dépenses de l'ENISA et exécuter le budget. Le directeur exécutif devrait, en outre, avoir la possibilité de créer des groupes de travail ad hoc pour traiter de questions spécifiques, en particulier de questions de nature scientifique, technique, juridique ou socio-économique. La création d'un groupe de travail ad hoc est notamment jugée nécessaire pour la préparation d'un schéma européen de

certification de cybersécurité candidat spécifique (ci-après dénommé «schéma candidat»). Le directeur exécutif devrait veiller à ce que les membres des groupes de travail ad hoc soient sélectionnés selon les critères de compétence les plus élevés, visant à assurer un équilibre hommes-femmes et un équilibre adéquat, en fonction des questions spécifiques concernées, entre les administrations publiques des États membres, les institutions, organes et organismes de l'Union et le secteur privé, y compris les entreprises du secteur, les utilisateurs et les experts universitaires en matière de sécurité des réseaux et de l'information.

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

(61) L'ENISA devrait disposer, à titre d'organe consultatif, d'un groupe consultatif de l'ENISA pour assurer un dialogue régulier avec le secteur privé, les organisations de consommateurs et d'autres parties prenantes concernées. Le groupe consultatif de l'ENISA, institué par le conseil d'administration sur proposition du directeur exécutif, devrait s'attacher à examiner des questions pertinentes pour les parties prenantes et devrait les porter à l'attention de l'ENISA. Le groupe consultatif de l'ENISA devrait être consulté en particulier au sujet du projet de programme de travail annuel de l'ENISA. La composition du groupe consultatif de l'ENISA et les tâches assignées à ce groupe devraient assurer une représentation suffisante des parties prenantes dans les travaux de l'ENISA.

(62) Le groupe des parties prenantes pour la certification de cybersécurité devrait être institué pour aider l'ENISA et la Commission à faciliter la consultation des parties prenantes concernées. Le groupe des parties prenantes pour la certification de cybersécurité devrait être composé de membres représentant le secteur dans des proportions équilibrées, du côté tant de la demande que de l'offre de produits TIC et services TIC, y compris, en particulier, les PME, les fournisseurs de services numériques, les organismes européens et internationaux de normalisation, les organismes d'accréditation nationaux, les autorités de contrôle de la protection des données, les organismes d'évaluation de la conformité en application du règlement (CE) n° 765/2008 du Parlement européen et du Conseil ([16]), et les universités ainsi que les organisations de consommateurs.

(63) L'ENISA devrait disposer de règles en matière de prévention et de gestion des conflits d'intérêts. L'ENISA devrait aussi appliquer les dispositions pertinentes du droit de l'Union en ce qui concerne l'accès du public aux documents prévu par le règlement (CE) n° 1049/2001 du Parlement européen et du Conseil ([17]). Le traitement des données à caractère personnel devrait être régi par le règlement (UE) 2018/1725 du Parlement européen et du Conseil ([18]). L'ENISA devrait respecter les dispositions applicables aux institutions, organes et organismes de l'Union et la législation nationale concernant le traitement des informations, notamment les informations non classifiées sensibles et les informations classifiées de l'Union européenne (ICUE).

(64) Pour garantir l'autonomie et l'indépendance complètes de l'ENISA et lui permettre d'exécuter des tâches supplémentaires, y compris des tâches urgentes imprévues, il convient de la doter d'un budget suffisant et autonome dont l'essentiel des recettes devrait provenir d'une contribution de l'Union et de contributions des pays tiers participant aux travaux de l'ENISA. Doter l'ENISA d'un budget adéquat est primordial pour garantir qu'elle dispose d'une capacité suffisante pour exécuter l'ensemble de ses tâches toujours plus nombreuses et atteindre ses objectifs. La majeure partie des effectifs de l'ENISA devrait se consacrer directement à la mise en œuvre opérationnelle du mandat de l'ENISA. L'État membre d'accueil et tout autre État membre devrait être autorisé à apporter des contributions volontaires au budget de l'ENISA. La procédure budgétaire de l'Union devrait rester applicable en ce qui concerne toute subvention imputable sur le budget général de l'Union. En outre, la Cour des comptes devrait contrôler les comptes de l'ENISA afin de garantir la transparence et la responsabilité.

(65) La certification de cybersécurité joue un rôle important dans l'amélioration de la sécurité des produits TIC, services TIC et processus TIC et le renforcement de la confiance qui leur est accordée. Le marché unique numérique, et en particulier l'économie des données et l'IdO, ne peuvent prospérer que si le grand public est convaincu que ces produits, services et processus offrent un certain niveau de cybersécurité. Les voitures connectées et automatisées, les dispositifs médicaux électroniques, les systèmes de contrôle-commande industriels et les réseaux intelligents ne sont que quelques exemples de secteurs dans lesquels la certification est déjà largement utilisée ou est susceptible de l'être dans un avenir proche. Les secteurs régis par la directive (UE) 2016/1148 sont également des secteurs où la certification de cybersécurité joue un rôle critique.

([16]) Règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93 du Conseil (JO L 218 du 13.8.2008, p. 30).

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

([18]) Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

(66) Dans la communication de 2016 intitulée «Renforcer le système européen de cyber-résilience et promouvoir la compétitivité et l'innovation dans le secteur européen de la cybersécurité», la Commission a souligné le besoin de produits et de solutions de très bonne qualité, abordables et interopérables en matière de cybersécurité. L'offre de produits TIC, services TIC et processus TIC au sein du marché unique reste très fragmentée sur le plan géographique. Cela est dû au fait que le secteur de la cybersécurité en Europe s'est développé principalement en fonction de la demande des gouvernements nationaux. En outre, le manque de solutions interopérables (normes techniques), de pratiques et de dispositifs de certification à l'échelle de l'Union constitue l'une des autres lacunes affectant le marché unique dans le domaine de la cybersécurité. Il en résulte que les entreprises européennes ont des difficultés à être concurrentielles au niveau national, à l'échelon de l'Union et au niveau mondial. Cela restreint également le choix des technologies viables et utilisables en matière de cybersécurité qui s'offre aux particuliers et aux entreprises. De la même façon, dans la communication de 2017 sur la révision à mi-parcours de la mise en œuvre de la stratégie pour le marché unique numérique — Un marché unique numérique connecté pour tous, la Commission a insisté sur le besoin de produits et systèmes connectés qui soient sûrs, et a indiqué que la création d'un cadre européen de la sécurité des TIC fixant des règles sur les modalités d'organisation de la certification de sécurité des TIC dans l'Union pourrait à la fois préserver la confiance dans l'internet et permettre de lutter contre la fragmentation actuelle du marché intérieur.

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

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

(69) Dès lors, il est nécessaire d'adopter une approche commune et d'établir un cadre européen de certification de cybersécurité établissant les principales exigences horizontales pour les schémas européens de certification de cybersécurité à développer, et permettant la reconnaissance et l'utilisation dans tous les États membres des certificats de cybersécurité européens et des déclarations de conformité de l'Union européenne pour les produits TIC, services TIC ou processus TIC. Ce faisant, il est essentiel de s'appuyer sur des schémas nationaux et internationaux existants, ainsi que sur des systèmes de reconnaissance mutuelle, en particulier le SOG-IS, et de créer les conditions d'une transition en douceur des schémas existants relevant de ces systèmes vers les schémas relevant du nouveau cadre européen de certification de cybersécurité. Le cadre européen de certification de cybersécurité devrait poursuivre un double objectif. Tout d'abord, il devrait contribuer à renforcer la confiance dans les produits TIC, services TIC et processus TIC qui ont été certifiés au titre des schémas européens de certification de cybersécurité. Ensuite, il devrait aider à éviter la multiplication de schémas de certification de cybersécurité nationales contradictoires ou faisant double emploi, réduisant ainsi les coûts à la charge des entreprises exerçant leurs activités sur le marché unique numérique. Les schémas européens de certification de cybersécurité devraient être non discriminatoires et fondés sur des normes européennes ou internationales, sauf si ces normes sont inefficaces ou inappropriées pour remplir les objectifs légitimes de l'Union à cet égard.

(70) Le cadre européen de certification de cybersécurité devrait être établi de manière homogène dans tous les États membres afin d'éviter la pratique du «shopping de certifications» en raison des différents niveaux d'exigence dans les différents États membres.

(71) Les schémas européens de certification de cybersécurité devraient reposer sur les éléments déjà existants au niveau international et national et, au besoin, sur les spécifications techniques des forums et consortiums, en tirant les leçons des points forts actuels et en évaluant et en corrigeant les points faibles.

(72) Des solutions de cybersécurité flexibles sont nécessaires pour que les entreprises du secteur gardent une longueur d'avance sur les cybermenaces; dès lors, tout schéma de certification devrait être conçu de manière à éviter le risque d'obsolescence rapide.

(73) La Commission devrait être habilitée à adopter des schémas européens de certification de cybersécurité concernant des groupes spécifiques de produits TIC, services TIC et processus TIC. Ces schémas devraient être mis en œuvre et contrôlés par des autorités nationales de certification de cybersécurité, et les certificats délivrés au titre de ces schémas devraient être valables et reconnus sur tout le territoire de l'Union. Les schémas de certification gérés par les entreprises du secteur ou d'autres organismes privés devraient être exclus du champ d'application du présent règlement. Toutefois, les organismes qui gèrent de tels schémas devraient pouvoir proposer que la Commission les prenne pour base en vue de les approuver en tant que schéma européen de certification de cybersécurité.

(74) Les dispositions du présent règlement devraient être sans préjudice du droit de l'Union qui prévoit des règles spécifiques concernant la certification des produits TIC, services TIC et processus TIC. En particulier, le règlement (UE) 2016/679 fixe des dispositions en vue de la mise en place de mécanismes de certification ainsi que de labels et de marques en matière de protection des données aux fins de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent ledit règlement. Ces mécanismes de certification et ces labels et marques en matière de protection des données devraient permettre aux personnes concernées d'évaluer rapidement le niveau de protection des données offert par les produits TIC, services TIC et processus TIC en question. Le présent règlement est sans préjudice de la certification des opérations de traitement des données au titre du règlement (UE) 2016/679, y compris lorsque ces opérations sont intégrées dans des produits TIC, services TIC et processus TIC.

(75) Les schémas européens de certification de cybersécurité devraient avoir pour finalité de garantir que les produits TIC, services TIC et processus TIC certifiés selon de tels schémas respectent les exigences définies qui visent à protéger la disponibilité, l'authenticité, l'intégrité et la confidentialité de données stockées, transmises ou traitées, ou des fonctions connexes de ces produits, services et processus tout au long de leur cycle de vie, ou des services qu'ils offrent ou qui sont accessibles par leur intermédiaire. Il n'est pas possible d'exposer en détail les exigences de cybersécurité se rapportant à tous les produits TIC, services TIC et processus TIC dans le présent règlement. Les produits TIC, services TIC et processus TIC et les besoins de cybersécurité relatifs à ces produits, services et processus sont si divers qu'il est très difficile d'élaborer des exigences de cybersécurité générales qui soient valables en toutes circonstances. Il est donc nécessaire d'adopter, aux fins de la certification, une notion large et générale de la cybersécurité, laquelle devrait être complétée par une série d'objectifs spécifiques en matière de cybersécurité à prendre en compte lors de la conception de schémas européens de certification de cybersécurité. Les modalités selon lesquelles ces objectifs doivent être atteints pour des produits TIC, services TIC et processus TIC spécifiques devraient ensuite être précisées en détail au niveau de chaque schéma de certification adopté par la Commission, par exemple en faisant référence à des normes ou à des spécifications techniques s'il n'existe aucune norme appropriée.

(76) Les spécifications techniques à utiliser dans les schémas européens de certification de cybersécurité devraient respecter les exigences énoncées à l'annexe II du règlement (UE) n° 1025/2012 du Parlement européen et du Conseil ([19]). Il pourrait toutefois être jugé nécessaire de s'écarter quelque peu de ces exigences dans des cas dûment justifiés, lorsque ces spécifications techniques doivent être utilisées dans un schéma européen de certification de cybersécurité renvoyant à un niveau d'assurance dit «élevé». Les motifs de ces écarts devraient être rendus publics.

(77) L'évaluation de la conformité est une procédure consistant à évaluer s'il est satisfait aux exigences relatives à un produit TIC, service TIC ou processus TIC qui ont été définies. Cette procédure est réalisée par un tiers indépendant, autre que le fabricant ou le fournisseur des produits TIC, services TIC ou processus TIC qui font l'objet de l'évaluation. Un certificat de cybersécurité européen devrait être délivré à l'issue d'une procédure d'évaluation d'un produit TIC, service TIC ou processus TIC réussie. Il convient de considérer le certificat de cybersécurité européen comme une confirmation que l'évaluation a été dûment réalisée. En fonction du niveau d'assurance, le schéma européen de certification de cybersécurité devrait indiquer si le certificat de cybersécurité européen doit être délivré par un organisme privé ou public. L'évaluation de la conformité et la certification ne peuvent en soi garantir que les produits TIC, services TIC et processus TIC certifiés sont sécurisés du point de vue de la cybersécurité. Il s'agit plutôt de procédures et de méthodologies techniques visant à attester que des produits TIC, services TIC et processus TIC ont été soumis à des essais et qu'ils respectent certaines exigences de cybersécurité établies par ailleurs, par exemple dans des normes techniques.

(78) Le choix, par les utilisateurs de certificats de cybersécurité européens, de la certification appropriée et des exigences de sécurité correspondantes devrait se fonder sur une analyse des risques associés à l'utilisation des produits TIC, services TIC ou processus TIC. En conséquence, le niveau d'assurance devrait correspondre au niveau de risque associé à l'utilisation prévue d'un produit TIC, service TIC ou processus TIC.

([19]) Règlement (UE) n° 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, 98/34/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 n° 1673/2006/CE du Parlement européen et du Conseil (JO L 316 du 14.11.2012, p. 12).

(79) Les schémas européens de certification de cybersécurité pourraient prévoir une évaluation de la conformité devant être effectuée sous la seule responsabilité du fabricant ou du fournisseur de produits TIC, services TIC ou processus TIC (ci-après dénommée «autoévaluation de la conformité»). En pareils cas, il devrait suffire que le fabricant ou le fournisseur de produits TIC, services TIC ou processus TIC effectue lui-même tous les contrôles pour garantir que les produits TIC, services TIC ou processus TIC sont conformes au schéma européen de certification de cybersécurité. L'autoévaluation de la conformité devrait être considérée comme appropriée pour les produits TIC et services TIC de faible complexité ou pour les processus TIC qui présentent un risque faible pour le public, tels que des mécanismes de conception et de production simples. En outre, l'autoévaluation de la conformité ne devrait être autorisée pour les produits TIC, services TIC ou processus TIC que lorsqu'ils correspondent à un niveau d'assurance dit «élémentaire».

(80) Les schémas européens de certification de cybersécurité pourraient permettre à la fois les autoévaluations de la conformité et les certifications de produits TIC, services TIC ou processus TIC. Dans ce cas, le schéma devrait prévoir des moyens clairs et compréhensibles pour les consommateurs ou les autres utilisateurs de distinguer entre les produits TIC, services TIC ou processus TIC à l'égard desquels le fabricant ou le fournisseur des produits TIC, services TIC ou processus TIC est responsable de l'évaluation, et les produits TIC, services TIC et processus TIC qui sont certifiés par un tiers.

(81) Le fabricant ou le fournisseur de produits TIC, services TIC ou processus TIC qui effectue une autoévaluation de la conformité devrait pouvoir délivrer et signer la déclaration de conformité de l'Union européenne dans le cadre de la procédure d'évaluation de la conformité. Une déclaration de conformité de l'Union européenne est un document qui indique qu'un produit TIC, service TIC ou processus TIC spécifique respecte les exigences du schéma européen de certification de cybersécurité. En délivrant et en signant la déclaration de conformité de l'Union européenne, le fabricant ou le fournisseur de produits TIC, services TIC ou processus TIC assume la responsabilité du respect par le produit TIC, service TIC ou processus TIC des exigences légales du schéma européen de certification de cybersécurité. Une copie de la déclaration de conformité de l'Union européenne devrait être soumise à l'autorité nationale de certification de cybersécurité et à l'ENISA.

(82) Le fabricant ou le fournisseur de produits TIC, services TIC ou processus TIC devrait mettre à la disposition de l'autorité nationale de certification de cybersécurité compétente, pour une durée fixée dans le schéma européen de certification de cybersécurité concerné, la déclaration de conformité de l'Union européenne, la documentation technique et toutes les autres informations pertinentes relatives à la conformité des produits TIC, services TIC ou processus TIC avec un schéma européen de certification de cybersécurité. La documentation technique devrait préciser les exigences applicables au titre du schéma et devrait couvrir la conception, la fabrication et le fonctionnement du produit TIC, service TIC ou processus TIC dans la mesure nécessaire à l'autoévaluation de la conformité. La documentation technique devrait être compilée de façon à permettre d'évaluer si un produit TIC ou un service TIC respecte les exigences applicables au titre de ce schéma.

(83) La gouvernance du cadre européen de certification de cybersécurité prend en compte la participation des États membres ainsi qu'une participation appropriée des parties prenantes, et définit le rôle de la Commission pendant la planification et la proposition, la demande, l'élaboration, l'adoption ainsi que l'évaluation des schémas européens de certification de cybersécurité.

(84) La Commission devrait préparer, avec le soutien du groupe européen de certification de cybersécurité (GECC) et du groupe des parties prenantes pour la certification de cybersécurité et à la suite d'une large consultation ouverte, un programme de travail glissant de l'Union pour les schémas européens de certification de cybersécurité et devrait le publier sous la forme d'un instrument non contraignant. Le programme de travail glissant de l'Union devrait consister en un document stratégique permettant aux entreprises du secteur, aux autorités nationales et aux organismes de normalisation, en particulier, de se préparer à l'avance dans la perspective des futurs schémas européens de certification de cybersécurité. Le programme de travail glissant de l'Union devrait comporter un aperçu pluriannuel des demandes de schémas candidats que la Commission compte adresser à l'ENISA pour préparation, sur la base de motifs spécifiques. La Commission devrait tenir compte du programme de travail glissant de l'Union lors de la préparation de son plan glissant pour la normalisation des TIC et des demandes de normalisation adressées à des organismes européens de normalisation. Compte tenu de la rapidité de l'introduction et de l'adoption des nouvelles technologies, de l'apparition de risques liés à la cybersécurité auparavant inconnus et de l'évolution de la législation et des marchés, la Commission ou le GECC devrait être habilité(e) à demander à l'ENISA de préparer des schémas candidats qui n'ont pas été prévus dans le programme de travail glissant de l'Union. En pareils cas, la Commission et le GECC devraient en outre évaluer le bien-fondé d'une telle demande en tenant compte des finalités et objectifs généraux du présent règlement et de la nécessité d'assurer la continuité en ce qui concerne la planification et l'utilisation des ressources par l'ENISA.

À la suite d'une telle demande, l'ENISA devrait préparer les schémas candidats pour des produits TIC, services TIC et processus TIC spécifiques sans retard injustifié. La Commission devrait évaluer l'incidence positive et négative de sa demande sur le marché spécifique en question, en particulier son impact sur les PME, l'innovation, les obstacles à l'entrée sur ce marché et les coûts pour les utilisateurs finaux. Sur la base du schéma candidat préparé par l'ENISA, la Commission devrait alors être habilitée à adopter le schéma européen de certification de cybersécurité par voie d'actes d'exécution. Compte tenu de la finalité générale du présent règlement et des objectifs de sécurité qui y sont fixés, les schémas européens de certification de cybersécurité adoptés par la Commission devraient préciser un ensemble minimal d'éléments relatifs à l'objet, au champ d'application et au fonctionnement du schéma considéré. Ces éléments devraient notamment comprendre le champ d'application et l'objet de la certification de cybersécurité, y compris l'indication des catégories de produits TIC, services TIC et processus TIC couverts, la description détaillée des exigences de cybersécurité, par exemple par référence à des normes ou des spécifications techniques, les critères et méthodes d'évaluation spécifiques, ainsi que le niveau d'assurance visé («élémentaire», «substantiel» ou «élevé»), et les niveaux d'évaluation s'il y a lieu. L'ENISA devrait pouvoir refuser une demande adressée par le GECC. De telles décisions devraient être prises par le conseil d'administration et devraient être dûment motivées.

(85) L'ENISA devrait maintenir un site internet fournissant des informations sur les schémas européens de certification de cybersécurité et leur donnant une visibilité, qui devrait, entre autres, comprendre les demandes de préparation d'un schéma candidat ainsi que les retours d'information reçus lors du processus de consultation réalisé par l'ENISA au cours de la phase préparatoire. Le site internet devrait en outre fournir des informations sur les certificats de cybersécurité européens et les déclarations de conformité de l'Union européenne délivrés en application du présent règlement, notamment des informations concernant le retrait et l'expiration de tels certificats de cybersécurité européens et déclarations de conformité de l'Union européenne. Le site internet devrait en outre indiquer les schémas nationaux de certification de cybersécurité qui ont été remplacés par un schéma européen de certification de cybersécurité.

(86) Le niveau d'assurance d'un schéma européen de certification constitue le fondement permettant de garantir qu'un produit TIC, service TIC ou processus TIC satisfait aux exigences de sécurité d'un schéma européen de certification de cybersécurité spécifique. Pour assurer la cohérence du cadre européen de certification de cybersécurité, un schéma européen de certification de cybersécurité devrait pouvoir préciser les niveaux d'assurance pour les certificats de cybersécurité européens et les déclarations de conformité de l'Union européenne délivrés dans le cadre de ce schéma. Chaque certificat de cybersécurité européen pourrait renvoyer à l'un des niveaux d'assurance, à savoir «élémentaire», «substantiel» ou «élevé», tandis que la déclaration de conformité de l'Union européenne pourrait ne renvoyer qu'au niveau d'assurance dit «élémentaire». Les niveaux d'assurance prévoiraient la rigueur et l'ampleur correspondantes de l'évaluation du produit TIC, du service TIC ou du processus TIC et seraient déterminés par référence aux spécifications techniques, normes et procédures qui y sont liées, y compris les contrôles techniques, dont l'objectif est de limiter les incidents ou de les prévenir. Chaque niveau d'assurance devrait être cohérent dans les différents domaines sectoriels dans lesquels la certification s'applique.

(87) Un schéma européen de certification de cybersécurité pourrait préciser plusieurs niveaux d'évaluation, en fonction de la rigueur et de l'ampleur de la méthode d'évaluation utilisée. Les niveaux d'évaluation devraient correspondre à l'un des niveaux d'assurance et être associés à une combinaison appropriée de composantes d'assurance. Pour tous les niveaux d'assurance, le produit TIC, service TIC ou processus TIC devrait contenir un certain nombre de fonctions sécurisées, telles qu'elles sont définies par le schéma, pouvant comprendre: une configuration sécurisée prête à l'emploi, un code signé, une mise à jour sécurisée, ainsi que la limitation de l'exploitation de failles et des protections complètes («full stack») ou du tas de la mémoire. Ces fonctions devraient faire l'objet d'un développement et d'une maintenance fondés sur des approches de développement mettant l'accent sur la sécurité et des outils associés, afin de garantir que des mécanismes efficaces au niveau tant du logiciel que du matériel sont incorporés de manière fiable.

(88) Pour le niveau d'assurance dit «élémentaire», l'évaluation devrait au moins porter sur les composantes d'assurance suivantes: l'évaluation devrait comprendre au moins un examen, par l'organisme d'évaluation de la conformité, de la documentation technique accompagnant le produit TIC, service TIC ou processus TIC. Lorsque la certification inclut des processus TIC, le processus de conception, de développement et de maintenance d'un produit TIC ou service TIC devrait également être soumis à l'examen technique. Lorsqu'un schéma européen de certification de cybersécurité prévoit une autoévaluation de la conformité, il devrait suffire que le fabricant ou le fournisseur de produits TIC, services TIC ou processus TIC ait effectué une autoévaluation de la conformité du produit TIC, service TIC ou processus TIC avec le schéma de certification.

(89) Pour le niveau d'assurance dit «substantiel», l'évaluation devrait au moins porter sur, outre les exigences liées au niveau d'assurance dit «élémentaire», la vérification de la conformité des fonctionnalités de sécurité du produit TIC, service TIC ou processus TIC avec sa documentation technique.

(90) Pour le niveau d'assurance dit «élevé», l'évaluation devrait au moins porter sur, outre les exigences liées au niveau d'assurance dit «substantiel», un test d'efficacité évaluant la résistance des fonctionnalités de sécurité du produit TIC, service TIC ou processus TIC face à des cyberattaques élaborées lancées par des personnes aux aptitudes solides et aux ressources importantes.

(91) Le recours à la certification de cybersécurité européenne et aux déclarations de conformité de l'Union européenne devrait rester volontaire, sauf disposition contraire du droit de l'Union ou du droit d'un État membre adoptée conformément au droit de l'Union. En l'absence d'harmonisation du droit de l'Union, les États membres peuvent adopter des réglementations techniques nationales prévoyant une certification obligatoire dans le cadre du schéma européen de certification de cybersécurité conformément à la directive (UE) 2015/1535 du Parlement européen et du Conseil ([20]). Les États membres ont aussi recours à la certification européenne de cybersécurité dans le cadre d'un marché public et de la directive 2014/24/UE du Parlement européen et du Conseil ([21]).

(92) Dans certains domaines, il pourrait s'avérer nécessaire, à l'avenir, d'imposer certaines exigences spécifiques en matière de cybersécurité et de rendre la certification y afférente obligatoire pour certains produits TIC, services TIC ou processus TIC, afin d'améliorer le niveau de la cybersécurité dans l'Union. À intervalles réguliers, la Commission devrait assurer un suivi de l'incidence des schémas européens de certification de cybersécurité adoptés sur la disponibilité dans le marché intérieur de produits TIC, services TIC et processus TIC sécurisés et devrait régulièrement évaluer le niveau d'utilisation des schémas de certification par les fabricants ou les fournisseurs de produits TIC, services TIC ou processus TIC dans l'Union. Il convient d'évaluer l'efficacité des schémas européens de certification de cybersécurité et la question de savoir si certains schémas devraient être rendus obligatoires à la lumière de la législation de l'Union relative à la cybersécurité, en particulier la directive (UE) 2016/1148, en tenant compte de la sécurité du réseau et des systèmes d'information utilisés par les opérateurs de services essentiels.

(93) Les certificats de cybersécurité européens et les déclarations de conformité de l'Union européenne devraient aider les utilisateurs finaux à faire des choix éclairés. Dès lors, les produits TIC, services TIC et processus TIC qui ont été certifiés ou pour lesquels une déclaration de conformité de l'Union européenne a été émise, devraient être accompagnés d'informations structurées, adaptées au niveau technique attendu de l'utilisateur final auquel ils sont destinés. Toutes ces informations devraient être disponibles en ligne et, le cas échéant, sous une forme physique. L'utilisateur final devrait avoir accès à des informations concernant le numéro de référence du schéma de certification, le niveau d'assurance, la description des risques liés à la cybersécurité qui sont associés au produit TIC, service TIC ou processus TIC, et l'autorité ou l'organisme de délivrance, ou devrait être en mesure d'obtenir une copie du certificat de cybersécurité européen. En outre, l'utilisateur final devrait recevoir des informations sur la politique d'assistance en matière de cybersécurité du fabricant ou du fournisseur de produits TIC, services TIC ou processus TIC (à savoir combien de temps l'utilisateur final peut escompter recevoir des mises à jour ou des correctifs en matière de cybersécurité). Le cas échéant, des orientations en ce qui concerne les mesures que l'utilisateur final peut prendre ou les paramétrages qu'il peut effectuer pour maintenir ou accroître la cybersécurité du produit TIC ou service TIC et des informations de contact d'un point de contact unique auquel s'adresser ou auprès duquel recevoir une aide en cas de cyberattaque (outre le signalement automatique) devraient être fournis. Ces informations devraient être actualisées régulièrement et être mises à disposition sur un site internet fournissant des informations sur les schémas européens de certification de cybersécurité.

(94) En vue d'atteindre les objectifs du présent règlement et d'éviter la fragmentation du marché intérieur, les procédures ou schémas nationaux de certification de cybersécurité applicables aux produits TIC, services TIC ou processus TIC couverts par un schéma européen de certification de cybersécurité devraient cesser de produire leurs effets à compter d'une date fixée par la Commission par voie d'actes d'exécution. De plus, les États membres devraient s'abstenir d'instaurer de nouveaux schémas nationaux de certification de cybersécurité applicables aux produits TIC, services TIC ou processus TIC déjà couverts par un schéma européen de certification de cybersécurité existant. Toutefois, il convient de ne pas empêcher les États membres d'adopter ou de maintenir des schémas nationaux de certification de cybersécurité à des fins de sécurité nationale. Les États membres devraient informer la Commission et le GECC de leur intention éventuelle d'élaborer de nouveaux schémas nationaux de certification de cybersécurité. La Commission et le GECC devraient évaluer l'incidence des nouveaux schémas nationaux de certification de cybersécurité sur le bon fonctionnement du marché intérieur, à la lumière de tout intérêt stratégique qu'il y aurait à demander, en leur lieu et place, un schéma européen de certification de cybersécurité.

(95) Les schémas européens de certification de cybersécurité ont vocation à contribuer à harmoniser les pratiques de cybersécurité au sein de l'Union. Ils doivent contribuer à augmenter le niveau de cybersécurité dans l'Union. La conception des schémas européens de certification de cybersécurité devrait également prendre en compte et permettre la mise au point d'innovations dans le domaine de la cybersécurité.

([20]) 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).

([21]) Directive 2014/24/UE du Parlement européen et du Conseil du 26 février 2014 sur la passation des marchés publics et abrogeant la directive 2004/18/CE (JO L 94 du 28.3.2014, p. 65).

(96) Les schémas européens de certification de cybersécurité devraient tenir compte des méthodes actuelles de développement des logiciels et du matériel et, en particulier, de l'incidence sur des certificats de cybersécurité européens individuels de mises à jour fréquentes des logiciels ou des micrologiciels. Les schémas européens de certification de cybersécurité devraient préciser les conditions dans lesquelles une mise à jour peut nécessiter qu'un produit TIC, service TIC ou processus TIC doive être de nouveau certifié ou que le champ d'application d'un certificat de cybersécurité européen particulier doive être réduit, compte tenu des éventuels effets négatifs de la mise à jour sur le respect des exigences de ce certificat en matière de sécurité.

(97) Une fois qu'un schéma européen de certification de cybersécurité a été adopté, les fabricants ou les fournisseurs de produits TIC, services TIC ou processus TIC devraient être en mesure de soumettre des demandes de certification de leurs produits TIC ou services TIC à l'organisme d'évaluation de la conformité de leur choix établi où que ce soit dans l'Union. Les organismes d'évaluation de la conformité devraient être accrédités par un organisme d'accréditation national s'ils satisfont à certaines exigences définies telles qu'elles sont énoncées dans le présent règlement. L'accréditation devrait être accordée pour une durée maximale de cinq ans et devrait pouvoir être renouvelée dans les mêmes conditions, pourvu que l'organisme d'évaluation de la conformité satisfasse encore aux exigences. L'accréditation devrait être limitée, suspendue ou révoquée par des organismes d'accréditation nationaux lorsque les conditions de l'accréditation ne sont pas ou ne sont plus remplies ou lorsque l'organisme d'évaluation de la conformité viole le présent règlement.

(98) Les références faites dans la législation nationale à des normes nationales qui ont cessé de produire leurs effets en raison de l'entrée en vigueur d'un schéma européen de certification de cybersécurité peuvent être une source de confusion. Dès lors, les États membres devraient tenir compte, dans leur législation nationale, de l'adoption d'un schéma européen de certification de cybersécurité.

(99) Pour parvenir à l'équivalence des normes dans toute l'Union, faciliter la reconnaissance mutuelle et favoriser l'acceptation globale des certificats de cybersécurité européens et des déclarations de conformité de l'Union européenne, il est nécessaire de mettre en place un système d'examen par les pairs entre les autorités nationales de certification de cybersécurité. L'examen par les pairs devrait couvrir les procédures de contrôle de la conformité des produits TIC, services TIC et processus TIC avec les certificats de cybersécurité européens, de surveillance du respect des obligations des fabricants ou des fournisseurs de produits TIC, services TIC ou processus TIC qui procèdent à une autoévaluation de la conformité, et de surveillance des organismes d'évaluation de la conformité ainsi que de l'adéquation des compétences du personnel des organismes qui délivrent les certificats pour les niveaux d'assurance dits «élevés». La Commission devrait pouvoir, par voie d'actes d'exécution, établir au moins un plan quinquennal pour les examens par les pairs, et fixer les critères et les méthodes de fonctionnement du système d'examen par les pairs.

(100) Sans préjudice du système général d'examen par les pairs à mettre en place entre toutes les autorités nationales de certification de cybersécurité au sein du cadre européen de certification de cybersécurité, certains schémas européens de certification de cybersécurité peuvent comporter un mécanisme d'évaluation par les pairs pour les organismes délivrant des certificats de cybersécurité européens pour des produits TIC, services TIC et processus TIC avec un niveau d'assurance dit «élevé» en application de ces schémas. Le GECC devrait soutenir la mise en œuvre de ces mécanismes d'évaluation par les pairs. Les évaluations par les pairs devraient en particulier évaluer si les organismes concernés s'acquittent de leurs tâches de façon harmonisée, et peuvent comporter des mécanismes de recours. Les résultats des évaluations par les pairs devraient être rendus publics. Les organismes concernés peuvent adopter des mesures appropriées pour adapter leurs pratiques et leurs compétences en conséquence.

(101) Les États membres devraient désigner une ou plusieurs autorités nationales de certification de cybersécurité afin de contrôler le respect des obligations découlant du présent règlement. Une autorité nationale de certification de cybersécurité peut être une autorité existante ou une nouvelle autorité. Un État membre devrait également pouvoir désigner, après en être convenu avec un autre État membre, une ou plusieurs autorités nationales de certification de cybersécurité sur le territoire de cet autre État membre.

(102) Les autorités nationales de certification de cybersécurité devraient en particulier contrôler et faire respecter les obligations qui incombent aux fabricants ou fournisseurs de produits TIC, services TIC ou processus TIC établis sur leur territoire respectif en ce qui concerne la déclaration de conformité de l'Union européenne, assister les organismes nationaux d'accréditation dans le contrôle et la supervision des activités des organismes d'évaluation de la conformité en leur offrant leurs compétences et en leur fournissant des informations utiles, autoriser les organismes d'évaluation de la conformité à exécuter leurs tâches lorsque ces organismes satisfont aux exigences supplémentaires fixées dans un schéma européen de certification de cybersécurité, et suivre les évolutions pertinentes dans le domaine de la certification de cybersécurité. Les autorités nationales de certification de cybersécurité devraient également traiter les réclamations introduites par des personnes physiques ou morales en rapport avec les

certificats de cybersécurité européens que ces autorités ont délivrés ou en rapport avec des certificats de cybersécurité européens délivrés par des organismes d'évaluation de la conformité, lorsque de tels certificats indiquent un niveau d'assurance dit «élevé», devraient examiner l'objet de la réclamation dans la mesure nécessaire et devraient informer l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable. De plus, les autorités nationales de certification de cybersécurité devraient coopérer avec d'autres autorités nationales de certification de cybersécurité ou d'autres autorités publiques, notamment en partageant des informations sur l'éventuel non-respect par des produits TIC, services TIC et processus TIC des exigences du présent règlement ou de certains schémas européens de certification de cybersécurité spécifiques. La Commission devrait faciliter ce partage d'informations grâce à la mise à disposition d'un système général de soutien à l'information électronique, par exemple, le système d'information et de communication pour la surveillance des marchés (ICSMS) et le système européen d'échange rapide sur les produits dangereux (RAPEX) déjà utilisés par les autorités de surveillance du marché en vertu du règlement (CE) n° 765/2008.

(103) Afin d'assurer une application cohérente du cadre européen de certification de cybersécurité, un GECC qui est composé de représentants des autorités nationales de certification de cybersécurité ou d'autres autorités nationales compétentes devrait être mis en place. Les tâches principales du GECC devraient consister à conseiller et assister la Commission dans ses efforts pour assurer une mise en œuvre et une application cohérentes du cadre européen de certification de cybersécurité, à assister l'ENISA et à coopérer étroitement avec elle dans la préparation des schémas de certification de cybersécurité candidats, à demander à l'ENISA, dans des cas dûment justifiés, de préparer un schéma candidat, à adopter des avis adressés à l'ENISA sur les schémas candidats et à adopter des avis à l'intention de la Commission concernant la maintenance et le réexamen de schémas européens de certification de cybersécurité existants. Le GECC devrait faciliter l'échange de bonnes pratiques et de compétences entre les diverses autorités nationales de certification de cybersécurité qui sont responsables de l'accréditation des organismes d'évaluation de la conformité et de la délivrance des certificats de cybersécurité européens.

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

(105) Pour faciliter encore davantage les échanges, et compte tenu du fait que les chaînes d'approvisionnement TIC sont mondiales, des accords de reconnaissance mutuelle concernant les certificats de cybersécurité européens peuvent être conclus par l'Union conformément à l'article 218 du traité sur le fonctionnement de l'Union européenne. La Commission, tenant compte de l'avis de l'ENISA et du GECC, peut recommander l'ouverture de négociations à cette fin. Chaque schéma européen de certification de cybersécurité devrait prévoir des conditions spécifiques pour de tels accords de reconnaissance mutuelle avec des pays tiers.

(106) Afin d'assurer des conditions uniformes d'exécution du présent règlement, il convient de conférer des compétences d'exécution à la Commission. Ces compétences devraient être exercées en conformité avec le règlement (UE) n° 182/2011 du Parlement européen et du Conseil ([22]).

(107) Il convient d'avoir recours à la procédure d'examen pour l'adoption d'actes d'exécution concernant les schémas européens de certification de cybersécurité applicables à des produits TIC, services TIC ou processus TIC, pour l'adoption d'actes d'exécution concernant les modalités d'exécution des enquêtes menées par l'ENISA, pour l'adoption d'actes d'exécution concernant un plan pour l'examen par les pairs des autorités nationales de certification de cybersécurité et pour l'adoption d'actes d'exécution concernant les circonstances, les formats et les procédures de notification à la Commission des organismes d'évaluation de la conformité accrédités par les autorités nationales de certification de cybersécurité.

(108) Les activités de l'ENISA devraient faire l'objet d'évaluations régulières et indépendantes. Ces évaluations devraient porter sur les objectifs, les méthodes de travail et la pertinence des tâches de l'ENISA, en particulier les tâches qui ont trait à la coopération opérationnelle au niveau de l'Union. Ces évaluations devraient également porter sur l'impact, l'efficacité et l'efficience du cadre européen de certification de cybersécurité. En cas de réexamen, la Commission devrait évaluer comment le rôle de l'ENISA en tant que point de référence pour les conseils et les compétences peut être renforcé, et devrait également évaluer le rôle que l'ENISA pourrait jouer pour soutenir l'évaluation des produits TIC, services TIC et processus TIC de pays tiers qui ne respectent pas les règles de l'Union, lorsque ces produits, services et processus entrent dans l'Union.

([22]) Règlement (UE) n° 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).

(109) Étant donné que les objectifs du présent règlement ne peuvent pas être atteints de manière suffisante par les États membres, mais peuvent, en raison de ses dimensions et de ses effets, l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures, conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité tel qu'énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

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

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

TITRE I

DISPOSITIONS GÉNÉRALES

Article premier

Objet et champ d'application

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

a) les objectifs, les tâches et les questions organisationnelles concernant l'ENISA (l'Agence de l'Union européenne pour la cybersécurité); et

b) un cadre pour la mise en place de schémas européens de certification de cybersécurité dans le but de garantir un niveau adéquat de cybersécurité des produits TIC, services TIC et processus TIC dans l'Union, ainsi que dans le but d'éviter la fragmentation du marché intérieur pour ce qui est des schémas de certification dans l'Union.

Le cadre visé au premier alinéa, point b), s'applique sans préjudice des dispositions spécifiques d'autres actes juridiques de l'Union en matière de certification volontaire ou obligatoire.

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

Article 2

Définitions

Aux fins du présent règlement, on entend par:

1) «cybersécurité», les actions nécessaires pour protéger les réseaux et les systèmes d'information, les utilisateurs de ces systèmes et les autres personnes exposées aux cybermenaces;

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

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

4) «opérateur de services essentiels», un opérateur de services essentiels au sens de l'article 4, point 4), de la directive (UE) 2016/1148;

5) «fournisseur de service numérique», un fournisseur de service numérique au sens de l'article 4, point 6), de la directive (UE) 2016/1148;

6) «incident», un incident au sens de l'article 4, point 7), de la directive (UE) 2016/1148;

7) «gestion d'incident», la gestion d'incident au sens de l'article 4, point 8), de la directive (UE) 2016/1148;

8) «cybermenace», toute circonstance, tout événement ou toute action potentiels susceptibles de nuire ou de porter autrement atteinte aux réseaux et systèmes d'information, aux utilisateurs de tels systèmes et à d'autres personnes, ou encore de provoquer des interruptions de ces réseaux et systèmes;

9) «schéma européen de certification de cybersécurité», un ensemble complet de règles, d'exigences techniques, de normes et de procédures qui sont établies à l'échelon de l'Union et qui s'appliquent à la certification ou à l'évaluation de la conformité de produits TIC, services TIC ou processus TIC spécifiques;

10) «schéma national de certification de cybersécurité», un ensemble complet de règles, d'exigences techniques, de normes et de procédures élaborées et adoptées par une autorité publique nationale et qui s'appliquent à la certification ou à l'évaluation de la conformité des produits TIC, services TIC et processus TIC relevant de ce schéma spécifique;

11) «certificat de cybersécurité européen», un document délivré par un organisme compétent attestant qu'un produit TIC, service TIC ou processus TIC donné a été évalué en ce qui concerne sa conformité aux exigences de sécurité spécifiques fixées dans un schéma européen de certification de cybersécurité;

12) «produit TIC», un élément ou un groupe d'éléments appartenant à un réseau ou à un schéma d'information;

13) «service TIC», un service consistant intégralement ou principalement à transmettre, stocker, récupérer ou traiter des informations au moyen de réseaux et de systèmes d'information;

14) «processus TIC», un ensemble d'activités exécutées pour concevoir, développer ou fournir un produit TIC ou service TIC ou en assurer la maintenance;

15) «accréditation», l'accréditation au sens de l'article 2, point 10), du règlement (CE) n° 765/2008;

16) «organisme national d'accréditation», un organisme national d'accréditation au sens de l'article 2, point 11), du règlement (CE) n° 765/2008;

17) «évaluation de la conformité», une évaluation de la conformité au sens de l'article 2, point 12), du règlement (CE) n° 765/2008;

18) «organisme d'évaluation de la conformité», un organisme d'évaluation de la conformité au sens de l'article 2, point 13), du règlement (CE) n° 765/2008;

19) «norme», une norme au sens de l'article 2, point 1), du règlement (UE) n° 1025/2012;

20) «spécification technique», un document qui établit les exigences techniques auxquelles un produit TIC, service TIC ou processus TIC doit répondre ou des procédures d'évaluation de la conformité afférentes à un produit TIC, service TIC ou processus TIC;

21) «niveau d'assurance», le fondement permettant de garantir qu'un produit TIC, service TIC ou processus TIC satisfait aux exigences de sécurité d'un schéma européen de certification de cybersécurité spécifique, indique le niveau auquel un produit TIC, service TIC ou processus TIC a été évalué mais, en tant que tel, ne mesure pas la sécurité du produit TIC, service TIC ou processus TIC concerné;

22) «autoévaluation de la conformité», une action effectuée par un fabricant ou un fournisseur de produits TIC, services TIC ou processus TIC, qui évalue si ces produits TIC, services TIC ou processus TIC satisfont aux exigences fixées dans un schéma européen de certification de cybersécurité spécifique.

TITRE II

ENISA (L'AGENCE DE L'UNION EUROPÉENNE POUR LA CYBERSÉCURITÉ)

CHAPITRE I

Mandat et objectifs

Article 3

Mandat

1. L'ENISA exécute les tâches qui lui sont assignées par le présent règlement dans le but de parvenir à un niveau commun élevé de cybersécurité dans l'ensemble de l'Union, y compris en aidant activement les États membres et les institutions, organes et organismes de l'Union à améliorer la cybersécurité. L'ENISA sert de point de référence pour les conseils et compétences en matière de cybersécurité pour les institutions, organes et organismes de l'Union ainsi que pour les autres parties prenantes concernées de l'Union.

L'ENISA contribue à réduire la fragmentation du marché intérieur en s'acquittant des tâches qui lui sont assignées en vertu du présent règlement.

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

3. Dans l'accomplissement de ses tâches, l'ENISA agit de façon indépendante tout en évitant la duplication des activités des États membres et en tenant compte des compétences existantes des États membres.

4. L'ENISA développe ses ressources propres, y compris les capacités et les aptitudes techniques et humaines, nécessaires pour exécuter les tâches qui lui sont assignées en vertu du présent règlement.

Article 4

Objectifs

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

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

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

4. L'ENISA favorise la coopération, notamment le partage d'informations et la coordination au niveau de l'Union, entre les États membres, les institutions, organes et organismes de l'Union et les parties prenantes concernées des secteurs public et privé en ce qui concerne les questions liées à la cybersécurité.

5. L'ENISA contribue à renforcer les capacités dans le domaine de la cybersécurité au niveau de l'Union afin de soutenir les actions des États membres pour prévenir les cybermenaces et réagir à celles-ci, notamment en cas d'incidents transfrontières.

6. L'ENISA favorise le recours à la certification européenne de cybersécurité en vue d'éviter la fragmentation du marché intérieur. L'ENISA contribue à l'établissement et au maintien d'un cadre européen de certification de cybersécurité, conformément au titre III du présent règlement, en vue de rendre plus transparente la cybersécurité des produits TIC, services TIC et processus TIC et, partant, de rehausser la confiance dans le marché intérieur numérique et la compétitivité de ce dernier.

7. L'ENISA promeut un niveau élevé de sensibilisation des citoyens, des organisations et des entreprises aux questions liées à la cybersécurité, y compris en matière d'hygiène informatique et d'habileté numérique.

CHAPITRE II

Tâches

Article 5

Élaboration et mise en œuvre de la politique et du droit de l'Union

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

1) en apportant son concours et en fournissant des conseils concernant l'élaboration et la révision de la politique et du droit de l'Union dans le domaine de la cybersécurité, et concernant les initiatives politiques et législatives sectorielles mettant en jeu des questions liées à la cybersécurité, notamment en fournissant des avis et des analyses indépendants, ainsi qu'en effectuant des travaux préparatoires;

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

3) en aidant les États membres et les institutions, organes et organismes de l'Union à élaborer et à promouvoir des politiques en matière de cybersécurité visant à soutenir la disponibilité ou l'intégrité générales du noyau public de l'internet ouvert;

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

5) en soutenant:

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

   b) la promotion d'une amélioration du niveau de sécurité des communications électroniques, y compris en fournissant des conseils et des compétences, ainsi qu'en facilitant l'échange de meilleures pratiques entre les autorités compétentes;

   c) les États membres dans la mise en œuvre d'aspects spécifiques en matière de cybersécurité des politiques et du droit de l'Union concernant la protection des données et la vie privée, y compris en fournissant des avis au comité européen de la protection des données à sa demande;

6) en soutenant le réexamen périodique des activités liées aux politiques de l'Union, par la préparation d'un rapport annuel sur l'état d'avancement de la mise en œuvre du cadre juridique applicable en ce qui concerne:

   a) les informations sur les notifications d'incidents des États membres transmises par les points de contact uniques au groupe de coopération conformément à l'article 10, paragraphe 3, de la directive (UE) 2016/1148;

   b) les résumés des notifications d'atteinte à la sécurité ou de perte d'intégrité reçues des prestataires de services de confiance et transmises à l'ENISA par les organes de contrôle, conformément à l'article 19, paragraphe 3, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil ([23]);

   c) les notifications d'incidents de sécurité transmises par les fournisseurs de réseaux de communications publics ou de services de communications électroniques accessibles au public, fournies à l'ENISA par les autorités compétentes, conformément à l'article 40 de la directive (UE) 2018/1972.

([23]) Règlement (UE) n° 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).

Article 6

Renforcement des capacités

1. L'ENISA assiste:

a) les États membres dans leurs efforts pour améliorer la prévention, la détection et l'analyse des cybermenaces et incidents, ainsi que la capacité d'y réagir, en leur fournissant des connaissances et des compétences;

b) les États membres et les institutions, organes et organismes de l'Union pour établir et mettre en œuvre, sur une base volontaire, des politiques en matière de divulgation des vulnérabilités;

c) les institutions, organes et organismes de l'Union dans leurs efforts pour améliorer la prévention, la détection et l'analyse des cybermenaces et incidents, et pour améliorer leur capacité à y réagir, notamment en apportant un soutien adapté à la CERT-UE;

d) les États membres dans la mise en place de CSIRT nationaux, lorsqu'ils le demandent conformément à l'article 9, paragraphe 5, de la directive (UE) 2016/1148;

e) les États membres dans l'élaboration de stratégies nationales en matière de sécurité des réseaux et des systèmes d'information, lorsqu'ils le demandent conformément à l'article 7, paragraphe 2, de la directive (UE) 2016/1148, et favorise la diffusion de ces stratégies et prend note de l'avancement de leur mise en œuvre dans toute l'Union afin de promouvoir les meilleures pratiques;

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

g) les CSIRT nationaux et de l'Union dans le relèvement du niveau de leurs capacités, y compris en favorisant le dialogue et les échanges d'informations, pour faire en sorte que chaque CSIRT, eu égard à l'état de l'art, possède un socle commun de capacités minimales et fonctionne selon les meilleures pratiques;

h) les États membres en organisant régulièrement les exercices de cybersécurité au niveau de l'Union visés à l'article 7, paragraphe 5, au moins tous les deux ans, et en formulant des recommandations en vue d'actions sur la base de l'évaluation de ces exercices et des enseignements qui en ont été tirés;

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

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

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

Article 7

Coopération opérationnelle au niveau de l'Union

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

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

a) en échangeant savoir-faire et meilleures pratiques;

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

c) en établissant les modalités pratiques de l'exécution de tâches spécifiques, après consultation de la Commission.

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

4. L'ENISA soutient les États membres en ce qui concerne la coopération opérationnelle au sein du réseau des CSIRT:

a) en prodiguant des conseils sur la façon d'améliorer leur capacité à prévenir et à détecter les incidents ainsi qu'à y réagir et, à la demande d'un ou de plusieurs États membres, en prodiguant des conseils concernant une cybermenace spécifique;

b) en prêtant son assistance, à la demande d'un ou de plusieurs États membres, dans l'évaluation des incidents ayant un impact significatif ou substantiel, en les faisant bénéficier de compétences et en facilitant la gestion technique de tels incidents, en particulier en soutenant le partage volontaire d'informations et de solutions techniques pertinentes entre États membres;

c) en analysant les vulnérabilités et les incidents à l'aide des informations publiquement disponibles ou des informations fournies volontairement par les États membres à cet effet; et

d) à la demande d'un ou de plusieurs États membres, en apportant un soutien en rapport avec les enquêtes techniques ex post sur les incidents ayant un impact significatif ou substantiel au sens de la directive (UE) 2016/1148.

Dans l'accomplissement de ces tâches, l'ENISA mène avec la CERT-UE une coopération structurée afin de tirer avantage des synergies et d'éviter une duplication des activités.

5. L'ENISA organise régulièrement des exercices de cybersécurité à l'échelle de l'Union, et aide, à leur demande, les États membres et les institutions, organes et organismes de l'Union à organiser des exercices de cybersécurité. De tels exercices de cybersécurité à l'échelle de l'Union peuvent comporter des aspects techniques, opérationnels ou stratégiques. Tous les deux ans, l'ENISA organise un exercice global à grande échelle.

Le cas échéant, l'ENISA contribue également à des exercices de cybersécurité sectoriels, qu'elle aide à organiser, en collaboration avec des organisations compétentes qui peuvent participer également à des exercices de cybersécurité à l'échelle de l'Union.

6. L'ENISA prépare à intervalles réguliers, en coopération étroite avec les États membres, un rapport approfondi de situation technique en matière de cybersécurité de l'Union européenne sur les incidents et cybermenaces dans l'Union, sur la base d'informations publiquement disponibles, de ses propres analyses et des rapports que lui communiquent notamment les CSIRT des États membres ou les points de contact uniques institués par la directive (UE) 2016/1148, sur une base volontaire dans les deux cas, l'EC3 et la CERT-UE.

7. L'ENISA contribue à l'élaboration d'une réaction concertée au niveau de l'Union et des États membres en cas d'incidents ou de crises transfrontières de cybersécurité majeurs, principalement:

a) en agrégeant et en analysant des rapports provenant de sources nationales qui sont dans le domaine public ou qui sont partagés sur une base volontaire en vue de contribuer à former une appréciation commune de la situation;

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

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

d) en soutenant les institutions, organes et organismes de l'Union et, à leur demande, les États membres dans la communication publique relative à tels incidents ou crises;

e) en mettant à l'épreuve les plans de coopération destinés à réagir à de tels incidents ou crises au niveau de l'Union et en aidant les États membres, à leur demande, à mettre de tels plans à l'épreuve au niveau national.

Article 8

Marché, certification de cybersécurité et normalisation

1. L'ENISA soutient et favorise l'élaboration et la mise en œuvre de la politique de l'Union en matière de certification de cybersécurité des produits TIC, services TIC et processus TIC, telle qu'elle est établie au titre III du présent règlement:

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

b) en préparant des schémas européens de certification de cybersécurité candidats (ci-après dénommés «schémas candidats») pour des produits TIC, services TIC et processus TIC, conformément à l'article 49;

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

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

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

2. L'ENISA assure le secrétariat du groupe des parties prenantes pour la certification de cybersécurité, conformément à l'article 22, paragraphe 4.

3. L'ENISA compile et publie des lignes directrices et met au point des bonnes pratiques en ce qui concerne les exigences de cybersécurité de produits TIC, services TIC et processus TIC, en coopération avec les autorités nationales de certification de cybersécurité et les entreprises du secteur d'une façon formelle, structurée et transparente.

4. L'ENISA contribue à un renforcement des capacités en matière de processus d'évaluation et de certification, en compilant et en délivrant des lignes directrices ainsi qu'en fournissant un soutien aux États membres, à leur demande.

5. L'ENISA facilite l'établissement et l'adoption de normes européennes et internationales en matière de gestion des risques et de sécurité des produits TIC, services TIC et processus TIC.

6. L'ENISA formule, en collaboration avec les États membres et les entreprises du secteur, des avis et des lignes directrices concernant les domaines techniques liés aux exigences de sécurité qui s'imposent aux opérateurs de services essentiels et aux fournisseurs de services numériques, et concernant les normes existantes, y compris les normes nationales des États membres, en application de l'article 19, paragraphe 2, de la directive (UE) 2016/1148.

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

Article 9

Connaissance et information

L'ENISA:

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

b) produit des analyses stratégiques à long terme des cybermenaces et des incidents afin d'identifier les tendances émergentes et de contribuer à prévenir les incidents;

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

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

e) collecte et analyse des informations du domaine public sur les incidents importants, et rédige des rapports en vue de fournir des orientations aux citoyens, organisations et entreprises dans toute l'Union.

Article 10

Sensibilisation et éducation

L'ENISA:

a) sensibilise le public aux risques liés à la cybersécurité et fournit, à l'intention des citoyens, des organisations et des entreprises, des orientations sur les bonnes pratiques à adopter par les utilisateurs individuels, y compris en matière d'hygiène informatique et d'habileté numérique;

b) en coopération avec les États membres, ainsi que les institutions, organes et organismes de l'Union et les entreprises du secteur, organise à intervalles réguliers des campagnes d'information afin de renforcer la cybersécurité et d'en accroître la visibilité dans l'Union, et encourage un large débat public;

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

d) encourage une coordination plus étroite et l'échange de meilleures pratiques entre les États membres en matière de sensibilisation et d'éducation à la cybersécurité.

Article 11

Recherche et innovation

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

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

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

c) contribue au programme stratégique de recherche et d'innovation au niveau de l'Union dans le domaine de la cybersécurité.

Article 12

Coopération internationale

L'ENISA contribue aux efforts de l'Union pour coopérer avec les pays tiers et les organisations internationales, ainsi qu'au sein des cadres internationaux de coopération pertinents, afin de promouvoir une coopération internationale sur les problèmes de cybersécurité:

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

b) à la demande de la Commission, en facilitant l'échange de meilleures pratiques;

c) à la demande de la Commission, en lui faisant bénéficier de ses compétences;

d) en fournissant des conseils et un soutien à la Commission sur les questions relatives aux accords de reconnaissance mutuelle des certificats de cybersécurité avec des pays tiers, en collaboration avec le GECC institué en vertu de l'article 62.

CHAPITRE III

Organisation de l'ENISA

Article 13

Structure de l'ENISA

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

a) un conseil d'administration;

b) un conseil exécutif;

c) un directeur exécutif;

d) un groupe consultatif de l'ENISA;

e) un réseau des agents de liaison nationaux.

Section 1

Conseil d'administration

Article 14

Composition du conseil d'administration

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

2. Chaque membre du conseil d'administration dispose d'un suppléant. Ce suppléant représente le membre en son absence.

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

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

Article 15

Fonctions du conseil d'administration

1. Le conseil d'administration:

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

b) adopte le projet de document unique de programmation de l'ENISA visé à l'article 24, avant de le soumettre pour avis à la Commission;

c) adopte le document unique de programmation de l'ENISA, en tenant compte de l'avis de la Commission;

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

e) adopte le budget annuel de l'ENISA et exerce d'autres fonctions en ce qui concerne le budget de l'ENISA conformément au chapitre IV;

f) évalue et adopte le rapport annuel consolidé sur les activités de l'ENISA, y compris les comptes et une description de la manière dont l'ENISA a atteint ses indicateurs de performance, et transmet, au plus tard le 1er juillet de l'année suivante, le rapport annuel et l'évaluation de ce rapport au Parlement européen, au Conseil, à la Commission et à la Cour des comptes; elle publie le rapport annuel;

g) adopte les règles financières applicables à l'ENISA, conformément à l'article 32;

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

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

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

k) adopte son règlement intérieur, y compris les règles relatives aux décisions provisoires sur la délégation de tâches spécifiques, en vertu de l'article 19, paragraphe 7;

l) exerce, à l'égard du personnel de l'ENISA, les compétences qui sont dévolues par le statut des fonctionnaires de l'Union européenne (ci-après dénommé «statut des fonctionnaires») et le régime applicable aux autres agents de l'Union européenne (ci-après dénommé «régime applicable aux autres agents»), fixés par le règlement (CEE, Euratom, CECA) no 259/68 du Conseil ([24]), à l'autorité investie du pouvoir de nomination et à l'autorité habilitée à conclure les contrats d'engagement (ci-après dénommées «compétences de l'autorité investie du pouvoir de nomination») conformément au paragraphe 2 du présent article;

m) arrête les règles d'exécution du statut des fonctionnaires et du régime applicable aux autres agents conformément à la procédure prévue à l'article 110 du statut des fonctionnaires;

n) nomme le directeur exécutif et, le cas échéant, proroge son mandat ou le démet de ses fonctions conformément à l'article 36;

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

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

q) autorise la conclusion d'arrangements de travail conformément à l'article 7;

r) autorise l'élaboration ou la conclusion d'arrangements de travail conformément à l'article 42.

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

([24]) JO L 56 du 4.3.1968, p. 1.

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

Article 16

Présidence du conseil d'administration

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

Article 17

Réunions du conseil d'administration

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

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

3. Le directeur exécutif participe aux réunions du conseil d'administration mais ne dispose pas du droit de vote.

4. Sur invitation du président, des membres du groupe consultatif de l'ENISA peuvent participer aux réunions du conseil d'administration, mais ne disposent pas du droit de vote.

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

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

Article 18

Règles de vote du conseil d'administration

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

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

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

4. Le président du conseil d'administration prend part au vote.

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

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

Section 2

Conseil exécutif

Article 19

Conseil exécutif

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

2. Le conseil exécutif:

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

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

c) sans préjudice des tâches du directeur exécutif énoncées à l'article 20, assiste et conseille le directeur exécutif dans la mise en œuvre des décisions du conseil d'administration relatives à des questions administratives et budgétaires, conformément à l'article 20.

3. Le conseil exécutif est composé de cinq membres. Les membres du conseil exécutif sont nommés parmi les membres du conseil d'administration. Un des membres est le président du conseil d'administration, qui peut également présider le conseil exécutif, et un autre membre est un des représentants de la Commission. Les nominations des membres du conseil exécutif visent à assurer une représentation hommes-femmes équilibrée au sein du conseil exécutif. Le directeur exécutif participe aux réunions du conseil exécutif, mais ne dispose pas du droit de vote.

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

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

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

7. Lorsque l'urgence le requiert, le conseil exécutif peut prendre certaines décisions provisoires au nom du conseil d'administration, en particulier sur des questions de gestion administrative, comme la suspension de la délégation des compétences dévolues à l'autorité investie du pouvoir de nomination, et sur des questions budgétaires. De telles décisions provisoires sont notifiées sans retard indu. Le conseil d'administration décide ensuite s'il approuve ou s'il rejette la décision provisoire trois mois au plus tard après la prise de décision. Le conseil exécutif ne prend pas de décisions au nom du conseil d'administration qui doivent être approuvées par une majorité des deux tiers des membres du conseil d'administration.

Section 3

Directeur exécutif

Article 20

Tâches du directeur exécutif

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

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

3. Le directeur exécutif est chargé:

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

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

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

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

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

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

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

h) de préparer le projet de règles financières applicables à l'ENISA visé à l'article 32;

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

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

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

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

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

n) d'exécuter les autres tâches qui sont assignées au directeur exécutif par le présent règlement.

4. En tant que de besoin et dans le cadre des objectifs et tâches de l'ENISA, le directeur exécutif peut créer des groupes de travail ad hoc composés d'experts, y compris des experts des autorités compétentes des États membres. Le directeur exécutif en informe le conseil d'administration au préalable. Les procédures concernant en particulier la composition des groupes de travail, la nomination par le directeur exécutif des experts qui composent les groupes de travail et le fonctionnement de ces groupes sont précisées dans les règles internes de fonctionnement de l'ENISA.

5. Lorsque cela s'avère nécessaire, à l'effet d'exécuter les tâches de l'ENISA de manière efficiente et efficace et sur la base d'une analyse coûts-bénéfices appropriée, le directeur exécutif peut décider d'établir un ou plusieurs bureaux locaux dans un ou plusieurs États membres. Avant de prendre une décision sur l'établissement d'un bureau local, le directeur exécutif demande l'avis des États membres concernés, notamment l'État membre dans lequel est situé le siège de l'ENISA, et obtient le consentement préalable de la Commission et du conseil d'administration. En cas de désaccord, au cours de la procédure de consultation, entre le directeur exécutif et les États membres concernés, la question est soumise au Conseil pour discussion. Les effectifs agrégés de l'ensemble des bureaux locaux sont maintenus au minimum et ne dépassent pas 40 % des effectifs totaux de l'ENISA en place dans l'État membre où se situe le siège de l'ENISA. Les effectifs de chaque bureau local ne dépassent pas 10 % des effectifs totaux de l'ENISA en place dans l'État membre où se situe le siège de l'ENISA.

La décision établissant un bureau local précise la portée des activités confiées à ce bureau local de manière à éviter des coûts inutiles et une duplication des fonctions administratives de l'ENISA.

Section 4

Groupe consultatif de l'ENISA, groupe des parties prenantes pour la certification de cybersécurité et réseau des agents de liaison nationaux

Article 21

Groupe consultatif de l'ENISA

1. Le conseil d'administration crée de manière transparente, sur proposition du directeur exécutif, le groupe consultatif de l'ENISA composé d'experts reconnus représentant les parties prenantes concernées, telles que les entreprises du secteur des TIC, les fournisseurs de réseaux ou de services de communications électroniques accessibles au public, les PME, les opérateurs de services essentiels, les organisations de consommateurs, les experts universitaires en matière de cybersécurité, les représentants des autorités compétentes qui ont fait l'objet d'une notification conformément à la directive (UE) 2018/1972, les organisations européennes de normalisation ainsi que les autorités chargées de l'application de la loi et les autorités de contrôle de la protection des données. Le conseil d'administration s'efforce d'assurer un équilibre approprié entre les hommes et les femmes et un équilibre géographique, ainsi qu'un équilibre entre les différents groupes de parties prenantes.

2. Les procédures applicables au groupe consultatif de l'ENISA, notamment en ce qui concerne sa composition, la proposition du directeur exécutif visée au paragraphe 1, le nombre de membres et leur nomination, ainsi que le fonctionnement du groupe consultatif de l'ENISA sont précisées dans les règles internes de fonctionnement de l'ENISA et sont rendues publiques.

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

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

5. Le groupe consultatif de l'ENISA conseille l'ENISA en ce qui concerne l'exécution des tâches de celle-ci, excepté l'application des dispositions du titre III du présent règlement. Il conseille en particulier le directeur exécutif pour ce qui est de l'élaboration d'une proposition de programme de travail annuel pour l'ENISA et de la communication à assurer avec les parties prenantes concernées sur les questions liées au programme de travail annuel.

6. Le groupe consultatif de l'ENISA informe régulièrement le conseil d'administration de ses activités.

Article 22

Groupe des parties prenantes pour la certification de cybersécurité

1. Il est établi un groupe des parties prenantes pour la certification de cybersécurité.

2. Le groupe des parties prenantes pour la certification de cybersécurité se compose de membres sélectionnés parmi des experts reconnus représentant les parties prenantes concernées. La Commission, à la suite d'un appel transparent et ouvert, sélectionne, sur la base d'une proposition de l'ENISA, les membres du groupe des parties prenantes pour la certification de cybersécurité en assurant un équilibre entre les différents groupes de parties prenantes ainsi qu'un équilibre approprié entre les hommes et les femmes et un équilibre géographique.

3. Le groupe des parties prenantes pour la certification de cybersécurité est chargé:

a) de conseiller la Commission sur des questions stratégiques relatives au cadre européen de certification de cybersécurité;

b) sur demande, de conseiller l'ENISA sur des questions générales et stratégiques concernant les tâches de l'ENISA relatives au marché, à la certification de cybersécurité et à la normalisation;

c) d'aider la Commission à préparer le programme de travail glissant de l'Union visé à l'article 47;

d) de rendre un avis sur le programme de travail glissant de l'Union conformément à l'article 47, paragraphe 4; et

e) en cas d'urgence, de donner un avis à la Commission et au GECC sur la nécessité de disposer de schémas de certification supplémentaires qui ne sont pas compris dans le programme de travail glissant de l'Union, comme indiqué aux articles 47 et 48.

4. Le groupe des parties prenantes pour la certification de cybersécurité est coprésidé par les représentants de la Commission et de l'ENISA, et son secrétariat est assuré par l'ENISA.

Article 23

Réseau des agents de liaison nationaux

1. Le conseil d'administration crée, sur proposition du directeur exécutif, un réseau des agents de liaison nationaux composé de représentants de tous les États membres (les agents de liaison nationaux). Chaque État membre nomme un représentant au sein du réseau des agents de liaison nationaux. Les réunions du réseau des agents de liaison nationaux peuvent se tenir dans différentes configurations d'experts.

2. Le réseau des agents de liaison nationaux facilite en particulier l'échange d'informations entre l'ENISA et les États membres et aide l'ENISA à faire connaître ses activités et à diffuser les résultats de ses travaux et ses recommandations auprès des parties prenantes concernées dans l'ensemble de l'Union.

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

4. Si les agents de liaison nationaux coopèrent étroitement avec les représentants du conseil d'administration de leurs États membres respectifs, le réseau des agents de liaison nationaux en lui-même ne doit pas dupliquer le travail du conseil d'administration ou d'autres instances de l'Union.

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

Section 5

Fonctionnement

Article 24

Document unique de programmation

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

2. Le directeur exécutif établit chaque année un projet de document unique de programmation contenant sa programmation annuelle et pluriannuelle, ainsi que la planification des ressources financières et humaines correspondantes, conformément à l'article 32 du règlement délégué (UE) n° 1271/2013 de la Commission ([25]), et tenant compte des lignes directrices fixées par la Commission.

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

4. Le document unique de programmation devient définitif après l'adoption définitive du budget général de l'Union et il est adapté en tant que de besoin.

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

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

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

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

8. La programmation des ressources est actualisée chaque année. La programmation stratégique est actualisée en tant que de besoin, notamment pour tenir compte, si nécessaire, des résultats de l'évaluation visée à l'article 67.

Article 25

Déclaration d'intérêts

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

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

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

Article 26

Transparence

1. L'ENISA exerce ses activités avec un niveau élevé de transparence et conformément à l'article 28.

2. L'ENISA veille à ce que le public et toute partie intéressée reçoivent une information appropriée, objective, fiable et facilement accessible, notamment en ce qui concerne le résultat de ses travaux. Elle rend également publiques les déclarations d'intérêt faites conformément à l'article 25.

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

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

Article 27

Confidentialité

1. Sans préjudice de l'article 28, l'ENISA ne divulgue pas à des tiers les informations qu'elle traite ou qu'elle reçoit et pour lesquelles une demande motivée de traitement confidentiel a été faite.

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

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

4. Si l'exécution des tâches de l'ENISA l'exige, le conseil d'administration décide d'autoriser l'ENISA à traiter des informations classifiées. Dans ce cas, l'ENISA, en accord avec les services de la Commission, adopte des règles de sécurité respectant les principes de sécurité énoncés dans les décisions (UE, Euratom) 2015/443 ([26]) et 2015/444 ([27]) de la Commission. Ces règles de sécurité comprennent des dispositions relatives à l'échange, au traitement et à l'archivage des informations classifiées.

Article 28

Accès aux documents

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

2. Le conseil d'administration adopte les modalités d'application du règlement (CE) n° 1049/2001 au plus tard le 28 décembre 2019.

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

CHAPITRE IV

Établissement et structure du budget de l'ENISA

Article 29

Établissement du budget de l'ENISA

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

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

3. Le conseil d'administration transmet, au plus tard le 31 janvier de chaque année, l'état prévisionnel, qui fait partie du projet de document unique de programmation, à la Commission et aux pays tiers avec lesquels l'Union a conclu des accords tels qu'ils sont visés à l'article 42, paragraphe 2.

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

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

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

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

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

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

Article 30

Structure du budget de l'ENISA

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

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

b) de recettes allouées à des postes de dépense spécifiques conformément à ses règles financières visées à l'article 32;

c) d'un financement de l'Union sous la forme de conventions de délégation ou de subventions ad hoc, conformément à ses règles financières visées à l'article 32 et aux dispositions des instruments pertinents appuyant les politiques de l'Union;

d) de contributions de pays tiers participant aux travaux de l'ENISA conformément à l'article 42;

e) de toute contribution volontaire des États membres en espèces ou en nature.

Les États membres qui apportent des contributions volontaires en vertu du premier alinéa, point e), ne peuvent prétendre à aucun droit ou service spécifique du fait de celles-ci.

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

Article 31

Exécution du budget de l'ENISA

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

2. 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.

3. Le comptable de l'ENISA transmet les comptes provisoires pour l'exercice (exercice N) au comptable de la Commission et à la Cour des comptes au plus tard le 1er mars de l'exercice suivant (exercice N + 1).

4. À la réception des observations formulées par la Cour des comptes sur les comptes provisoires de l'ENISA en vertu de l'article 246 du règlement (UE, Euratom) 2018/1046 du Parlement européen et du Conseil ([28]), le comptable de l'ENISA établit les comptes définitifs de l'ENISA sous sa propre responsabilité et les soumet au conseil d'administration pour avis.

5. Le conseil d'administration rend un avis sur les comptes définitifs de l'ENISA.

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

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

([28]) Règlement (UE, Euratom) 2018/1046 du Parlement européen et du Conseil du 18 juillet 2018 relatif aux règles financières applicables au budget général de l'Union, modifiant les règlements (UE) nº 1296/2013, (UE) nº 1301/2013, (UE) nº 1303/2013, (UE) nº 1304/2013, (UE) nº 1309/2013, (UE) nº 1316/2013, (UE) nº 223/2014, (UE) nº 283/2014 et la décision nº 541/2014/UE, et abrogeant le règlement (UE, Euratom) nº 966/2012 (JO L 193 du 30.7.2018, p. 1).

8. À la même date que celle de la transmission des comptes définitifs de l'ENISA, le comptable de l'ENISA transmet également à la Cour des comptes une lettre de déclaration concernant ces comptes définitifs, avec copie au comptable de la Commission.

9. Au plus tard le 15 novembre de l'année N + 1, le directeur exécutif publie les comptes définitifs de l'ENISA au *Journal officiel de l'Union européenne*.

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

11. Le directeur exécutif soumet au Parlement européen, à la demande de celui-ci, toute information nécessaire au bon déroulement de la procédure de décharge pour l'exercice budgétaire en question, conformément à l'article 261, paragraphe 3, du règlement (UE, Euratom) 2018/1046.

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

Article 32

Règles financières

Les règles financières applicables à l'ENISA sont arrêtées par le conseil d'administration, après consultation de la Commission. Elles ne peuvent s'écarter du règlement délégué (UE) nº 1271/2013 que si le fonctionnement de l'ENISA le nécessite spécifiquement et moyennant l'accord préalable de la Commission.

Article 33

Lutte contre la fraude

1. Afin de faciliter la lutte contre la fraude, la corruption et d'autres activités illégales au titre du règlement (UE, Euratom) nº 883/2013 du Parlement européen et du Conseil ([29]), l'ENISA adhère, au plus tard 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'Office européen de lutte antifraude (OLAF) ([30]). L'ENISA adopte les dispositions appropriées applicables à tout le personnel de l'ENISA, en utilisant le modèle figurant à l'annexe dudit accord.

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

3. L'OLAF peut effectuer des enquêtes, y compris des contrôles et vérifications sur place, conformément aux dispositions et procédures prévues par le règlement (UE, Euratom) nº 883/2013 et le règlement (Euratom, CE) nº 2185/96 du Conseil ([31]), en vue d'établir l'existence éventuelle d'une fraude, d'un acte de corruption ou de toute autre activité illégale portant atteinte aux intérêts financiers de l'Union, en lien avec une subvention ou un contrat financés par l'ENISA.

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

([29]) Règlement (UE, Euratom) nº 883/2013 du Parlement européen et du Conseil du 11 septembre 2013 relatif aux enquêtes effectuées par l'Office européen de lutte antifraude (OLAF) et abrogeant le règlement (CE) nº 1073/1999 du Parlement européen et du Conseil et le règlement (Euratom) nº 1074/1999 du Conseil (JO L 248 du 18.9.2013, p. 1).

([30]) JO L 136 du 31.5.1999, p. 15.

([31]) Règlement (Euratom, CE) nº 2185/96 du Conseil du 11 novembre 1996 relatif aux contrôles et vérifications sur place effectués par la Commission pour la protection des intérêts financiers des Communautés européennes contre les fraudes et autres irrégularités (JO L 292 du 15.11.1996, p. 2).

CHAPITRE V

Personnel

Article 34

Dispositions générales

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

Article 35

Privilèges et immunités

Le protocole n° 7 sur les privilèges et immunités de l'Union européenne, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, s'applique à l'ENISA ainsi qu'à son personnel.

Article 36

Directeur exécutif

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

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

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

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

5. Le mandat du directeur exécutif est de cinq ans. Au terme de cette période, la Commission procède à une évaluation du travail accompli par le directeur exécutif et des tâches et défis futurs de l'ENISA.

6. Le conseil d'administration statue sur la nomination, la prorogation du mandat et la révocation du directeur exécutif conformément à l'article 18, paragraphe 2.

7. Le conseil d'administration, sur proposition de la Commission tenant compte de l'évaluation visée au paragraphe 5, peut proroger une fois le mandat du directeur exécutif pour une durée de cinq ans.

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

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

10. Le directeur exécutif ne peut être démis de ses fonctions que sur décision du conseil d'administration, statuant sur proposition de la Commission.

Article 37

Experts nationaux détachés et personnel autre

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

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

CHAPITRE VI

Dispositions générales concernant l'ENISA

Article 38

Statut juridique de l'ENISA

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

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

3. L'ENISA est représentée par le directeur exécutif.

Article 39

Responsabilité de l'ENISA

1. La responsabilité contractuelle de l'ENISA est régie par le droit applicable au contrat en question.

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

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

4. La Cour de justice de l'Union européenne est compétente pour traiter de tout litige relatif à la réparation d'un dommage visé au paragraphe 3.

5. La responsabilité personnelle du personnel de l'ENISA envers l'ENISA est régie par les dispositions pertinentes applicables au personnel de l'ENISA.

Article 40

Régime linguistique

1. Le règlement n° 1 du Conseil ([32]) s'applique à l'ENISA. Les États membres et les autres organismes désignés par les États membres peuvent s'adresser à l'ENISA et recevoir une réponse dans la langue officielle des institutions de l'Union qu'ils choisissent.

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

Article 41

Protection des données à caractère personnel

1. Les opérations de traitement de données à caractère personnel effectuées par l'ENISA sont soumises au règlement (UE) 2018/1725.

2. Le conseil d'administration adopte les dispositions d'application visées à l'article 45, paragraphe 3, du règlement (UE) 2018/1725. Le conseil d'administration peut adopter des mesures supplémentaires nécessaires pour l'application du règlement (UE) 2018/1725 par l'ENISA.

([32]) Règlement n° 1 du Conseil portant fixation du régime linguistique de la Communauté économique européenne (JO 17 du 6.10.1958, p. 385/58).

Article 42

Coopération avec des pays tiers et des organisations internationales

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

2. L'ENISA est ouverte à la participation des pays tiers qui ont conclu des accords en ce sens avec l'Union. Conformément aux dispositions pertinentes de tels accords, des arrangements de travail sont élaborés pour préciser notamment la nature, l'étendue et les modalités de la participation de ces pays tiers aux travaux de l'ENISA, et contiennent des dispositions relatives à la participation aux initiatives prises par l'ENISA, aux contributions financières et au personnel. En ce qui concerne les questions relatives au personnel, lesdits arrangements de travail respectent le statut des fonctionnaires et le régime applicable aux autres agents.

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

Article 43

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

Après consultation de la Commission, l'ENISA adopte des règles de sécurité en appliquant les principes de sécurité énoncés dans les règles de sécurité de la Commission visant à protéger les informations sensibles non classifiées et les ICUE, énoncées dans les décisions (UE, Euratom) 2015/443 et (UE, Euratom) 2015/444. Les règles de sécurité de l'ENISA couvrent les dispositions relatives à l'échange, au traitement et au stockage de ces informations.

Article 44

Accord de siège et conditions de fonctionnement

1. Les dispositions requises pour l'implantation de l'ENISA dans l'État membre du siège et les prestations à fournir par cet État membre, ainsi que les règles particulières qui sont applicables dans ledit État membre au directeur exécutif, aux membres du conseil d'administration, au personnel de l'ENISA et aux membres de leurs familles sont arrêtées dans un accord de siège conclu entre l'ENISA et l'État membre du siège, après approbation par le conseil d'administration.

2. L'État membre du siège de l'ENISA offre les meilleures conditions possibles pour assurer le bon fonctionnement de l'ENISA, en tenant compte de l'accessibilité de l'emplacement, de l'existence de services d'éducation appropriés pour les enfants des membres du personnel et d'un accès adéquat au marché du travail, à la sécurité sociale et aux soins médicaux pour les enfants et les conjoints des membres du personnel.

Article 45

Contrôle administratif

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

TITRE III

CADRE DE CERTIFICATION DE CYBERSÉCURITÉ

Article 46

Cadre européen de certification de cybersécurité

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

2. Le cadre européen de certification de cybersécurité prévoit un mécanisme visant à établir des schémas européens de certification de cybersécurité et à attester que les produits TIC, services TIC et processus TIC qui ont été évalués conformément à ces schémas satisfont à des exigences de sécurité définies, dans le but de protéger la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou traitées ou des fonctions ou services qui sont offerts par ces produits, services et processus ou accessibles par leur intermédiaire tout au long de leur cycle de vie.

Article 47

Le programme de travail glissant de l'Union pour la certification européenne de cybersécurité

1. La Commission publie un programme de travail glissant de l'Union pour la certification européenne de cybersécurité (ci-après dénommé «programme de travail glissant de l'Union») qui recense les priorités stratégiques pour les futurs schémas européens de certification de cybersécurité.

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

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

a) la disponibilité et le développement de schémas nationaux de certification de cybersécurité couvrant toute catégorie spécifique de produits TIC, services TIC ou processus TIC et, en particulier, en ce qui concerne le risque de fragmentation;

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

c) la demande du marché;

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

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

4. La Commission tient dûment compte des avis du GECC et du groupe des parties prenantes pour la certification de cybersécurité sur le projet de programme de travail glissant de l'Union.

5. Le premier programme de travail glissant de l'Union est publié au plus tard le 28 juin 2020. Le programme de travail glissant de l'Union est mis à jour au moins tous les trois ans, et plus souvent si nécessaire.

Article 48

Demande de schéma européen de certification de cybersécurité

1. La Commission peut demander à l'ENISA de préparer un schéma candidat ou de réexaminer un schéma européen de certification de cybersécurité existant sur la base du programme de travail glissant de l'Union.

2. Dans des cas dûment justifiés, la Commission ou le GECC peut demander à l'ENISA de préparer un schéma candidat ou de réexaminer un schéma européen de certification de cybersécurité existant qui n'est pas inclus dans le programme de travail glissant de l'Union. Le programme de travail glissant de l'Union est mis à jour en conséquence.

Article 49

Préparation, adoption et réexamen d'un schéma européen de certification de cybersécurité

1. À la suite d'une demande formulée par la Commission en vertu de l'article 48, l'ENISA prépare un schéma candidat qui satisfait aux exigences énoncées aux articles 51, 52 et 54.

2. À la suite d'une demande formulée par le GECC en vertu de l'article 48, paragraphe 2, l'ENISA peut préparer un schéma candidat qui satisfait aux exigences énoncées aux articles 51, 52 et 54. Si l'ENISA rejette une telle demande, elle doit motiver son refus. Toute décision de rejeter une telle demande est prise par le conseil d'administration.

3. Lors de la préparation d'un schéma candidat, l'ENISA consulte toutes les parties prenantes concernées au moyen d'un processus de consultation formel, ouvert, transparent et inclusif.

4. Pour chaque schéma candidat, l'ENISA crée un groupe de travail ad hoc, conformément à l'article 20, paragraphe 4, afin qu'il lui fournisse des conseils et des compétences spécifiques.

5. L'ENISA coopère étroitement avec le GECC. Celui-ci fournit aide et expertise à l'ENISA dans le cadre de la préparation du schéma candidat et adopte un avis sur le schéma candidat.

6. L'ENISA tient le plus grand compte de l'avis du GECC avant de transmettre à la Commission le schéma candidat préparé conformément aux paragraphes 3, 4 et 5. L'avis du GECC n'est pas contraignant pour l'ENISA, et l'absence d'un tel avis n'empêche pas l'ENISA de transmettre le schéma candidat à la Commission.

7. La Commission, se fondant sur le schéma candidat préparé par l'ENISA, peut adopter des actes d'exécution prévoyant un schéma européen de certification de cybersécurité pour les produits TIC, services TIC et processus TIC qui satisfont aux exigences des articles 51, 52 et 54. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 66, paragraphe 2.

8. L'ENISA procède au moins tous les cinq ans à une évaluation de chacun des schémas européens de certification de cybersécurité adoptés, en tenant compte des informations reçues en retour des parties intéressées. Si nécessaire, la Commission ou le GECC peut demander à l'ENISA de lancer le processus d'élaboration d'un schéma candidat révisé, conformément à l'article 48 et au présent article.

Article 50

Site internet sur les schémas européens de certification de cybersécurité

1. L'ENISA tient à jour un site internet dédié qui fournit des informations sur les schémas européens de certification de cybersécurité, les certificats de cybersécurité européens et les déclarations de conformité de l'Union européenne, et leur assure une publicité, y compris des informations relatives aux schémas européens de certification de cybersécurité qui ne sont plus valables, aux certificats de cybersécurité européens qui ont été retirés ou ont expiré et aux déclarations de conformité de l'Union européenne, ainsi qu'au répertoire de liens vers des informations relatives à la cybersécurité fournies conformément à l'article 55.

2. Le cas échéant, le site internet visé au paragraphe 1 indique également les schémas nationaux de certification de cybersécurité qui ont été remplacés par un schéma européen de certification de cybersécurité.

Article 51

Objectifs de sécurité des schémas européens de certification de cybersécurité

Un schéma européen de certification de cybersécurité est conçu de façon à réaliser, selon le cas, au moins les objectifs de sécurité suivants:

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

b) protéger les données stockées, transmises ou traitées de toute autre façon contre la destruction accidentelle ou non autorisée, la perte ou l'altération, ou l'absence de disponibilité, au cours de l'ensemble du cycle de vie du produit TIC, service TIC ou processus TIC;

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

d) identifier et documenter les dépendances et vulnérabilités connues;

e) garder une trace des données, fonctions ou services qui ont été consultés, utilisés ou traités de toute autre façon, du moment où ils l'ont été et par qui;

f) faire en sorte qu'il soit possible de vérifier quels données, services ou fonctions ont été consultés, utilisés ou traités de toute autre façon, à quel moment et par qui;

g) vérifier que les produits TIC, services TIC et processus TIC ne contiennent pas de vulnérabilités connues;

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

i) faire en sorte que les produits TIC, services TIC et processus TIC soient sécurisés par défaut et dès la conception;

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

Article 52

Niveaux d'assurance des schémas européens de certification de cybersécurité

1. Un schéma européen de certification de cybersécurité peut préciser un ou plusieurs des niveaux d'assurance suivants pour les produits TIC, services TIC et processus TIC: «élémentaire», «substantiel» ou «élevé». Le niveau d'assurance correspond au niveau de risque associé à l'utilisation prévue du produit TIC, service TIC ou processus TIC, en termes de probabilité et de répercussions d'un incident.

2. Les certificats de cybersécurité européens et les déclarations de conformité de l'Union européenne mentionnent tout niveau d'assurance précisé dans le schéma européen de certification de cybersécurité dans le cadre duquel le certificat de cybersécurité européen ou la déclaration de conformité de l'Union européenne a été délivré(e).

3. Les exigences de sécurité correspondant à chaque niveau d'assurance sont fournies dans le schéma européen de certification de cybersécurité concerné, y compris les fonctionnalités de sécurité correspondantes ainsi que la rigueur et l'ampleur correspondantes de l'évaluation à laquelle le produit TIC, service TIC ou processus TIC doit être soumis.

4. Le certificat ou la déclaration de conformité de l'Union européenne fait référence aux spécifications techniques, aux normes et aux procédures connexes, y compris les contrôles techniques, l'objectif étant de réduire le risque d'incidents de cybersécurité ou de les prévenir.

5. Un certificat de cybersécurité européen ou une déclaration de conformité de l'Union européenne qui se réfère au niveau d'assurance dit «élémentaire» offre l'assurance que les produits TIC, services TIC et processus TIC pour lesquels ce certificatif ou cette déclaration de conformité de l'Union européenne est délivré(e) satisfont aux exigences de sécurité correspondantes, y compris les fonctionnalités de sécurité, et qu'ils ont été évalués à un niveau qui vise à minimiser les risques élémentaires connus d'incidents et de cyberattaques. Les activités d'évaluation à entreprendre comprennent au moins un examen de la documentation technique. Lorsqu'un tel examen n'est pas approprié, des activités d'évaluation de substitution ayant un effet équivalent sont entreprises.

6. Un certificat de cybersécurité européen qui se réfère au niveau d'assurance dit «substantiel» offre l'assurance que les produits TIC, services TIC et processus TIC pour lesquels ce certificat est délivré satisfont aux exigences de sécurité correspondantes, y compris des fonctionnalités de sécurité, et qu'ils ont été évalués à un niveau qui vise à minimiser les risques liés à la cybersécurité connus, et le risque d'incidents et de cyberattaques émanant d'acteurs aux aptitudes et aux ressources limitées. Les activités d'évaluation à entreprendre comprennent au moins: un examen visant à démontrer l'absence de vulnérabilités connues du public et des vérifications tendant à démontrer que les produits TIC, services TIC ou processus TIC mettent correctement en œuvre les fonctionnalités de sécurité nécessaires. Lorsque de telles activités d'évaluation ne sont pas appropriées, des activités d'évaluation de substitution ayant un effet équivalent sont entreprises.

7. Un certificat de cybersécurité européen qui se réfère au niveau d'assurance dit «élevé» offre l'assurance que les produits TIC, services TIC et processus TIC pour lesquels ce certificat est délivré satisfont aux exigences de sécurité correspondantes, y compris des fonctionnalités de sécurité, et qu'ils ont été évalués à un niveau qui vise à minimiser le risque que des cyberattaques de pointe soient menées par des acteurs aux aptitudes solides et aux ressources importantes. Les activités d'évaluation à entreprendre comprennent au moins: un examen démontrant l'absence de vulnérabilités connues du public, des vérifications tendant à démontrer que les produits TIC, services TIC ou processus TIC mettent correctement en œuvre les fonctionnalités de sécurité nécessaires, au niveau de l'état de l'art; et une évaluation de leur résistance à des attaques menées par des acteurs compétents, au moyen de tests de pénétration. Lorsque de telles activités d'évaluation ne sont pas appropriées, des activités d'évaluation de substitution ayant un effet équivalent sont entreprises.

8. Un schéma européen de certification de cybersécurité peut préciser plusieurs niveaux d'évaluation en fonction de la rigueur et de l'ampleur de la méthode d'évaluation utilisée. Chaque niveau d'évaluation correspond à l'un des niveaux d'assurance et il est défini par une combinaison appropriée de composantes d'assurance.

Article 53

Autoévaluation de la conformité

1. Un schéma européen de certification de cybersécurité peut permettre la réalisation d'une autoévaluation de la conformité sous la seule responsabilité du fabricant ou du fournisseur de produits TIC, services TIC ou processus TIC. L'autoévaluation de la conformité n'est autorisée que pour les produits TIC, services TIC et processus TIC qui présentent un risque faible schéma correspondant au niveau d'assurance dit «élémentaire».

2. Le fabricant ou le fournisseur de produits TIC, services TIC ou processus TIC peut délivrer une déclaration de conformité de l'Union européenne indiquant que le respect des exigences énoncées dans le schéma a été démontré. En délivrant une telle déclaration, le fabricant ou fournisseur de produits TIC, services TIC ou processus TIC assume la responsabilité du respect par le produit TIC, service TIC ou processus TIC des exigences fixées dans ce schéma.

3. Le fabricant ou fournisseur de produits TIC, services TIC ou processus TIC garde à la disposition de l'autorité nationale de certification de cybersécurité visée à l'article 58 la déclaration de conformité de l'Union européenne, la documentation technique et toutes les autres informations pertinentes relatives à la conformité des produits TIC ou services TIC avec le schéma pendant la durée prévue dans le schéma européen de certification de cybersécurité correspondant. Une copie de la déclaration de conformité de l'Union européenne est transmise à l'autorité nationale de certification de cybersécurité et à l'ENISA.

4. La délivrance d'une déclaration de conformité de l'Union européenne est volontaire, sauf disposition contraire du droit de l'Union ou du droit d'un État membre.

5. Les déclarations de conformité de l'Union européenne sont reconnues dans tous les États membres.

Article 54

Éléments des schémas européens de certification de cybersécurité

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

a) l'objet et le champ d'application du schéma de certification, notamment le type ou les catégories de produits TIC, services TIC et processus TIC couverts;

b) une description claire de la finalité du schéma et de la façon dont les normes, les méthodes d'évaluation et les niveaux d'assurance sélectionnés correspondent aux besoins des utilisateurs auxquels le schéma est destiné;

c) des références aux normes internationales, européennes ou nationales appliquées dans le cadre de l'évaluation ou, lorsque de telles normes n'existent pas ou ne sont pas appropriées, à des spécifications techniques qui satisfont aux exigences énoncées à l'annexe II du règlement (UE) n° 1025/2012 ou, lorsque de telles spécifications ne sont pas disponibles, à des spécifications techniques ou d'autres exigences de cybersécurité définies dans le schéma européen de certification de cybersécurité;

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

e) une mention indiquant si l'autoévaluation de la conformité est autorisée dans le cadre du schéma;

f) le cas échéant, des exigences spécifiques ou supplémentaires auxquelles sont soumis les organismes d'évaluation de la conformité aux fins de garantir qu'ils disposent des compétences techniques nécessaires pour évaluer les exigences de cybersécurité;

g) les critères et méthodes d'évaluation spécifiques qui doivent être utilisés, notamment les types d'évaluation, afin de démontrer que les objectifs de sécurité visés à l'article 51 sont atteints;

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

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

j) les règles relatives au contrôle du respect par les produits TIC, services TIC et processus TIC des exigences liées aux certificats de cybersécurité européens ou aux déclarations de conformité de l'Union européenne, notamment les mécanismes permettant de démontrer le respect constant des exigences de cybersécurité qui ont été définies;

k) le cas échéant, les conditions permettant de délivrer, de maintenir, de prolonger et de renouveler les certificats européen de cybersécurité, ainsi que les conditions auxquelles il est possible d'étendre ou de réduire leur champ d'application;

l) les règles relatives aux conséquences pour les produits TIC, services TIC et processus TIC qui ont été certifiés ou pour lesquels une déclaration de conformité de l'Union européenne a été délivrée, mais qui ne respectent pas les exigences du schéma;

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

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

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

p) le contenu et le format des certificats de cybersécurité européens et des déclarations de conformité de l'Union européenne à délivrer;

q) la période de disponibilité de la déclaration de conformité de l'Union européenne, de la documentation technique et de toutes les autres informations pertinentes qui doivent être mises à disposition par le fabricant ou le fournisseur de produits TIC, services TIC ou processus TIC;

r) la durée maximale de validité des certificats de cybersécurité européens délivrés dans le cadre du schéma;

s) la politique de divulgation concernant les certificats de cybersécurité européens délivrés, modifiés ou retirés dans le cadre du schéma;

t) les conditions de reconnaissance mutuelle des schémas de certification avec les pays tiers;

u) le cas échéant, les règles relatives à tout mécanisme d'évaluation par les pairs établi par le schéma pour les autorités ou organismes qui délivrent des certificats de cybersécurité européens pour le niveau d'assurance dit «élevé» en vertu de l'article 56, paragraphe 6. Un tel mécanisme est sans préjudice de l'examen par les pairs prévu à l'article 59;

v) le format et les procédures que les fabricants ou les fournisseurs de produits TIC, services TIC ou processus TIC doivent appliquer pour fournir et mettre à jour les informations supplémentaires en matière de cybersécurité conformément à l'article 55.

2. Les exigences du schéma européen de certification de cybersécurité qui ont été définies sont cohérentes avec toute exigence légale applicable, notamment les exigences découlant de dispositions harmonisées du droit de l'Union.

3. Lorsqu'un acte juridique spécifique de l'Union le prévoit, un certificat ou une déclaration de conformité de l'Union européenne délivré(e) dans le cadre d'un schéma européen de certification de cybersécurité peut être utilisé(e) pour démontrer la présomption de conformité aux exigences de cet acte juridique.

4. En l'absence de dispositions harmonisées du droit de l'Union, le droit d'un État membre peut aussi prévoir qu'un schéma européen de certification de cybersécurité peut être utilisé pour établir la présomption de conformité aux exigences légales.

Article 55

Informations supplémentaires en matière de cybersécurité pour les produits TIC, services TIC et processus TIC certifiés

1. Le fabricant ou le fournisseur de produits TIC, services TIC ou processus TIC certifiés ou de produits TIC, services TIC et processus TIC pour lesquels une déclaration de conformité de l'Union européenne a été délivrée met les informations supplémentaires en matière de cybersécurité qui suivent à la disposition du public:

a) des orientations et des recommandations pour aider les utilisateurs finaux à assurer, de façon sécurisée, la configuration, l'installation, le déploiement, le fonctionnement et la maintenance des produits TIC ou services TIC;

b) la période pendant laquelle une assistance en matière de sécurité sera offerte aux utilisateurs finaux, en particulier en ce qui concerne la disponibilité de mises à jour liées à la cybersécurité;

c) les informations de contact du fabricant ou du fournisseur et les méthodes acceptées pour recevoir des informations concernant des vulnérabilités de la part d'utilisateurs finaux et de chercheurs dans le domaine de la sécurité;

d) une mention relative aux répertoires en ligne recensant les vulnérabilités publiquement divulguées liées au produit TIC, service TIC ou processus TIC ainsi que tout conseil pertinent en matière de cybersécurité.

2. Les informations visées au paragraphe 1 sont disponibles sous forme électronique et restent disponibles et actualisées en tant que de besoin au moins jusqu'à l'expiration du certificat de cybersécurité européen ou de la déclaration de conformité de l'Union européenne correspondant(e).

Article 56

Certification de cybersécurité

1. Les produits TIC, services TIC et processus TIC qui ont été certifiés dans le cadre d'un schéma européen de certification de cybersécurité adopté en vertu de l'article 49 sont présumés respecter les exigences de ce schéma.

2. La certification de cybersécurité est volontaire, sauf disposition contraire du droit de l'Union ou du droit d'un État membre.

3. La Commission évalue régulièrement l'efficacité et l'utilisation des schémas européens de certification de cybersécurité adoptés ainsi que la question de savoir si un schéma européen de certification de cybersécurité spécifique doit être rendu obligatoire, au moyen de dispositions pertinentes du droit de l'Union, pour garantir un niveau adéquat de cybersécurité des produits TIC, services TIC et processus TIC dans l'Union et améliorer le fonctionnement du marché intérieur. La première de ces évaluations est effectuée le 31 décembre 2023 au plus tard, et les évaluations suivantes sont effectuées au moins tous les deux ans par la suite. Sur la base des résultats de ces évaluations, la Commission recense les produits TIC, services TIC et processus TIC couverts par un schéma de certification existant qui doivent relever d'un schéma de certification obligatoire.

La Commission met l'accent en priorité sur les secteurs dont la liste figure à l'annexe II de la directive (UE) 2016/1148 qui sont évalués au plus tard deux ans après l'adoption du premier schéma européen de certification de cybersécurité.

Lorsqu'elle prépare l'évaluation, la Commission:

a) tient compte de l'incidence des mesures, du point de vue des coûts, sur les fabricants ou fournisseurs de ces produits TIC, services TIC ou processus TIC et sur les utilisateurs, ainsi que des avantages sociétaux ou économiques résultant du renforcement escompté du niveau de sécurité des produits TIC, services TIC ou processus TIC ciblés;

b) tient compte de l'existence et de la mise en œuvre du droit des États membres et des pays tiers concernés;

c) engage un processus de consultation ouvert, transparent et inclusif avec toutes les parties prenantes concernées et les États membres;

d) prend en considération les délais de mise en œuvre ainsi que les mesures et périodes transitoires, en ce qui concerne, en particulier, l'incidence éventuelle de la mesure sur les fabricants ou les fournisseurs de produits TIC, services TIC ou processus TIC, y compris les PME;

e) propose la façon la plus rapide et la plus efficace de mettre en œuvre la transition des schémas de certification volontaires vers les schémas de certification obligatoires.

4. Les organismes d'évaluation de la conformité visés à l'article 60 délivrent des certificats de cybersécurité européens au titre du présent article attestant du niveau d'assurance dit «élémentaire» ou «substantiel» sur la base des critères figurant dans le schéma européen de certification de cybersécurité adopté par la Commission conformément à l'article 49.

5. Par dérogation au paragraphe 4, dans des cas dûment justifiés, un schéma européen de certification de cybersécurité peut prévoir que seul un organisme public peut délivrer des certificats de cybersécurité européens dans le cadre dudit schéma. Cet organisme est l'une des entités suivantes:

a) une autorité nationale de certification de cybersécurité visée à l'article 58, paragraphe 1; ou

b) un organisme public accrédité en tant qu'organisme d'évaluation de la conformité conformément à l'article 60, paragraphe 1.

6. Lorsqu'un schéma européen de certification de cybersécurité adopté au titre de l'article 49 exige un niveau d'assurance dit «élevé», le certificat de cybersécurité européen dans le cadre de ce schéma ne doit être délivré que par une autorité nationale de certification de cybersécurité ou, dans les cas suivants, par un organisme d'évaluation de la conformité:

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

b) sur la base d'une délégation préalable de la tâche consistant à délivrer de tels certificats de cybersécurité européens à un organisme d'évaluation de la conformité par l'autorité nationale de certification de cybersécurité.

7. La personne physique ou morale qui soumet des produits TIC, services TIC ou processus TIC à la certification met à la disposition de l'autorité nationale de certification de cybersécurité visée à l'article 58, lorsque cette autorité est l'organisme délivrant le certificat de cybersécurité européen, ou de l'organisme d'évaluation de la conformité visé à l'article 60 toutes les informations nécessaires pour procéder à la certification.

8. Le titulaire d'un certificat de cybersécurité européen informe l'autorité ou l'organisme visé au paragraphe 7 de toute vulnérabilité ou irrégularité détectée ultérieurement concernant la sécurité du produit TIC, service TIC ou processus TIC certifié susceptible d'avoir une incidence sur son respect des exigences liées à la certification. Cette autorité ou cet organisme transmet ces informations sans retard injustifié à l'autorité nationale de certification de cybersécurité concernée.

9. Un certificat de cybersécurité européen est délivré pour la durée prévue par le schéma européen de certification de cybersécurité concerné et peut être renouvelé, pourvu que les exigences applicables continuent d'être satisfaites.

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

Article 57

Schémas nationaux de certification de cybersécurité et certificats

1. Sans préjudice du paragraphe 3 du présent article, les schémas nationaux de certification de cybersécurité et les procédures connexes pour les produits TIC, services TIC et processus TIC couverts par un schéma européen de certification de cybersécurité cessent de produire leurs effets à partir de la date fixée dans l'acte d'exécution adopté en application de l'article 49, paragraphe 7. Les schémas nationaux de certification de cybersécurité et les procédures connexes pour les produits TIC, services TIC et processus TIC qui ne sont pas couverts par un schéma européen de certification de cybersécurité continuent à exister.

2. Les États membres s'abstiennent d'instaurer de nouveaux schémas nationaux de certification de cybersécurité pour les produits TIC, services TIC et processus TIC qui sont déjà couverts par un schéma européen de certification de cybersécurité en vigueur.

3. Les certificats existants, qui ont été délivrés dans le cadre de schémas nationaux de certification de cybersécurité et qui sont couverts par un schéma européen de certification de cybersécurité, restent valables jusqu'à leur date d'expiration.

4. En vue d'éviter la fragmentation du marché intérieur, les États membres informent la Commission et le GECC de leur intention éventuelle d'élaborer de nouveaux schémas nationaux de certification de cybersécurité.

Article 58

Autorités nationales de certification de cybersécurité

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

2. Chaque État membre informe la Commission de l'identité des autorités nationales de certification de cybersécurité désignées. Lorsqu'un État membre désigne plus d'une autorité, il communique en outre à la Commission des informations sur les tâches confiées à chacune de ces autorités.

3. Sans préjudice de l'article 56, paragraphe 5, point a), et de l'article 56, paragraphe 6, chaque autorité nationale de certification de cybersécurité est indépendante des entités qu'elle surveille en ce qui concerne son organisation, ses décisions de financement, sa structure juridique et son processus décisionnel.

4. Les États membres veillent à ce que les activités des autorités nationales de certification de cybersécurité liées à la délivrance de certificats de cybersécurité européens visées à l'article 56, paragraphe 5, point a), et à l'article 56, paragraphe 6, soient strictement distinctes de leurs activités de supervision visées au présent article, et à ce que ces activités soient exécutées indépendamment l'une de l'autre.

5. Les États membres veillent à ce que les autorités nationales de certification de cybersécurité disposent de ressources adéquates pour exercer leurs pouvoirs et exécuter leurs tâches de manière efficace et efficiente.

6. Afin d'assurer la mise en œuvre efficace du présent règlement, il convient que les autorités nationales de certification de cybersécurité participent de manière active, efficace, efficiente et sécurisée au GECC.

7. Les autorités nationales de certification de cybersécurité:

a) supervisent et font respecter les règles prévues dans les schémas européens de certification de cybersécurité, en application de l'article 54, paragraphe 1, point j), aux fins du contrôle du respect par les produits TIC, services TIC et processus TIC des exigences des certificats de cybersécurité européens délivrés sur leurs territoires respectifs, en coopération avec les autres autorités compétentes de surveillance du marché;

b) contrôlent le respect des obligations qui incombent aux fabricants ou fournisseurs de produits TIC, services TIC ou processus TIC qui sont établis sur leurs territoires respectifs et qui procèdent à une autoévaluation de conformité et font respecter ces obligations, et contrôlent, en particulier, le respect des obligations de ces fabricants ou fournisseurs visées à l'article 53, paragraphes 2 et 3, et dans le schéma européen de certification de cybersécurité correspondant, et font respecter ces obligations;

c) sans préjudice de l'article 60, paragraphe 3, assistent et soutiennent activement les organismes nationaux d'accréditation dans le contrôle et la supervision des activités des organismes d'évaluation de la conformité aux fins du présent règlement;

d) contrôlent et supervisent les activités des organismes publics visées à l'article 56, paragraphe 5;

e) lorsqu'il y a lieu, autorisent les organismes d'évaluation de la conformité à effectuer leurs tâches conformément à l'article 60, paragraphe 3, et limitent, suspendent ou retirent les autorisations existantes lorsque les organismes d'évaluation de la conformité violent les exigences du présent règlement;

f) traitent les réclamations introduites par des personnes physiques ou morales en rapport avec les certificats de cybersécurité européens délivrés par des autorités nationales de certification de cybersécurité ou en rapport avec les certificats de cybersécurité européens délivrés par des organismes d'évaluation de la conformité conformément à l'article 56, paragraphe 6, ou en rapport avec les déclarations de conformité de l'Union européenne délivrées au titre de l'article 53, examinent l'objet de ces réclamations dans la mesure nécessaire et informent l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable;

g) communiquent à l'ENISA et au GECC un résumé annuel des activités entreprises en application des points b), c) et d) du présent paragraphe ou du paragraphe 8;

h) coopèrent avec les autres autorités nationales de certification de cybersécurité ou d'autres autorités publiques, notamment en partageant des informations sur l'éventuel non-respect par des produits TIC, services TIC et processus TIC des exigences du présent règlement ou des exigences de schémas de certification de cybersécurité spécifiques; et

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

8. Chaque autorité nationale de certification de cybersécurité dispose au moins des pouvoirs suivants:

a) de demander aux organismes d'évaluation de la conformité, aux titulaires de certificats de cybersécurité européens et aux émetteurs de déclarations de conformité de l'Union européenne de lui communiquer toute information dont elle a besoin pour l'exécution de ses tâches;

b) d'effectuer des enquêtes, sous la forme d'audits, auprès des organismes d'évaluation de la conformité, des titulaires de certificats de cybersécurité européens et des émetteurs de déclarations de conformité de l'Union européenne afin de vérifier qu'ils respectent le présent titre;

c) de prendre les mesures appropriées, conformément au droit national, pour veiller à ce que les organismes d'évaluation de la conformité, les titulaires de certificats de cybersécurité européens et les émetteurs de déclarations de conformité de l'Union européenne respectent le présent règlement ou un schéma européen de certification de cybersécurité;

d) d'obtenir l'accès aux locaux des organismes d'évaluation de la conformité ou des titulaires de certificats de cybersécurité européens afin d'effectuer des enquêtes conformément au droit procédural de l'Union ou au droit procédural d'un État membre;

e) de retirer, conformément au droit national, les certificats de cybersécurité européens délivrés par les autorités nationales de certification de cybersécurité ou les certificats de cybersécurité européens délivrés par les organismes d'évaluation de la conformité conformément à l'article 56, paragraphe 6, lorsque de tels certificats ne respectent pas le présent règlement ou un schéma européen de certification de cybersécurité;

f) d'imposer des sanctions conformément au droit national, comme le prévoit l'article 65, et d'exiger la cessation immédiate des violations des obligations énoncées dans le présent règlement.

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

Article 59

Examen par les pairs

1. Dans un souci d'équivalence des normes, dans l'ensemble de l'Union, en ce qui concerne les certificats de cybersécurité européens et les déclarations de conformité de l'Union européenne, les autorités nationales de certification de cybersécurité font l'objet d'un examen par les pairs.

2. L'examen par les pairs est effectué selon des critères et des procédures d'évaluation cohérents et transparents, en particulier en ce qui concerne les exigences structurelles et celles relatives aux ressources humaines et aux processus, ainsi que la confidentialité et les plaintes.

3. L'examen par les pairs évalue:

a) lorsqu'il y a lieu, la question de savoir si les activités des autorités nationales de certification de cybersécurité liées à la délivrance de certificats de cybersécurité européens visées à l'article 56, paragraphe 5, point a), et à l'article 56, paragraphe 6, sont strictement distinctes des activités de supervision visées à l'article 58, et celle de savoir si ces activités sont exercées indépendamment l'une de l'autre;

b) les procédures permettant de superviser et de faire respecter les règles relatives au contrôle du respect par les produits TIC, services TIC et processus TIC des certificats de cybersécurité européens, conformément à l'article 58, paragraphe 7, point a);

c) les procédures permettant de contrôler et de faire respecter les obligations des fabricants et des fournisseurs de produits TIC, services TIC ou processus TIC, conformément à l'article 58, paragraphe 7, point b);

d) les procédures permettant de contrôler, d'autoriser et de superviser les activités des organismes d'évaluation de la conformité;

e) lorsqu'il y a lieu, la question de savoir si le personnel des autorités ou organismes qui délivrent des certificats pour un niveau d'assurance dit «élevé», conformément à l'article 56, paragraphe 6, dispose des compétences nécessaires.

4. L'examen par les pairs est réalisé au moins une fois tous les cinq ans par au moins deux autorités nationales de certification de cybersécurité d'autres États membres et par la Commission. L'ENISA peut participer à l'examen par les pairs.

5. La Commission peut adopter des actes d'exécution établissant un plan pour l'examen par les pairs couvrant une période d'au moins cinq ans et définissant les critères concernant la composition de l'équipe chargée de l'examen par les pairs, la méthode utilisée pour mener cet examen, ainsi que le programme, la fréquence et les autres tâches y afférentes. Lors de l'adoption de ces actes d'exécution, la Commission tient dûment compte des observations formulées par le GECC. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 66, paragraphe 2.

6. Les résultats des examens par les pairs sont examinés par le GECC, qui établit des résumés pouvant être rendu publics et qui émet, au besoin, des lignes directrices ou des recommandations sur les actions à entreprendre ou les mesures à prendre par les entités concernées.

Article 60

Organismes d'évaluation de la conformité

1. Les organismes d'évaluation de la conformité sont accrédités par les organismes nationaux d'accréditation désignés conformément au règlement (CE) nº 765/2008. Cette accréditation n'est délivrée que lorsque l'organisme d'évaluation de la conformité satisfait aux exigences énoncées à l'annexe du présent règlement.

2. Lorsqu'un certificat de cybersécurité européen est délivré par une autorité nationale de certification de cybersécurité en vertu de l'article 56, paragraphe 5, point a), et de l'article 56, paragraphe 6, l'organisme de certification de l'autorité nationale de certification de cybersécurité est accrédité en tant qu'organisme d'évaluation de la conformité conformément au paragraphe 1 du présent article.

3. Lorsque les schémas européens de certification de cybersécurité fixent des exigences spécifiques ou supplémentaires en application de l'article 54, paragraphe 1, point f), seuls les organismes d'évaluation de la conformité qui satisfont à ces exigences sont autorisés par l'autorité nationale de certification de cybersécurité à effectuer les tâches prévues dans le cadre de ces schémas.

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

Article 61

Notification

1. Pour chaque schéma européen de certification de cybersécurité, les autorités nationales de certification de cybersécurité notifient à la Commission le nom des organismes d'évaluation de la conformité accrédités et, le cas échéant, autorisés en vertu de l'article 60, paragraphe 3, à délivrer des certificats de cybersécurité européens aux niveaux d'assurance déterminés tels qu'ils sont visés à l'article 52. Les autorités nationales de certification de cybersécurité informent la Commission, sans retard indu, de toute modification ultérieure qui y est apportée.

2. Un an après la date d'entrée en vigueur d'un schéma européen de certification de cybersécurité, la Commission publie au *Journal officiel de l'Union européenne* une liste des organismes d'évaluation de la conformité qui ont fait l'objet d'une notification dans le cadre de ce schéma.

3. Si la Commission reçoit une notification après l'expiration du délai visé au paragraphe 2, elle publie les modifications apportées à la liste des organismes d'évaluation de la conformité qui ont fait l'objet d'une notification au *Journal officiel de l'Union européenne* dans un délai de deux mois à compter de la date de réception de cette notification.

4. Une autorité nationale de certification de cybersécurité peut présenter à la Commission une demande visant à retirer de la liste visée au paragraphe 2 un organisme d'évaluation de la conformité qui a fait l'objet d'une notification par cette autorité. La Commission publie au *Journal officiel de l'Union européenne* les modifications correspondantes apportées à la liste dans un délai d'un mois à compter de la date de réception de la demande présentée par l'autorité nationale de certification de cybersécurité.

5. La Commission peut adopter des actes d'exécution visant à établir les circonstances, formats et procédures pour les notifications visées au paragraphe 1 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 66, paragraphe 2.

Article 62

Groupe européen de certification de cybersécurité

1. Le groupe européen de certification de cybersécurité (GECC) est institué.

2. Le GECC est composé de représentants d'autorités nationales de certification de cybersécurité ou de représentants d'autres autorités nationales compétentes. Un membre du GECC ne peut représenter plus de deux États membres.

3. Les parties prenantes et les tiers concernés peuvent être invités à assister aux réunions du GECC et à participer à ses travaux.

4. Le GECC a pour mission:

a) de conseiller et d'assister la Commission dans ses efforts pour assurer une mise en œuvre et une application cohérentes du présent titre, notamment en ce qui concerne le programme de travail glissant de l'Union, les questions de politique de certification de cybersécurité, la coordination des approches politiques et la préparation de schémas européens de certification de cybersécurité;

b) d'assister et de conseiller l'ENISA et de coopérer avec elle en ce qui concerne la préparation d'un schéma candidat en vertu de l'article 49;

c) d'adopter un avis sur les schémas candidats préparés par l'ENISA en vertu de l'article 49;

d) de demander à l'ENISA de préparer un schéma candidat en vertu de l'article 48, paragraphe 2;

e) d'adopter des avis adressés à la Commission concernant la maintenance et le réexamen de schémas européens de certification de cybersécurité existants;

f) d'examiner les évolutions pertinentes dans le domaine de la certification de cybersécurité et d'échanger des informations et de bonnes pratiques sur les schémas de certification de cybersécurité;

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

h) de fournir un soutien à la mise en œuvre des mécanismes d'évaluation par les pairs conformément aux règles fixées dans un schéma européen de certification de cybersécurité en vertu de l'article 54, paragraphe 1, point u);

i) de faciliter l'alignement des schémas européens de certification de cybersécurité sur les normes internationalement reconnues, y compris en examinant les schémas européens de certification de cybersécurité existants et, s'il y a lieu, en recommandant à l'ENISA de nouer le dialogue avec les organisations internationales de normalisation compétentes dans le but de remédier à des insuffisances ou à des lacunes affectant les normes internationalement reconnues en vigueur.

5. Avec l'aide de l'ENISA, la Commission préside le GECC et en assure le secrétariat, conformément à l'article 8, paragraphe 1, point e).

Article 63

Droit d'introduire une réclamation

1. Les personnes physiques et morales ont le droit d'introduire une réclamation auprès de l'émetteur d'un certificat de cybersécurité européen ou, lorsque la réclamation est en rapport avec un certificat de cybersécurité européen délivré par un organisme d'évaluation de la conformité agissant conformément à l'article 56, paragraphe 6, auprès de l'autorité nationale de certification de cybersécurité concernée.

2. L'autorité ou l'organisme auprès duquel la réclamation a été introduite informe l'auteur de la réclamation de l'état d'avancement de la procédure et de la décision prise, et l'informe de son droit à un recours juridictionnel effectif visé à l'article 64.

Article 64

Droit à un recours juridictionnel effectif

1. Nonobstant tout recours administratif ou tout autre recours non juridictionnel, les personnes physiques ou morales disposent d'un droit de recours juridictionnel effectif en ce qui concerne:

a) les décisions prises par l'autorité ou l'organisme visé à l'article 63, paragraphe 1, y compris, le cas échéant, en ce qui concerne la délivrance non justifiée, la non-délivrance ou la reconnaissance d'un certificat de cybersécurité européen détenu par ces personnes physiques ou morales;

b) l'absence de réaction à une réclamation introduite auprès de l'autorité ou de l'organisme visé à l'article 63, paragraphe 1.

2. Les recours formés en vertu du présent article sont portés devant les juridictions de l'État membre dans lequel se trouve l'autorité ou l'organisme à l'encontre duquel le recours juridictionnel a été formé.

Article 65

Sanctions

Les États membres déterminent le régime des sanctions applicables aux violations des dispositions du présent titre et aux violations des schémas européens de certification de cybersécurité et prennent toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions. Ces sanctions doivent être effectives, proportionnées et dissuasives. Les États membres informent la Commission sans retard du régime ainsi déterminé et des mesures ainsi prises, de même que de toute modification apportée ultérieurement à ce régime ou à ces mesures.

TITRE IV

DISPOSITIONS FINALES

Article 66

Comité

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

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

Article 67

Évaluation et révision

1. Au plus tard le 28 juin 2024, et tous les cinq ans par la suite, la Commission évalue l'incidence, l'efficacité et l'efficience de l'ENISA et de ses méthodes de travail, ainsi que la nécessité éventuelle de modifier le mandat de l'ENISA et les conséquences financières d'une telle modification. L'évaluation tient compte de toute information communiquée en retour à l'ENISA en réaction à ses activités. Lorsque la Commission estime que le maintien du fonctionnement de l'ENISA n'est plus justifié au regard des objectifs, du mandat et des tâches qui lui ont été assignées, elle peut proposer que les dispositions du présent règlement relatives à l'ENISA soient modifiées.

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

3. L'évaluation examine s'il est nécessaire de fixer des exigences essentielles en matière de cybersécurité comme condition d'accès au marché intérieur pour empêcher que des produits TIC, services TIC et processus TIC qui ne satisfont pas aux exigences de base en matière de cybersécurité entrent sur le marché de l'Union.

4. Au plus tard le 28 juin 2024, et tous les cinq ans par la suite, la Commission transmet le rapport d'évaluation, accompagné de ses conclusions, au Parlement européen, au Conseil et au conseil d'administration. Les conclusions de ce rapport sont rendues publiques.

Article 68

Abrogation et succession

1. Le règlement (UE) n° 526/2013 est abrogé avec effet au 27 juin 2019.

2. Les références au règlement (UE) n° 526/2013 et à l'ENISA telle qu'instituée par le présent règlement s'entendent comme faites au présent règlement et à l'ENISA telle qu'instituée par le présent règlement.

3. L'ENISA instituée par le présent règlement succède à l'ENISA instituée par le règlement (UE) n° 526/2013 en ce qui concerne tous les droits de propriété, accords, obligations légales, contrats de travail, engagements financiers et responsabilités. Toutes les décisions du conseil d'administration et du conseil exécutif adoptées conformément au règlement (UE) n° 526/2013 restent valables, pour autant qu'elles respectent le présent règlement.

4. L'ENISA est instituée pour une durée indéterminée à compter du 27 juin 2019.

5. Le directeur exécutif nommé en vertu de l'article 24, paragraphe 4, du règlement (UE) n° 526/2013 reste en fonction et exerce les fonctions du directeur exécutif visées à l'article 20 du présent règlement pour la durée restante de son mandat. Les autres conditions de son contrat demeurent inchangées.

6. Les membres du conseil d'administration et leurs suppléants nommés en application de l'article 6 du règlement (UE) n° 526/2013 restent en fonction et exercent les fonctions du conseil d'administration visées à l'article 15 du présent règlement pour la durée restante de leur mandat.

Article 69

Entrée en vigueur

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

2. Les articles 58, 60, 61, 63, 64 et 65 s'appliquent à partir du 28 juin 2021.

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

Fait à Strasbourg, le 17 avril 2019.

Par le Parlement européen	*Par le Conseil*
Le président	*Le président*
A. TAJANI	G. CIAMBA

ANNEXE

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

Les organismes d'évaluation de la conformité qui souhaitent être accrédités satisfont aux exigences ci-dessous.

1. Un organisme d'évaluation de la conformité est constitué en vertu du droit national et possède la personnalité juridique.

2. Un organisme d'évaluation de la conformité est un organisme tiers qui est indépendant de l'organisation ou des produits TIC, services TIC ou processus TIC qu'il évalue.

3. Un organisme appartenant à une association d'entreprises ou à une fédération professionnelle qui représente des entreprises participant à la conception, à la fabrication, à la fourniture, à l'assemblage, à l'utilisation ou à l'entretien des produits TIC, services TIC ou processus TIC qu'il évalue peut être considéré comme un organisme d'évaluation de la conformité à condition que son indépendance et que l'absence de tout conflit d'intérêts soient démontrées.

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

5. Les organismes d'évaluation de la conformité, leurs cadres supérieurs et les personnes chargées d'exécuter les tâches d'évaluation de la conformité ne peuvent intervenir, ni directement ni comme mandataires, dans la conception, la fabrication ou la construction, la commercialisation, l'installation, l'utilisation ou l'entretien des produits TIC, services TIC ou processus TIC. Les organismes d'évaluation de la conformité, leurs cadres supérieurs et les personnes chargées d'exécuter les tâches d'évaluation de la conformité ne peuvent participer à aucune activité qui peut entrer en conflit avec l'indépendance de leur jugement ou leur intégrité en ce qui concerne leurs activités d'évaluation de la conformité. Cette interdiction s'applique, en particulier pour les services de conseil.

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

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

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

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

10. En toutes circonstances et pour chaque procédure d'évaluation de la conformité, ainsi que pour chaque type ou catégorie ou sous-catégorie de produits TIC, services TIC ou processus TIC, un organisme d'évaluation de la conformité dispose à suffisance:

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

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

c) de procédures pour accomplir ses activités qui tiennent dûment compte de la taille des entreprises, du secteur dans lequel elles exercent leurs activités, de leur structure, du degré de complexité de la technologie du produit TIC, service TIC ou processus TIC en question et de la nature, en masse ou en série, du processus de production.

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

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

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

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

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

d) l'aptitude à rédiger les attestations, procès-verbaux et rapports qui prouvent que des évaluations de conformité ont été effectuées.

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

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

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

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

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

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

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

20. Les organismes d'évaluation de la conformité veillent à ce que les laboratoires d'essai auxquels il est fait appel à des fins d'évaluation de la conformité respectent les exigences de la norme pertinente qui est harmonisée au titre du règlement (CE) n° 765/2008 en ce qui concerne l'accréditation de laboratoires qui réalisent des essais.

DIRECTIVES

DIRECTIVE (UE) 2019/882 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 17 avril 2019

relative aux exigences en matière d'accessibilité applicables aux produits et services

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

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

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 114,

vu la proposition de la Commission européenne,

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

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

statuant conformément à la procédure législative ordinaire ([2]),

considérant ce qui suit:

(1) La présente directive a pour objet de contribuer au bon fonctionnement du marché intérieur en rapprochant les dispositions législatives, réglementaires et administratives des États membres en ce qui concerne les exigences en matière d'accessibilité applicables à certains produits et services, grâce, notamment, à l'élimination et à la prévention des obstacles qui entravent la libre circulation de certains produits et services accessibles découlant d'exigences divergentes en matière d'accessibilité dans les États membres. Cela augmenterait la disponibilité des produits et services accessibles au sein du marché intérieur et améliorerait l'accessibilité des informations pertinentes.

(2) La demande de produits et services accessibles est forte et il est prévu que le nombre de personnes handicapées augmente considérablement. Un environnement dans lequel les produits et les services sont plus accessibles permet de créer une société plus inclusive et facilite l'autonomie des personnes handicapées. Dans ce contexte, il convient de garder à l'esprit que la prévalence du handicap dans l'Union est plus élevée chez les femmes que chez les hommes.

(3) La définition des personnes handicapées retenue dans la présente directive est conforme à la convention des Nations unies relative aux droits des personnes handicapées, adoptée le 13 décembre 2006 (ci-après dénommée la «convention»), à laquelle l'Union est partie depuis le 21 janvier 2011 et que tous les États membres ont ratifiée. La convention définit les personnes handicapées comme «des personnes qui présentent des incapacités physiques, mentales, intellectuelles ou sensorielles durables dont l'interaction avec diverses barrières peut faire obstacle à leur pleine et effective participation à la société sur la base de l'égalité avec les autres». La présente directive promeut la participation pleine et effective des personnes handicapées sur un pied d'égalité, en améliorant leur accès aux produits et services courants qui, du fait de leur conception initiale ou de leur adaptation ultérieure, répondent à leurs besoins spécifiques.

(4) D'autres personnes qui doivent faire face à des limitations fonctionnelles, telles que les personnes âgées, les femmes enceintes et les personnes voyageant avec des bagages, bénéficieraient aussi de la présente directive. La notion de «personnes présentant des limitations fonctionnelles» visée dans la présente directive inclut les personnes présentant des incapacités physiques, mentales, intellectuelles ou sensorielles, des incapacités liées à l'âge ou toute autre limitation des performances du corps humain, permanente ou temporaire, dont l'interaction avec divers obstacles peut limiter l'accès à des produits et services et conduire à une situation nécessitant une adaptation desdits produits et services à leurs besoins particuliers.

(5) La disparité des dispositions législatives, réglementaires et administratives des États membres en ce qui concerne l'accessibilité de produits et de services pour les personnes handicapées crée des obstacles à la libre circulation des produits et services et fausse la concurrence effective sur le marché intérieur. Pour certains produits et services, ces disparités devraient s'accroître dans l'Union après l'entrée en vigueur de la convention. Ces obstacles portent tout particulièrement préjudice aux opérateurs économiques, notamment aux petites et moyennes entreprises (PME).

([1]) JO C 303 du 19.8.2016, p. 103.
([2]) Position du Parlement européen du 13 mars 2019 (non encore parue au Journal officiel) et décision du Conseil du 9 avril 2019.

(6) Les divergences entre les exigences nationales en matière d'accessibilité dissuadent notamment les professionnels individuels, les PME et les microentreprises de se lancer dans des activités commerciales en dehors de leurs marchés nationaux. Les exigences en matière d'accessibilité fixées par les États membres à l'échelle nationale, voire régionale ou locale, diffèrent tant du point de vue de leur champ d'application que de leur degré de précision. Ces divergences ont une incidence négative sur la compétitivité et la croissance en raison du surcoût engendré par la mise au point et la commercialisation, pour chaque marché national, de produits et services accessibles.

(7) Les consommateurs de produits et services accessibles et de technologies d'assistance doivent s'accommoder de prix élevés du fait de la concurrence limitée qui existe entre les fournisseurs. La fragmentation des réglementations nationales limite les avantages qui pourraient résulter du partage d'expériences en matière d'adaptation aux évolutions sociétales et technologiques avec des pairs nationaux et internationaux.

(8) Il est donc nécessaire de rapprocher les mesures nationales à l'échelle de l'Union pour assurer le bon fonctionnement du marché intérieur et mettre un terme à la fragmentation du marché des produits et services accessibles, pour réaliser des économies d'échelle, pour faciliter les échanges et la mobilité transfrontières, ainsi que pour aider les opérateurs économiques à concentrer des ressources sur l'innovation plutôt qu'à les utiliser pour faire face aux dépenses découlant de la fragmentation des législations à travers l'Union.

(9) Les avantages d'une harmonisation des exigences en matière d'accessibilité pour le marché intérieur ont été mis en évidence par l'application de la directive 2014/33/UE du Parlement européen et du Conseil [3] concernant les ascenseurs et du règlement (CE) n° 661/2009 du Parlement européen et du Conseil [4] dans le domaine des transports.

(10) Dans la déclaration n° 22 relative aux personnes handicapées, annexée au traité d'Amsterdam, la Conférence des représentants des gouvernements des États membres est convenue que, lors de l'élaboration de mesures en vertu de l'article 114 du traité sur le fonctionnement de l'Union européenne, les institutions de l'Union doivent tenir compte des besoins des personnes handicapées.

(11) L'objectif général de la communication de la Commission du 6 mai 2015 intitulée «Une stratégie pour un marché unique numérique en Europe» est de procurer des avantages économiques et sociaux durables grâce à un marché unique numérique connecté, en facilitant ainsi les échanges commerciaux et en favorisant l'emploi au sein de l'Union. Les consommateurs de l'Union ne profitent toujours pas pleinement des avantages en matière de prix et de choix que peut offrir le marché unique car les transactions en ligne transfrontières sont encore très limitées. La fragmentation a aussi pour effet de limiter la demande de transactions transfrontières de commerce électronique. Il convient également de mener des actions concertées pour faire en sorte que le contenu électronique, les services de communications électroniques et l'accès aux services de médias audiovisuels soient totalement accessibles aux personnes handicapées. Il est donc nécessaire d'harmoniser les exigences en matière d'accessibilité sur le marché unique numérique et de veiller à ce que tous les citoyens de l'Union, quelles que soient leurs capacités, puissent profiter de ses avantages.

(12) Depuis que l'Union est devenue partie à la convention, les dispositions de celle-ci font partie intégrante de l'ordre juridique de l'Union et lient les institutions et les États membres de l'Union.

(13) La convention exige de ses parties qu'elles prennent des mesures appropriées pour assurer aux personnes handicapées, sur la base de l'égalité avec les autres, l'accès à l'environnement physique, aux transports, à l'information et à la communication, y compris aux systèmes et technologies de l'information et de la communication, et aux autres équipements et services ouverts ou fournis au public, tant dans les zones urbaines que rurales. Le comité des droits des personnes handicapées des Nations unies a constaté la nécessité d'instaurer un cadre législatif prévoyant des critères concrets, contraignants et temporels pour le suivi de l'instauration progressive des mesures en matière d'accessibilité.

(14) La convention demande à ses parties d'entreprendre ou d'encourager la recherche et le développement, et d'encourager l'offre et l'utilisation de nouvelles technologies – y compris les technologies de l'information et de la communication, les aides à la mobilité, les appareils et accessoires et les technologies d'assistance – qui soient adaptées aux personnes handicapées. La convention invite également à privilégier les technologies abordables.

[3] Directive 2014/33/UE du Parlement européen et du Conseil du 26 février 2014 relative à l'harmonisation des législations des États membres concernant les ascenseurs et les composants de sécurité pour ascenseurs (JO L 96 du 29.3.2014, p. 251).

[4] Règlement (CE) n° 661/2009 du Parlement européen et du Conseil du 13 juillet 2009 concernant les prescriptions pour l'homologation relatives à la sécurité générale des véhicules à moteur, de leurs remorques et des systèmes, composants et entités techniques distinctes qui leur sont destinés (JO L 200 du 31.7.2009, p. 1).

(15) L'entrée en vigueur de la convention dans l'ordre juridique des États membres rend nécessaire l'adoption de dispositions nationales supplémentaires en matière d'accessibilité des produits et services. Sans une action de l'Union, ces dispositions accroîtraient encore les divergences entre les dispositions législatives, réglementaires et administratives des États membres.

(16) Il est donc nécessaire de faciliter l'application de la convention dans l'Union en prévoyant des règles communes de l'Union. La présente directive encourage également les États membres dans les efforts qu'ils déploient afin de respecter, de manière harmonisée, leurs engagements nationaux ainsi que les obligations qui leur incombent en vertu de la convention en matière d'accessibilité.

(17) La communication de la Commission du 15 novembre 2010 intitulée «Stratégie européenne 2010-2020 en faveur des personnes handicapées: un engagement renouvelé pour une Europe sans entraves», en phase avec la convention, mentionne l'accessibilité parmi les huit domaines d'intervention qu'elle a répertoriés, indique qu'il s'agit d'un préalable fondamental à la participation à la société, et a pour objectif de garantir l'accessibilité des produits et des services.

(18) Les produits et services relevant du champ d'application de la présente directive ont été sélectionnés sur la base d'un examen réalisé au cours de l'élaboration de l'analyse d'impact, qui a recensé des produits et services pertinents pour les personnes handicapées, pour lesquels les États membres ont adopté ou sont susceptibles d'adopter des exigences nationales divergentes en matière d'accessibilité qui perturbent le fonctionnement du marché intérieur.

(19) Afin d'assurer l'accessibilité des services relevant du champ d'application de la présente directive, les produits utilisés pour la fourniture de ces services avec lesquels le consommateur interagit devraient également être conformes aux exigences applicables en matière d'accessibilité prévues par la présente directive.

(20) Même lorsqu'un service est intégralement ou partiellement sous-traité à un tiers, son accessibilité ne devrait pas être compromise et les prestataires de services devraient se conformer aux obligations de la présente directive. Les prestataires de services devraient également veiller à ce que leur personnel soit formé de manière adéquate et continue afin de s'assurer qu'il dispose de connaissances solides sur l'utilisation de produits et services accessibles. Cette formation devrait porter sur des questions telles que la fourniture d'informations, le conseil et la publicité.

(21) Des exigences en matière d'accessibilité devraient être introduites d'une manière qui entraîne le moins de contraintes possible pour les opérateurs économiques et les États membres.

(22) Il est nécessaire de préciser les exigences en matière d'accessibilité applicables à la mise sur le marché des produits et services relevant du champ d'application de la présente directive afin de garantir leur libre circulation sur le marché intérieur.

(23) La présente directive devrait rendre obligatoires les exigences fonctionnelles en matière d'accessibilité qui devraient être formulées sous la forme d'objectifs généraux. Ces exigences devraient être suffisamment précises pour créer des obligations juridiquement contraignantes et suffisamment détaillées afin de permettre d'évaluer la conformité dans le but de garantir le bon fonctionnement du marché intérieur pour les produits et services concernés par la présente directive, tout en laissant une certaine souplesse pour permettre l'innovation.

(24) La présente directive contient un certain nombre de critères en matière de performances fonctionnelles qui sont liés aux modes de fonctionnement des produits et services. Ces critères ne doivent pas s'entendre comme étant une solution générale de substitution aux exigences en matière d'accessibilité de la présente directive, mais devraient être utilisés dans des cas très spécifiques uniquement. Lorsque les exigences en matière d'accessibilité de la présente directive ne traitent pas d'une ou plusieurs fonctions ou caractéristiques spécifiques des produits ou services, il conviendrait d'appliquer lesdits critères aux fonctions ou caractéristiques en question, afin de le rendre accessible. Par ailleurs, dans le cas où une exigence en matière d'accessibilité comporterait des exigences techniques spécifiques et où le produit ou service visé fournirait une solution technique alternative pour ces exigences techniques, cette solution technique alternative devrait toujours être conforme aux exigences connexes en matière d'accessibilité et devrait donner lieu à une accessibilité équivalente ou accrue par l'application des critères pertinents en matière de performances fonctionnelles.

(25) La présente directive devrait s'appliquer aux systèmes informatiques matériels à usage général du grand public. Pour que ces systèmes fonctionnent de manière accessible, il y a lieu que leurs systèmes d'exploitation soient également accessibles. Ces systèmes informatiques matériels se caractérisent par leur nature polyvalente et leur capacité à réaliser, avec les logiciels appropriés, les opérations informatiques les plus courantes demandées par les consommateurs, et sont destinés à être utilisés par les consommateurs. Les ordinateurs personnels, y compris les ordinateurs de bureau, les ordinateurs portables, les smartphones et les tablettes constituent des exemples de systèmes

informatiques matériels. Les ordinateurs spécialisés incorporés dans des produits électroniques de consommation ne constituent pas des systèmes informatiques matériels à usage général du grand public. La présente directive ne devrait pas s'appliquer aux composants seuls ayant des fonctions spécifiques, pris séparément, tels que les cartes mères ou les puces mémoire, qui sont utilisés dans ces systèmes ou pourraient l'être.

(26) La présente directive devrait également s'appliquer aux terminaux de paiement, y compris leurs matériels et leurs logiciels, et à certains terminaux en libre-service interactifs, y compris leurs matériels et logiciels, destinés à être utilisés pour fournir des services relevant de la présente directive, par exemple les guichets de banque automatiques, les distributeurs automatiques délivrant des tickets physiques donnant accès à des services, tels que les distributeurs de titres de transport, les distributeurs de tickets de file d'attente dans les agences bancaires, les bornes d'enregistrement automatiques et les terminaux en libre-service interactifs fournissant des informations, y compris les écrans d'information interactifs.

(27) Il convient cependant d'exclure du champ d'application de la présente directive certains terminaux en libre-service interactifs fournissant des informations installés en tant que parties intégrantes de véhicules, d'aéronefs, de navires ou de matériel roulant dans la mesure où ces terminaux font partie de véhicules, d'aéronefs, de navires ou de matériel roulant ne relevant pas de la présente directive.

(28) La présente directive devrait également s'appliquer aux services de communications électroniques, y compris les communications d'urgence tels qu'elles sont définies dans la directive (UE) 2018/1972 du Parlement européen et du Conseil ([5]). Actuellement, les mesures prises par les États membres pour assurer l'accès des personnes handicapées sont divergentes et ne sont pas harmonisées dans l'ensemble du marché intérieur. Veiller à ce que les mêmes exigences en matière d'accessibilité s'appliquent dans l'ensemble de l'Union entraînera des économies d'échelle pour les opérateurs économiques qui exercent leurs activités dans plusieurs États membres et contribuera à l'accès effectif des personnes handicapées dans leur propre État membre et lorsqu'elles voyagent dans d'autres États membres. Pour que les services de communications électroniques, y compris les communications d'urgence, soient accessibles, les prestataires devraient, en plus de la communication vocale, fournir du texte en temps réel, et des services de conversation totale lorsqu'ils proposent de la vidéo, en assurant la synchronisation de tous ces moyens de communication. Outre les exigences de la présente directive, les États membres devraient, conformément à la directive (UE) 2018/1972, être en mesure de déterminer un fournisseur de services de relais que les personnes handicapées pourraient utiliser.

(29) La présente directive harmonise les exigences en matière d'accessibilité applicables aux services de communications électroniques et aux produits connexes et complète la directive (UE) 2018/1972, laquelle fixe des exigences en matière d'équivalence d'accès et de choix pour les utilisateurs finals handicapés. La directive (UE) 2018/1972 fixe également des exigences relevant des obligations de service universel en ce qui concerne le caractère abordable des services d'accès à l'internet et de communications vocales, ainsi que la disponibilité et le caractère abordable des équipements terminaux connexes, des équipements spécifiques et des services spécifiques pour les consommateurs handicapés.

(30) La présente directive devrait également s'appliquer aux équipements terminaux grand public avec des capacités informatiques interactives, dont il est prévisible qu'ils seront principalement utilisés pour accéder à des services de communications électroniques. Aux fins de la présente directive, il convient de considérer ces équipements comme comprenant les équipements faisant partie de la configuration utilisée pour accéder aux services de communications électroniques, tels qu'un routeur ou un modem.

(31) Aux fins de la présente directive, l'accès aux services de médias audiovisuels devrait signifier que les services donnant accès au contenu audiovisuel sont accessibles, ainsi que les mécanismes permettant aux utilisateurs qui sont des personnes handicapées d'utiliser leurs technologies d'assistance. Les services fournissant un accès à des services de médias audiovisuels pourraient inclure des sites internet, des applications en ligne, des applications intégrées dans des décodeurs, des applications téléchargeables, des services intégrés sur appareils mobiles, notamment des applications mobiles, et des lecteurs de médias connexes ainsi que des services de télévision connectée. L'accessibilité des services de médias audiovisuels est régie par la directive 2010/13/UE du Parlement européen et du Conseil ([6]), sauf en ce qui concerne l'accessibilité des guides électroniques de programme (GEP) qui font partie de la définition des services fournissant un accès à des services de médias audiovisuels auxquels la présente directive s'applique.

(32) Dans le cadre des services de transport aérien, ferroviaire, par voie de navigation intérieure et par autobus de voyageurs et de passagers, la présente directive devrait s'appliquer, entre autres, à la fourniture d'informations sur les services de transport, notamment d'informations en temps réel sur le voyage, via des sites internet, des services intégrés sur des appareils mobiles, des écrans d'information interactifs et des terminaux en libre-service

([5]) 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).

([6]) Directive 2010/13/UE du Parlement européen et du Conseil du 10 mars 2010 visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels (JO L 95 du 15.4.2010, p. 1).

interactifs, dont les personnes handicapées ont besoin pour voyager. Il pourrait s'agir d'informations sur les produits et services en matière de transport de voyageurs et de passagers du prestataire de services, d'informations fournies avant ou pendant le voyage et lorsqu'un service est annulé ou que son départ est retardé. D'autres éléments d'information pourraient aussi porter sur les prix et les promotions.

(33) La présente directive devrait également s'appliquer aux sites internet, aux services intégrés sur appareils mobiles, y compris les applications mobiles mises au point ou à disposition par les exploitants de services de transport de voyageurs et de passagers relevant de la présente directive, ou en leur nom, aux services de billetterie électronique, aux billets électroniques et aux terminaux en libre-service interactifs.

(34) La détermination du champ d'application de la présente directive en ce qui concerne les services de transport aérien, ferroviaire, par voie de navigation intérieure et par autobus de voyageurs et de passagers devrait s'appuyer sur la législation sectorielle existante concernant les droits des voyageurs et des passagers. Lorsque la présente directive ne s'applique pas à certains types de services de transport, les États membres devraient encourager les prestataires de services à appliquer les exigences en matière d'accessibilité de la présente directive.

(35) La directive (UE) 2016/2102 du Parlement européen et du Conseil ([7]) prévoit déjà des obligations pour les organismes du secteur public qui fournissent des services de transport, y compris des services de transport urbains et suburbains et des services de transport régionaux, afin qu'ils rendent leurs sites internet accessibles. La présente directive prévoit des exemptions pour les microentreprises fournissant des services, y compris des services de transport urbains et suburbains et des services de transport régionaux. Elle comporte en outre des obligations pour garantir l'accessibilité des sites internet utilisés pour le commerce électronique. Puisque la présente directive contient des obligations destinées à la grande majorité des prestataires privés de services de transport afin qu'ils rendent leurs sites internet accessibles en ce qui concerne la vente en ligne de titres de transport, il n'est pas nécessaire d'y introduire d'autres exigences applicables aux sites internet des prestataires de services de transport urbains et suburbains et des prestataires de services de transport régionaux.

(36) Certains aspects des exigences en matière d'accessibilité, notamment en ce qui concerne la fourniture d'informations prévue par la présente directive, sont déjà régis par le droit de l'Union en vigueur dans le domaine du transport de passagers. Il s'agit notamment d'aspects du règlement (CE) n° 261/2004 du Parlement européen et du Conseil ([8]), du règlement (CE) n° 1107/2006 du Parlement européen et du Conseil ([9]), du règlement (CE) n° 1371/2007 du Parlement européen et du Conseil ([10]), du règlement (UE) n° 1177/2010 du Parlement européen et du Conseil ([11]) et du règlement (UE) n° 181/2011 du Parlement européen et du Conseil ([12]). Il s'agit également des actes pertinents adoptés sur la base de la directive 2008/57/CE du Parlement européen et du Conseil ([13]). Par souci de cohérence réglementaire, il convient que les exigences en matière d'accessibilité établies dans les règlements et actes précités continuent de s'appliquer. Cependant, les exigences supplémentaires énoncées dans la présente directive viendraient compléter les exigences existantes, améliorant ainsi le fonctionnement du marché intérieur dans le domaine des transports et procurant des avantages aux personnes handicapées.

(37) Certains éléments des services de transport ne devraient pas relever de la présente directive lorsqu'ils sont fournis hors du territoire des États membres, même lorsque le service est destiné au marché de l'Union. En ce qui concerne ces éléments, l'exploitant d'un service de transport de voyageurs ou de passagers ne devrait être tenu de veiller au respect des exigences de la présente directive qu'en ce qui concerne la partie du service qu'il propose sur le territoire de l'Union. Cependant, dans le cas du transport aérien, les transporteurs aériens de l'Union devraient veiller à ce qu'il soit également satisfait aux exigences applicables de la présente directive sur les vols au départ d'un

([7]) Directive (UE) 2016/2102 du Parlement européen et du Conseil du 26 octobre 2016 relative à l'accessibilité des sites internet et des applications mobiles des organismes du secteur public (JO L 327 du 2.12.2016, p. 1).

([8]) Règlement (CE) n° 261/2004 du Parlement européen et du Conseil du 11 février 2004 établissant des règles communes en matière d'indemnisation et d'assistance des passagers en cas de refus d'embarquement et d'annulation ou de retard important d'un vol, et abrogeant le règlement (CEE) n° 295/91 (JO L 46 du 17.2.2004, p. 1).

([9]) Règlement (CE) n° 1107/2006 du Parlement européen et du Conseil du 5 juillet 2006 concernant les droits des personnes handicapées et des personnes à mobilité réduite lorsqu'elles font des voyages aériens (JO L 204 du 26.7.2006, p. 1).

([10]) Règlement (CE) n° 1371/2007 du Parlement européen et du Conseil du 23 octobre 2007 sur les droits et obligations des voyageurs ferroviaires (JO L 315 du 3.12.2007, p. 14).

([11]) Règlement (UE) n° 1177/2010 du Parlement européen et du Conseil du 24 novembre 2010 concernant les droits des passagers voyageant par mer ou par voie de navigation intérieure et modifiant le règlement (CE) n° 2006/2004 (JO L 334 du 17.12.2010, p. 1).

([12]) Règlement (UE) n° 181/2011 du Parlement européen et du Conseil du 16 février 2011 concernant les droits des passagers dans le transport par autobus et autocar et modifiant le règlement (CE) n° 2006/2004 (JO L 55 du 28.2.2011, p. 1).

([13]) Directive 2008/57/CE du Parlement européen et du Conseil du 17 juin 2008 relative à l'interopérabilité du système ferroviaire au sein de la Communauté (JO L 191 du 18.7.2008, p. 1).

aéroport situé dans un pays tiers à destination d'un aéroport situé sur le territoire d'un État membre. Par ailleurs, tous les transporteurs aériens, y compris ceux qui ne disposent pas d'une licence dans l'Union, devraient veiller à ce qu'il soit satisfait aux exigences applicables de la présente directive sur les vols au départ du territoire de l'Union à destination du territoire d'un pays tiers.

(38) Les pouvoirs publics des villes devraient être encouragés à incorporer l'accessibilité sans obstacle aux services de transport urbains dans leurs plans de mobilité urbaine durable et à publier régulièrement une liste des bonnes pratiques en matière d'accessibilité sans obstacle aux transports publics urbains et à la mobilité.

(39) Le droit de l'Union en matière de services bancaires et financiers vise à protéger les utilisateurs de ces services et à leur fournir des informations dans l'ensemble de l'Union, mais ne comprend pas d'exigences en matière d'accessibilité. Afin que les personnes handicapées puissent utiliser ces services dans l'ensemble de l'Union, y compris lorsqu'ils sont fournis via des sites internet et des services intégrés sur appareils mobiles dont les applications mobiles, et prendre des décisions en connaissance de cause et qu'elles soient assurées de bénéficier d'une protection adéquate sur la base de l'égalité avec les autres consommateurs et afin que des conditions de concurrence équitables soient assurées aux prestataires de services, la présente directive devrait établir des exigences communes en matière d'accessibilité pour certains services bancaires et financiers aux consommateurs.

(40) Les exigences appropriées en matière d'accessibilité devraient également s'appliquer aux méthodes d'identification et aux services de signature et de paiement électroniques dans la mesure où ils sont nécessaires pour conclure des transactions dans le cadre des services bancaires aux consommateurs.

(41) Les fichiers de livres numériques reposent sur un codage informatique qui permet la circulation et la consultation d'une œuvre intellectuelle principalement textuelle et graphique. Le degré de précision du codage détermine l'accessibilité des fichiers de livres numériques, en particulier pour ce qui est de la qualification des différents éléments constitutifs de l'œuvre et de la description normalisée de sa structure. L'interopérabilité en termes d'accessibilité devrait optimaliser la compatibilité de ces fichiers avec les agents utilisateurs et les technologies d'assistance actuelles et futures. Les caractéristiques propres à des ouvrages particuliers comme les bandes dessinées, les livres pour enfants et les livres d'art devraient être prises en compte eu égard à toutes les exigences applicables en matière d'accessibilité. L'existence d'exigences en matière d'accessibilité divergentes d'un État membre à l'autre empêcherait les éditeurs et autres opérateurs économiques de tirer parti des atouts du marché intérieur et pourrait susciter des problèmes d'interopérabilité avec les liseuses numériques et limiter l'accès des consommateurs qui sont des personnes handicapées. Pour ce qui est des livres numériques, la notion de prestataire de services pourrait comprendre les éditeurs et les autres opérateurs économiques associés à la distribution.

Il est reconnu que les personnes handicapées sont toujours confrontées à des obstacles pour accéder aux contenus qui sont protégés par le droit d'auteur et des droits voisins et que certaines mesures ont déjà été prises pour remédier à cette situation, par exemple au moyen de l'adoption de la directive (UE) 2017/1564 du Parlement européen et du Conseil ([14]) et du règlement (UE) 2017/1563 du Parlement européen et du Conseil ([15]), et également que d'autres mesures de l'Union pourraient à l'avenir être prises à cet égard.

(42) La présente directive définit les services de commerce électronique comme des services fournis à distance, via des sites internet et des services intégrés sur appareils mobiles, par voie électronique et à la demande individuelle d'un consommateur, en vue de conclure un contrat de consommation. Aux fins de cette définition, on entend par «à distance» un service fourni sans que les parties soient simultanément présentes; par «par voie électronique» un service envoyé à l'origine et reçu à destination au moyen d'équipements électroniques de traitement (y compris la compression numérique) et de stockage de données, et qui est entièrement transmis, acheminé et reçu par voie filaire, par radio, par moyens optiques ou par d'autres moyens électromagnétiques; et par «à la demande individuelle d'un consommateur», un service fourni sur demande individuelle. Compte tenu de l'importance croissante des services de commerce électronique et de leur caractère hautement technologique, il est important de disposer d'exigences harmonisées quant à leur accessibilité.

([14]) Directive (UE) 2017/1564 du Parlement européen et du Conseil du 13 septembre 2017 sur certaines utilisations autorisées de certaines œuvres et d'autres objets protégés par le droit d'auteur et les droits voisins en faveur des aveugles, des déficients visuels et des personnes ayant d'autres difficultés de lecture des textes imprimés et modifiant la directive 2001/29/CE sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information (JO L 242 du 20.9.2017, p. 6).

([15]) Règlement (UE) 2017/1563 du Parlement européen et du Conseil du 13 septembre 2017 relatif à l'échange transfrontalier, entre l'Union et des pays tiers, d'exemplaires en format accessible de certaines œuvres et d'autres objets protégés par le droit d'auteur et les droits voisins en faveur des aveugles, des déficients visuels et des personnes ayant d'autres difficultés de lecture des textes imprimés (JO L 242 du 20.9.2017, p. 1).

(43) Les obligations en matière d'accessibilité pour les services de commerce électronique prévues par la présente directive devraient s'appliquer à la vente en ligne de tout produit ou service et, par conséquent, à la vente de tout produit ou service relevant en tant que tel de la présente directive.

(44) Les mesures relatives à l'accessibilité de la réception des communications d'urgence devraient être adoptées sans préjudice de l'organisation des services d'urgence, et ne devraient pas avoir d'incidence sur cette organisation, qui reste de la compétence exclusive des États membres.

(45) Conformément à la directive (UE) 2018/1972, les États membres doivent veiller à ce que les utilisateurs finals handicapés disposent d'un accès aux services d'urgence au moyen des communications d'urgence et qui soit équivalent à celui dont bénéficient les autres utilisateurs finals, conformément au droit de l'Union harmonisant les exigences en matière d'accessibilité applicables aux produits et services. La Commission et les autorités de régulation nationales et les autres autorités compétentes doivent prendre les mesures appropriées pour veiller à ce que, lorsqu'ils voyagent dans un autre État membre, les utilisateurs finals handicapés puissent accéder aux services d'urgence sur un pied d'égalité avec les autres utilisateurs, si possible sans qu'ils doivent s'enregistrer au préalable. Ces mesures visent à garantir l'interopérabilité entre les États membres et doivent être fondées dans toute la mesure du possible sur les normes ou spécifications européennes établies conformément à l'article 39 de la directive (UE) 2018/1972. Ces mesures n'empêchent pas les États membres d'adopter des obligations supplémentaires aux fins de la réalisation des objectifs énoncés dans ladite directive. Plutôt que de satisfaire aux exigences en matière d'accessibilité en ce qui concerne la réception des communications d'urgence pour les utilisateurs handicapés prévues par la présente directive, les États membres devraient avoir la faculté de déterminer un fournisseur de services de relais que les personnes handicapées pourraient utiliser pour communiquer avec le centre de réception des appels d'urgence, tant que ces centres de réception des appels d'urgence ne seront pas en mesure d'utiliser des services de communications électroniques via des protocoles internet pour garantir l'accessibilité de la réception des communications d'urgence. En tout état de cause, les obligations de la présente directive ne devraient pas s'entendre comme limitant ou réduisant les obligations en faveur des utilisateurs finals handicapés, y compris les obligations en matière d'accès équivalent aux services de communications électronique et aux services d'urgence ainsi que les obligations en matière d'accessibilité fixées dans la directive (UE) 2018/1972.

(46) La directive (UE) 2016/2102 définit des exigences en matière d'accessibilité pour les sites internet et les applications mobiles des organismes du secteur public et d'autres aspects connexes, en particulier des exigences relatives à la conformité des sites internet et des applications mobiles concernés. Cette directive comporte toutefois une liste spécifique d'exceptions. Des exceptions similaires sont d'application pour la présente directive. Certaines activités réalisées par l'intermédiaire de sites internet et d'applications mobiles d'organismes du secteur public, telles que les services de transport de voyageurs et de passagers ou les services de commerce électronique, qui relèvent du champ d'application de la présente directive, devraient en outre être conformes aux exigences applicables en matière d'accessibilité prévues par la présente directive afin de garantir que la vente en ligne de produits et services soit accessible aux personnes handicapées, que le vendeur soit un opérateur économique public ou privé. Les exigences en matière d'accessibilité prévues par la présente directive devraient être alignées sur les exigences de la directive (UE) 2016/2102, en dépit des différences qui existent par exemple en matière de suivi, d'établissement de rapports et de contrôle.

(47) Les quatre principes de l'accessibilité pour les sites internet et les applications mobiles, tels qu'ils sont énoncés dans la directive (UE) 2016/2102, sont la perceptibilité, c'est-à-dire que les informations et les composants des interfaces utilisateurs doivent pouvoir être présentés aux utilisateurs de manière à ce qu'ils les perçoivent; l'opérabilité, c'est-à-dire que les composants des interfaces utilisateurs et la navigation doivent pouvoir être utilisés; la compréhensibilité, c'est-à-dire que les informations et l'utilisation des interfaces utilisateurs doivent être compréhensibles; et la solidité, c'est-à-dire que le contenu doit être suffisamment solide pour être interprété de manière fiable par une grande diversité d'agents utilisateurs, y compris des technologies d'assistance. Ces principes valent également pour la présente directive.

(48) Les États membres devraient prendre toutes les mesures appropriées afin que, lorsque les produits et services relevant de la présente directive sont conformes aux exigences applicables en matière d'accessibilité, leur libre circulation dans l'Union ne soit pas entravée pour des raisons liées aux exigences en matière d'accessibilité.

(49) Dans certains cas, des exigences communes en matière d'accessibilité applicables à l'environnement bâti faciliteraient la libre circulation des services concernés et des personnes handicapées. C'est pourquoi la présente directive devrait permettre aux États membres d'inclure l'environnement bâti utilisé dans la fourniture des services dans le champ d'application de la présente directive, garantissant le respect des exigences en matière d'accessibilité énoncées à l'annexe III.

(50) L'accessibilité devrait résulter de l'élimination et de la prévention systématiques des obstacles, de préférence au moyen d'une approche caractérisée par la conception universelle («conception pour tous»), qui contribue à assurer

l'accès des personnes handicapées sur la base de l'égalité avec les autres. Selon la convention, cette approche désigne «la conception de produits, d'équipements, de programmes et de services qui puissent être utilisés par tous, dans toute la mesure possible, sans nécessiter ni adaptation ni conception spéciale». Conformément à la convention, «la 'conception universelle' n'exclut pas les appareils et accessoires fonctionnels pour des catégories particulières de personnes handicapées là où ils sont nécessaires». En outre, l'accessibilité ne devrait pas exclure la mise à disposition d'aménagements raisonnables, lorsque le droit national ou celui de l'Union l'exige. Il y a lieu d'interpréter les notions d'accessibilité et de conception universelle conformément à l'orientation générale n° 2(2014) — article 9: Accessibilité, rédigée par le comité des droits des personnes handicapées.

(51) Les produits et services entrant dans le champ d'application de la présente directive ne relèvent pas automatiquement du champ d'application de la directive 93/42/CEE du Conseil ([16]). Certaines technologies d'assistance qui sont des dispositifs médicaux pourraient toutefois relever du champ d'application de ladite directive.

(52) Dans l'Union, la plupart des emplois sont fournis par les PME et les microentreprises. Celles-ci ont une importance cruciale pour la croissance future, mais se heurtent très souvent à des difficultés et obstacles lors de l'élaboration de leurs produits ou services, en particulier dans un contexte transfrontière. Il est donc nécessaire de faciliter le travail des PME et des microentreprises en harmonisant les dispositions nationales en matière d'accessibilité, tout en maintenant les garde-fous nécessaires.

(53) Pour pouvoir bénéficier de la présente directive, les microentreprises et les PME doivent véritablement satisfaire aux exigences de la recommandation 2003/361/CE de la Commission ([17]) et de la jurisprudence pertinente, destinées à prévenir le contournement de ses règles.

(54) Afin de veiller à la cohérence du droit de l'Union, la présente directive devrait se fonder sur la décision n° 768/2008/CE du Parlement européen et du Conseil ([18]), dans la mesure où elle concerne des produits déjà soumis à d'autres actes de l'Union, tout en tenant compte des caractéristiques spécifiques des exigences en matière d'accessibilité énoncées dans la présente directive.

(55) Tous les opérateurs économiques relevant du champ d'application de la présente directive et intervenant dans la chaîne d'approvisionnement et de distribution devraient faire en sorte de ne mettre à disposition sur le marché que des produits conformes à la présente directive. Il devrait en être de même pour les opérateurs économiques fournissant des services. Il convient de prévoir une répartition claire et proportionnée des obligations correspondant au rôle de chaque opérateur économique dans le processus d'approvisionnement et de distribution.

(56) Les opérateurs économiques devraient être responsables de la conformité des produits et services, eu égard à leur rôle respectif dans la chaîne d'approvisionnement, de manière à garantir un niveau élevé de protection de l'accessibilité et une concurrence loyale sur le marché de l'Union.

(57) Les obligations de la présente directive devraient s'appliquer de la même manière aux opérateurs économiques du secteur public et du secteur privé.

(58) En raison de la connaissance détaillée qu'il a du processus de conception et de production, le fabricant est le mieux placé pour accomplir intégralement l'évaluation de la conformité. Si la responsabilité de la conformité des produits incombe au fabricant, les autorités de surveillance du marché devraient jouer un rôle essentiel en vérifiant que les produits mis à disposition dans l'Union sont fabriqués dans le respect du droit de l'Union.

(59) Les importateurs et les distributeurs devraient être associés aux tâches de surveillance du marché accomplies par les autorités nationales et y participer activement en communiquant aux autorités compétentes toutes les informations nécessaires sur le produit concerné.

(60) Les importateurs devraient veiller à ce que les produits en provenance de pays tiers qui entrent sur le marché de l'Union soient conformes à la présente directive, et veiller notamment à ce que les fabricants aient appliqué les procédures d'évaluation de la conformité adaptées à ces produits.

(61) Lors de la mise sur le marché d'un produit, les importateurs devraient indiquer sur le produit leur nom, leur raison sociale ou leur marque déposée et l'adresse à laquelle ils peuvent être contactés.

([16]) Directive 93/42/CEE du Conseil du 14 juin 1993 relative aux dispositifs médicaux (JO L 169 du 12.7.1993, p. 1).
([17]) 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).
([18]) Décision n° 768/2008/CE du Parlement européen et du Conseil du 9 juillet 2008 relative à un cadre commun pour la commercialisation des produits et abrogeant la décision 93/465/CEE du Conseil (JO L 218 du 13.8.2008, p. 82).

(62) Les distributeurs devraient veiller à ce que la façon dont ils manipulent le produit ne porte pas préjudice à la conformité de celui-ci avec les exigences de la présente directive en matière d'accessibilité.

(63) Tout opérateur économique qui met un produit sur le marché sous son nom ou sa marque propre ou modifie un produit déjà mis sur le marché de telle manière que sa conformité avec les exigences applicables risque d'en être compromise, devrait être considéré comme le fabricant et, donc, assumer les obligations incombant à celui-ci.

(64) Pour des raisons de proportionnalité, les exigences en matière d'accessibilité ne devraient s'appliquer que dans la mesure où elles n'imposent pas de charge disproportionnée à l'opérateur économique concerné ou dans la mesure où elles n'exigent pas que des changements significatifs soient apportés aux produits et services qui entraîneraient leur modification fondamentale à la lumière de la présente directive. Des mécanismes de contrôle devraient néanmoins être mis en place afin de vérifier le droit aux dérogations à l'applicabilité des exigences en matière d'accessibilité.

(65) La présente directive devrait suivre le principe «penser en priorité aux PME» et tenir compte des charges administratives qui pèsent sur elles. Plutôt que de prévoir des exceptions et des dérogations généralisées pour ces entreprises, elle devrait fixer des règles souples en matière d'évaluation de la conformité et établir des clauses de sauvegarde pour les opérateurs économiques. Par conséquent, lors de la fixation des règles de sélection et d'application des procédures d'évaluation de la conformité les plus appropriées, il convient de tenir compte de la situation des PME et de limiter les obligations d'évaluer la conformité des exigences en matière d'accessibilité de telle manière qu'elles n'imposent pas de charge disproportionnée aux PME. De plus, les autorités de surveillance du marché devraient opérer de manière proportionnée à la taille des entreprises et au caractère de petite série ou hors série de la production concernée, sans créer d'obstacles inutiles pour les PME et sans compromettre la protection de l'intérêt public.

(66) Dans des cas exceptionnels, lorsque le respect des exigences en matière d'accessibilité énoncées dans la présente directive ferait peser une charge disproportionnée sur les opérateurs économiques, ceux-ci ne devraient être tenus de s'y conformer que dans des proportions telles qu'elles ne leur imposent pas une charge disproportionnée. Dans des cas dûment justifiés, il s'avérerait raisonnablement impossible à un opérateur économique d'appliquer pleinement une ou plusieurs des exigences en matière d'accessibilité énoncées dans la présente directive. Cependant, l'opérateur économique devrait rendre un service ou un produit relevant de la présente directive le plus accessible possible en se conformant à ces exigences dans des proportions telles qu'elles ne lui imposent pas une charge disproportionnée. Les exigences en matière d'accessibilité dont l'opérateur économique n'a pas estimé qu'elles imposent une charge disproportionnée devraient s'appliquer pleinement. Les exceptions au respect d'une ou plusieurs exigences en matière d'accessibilité en raison de la charge disproportionnée qu'elles imposent ne devraient pas excéder ce qui est strictement nécessaire pour limiter cette charge à l'égard du produit ou service particulier concerné dans tel ou tel cas. Les mesures qui imposeraient une charge disproportionnée sont des mesures qui imposeraient une charge organisationnelle ou financière supplémentaire excessive à un opérateur économique, compte tenu néanmoins des bénéfices probables susceptibles d'en résulter pour les personnes handicapées conformément aux critères fixés dans la présente directive. Des critères fondés sur ces considérations devraient être définis afin de permettre tant aux opérateurs économiques qu'aux autorités compétentes de comparer différentes situations et d'évaluer de manière systématique s'il existe ou non une charge disproportionnée. Seuls des raisons légitimes devraient être prises en compte pour évaluer la mesure dans laquelle il ne peut être satisfait aux exigences en matière d'accessibilité compte tenu de la charge disproportionnée qu'elles imposeraient. L'absence de priorité ou le manque de temps ou de connaissances ne devraient pas être réputés constituer des raisons légitimes.

(67) Le caractère disproportionné de la charge devrait être évalué de manière globale au moyen des critères énoncés à l'annexe VI. L'évaluation de la charge disproportionnée devrait être étayée par des preuves apportées par l'opérateur économique en tenant compte des critères pertinents. Les prestataires de services devraient renouveler leur évaluation tous les cinq ans au moins.

(68) Lorsqu'il a fait usage des dispositions de la présente directive relatives à la modification fondamentale et/ou à la charge disproportionnée, l'opérateur économique devrait en informer les autorités compétentes. Uniquement à la demande des autorités compétentes, l'opérateur économique devrait communiquer une copie de l'évaluation en expliquant pourquoi son produit ou service n'est pas totalement accessible et en fournissant des preuves du caractère disproportionné de la charge ou de la modification fondamentale, ou les deux.

(69) Si l'évaluation requise permet à un prestataire de services de conclure qu'exiger que tous les terminaux en libre-service qui sont utilisés pour la fourniture des services relevant de la présente directive, soient conformes aux exigences en matière d'accessibilité énoncées dans la présente directive ferait peser une charge disproportionnée, le prestataire de services devrait néanmoins appliquer ces exigences dans des proportions telles qu'elles ne lui imposent pas une charge disproportionnée. Par conséquent, les prestataires de services devraient évaluer la mesure dans laquelle un degré limité d'accessibilité de tous les terminaux en libre-service ou un nombre limité de terminaux en libre-service pleinement accessibles leur permettrait d'éviter une charge disproportionnée qui leur serait imposée autrement, et ils devraient être tenus de satisfaire aux exigences en matière d'accessibilité énoncées dans la présente directive uniquement dans cette mesure.

(70) Les microentreprises se distinguent de toutes les autres entreprises par le caractère limité de leurs ressources humaines, de leur chiffre d'affaires annuel ou de leur bilan annuel. La charge que constitue la conformité avec les exigences en matière d'accessibilité représenta donc en général pour les microentreprises une part plus élevée de leurs ressources humaines et financières que pour les autres entreprises et plus probablement une part disproportionnée des coûts. Une part importante des coûts pour les microentreprises est due aux documents et registres qui doivent être établis et conservés pour démontrer la conformité avec les différentes exigences prévues par le droit de l'Union. Si l'ensemble des opérateurs économiques auxquels s'applique la présente directive devraient être en mesure d'évaluer le caractère proportionné de la conformité avec les exigences en matière d'accessibilité énoncées dans la présente directive et ne devraient satisfaire à celles-ci que dans la mesure où elles ne sont pas disproportionnées, demander une telle évaluation aux microentreprises fournissant des services constituerait en soi une charge disproportionnée. Par conséquent, les exigences et obligations de la présente directive ne devraient pas s'appliquer aux microentreprises qui fournissent des services relevant du champ d'application de la présente directive.

(71) Afin de réduire la charge administrative, il convient que la présente directive prévoie des exigences et obligations moindres pour les microentreprises qui exercent leur activité dans le domaine de la fabrication, de l'importation ou de la distribution des produits relevant de son champ d'application.

(72) Si parmi les microentreprises, certaines sont exemptées des obligations de la présente directive, elles devraient toutes être encouragées à fabriquer, importer ou distribuer des produits et à fournir des services qui soient conformes aux exigences en matière d'accessibilité énoncées dans la présente directive, afin de renforcer leur compétitivité et leur potentiel de croissance sur le marché intérieur. Les États membres devraient par conséquent fournir des lignes directrices et des outils aux microentreprises pour faciliter l'application des mesures nationales transposant la présente directive.

(73) Tous les opérateurs économiques devraient agir de manière responsable et en totale conformité avec les exigences légales en vigueur lorsqu'ils mettent des produits sur le marché ou les mettent à disposition sur le marché, ou lorsqu'ils fournissent des services sur le marché.

(74) Afin de faciliter l'évaluation de la conformité avec les exigences applicables en matière d'accessibilité, il est nécessaire d'instaurer une présomption de conformité pour les produits et services qui répondent aux normes harmonisées volontaires adoptées conformément au règlement (UE) n° 1025/2012 du Parlement européen et du Conseil ([19]) aux fins de l'élaboration des spécifications techniques détaillées de ces exigences. La Commission a déjà adressé aux organismes européens de normalisation un certain nombre de demandes de normalisation portant sur l'accessibilité, telles que les mandats de normalisation M/376, M/473 et M/420, qui seraient pertinentes pour l'élaboration de normes harmonisées.

(75) Le règlement (UE) n° 1025/2012 prévoit une procédure pour la présentation d'objections formelles à l'encontre de normes harmonisées jugées non conformes aux exigences de la présente directive.

(76) Les normes européennes devraient être ajustées aux conditions du marché, tenir compte de l'intérêt public, ainsi que des objectifs clairement formulés dans la demande d'élaboration de normes harmonisées adressée par la Commission à un ou plusieurs organismes européens de normalisation, et s'appuyer sur un consensus. En l'absence de normes harmonisées et, si nécessaire, à des fins d'harmonisation du marché intérieur, la Commission devrait être en mesure d'adopter dans certains cas des actes d'exécution établissant des spécifications techniques pour les exigences en matière d'accessibilité prévues par la présente directive. Le recours à des spécifications techniques devrait être limité à ces cas. La Commission devrait être en mesure d'adopter des spécifications techniques, par exemple lorsque le processus de normalisation est bloqué faute de consensus entre les parties prenantes ou lorsque l'élaboration d'une norme harmonisée rencontre un retard injustifié, par exemple parce que la qualité requise n'est pas atteinte. La Commission devrait accorder suffisamment de temps entre l'adoption d'une demande d'élaboration de normes harmonisées adressée à un ou plusieurs organismes européens de normalisation et l'adoption d'une spécification technique liée à la même exigence en matière d'accessibilité. La Commission ne devrait être autorisée à adopter une spécification technique qu'après avoir essayé d'assurer la couverture des exigences en matière d'accessibilité par le système européen de normalisation, sauf lorsque la Commission peut démontrer que les spécifications techniques respectent les exigences énoncées à l'annexe II du règlement (UE) n° 1025/2012.

(77) En vue d'établir des normes harmonisées et des spécifications techniques respectant, de la manière la plus efficace, les exigences en matière d'accessibilité prévues par la présente directive pour les produits et les services, la Commission devrait, dans la mesure du possible, associer au processus les organisations faîtières européennes représentant les intérêts des personnes handicapées et toutes les autres parties prenantes.

([19]) Règlement (UE) n° 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, 98/34/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 n° 1673/2006/CE du Parlement européen et du Conseil (JO L 316 du 14.11.2012, p. 12).

(78) En vue de garantir un accès effectif aux informations à des fins de surveillance du marché, les informations requises pour pouvoir déclarer qu'un produit est conforme à tous les actes applicables de l'Union devraient être mises à disposition dans une seule déclaration UE de conformité. Il convient, pour que la charge administrative pesant sur eux soit réduite, que les opérateurs économiques soient en mesure d'inclure dans cette déclaration UE de conformité toutes les déclarations de conformité individuelles pertinentes.

(79) Pour l'évaluation de la conformité des produits, la présente directive devrait utiliser la procédure du contrôle interne de la fabrication du «module A», décrite à l'annexe II de la décision n° 768/2008/CE, dans la mesure où elle permet aux opérateurs économiques de démontrer, et aux autorités compétentes de garantir, que les produits mis à disposition sur le marché sont conformes aux exigences en matière d'accessibilité, sans pour autant leur imposer une charge indue.

(80) Lorsqu'elles effectuent la surveillance d'un produit sur le marché et qu'elles vérifient la conformité d'un service, les autorités devraient également vérifier les évaluations de conformité, y compris si l'évaluation pertinente d'une modification fondamentale ou d'une charge disproportionnée a été correctement réalisée. Les autorités devraient s'acquitter de leurs obligations en coopération avec des personnes handicapées et les organisations qui les représentent, ainsi que leurs intérêts.

(81) Pour les services, il convient que les informations nécessaires à l'évaluation de la conformité avec les exigences en matière d'accessibilité énoncées dans la présente directive, soient fournies dans les conditions générales ou un document équivalent sans préjudice de la directive 2011/83/UE du Parlement européen et du Conseil ([20]).

(82) Le marquage CE, qui matérialise la conformité d'un produit avec les exigences en matière d'accessibilité prévues par la présente directive, est le résultat visible d'un processus global comprenant l'évaluation de la conformité au sens large. Il convient que la présente directive respecte les principes généraux régissant le marquage CE établis dans le règlement (CE) n° 765/2008 du Parlement européen et du Conseil ([21]) fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits. En plus de la déclaration de conformité UE, le fabricant devrait informer les consommateurs, à moindre coût, de l'accessibilité de ses produits.

(83) Conformément au règlement (CE) n° 765/2008, en apposant le marquage CE sur un produit, le fabricant déclare que celui-ci est conforme à toutes les exigences applicables en matière d'accessibilité et qu'il en assume l'entière responsabilité.

(84) Conformément à la décision n° 768/2008/CE, en ce qui concerne les produits, il incombe aux États membres de veiller à une surveillance du marché rigoureuse et efficace sur leur territoire, et ils devraient doter les autorités qui en ont la charge des moyens et des ressources nécessaires à cette fin.

(85) Les États membres devraient vérifier si les services sont conformes aux obligations de la présente directive et assurer le suivi des plaintes ou des rapports concernant les cas de non-conformité afin de garantir que des mesures correctives ont été prises.

(86) La Commission pourrait, s'il y a lieu, adopter, en concertation avec les parties intéressées, des lignes directrices non contraignantes contribuant à la coordination entre les autorités de surveillance du marché et les autorités chargées de vérifier la conformité des services. La Commission et les États membres devraient pouvoir mettre en place des initiatives en vue de partager les ressources et l'expertise des autorités.

(87) Les États membres devraient veiller à ce que les autorités de surveillance du marché et les autorités chargées de la conformité des services contrôlent si les opérateurs économiques ont respecté les critères énoncés à l'annexe VI, conformément aux chapitres VIII et IX. Les États membres devraient pouvoir désigner un organisme spécialisé chargé d'exécuter les obligations incombant aux autorités de surveillance du marché ou aux autorités chargées de la conformité des services au titre de la présente directive. Les États membres devraient pouvoir décider que les compétences d'un tel organisme devraient être limitées au champ d'application de la présente directive ou à certaines parties de celui-ci, sans préjudice des obligations incombant aux États membres au titre du règlement (CE) n° 765/2008.

([20]) Directive 2011/83/UE du Parlement européen et du Conseil du 25 octobre 2011 relative aux droits des consommateurs, modifiant la directive 93/13/CEE du Conseil et la directive 1999/44/CE du Parlement européen et du Conseil et abrogeant la directive 85/577/CEE du Conseil et la directive 97/7/CE du Parlement européen et du Conseil (JO L 304 du 22.11.2011, p. 64).

([21]) Règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93 du Conseil (JO L 218 du 13.8.2008, p. 30).

(88) Il convient d'instaurer une procédure de sauvegarde qui s'appliquerait en cas de désaccord entre les États membres sur les mesures prises par un État membre et qui permettent aux parties intéressées d'être informées des mesures qu'il est envisagé de prendre à l'égard des produits non conformes aux exigences en matière d'accessibilité prévues par la présente directive. La procédure de sauvegarde devrait également permettre aux autorités de surveillance du marché, en coopération avec les opérateurs économiques concernés, d'agir à un stade plus précoce en ce qui concerne ces produits.

(89) Lorsqu'il y a accord entre les États membres et la Commission quant au bien-fondé d'une mesure prise par un État membre, une intervention de la Commission ne devrait plus être nécessaire, sauf dans les cas où la non-conformité peut être attribuée aux lacunes dans les normes harmonisées ou les spécifications techniques.

(90) Les directives 2014/24/UE ([22]) et 2014/25/UE ([23]) du Parlement européen et du Conseil sur la passation des marchés publics, qui définissent des procédures pour la passation des marchés publics et les concours applicables à certains travaux, fournitures (produits) et services, établissent que, pour tous les marchés de travaux, fournitures ou services destinés à être utilisés par des personnes physiques, qu'il s'agisse du grand public ou du personnel du pouvoir adjudicateur, les spécifications techniques doivent être élaborées, sauf dans des cas dûment justifiés, de façon à tenir compte des critères d'accessibilité pour les personnes handicapées ou de la notion de conception pour tous les utilisateurs. En outre, ces directives exigent en outre que lorsque des exigences d'accessibilité contraignantes ont été arrêtées par un acte juridique de l'Union, les spécifications techniques soient définies par référence à ces normes en ce qui concerne les critères d'accessibilité pour les personnes handicapées ou la notion de conception pour tous les utilisateurs. La présente directive devrait établir des exigences d'accessibilité contraignantes pour les produits et services relevant de son champ d'application. Pour les produits et services ne relevant pas de son champ d'application, les exigences en matière d'accessibilité énoncées dans la présente directive ne sont pas contraignantes. Toutefois, l'application de ces exigences d'accessibilité pour respecter les obligations pertinentes énoncées dans des actes de l'Union autres que la présente directive faciliterait la mise en œuvre de l'accessibilité et contribuerait à la sécurité juridique et au rapprochement des exigences en matière d'accessibilité dans l'Union. Il convient de ne pas empêcher les autorités d'établir des exigences en matière d'accessibilité allant au-delà de celles qui sont énoncées à l'annexe I de la présente directive.

(91) La présente directive ne devrait pas modifier la nature obligatoire ou facultative des dispositions en matière d'accessibilité qui figurent dans d'autres actes de l'Union.

(92) La présente directive ne devrait s'appliquer qu'aux procédures de passation de marchés pour lesquelles l'avis d'appel à la concurrence a été envoyé, ou, s'il n'est pas prévu d'en envoyer un, qui ont été entamées par le pouvoir adjudicateur après la date de mise en application de la présente directive.

(93) Afin d'assurer la bonne application de la présente directive, le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne devrait être délégué à la Commission pour: préciser davantage les exigences en matière d'accessibilité qui, de façon intrinsèque, ne peuvent produire leurs effets escomptés à moins de faire l'objet de précisions complémentaires dans des actes juridiques contraignants de l'Union; modifier la période durant laquelle les opérateurs économiques doivent être en mesure d'identifier tout opérateur économique qui leur a fourni un produit ou tout opérateur économique auquel ils ont fourni un produit; et préciser de manière plus détaillée les critères pertinents que l'opérateur économique doit prendre en compte pour évaluer si la conformité avec les exigences en matière d'accessibilité imposerait une charge disproportionnée. 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» ([24]). 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.

(94) Afin d'assurer des conditions uniformes d'exécution de la présente directive, il convient de conférer des compétences d'exécution à la Commission en ce qui concerne les spécifications techniques. Ces compétences devraient être exercées en conformité avec le règlement (UE) n° 182/2011 du Parlement européen et du Conseil ([25]).

([22]) Directive 2014/24/UE du Parlement européen et du Conseil du 26 février 2014 sur la passation des marchés publics et abrogeant la directive 2004/18/CE (JO L 94 du 28.3.2014, p. 65).

([23]) Directive 2014/25/UE du Parlement européen et du Conseil du 26 février 2014 relative à la passation de marchés par des entités opérant dans les secteurs de l'eau, de l'énergie, des transports et des services postaux et abrogeant la directive 2004/17/CE (JO L 94 du 28.3.2014, p. 243).

([24]) JO L 123 du 12.5.2016, p. 1.

([25]) Règlement (UE) n° 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).

(95) Les États membres devraient veiller à ce que des moyens adéquats et efficaces existent pour assurer le respect de la présente directive et ils devraient dès lors mettre en place des mécanismes de contrôle appropriés, tels que des contrôles a posteriori par les autorités de surveillance du marché, afin de vérifier que la dérogation à l'application des exigences en matière d'accessibilité est justifiée. Lors du traitement de plaintes en matière d'accessibilité, les États membres devraient se conformer au principe général de bonne administration et, en particulier, à l'obligation des fonctionnaires de veiller à ce qu'une décision soit prise pour chaque plainte dans un délai raisonnable.

(96) Afin de faciliter la mise en œuvre uniforme de la présente directive, la Commission devrait établir un groupe de travail réunissant les autorités concernées et les parties prenantes pour faciliter l'échange d'informations et de bonnes pratiques et pour fournir des conseils. Il convient d'encourager la coopération entre les autorités et les parties prenantes, y compris les personnes handicapées et les organisations qui les représentent, notamment pour améliorer la cohérence de l'application des dispositions de la présente directive relatives aux exigences d'accessibilité et de surveiller la mise en œuvre de ses dispositions sur les modifications fondamentales et les charges disproportionnées.

(97) Compte tenu du cadre juridique existant en ce qui concerne les recours dans les domaines relevant des directives 2014/24/UE et 2014/25/UE, les dispositions de la présente directive relatives aux mesures d'exécution et aux sanctions ne devraient pas s'appliquer aux procédures de passation de marchés publics soumises aux obligations fixées par la présente directive. Une telle exclusion est sans préjudice de l'obligation que les traités font aux États membres de prendre toutes les mesures nécessaires pour garantir l'application et l'efficacité du droit de l'Union.

(98) Les sanctions devraient être adaptées à la nature des violations et aux circonstances afin qu'elles ne se substituent pas au respect, par les opérateurs économiques, de leurs obligations de rendre leurs produits ou leurs services accessibles.

(99) Les États membres devraient veiller à ce que, conformément à la législation de l'Union en vigueur, d'autres mécanismes de règlement des différends soient en place pour permettre la résolution de toute allégation de non-conformité avec les dispositions de la présente directive avant que les tribunaux ou les organes administratifs compétents ne soient saisis.

(100) Conformément à la déclaration politique commune du 28 septembre 2011 des États membres et de la Commission sur les documents explicatifs ([26]), les États membres se sont engagés à veiller, dans des cas justifiés, à ce que la notification de leurs mesures de transposition s'accompagne d'un ou de plusieurs documents expliquant le lien entre les éléments d'une directive et les parties correspondantes des instruments nationaux de transposition. En ce qui concerne la présente directive, le législateur estime que la transmission de ces documents est justifiée.

(101) Afin de donner aux prestataires de services suffisamment de temps pour s'adapter aux exigences de la présente directive, il est nécessaire de prévoir une période de transition de cinq ans après la date d'application de la présente directive, pendant laquelle les produits utilisés pour la fourniture d'un service qui ont été mis sur le marché avant cette date ne doivent pas nécessairement être conformes aux exigences en matière d'accessibilité au titre de la présente directive, sauf s'ils sont remplacés par les prestataires de services pendant la période de transition. Compte tenu du coût et de la durée importante du cycle de vie des terminaux en libre-service, il convient de prévoir que, lorsqu'ils sont utilisés pour la fourniture de services, ces terminaux puissent continuer à être utilisés jusqu'à la fin de leur durée de vie économique pour autant qu'ils ne soient pas remplacés au cours de cette période, qui ne doit toutefois pas dépasser vingt ans.

(102) Les exigences en matière d'accessibilité énoncées dans la présente directive devraient s'appliquer aux produits mis sur le marché et aux services fournis après la date d'application des mesures nationales transposant la présente directive, y compris les produits usagés et d'occasion importés d'un pays tiers et mis sur le marché après cette date.

(103) La présente directive respecte les droits fondamentaux et observe les principes consacrés notamment par la Charte des droits fondamentaux de l'Union européenne (ci-après dénommée la «Charte»). Elle vise en particulier à assurer le plein respect du droit des personnes handicapées de bénéficier de mesures visant à assurer leur autonomie, leur intégration sociale et professionnelle et leur participation à la vie de la communauté, et à promouvoir l'application des articles 21, 25 et 26 de la Charte.

(104) Étant donné que l'objectif de la présente directive, à savoir l'élimination des obstacles à la libre circulation de certains produits et services accessibles en vue de contribuer au bon fonctionnement du marché intérieur, ne peut pas être atteint de manière suffisante par les États membres car il requiert l'harmonisation des différentes règles actuellement en vigueur dans leurs systèmes juridiques respectifs, mais peut, en définissant des exigences et des règles communes en matière d'accessibilité pour le fonctionnement du marché intérieur, être mieux atteint au niveau de l'Union, celle-ci peut prendre des mesures, conformément au principe de subsidiarité énoncé 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,

([26]) JO C 369 du 17.12.2011, p. 14.

ONT ADOPTÉ LA PRÉSENTE DIRECTIVE:

CHAPITRE I

Dispositions générales

Article premier

Objet

La présente directive a pour objet de contribuer au bon fonctionnement du marché intérieur en rapprochant les dispositions législatives, réglementaires et administratives des États membres en ce qui concerne les exigences en matière d'accessibilité applicables à certains produits et services, grâce, notamment, à l'élimination et à la prévention des obstacles, qui entravent la libre circulation des produits et des services relevant de la présente directive, découlant d'exigences divergentes en matière d'accessibilité dans les États membres.

Article 2

Champ d'application

1. La présente directive s'applique aux produits ci-après, mis sur le marché après le 28 juin 2025:

a) systèmes informatiques matériels à usage général du grand public et systèmes d'exploitation relatifs à ces systèmes matériels;

b) terminaux en libre-service ci-après:

   i) terminaux de paiement;

   ii) terminaux en libre-service ci-après, destinés à la fourniture de services relevant de la présente directive:

      — guichets de banque automatiques,

      — distributeurs automatiques de titres de transport,

      — bornes d'enregistrement automatiques,

      — terminaux en libre-service interactifs fournissant des informations, à l'exclusion des terminaux installés en tant que parties intégrantes de véhicules, d'aéronefs, de navires ou de matériel roulant;

c) équipements terminaux grand public avec des capacités informatiques interactives, utilisés pour les services de communications électroniques;

d) équipements terminaux grand public avec des capacités informatiques interactives, utilisés pour accéder à des services de médias audiovisuels; et

e) liseuses numériques.

2. Sans préjudice de l'article 32, la présente directive s'applique aux services ci-après, fournis aux consommateurs après le 28 juin 2025:

a) services de communications électroniques, à l'exception des services de transmission utilisés pour la fourniture de services de machine à machine;

b) services fournissant un accès à des services de médias audiovisuels;

c) éléments ci-après de services de transport aérien, ferroviaire, par voie de navigation intérieure et par autobus de voyageurs et de passagers, à l'exception des services de transport urbains, suburbains et régionaux, pour lesquels seuls les éléments visés au point v) s'appliquent:

   i) sites internet;

   ii) services intégrés sur appareils mobiles, y compris les applications mobiles;

   iii) billets électroniques et services de billetterie électronique;

   iv) fourniture d'informations sur les services de transport, notamment d'informations en temps réel sur le voyage. En ce qui concerne les écrans d'information, ne sont concernés que les écrans interactifs situés sur le territoire de l'Union; et

v) terminaux en libre-service interactifs situés sur le territoire de l'Union, à l'exception de ceux installés en tant que parties intégrantes de véhicules, d'aéronefs, de navires et de matériel roulant utilisés pour fournir tout élément de ces services de transport de voyageurs et de passagers;

d) services bancaires aux consommateurs;

e) livres numériques et logiciels spécialisés; et

f) commerce électronique.

3. La présente directive s'applique à la réception des communications d'urgence dirigées vers le numéro d'urgence unique européen «112».

4. La présente directive ne s'applique pas aux contenus suivants des sites internet et des applications mobiles:

a) médias temporels préenregistrés publiés avant le 28 juin 2025;

b) formats de fichiers bureautiques publiés avant le 28 juin 2025;

c) cartes et services de cartographie en ligne, si les informations essentielles sont fournies sous une forme numérique accessible pour ce qui concerne les cartes destinées à la navigation;

d) contenus de tiers qui ne sont ni financés ni développés par l'opérateur économique concerné, et qui ne sont pas sous le contrôle de cet opérateur;

e) contenu des sites internet et des applications mobiles qui sont considérés comme des archives, à savoir qu'ils ne présentent que des contenus qui ne sont pas actualisés ou modifiés après le 28 juin 2025.

5. La présente directive est sans préjudice de la directive (UE) 2017/1564 et du règlement (UE) 2017/1563.

Article 3

Définitions

Aux fins de la présente directive, on entend par:

1) «personnes handicapées»: les personnes qui présentent une incapacité physique, mentale, intellectuelle ou sensorielle durable dont l'interaction avec diverses barrières peut faire obstacle à leur pleine et effective participation à la société sur la base de l'égalité avec les autres;

2) «produit»: une substance, une préparation ou une marchandise produite par un procédé de fabrication, à l'exclusion des denrées alimentaires, des aliments pour animaux, des plantes et animaux vivants, des produits d'origine humaine et des produits de plantes et d'animaux se rapportant directement à leur reproduction future;

3) «service»: un service tel que défini à l'article 4, point 1), de la directive 2006/123/CE du Parlement européen et du Conseil ([27]);

4) «prestataire de services»: toute personne physique ou morale qui fournit un service sur le marché de l'Union ou propose de fournir un service aux consommateurs dans l'Union;

5) «services de médias audiovisuels»: les services tels que définis à l'article 1er, paragraphe 1, point a), de la directive 2010/13/UE;

6) «services fournissant un accès à des services de médias audiovisuels»: les services transmis au moyen de réseaux de communications électroniques qui sont utilisés pour identifier et sélectionner les services de médias audiovisuels, recevoir des informations sur ces services et consulter ces services et tous les éléments fournis, tels que le sous-titrage pour les personnes sourdes ou malentendantes, l'audiodescription, le sous-titrage audio et l'interprétation en langue des signes, découlant de la mise en œuvre des mesures destinées à rendre ces services accessibles comme prévu à l'article 7 de la directive 2010/13/UE; et cela inclut les guides électroniques de programme (GEP);

7) «équipement terminal grand public avec des capacités informatiques interactives utilisé pour accéder à des services de médias audiovisuels»: tout équipement dont la finalité principale est de fournir un accès à des services de médias audiovisuels;

([27]) Directive 2006/123/CE du Parlement européen et du Conseil du 12 décembre 2006 relative aux services dans le marché intérieur (JO L 376 du 27.12.2006, p. 36).

8) «service de communications électroniques»: un service de communications électroniques tel que défini à l'article 2, point 4), de la directive (UE) 2018/1972;

9) «service de conversation totale»: un service de conversation totale tel que défini à l'article 2, point 35), de la directive (UE) 2018/1972;

10) «centre de réception des appels d'urgence» ou «PSAP»: un centre de réception des appels d'urgence ou PSAP tel que défini à l'article 2, point 36), de la directive (UE) 2018/1972;

11) «PSAP le plus approprié»: le PSAP le plus approprié tel que défini à l'article 2, point 37), de la directive (UE) 2018/1972;

12) «communication d'urgence»: une communication d'urgence telle que définie à l'article 2, point 38), de la directive (UE) 2018/1972;

13) «service d'urgence»: un service d'urgence tel que défini à l'article 2, point 39), de la directive (UE) 2018/1972;

14) «texte en temps réel»: une forme de conversation textuelle point-à-point ou multipoint où le texte qui est saisi est transmis caractère par caractère, de sorte que la communication est perçue par l'utilisateur comme continue;

15) «mise à disposition sur le marché»: toute fourniture d'un produit destiné à être distribué, consommé ou utilisé sur le marché de l'Union dans le cadre d'une activité commerciale, à titre onéreux ou gratuit;

16) «mise sur le marché»: la première mise à disposition d'un produit sur le marché de l'Union;

17) «fabricant»: toute personne physique ou morale qui fabrique, ou fait concevoir ou fabriquer un produit, et le commercialise sous son propre nom ou sa propre marque;

18) «mandataire»: toute personne physique ou morale établie dans l'Union ayant reçu un mandat écrit du fabricant pour agir en son nom aux fins de l'accomplissement de tâches déterminées;

19) «importateur»: toute personne physique ou morale établie dans l'Union qui met un produit provenant d'un pays tiers sur le marché de l'Union;

20) «distributeur»: toute personne physique ou morale faisant partie de la chaîne d'approvisionnement, autre que le fabricant ou l'importateur, qui met un produit à disposition sur le marché;

21) «opérateur économique»: le fabricant, le mandataire, l'importateur, le distributeur ou le prestataire de services;

22) «consommateur»: toute personne physique qui achète un produit concerné ou bénéficie d'un service concerné à des fins étrangères à son activité commerciale, industrielle, artisanale ou libérale;

23) «microentreprise»: une entreprise qui emploie moins de dix personnes et dont le chiffre d'affaires annuel n'excède pas 2 000 000 EUR ou dont le total du bilan annuel n'excède pas 2 000 000 EUR;

24) «petites et moyennes entreprises» ou «PME»: les entreprises qui emploient moins de 250 personnes et dont le chiffre d'affaires annuel n'excède pas 50 000 000 EUR ou dont le total du bilan annuel n'excède pas 43 000 000 EUR, à l'exclusion des microentreprises;

25) «norme harmonisée»: une norme harmonisée telle que définie à l'article 2, point 1) c), du règlement (UE) n° 1025/2012;

26) «spécification technique»: une spécification technique telle que définie à l'article 2, point 4), du règlement (UE) n° 1025/2012 qui précise les exigences à respecter en matière d'accessibilité applicables à un produit ou un service;

27) «retrait»: toute mesure visant à empêcher la mise à disposition sur le marché d'un produit présent dans la chaîne d'approvisionnement;

28) «services bancaires aux consommateurs»: la fourniture aux consommateurs des services bancaires et financiers ci-après:

a) les contrats de crédit régis par la directive 2008/48/CE du Parlement européen et du Conseil ([28]) ou par la directive 2014/17/UE du Parlement européen et du Conseil ([29]);

b) les services tels que définis aux points 1, 2, 4 et 5 de la section A et aux points 1, 2, 4 et 5 de la section B de l'annexe I de la directive 2014/65/UE du Parlement européen et du Conseil ([30]);

c) les services de paiement tels que définis à l'article 4, point 3), de la directive (UE) 2015/2366 du Parlement européen et du Conseil ([31]);

d) les services liés aux comptes de paiement tels qu'il sont définis à l'article 2, point 6), de la directive 2014/92/UE du Parlement européen et du Conseil ([32]); et

e) la monnaie électronique telle qu'elle est définie à l'article 2, point 2), de la directive 2009/110/CE du Parlement européen et du Conseil ([33]);

29) «terminal de paiement»: un appareil dont la finalité principale est de permettre de faire des paiements au moyen d'instruments de paiement tels que définis à l'article 4, point 14), de la directive (UE) 2015/2366, dans un point de vente physique et non dans un environnement virtuel;

30) «services de commerce électronique»: des services fournis à distance, via des sites internet, des services intégrés sur des appareils mobiles, par voie électronique et à la demande individuelle d'un consommateur, en vue de conclure un contrat de consommation;

31) «services de transport aérien de passagers»: les services commerciaux de transport aérien de passagers, tels qu'ils sont définis à l'article 2, point l), du règlement (CE) n° 1107/2006, au départ d'un aéroport, en transit par un aéroport ou à l'arrivée dans un aéroport, lorsque celui-ci est situé sur le territoire d'un État membre, y compris les vols au départ d'un aéroport situé dans un pays tiers à destination d'un aéroport situé sur le territoire d'un État membre lorsque les services sont assurés par des transporteurs aériens de l'Union;

32) «services de transport de passagers par autobus»: les services relevant de l'article 2, paragraphes 1 et 2, du règlement (UE) n° 181/2011;

33) «services de transport ferroviaire de voyageurs»: tous les services de transport ferroviaire de voyageurs visés à l'article 2, paragraphe 1, du règlement (CE) n° 1371/2007, à l'exception des services visés à l'article 2, paragraphe 2, dudit règlement;

34) «services de transport de passagers par voie de navigation intérieure»: les services de transport de passagers relevant de l'article 2, paragraphe 1, du règlement (UE) n° 1177/2010, à l'exception des services visés à l'article 2, paragraphe 2, dudit règlement;

35) «services de transport urbains et suburbains»: les services urbains ou suburbains, tels qu'ils sont définis à l'article 3, point 6), de la directive 2012/34/UE du Parlement européen et du Conseil ([34]), mais aux fins de la présente directive, ce terme ne couvre que les modes de transport suivants: chemin de fer, autobus et autocar, métro, tramway et trolleybus;

([28]) Directive 2008/48/CE du Parlement européen et du Conseil du 23 avril 2008 concernant les contrats de crédit aux consommateurs et abrogeant la directive 87/102/CEE du Conseil (JO L 133 du 22.5.2008, p. 66).

([29]) Directive 2014/17/UE du Parlement européen et du Conseil du 4 février 2014 sur les contrats de crédit aux consommateurs relatifs aux biens immobiliers à usage résidentiel et modifiant les directives 2008/48/CE et 2013/36/UE et le règlement (UE) n° 1093/2010 (JO L 60 du 28.2.2014, p. 34).

([30]) Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE (JO L 173 du 12.6.2014, p. 349).

([31]) Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et abrogeant la directive 2007/64/CE (JO L 337 du 23.12.2015, p. 35).

([32]) Directive 2014/92/UE du Parlement européen et du Conseil du 23 juillet 2014 sur la comparabilité des frais liés aux comptes de paiement, le changement de compte de paiement et l'accès à un compte de paiement assorti de prestations de base (JO L 257 du 28.8.2014, p. 214).

([33]) Directive 2009/110/CE du Parlement européen et du Conseil du 16 septembre 2009 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements, modifiant les directives 2005/60/CE et 2006/48/CE et abrogeant la directive 2000/46/CE (JO L 267 du 10.10.2009, p. 7).

([34]) Directive 2012/34/UE du Parlement européen et du Conseil du 21 novembre 2012 établissant un espace ferroviaire unique européen (JO L 343 du 14.12.2012, p. 32).

36) «services de transport régionaux»: les services régionaux, tels que définis à l'article 3, point 7), de la directive 2012/34/UE, mais aux fins de la présente directive, ce terme ne couvre que les modes de transport suivants: chemin de fer, autobus et autocar, métro, tramway et trolleybus;

37) «technologies d'assistance»: tout objet, pièce d'équipement, service ou système produit, y compris un logiciel, qui sert à accroître, à préserver, à remplacer ou à améliorer les capacités fonctionnelles des personnes handicapées, ou à atténuer et compenser les déficiences, les limitations d'activité ou les restrictions de participation;

38) «système d'exploitation»: un logiciel qui, notamment, gère l'interface du matériel périphérique, planifie des tâches, alloue de l'espace de stockage et présente une interface par défaut à l'utilisateur lorsque aucun programme d'application ne s'exécute, y compris une interface utilisateur graphique, que ce logiciel fasse partie intégrante d'un matériel informatique à usage général du grand public ou soit un logiciel autonome destiné à être exécuté sur un matériel informatique à usage général du grand public, mais à l'exclusion des chargeurs de systèmes d'exploitation, des systèmes d'entrée-sortie de base ou d'autres micrologiciels nécessaires au moment du démarrage ou lors de l'installation du système d'exploitation;

39) «système informatique matériel à usage général du grand public»: la combinaison de matériels formant un ordinateur complet, qui se caractérise par sa nature polyvalente et sa capacité à réaliser, avec les logiciels appropriés, la plupart des opérations informatiques courantes demandées par les consommateurs et qui est destinée à être utilisée par les consommateurs, y compris les ordinateurs individuels, en particulier les ordinateurs de bureau, les ordinateurs portables, les smartphones et les tablettes;

40) «capacité informatique interactive»: une fonctionnalité facilitant l'interaction entre l'utilisateur et l'appareil qui permet le traitement et la transmission de données, de la voix ou de la vidéo ou toute combinaison de celles-ci;

41) «livre numérique et logiciel spécialisé»: un service consistant à fournir des fichiers numériques transmettant une version électronique d'un livre, auquel l'utilisateur peut avoir accès, dans lequel il peut naviguer et qu'il peut lire et utiliser, ainsi que le logiciel, y compris les services intégrés sur appareils mobiles, y compris les applications mobiles, spécialisé pour l'accès à ces fichiers numériques, la navigation à l'intérieur de ceux-ci, leur lecture et leur utilisation, à l'exclusion des logiciels visés dans la définition figurant au point 42);

42) «liseuse numérique»: un équipement spécialisé, comprenant tant le matériel que le logiciel, utilisé pour accéder à des fichiers de livres numériques, naviguer à l'intérieur de ceux-ci, les lire et les utiliser;

43) «billet électronique»: tout système dans lequel un droit de voyager, sous la forme de titres de transport simples ou multiples, d'abonnements ou de crédit de voyage, est stocké sous forme électronique sur une carte de transport physique ou un autre dispositif, au lieu d'être imprimé sur papier;

44) «services de billetterie électronique»: tout système dans lequel des titres de transport de voyageurs et de passagers sont achetés notamment en ligne, au moyen d'un appareil doté de capacités informatiques interactives, et fournis à l'acheteur sous forme électronique, pour leur permettre d'être imprimés sur papier ou affichés pendant le voyage sur un appareil mobile doté de capacités informatiques interactives.

CHAPITRE II

Exigences en matière d'accessibilité et libre circulation

Article 4

Exigences en matière d'accessibilité

1. Les États membres veillent, conformément aux paragraphes 2, 3 et 5 du présent article, et sous réserve de l'article 14, à ce que les opérateurs économiques ne mettent sur le marché que les produits, et ne fournissent que les services, qui sont conformes aux exigences en matière d'accessibilité prévues à l'annexe I.

2. Tous les produits, sont conformes aux exigences en matière d'accessibilité prévues à l'annexe I, section I.

Tous les produits, à l'exception des terminaux en libre-service, sont conformes aux exigences en matière d'accessibilité prévues à l'annexe I, section II.

3. Sans préjudice du paragraphe 5, à l'exception des services de transport urbains et suburbains et des services de transport régionaux, tous les services, sont conformes aux exigences en matière d'accessibilité prévues à l'annexe I, section III.

Sans préjudice du paragraphe 5, tous les services, sont conformes aux exigences en matière d'accessibilité prévues à l'annexe I, section IV.

4. Les États membres peuvent décider, compte tenu des circonstances nationales, que l'environnement bâti utilisé par les clients de services relevant de la présente directive doive être conforme aux exigences en matière d'accessibilité prévues à l'annexe III, de manière à garantir une utilisation optimale par les personnes handicapées.

5. Les microentreprises qui proposent des services sont exonérées de l'obligation de se conformer aux exigences en matière d'accessibilité visées au paragraphe 3 du présent article et de toutes obligations relatives à la conformité avec ces exigences.

6. Les États membres fournissent des lignes directrices et des outils aux microentreprises pour faciliter l'application des mesures nationales transposant la présente directive. Les États membres élaborent ces outils en consultation avec les parties prenantes concernées.

7. Les États membres peuvent fournir aux opérateurs économiques les exemples indicatifs, figurant à l'annexe II, de solutions possibles pour contribuer au respect des exigences en matière d'accessibilité énoncées à l'annexe I.

8. Les États membres veillent à ce que la réception des communications d'urgence dirigées vers le numéro d'urgence unique européen «112», par le PSAP le plus approprié, soit conforme aux exigences spécifiques en matière d'accessibilité prévues à l'annexe I, section V, de la façon la mieux adaptée à l'organisation nationale des systèmes d'urgence.

9. La Commission est habilitée à adopter des actes délégués conformément à l'article 26 pour compléter l'annexe I en précisant davantage les exigences en matière d'accessibilité qui, de façon intrinsèque, ne peuvent produire leurs effets escomptés à moins de faire l'objet de précisions complémentaires dans des actes juridiques contraignants de l'Union, telles que les exigences relatives à l'interopérabilité.

Article 5

Droit de l'Union en vigueur dans le domaine du transport de passagers et de voyageurs

Les services conformes aux exigences concernant la fourniture d'informations accessibles et la fourniture d'informations relatives à l'accessibilité prévues par les règlements (CE) n° 261/2004, (CE) n° 1107/2006, (CE) n° 1371/2007, (UE) n° 1177/2010 et (UE) n° 181/2011 et les actes pertinents adoptés sur la base de la directive 2008/57/CE sont réputés conformes aux exigences correspondantes prévues par la présente directive. Lorsque la présente directive prévoit des exigences supplémentaires à celles prévues dans ces règlements et ces actes, celles-ci s'appliquent dans leur intégralité.

Article 6

Libre circulation

Les États membres ne font pas obstacle, pour des raisons liées aux exigences en matière d'accessibilité, à la mise à disposition sur le marché, sur leur territoire, des produits ou à la fourniture, sur leur territoire, des services qui sont conformes à la présente directive.

Chapitre III

Obligations des opérateurs économiques dans le secteur des produits

Article 7

Obligations des fabricants

1. Les fabricants s'assurent, lorsqu'ils mettent leurs produits sur le marché, que ceux-ci ont été conçus et fabriqués conformément à toutes les exigences applicables en matière d'accessibilité prévues par la présente directive.

2. Les fabricants établissent la documentation technique conformément à l'annexe IV et mettent ou font mettre en œuvre la procédure d'évaluation de la conformité prévue à ladite annexe.

Lorsqu'il a été démontré, à l'aide de cette procédure, qu'un produit respecte les exigences applicables en matière d'accessibilité, les fabricants établissent une déclaration UE de conformité et apposent le marquage CE.

3. Les fabricants conservent la documentation technique et la déclaration UE de conformité pendant cinq ans après que le produit a été mis sur le marché.

4. Les fabricants veillent à ce que des procédures soient en place pour garantir le maintien de la conformité de la production en série à la présente directive. Il est dûment tenu compte de toute modification dans la conception ou les caractéristiques du produit ainsi que de toute modification des normes harmonisées, ou des spécifications techniques, par rapport auxquelles la conformité d'un produit est déclarée.

5. Les fabricants veillent à ce que leurs produits portent un numéro de type, de lot ou de série ou tout autre élément permettant leur identification ou, lorsque la taille ou la nature du produit ne le permet pas, à ce que l'information requise soit fournie sur l'emballage ou dans un document accompagnant le produit.

6. Les fabricants indiquent leur nom, raison sociale ou marque déposée, ainsi que l'adresse à laquelle ils peuvent être contactés, sur le produit ou, lorsque cela n'est pas possible, sur son emballage ou dans un document accompagnant le produit. L'adresse doit préciser un point unique auquel le fabricant peut être contacté. Les coordonnées sont indiquées dans une langue aisément compréhensible par les utilisateurs finals et les autorités de surveillance du marché.

7. Les fabricants veillent à ce que le produit soit accompagné d'instructions et d'informations de sécurité fournies dans une langue aisément compréhensible par les consommateurs et autres utilisateurs finals, déterminée par l'État membre concerné. Ces instructions et ces informations, ainsi que tout étiquetage, sont clairs, compréhensibles et intelligibles.

8. Les fabricants qui considèrent ou ont des raisons de croire qu'un produit qu'ils ont mis sur le marché n'est pas conforme à la présente directive prennent immédiatement les mesures correctives nécessaires pour le mettre en conformité ou, le cas échéant, pour le retirer. En outre, lorsque le produit n'est pas conforme aux exigences en matière d'accessibilité énoncées dans la présente directive, les fabricants en informent immédiatement les autorités nationales compétentes des États membres dans lesquels ils ont mis le produit à disposition, en fournissant des précisions, notamment, sur la non-conformité et sur toute mesure corrective prise. Dans de tels cas, les fabricants tiennent un registre des produits non conformes aux exigences applicables en matière d'accessibilité et des plaintes y afférentes.

9. Sur demande motivée d'une autorité nationale compétente, les fabricants lui communiquent toutes les informations et tous les documents nécessaires pour démontrer la conformité du produit, dans une langue aisément compréhensible par cette autorité. Ils coopèrent avec l'autorité en question, à sa demande, à toute mesure prise en vue d'éliminer la non-conformité avec les exigences applicables en matière d'accessibilité des produits qu'ils ont mis sur le marché, notamment en mettant les produits en conformité avec lesdites exigences.

Article 8

Représentants autorisés

1. Le fabricant peut désigner un mandataire par un mandat écrit.

Les obligations prévues à l'article 7, paragraphe 1, et l'établissement de la documentation technique ne font pas partie de son mandat.

2. Le mandataire exécute les tâches indiquées dans le mandat reçu du fabricant. Le mandat autorise au minimum le mandataire:

a) à tenir la déclaration UE de conformité et la documentation technique à la disposition des autorités de surveillance du marché pendant cinq ans;

b) sur demande motivée d'une autorité nationale compétente, à lui communiquer toutes les informations et tous les documents nécessaires pour démontrer la conformité du produit;

c) à coopérer, à leur demande, avec les autorités nationales compétentes, à toute mesure prise en vue d'éliminer la non-conformité avec les exigences applicables en matière d'accessibilité des produits relevant de leur mandat.

Article 9

Obligations des importateurs

1. Les importateurs ne mettent que des produits conformes sur le marché.

2. Avant de mettre un produit sur le marché, les importateurs s'assurent que la procédure d'évaluation de la conformité prévue à l'annexe IV a été mise en œuvre par le fabricant. Ils s'assurent que le fabricant a établi la documentation technique prévue à ladite annexe, que le produit porte le marquage CE, qu'il est accompagné des documents requis et que le fabricant s'est conformé aux exigences prévues à l'article 7, paragraphes 5 et 6.

3. Lorsqu'un importateur considère ou a des raisons de croire qu'un produit n'est pas conforme aux exigences applicables en matière d'accessibilité énoncées dans la présente directive, l'importateur ne met pas le produit sur le marché tant que ce produit n'a pas été mis en conformité. En outre, lorsque le produit n'est pas conforme aux exigences applicables en matière d'accessibilité, l'importateur en informe le fabricant ainsi que les autorités de surveillance du marché.

4. Les importateurs indiquent leur nom, raison sociale ou marque déposée, ainsi que l'adresse à laquelle ils peuvent être contactés, sur le produit ou, lorsque cela n'est pas possible, sur son emballage ou dans un document accompagnant le produit. Les coordonnées sont indiquées dans une langue aisément compréhensible par les utilisateurs finals et les autorités de surveillance du marché.

5. Les importateurs veillent à ce que le produit soit accompagné d'instructions et d'informations de sécurité fournies dans une langue aisément compréhensible par les consommateurs et autres utilisateurs finals, déterminée par l'État membre concerné.

6. Tant qu'un produit est sous leur responsabilité, les importateurs s'assurent que les conditions de stockage ou de transport ne compromettent pas sa conformité avec les exigences applicables en matière d'accessibilité.

7. Pendant une durée de cinq ans, les importateurs tiennent une copie de la déclaration UE de conformité à la disposition des autorités de surveillance du marché et s'assurent que la documentation technique peut être fournie à ces autorités sur demande.

8. Les importateurs qui considèrent ou ont des raisons de croire qu'un produit qu'ils ont mis sur le marché n'est pas conforme à la présente directive prennent immédiatement les mesures correctives nécessaires pour le mettre en conformité ou, le cas échéant, pour le retirer. En outre, lorsque le produit n'est pas conforme aux exigences applicables en matière d'accessibilité, les importateurs en informent immédiatement les autorités nationales compétentes des États membres dans lesquels ils ont mis le produit à disposition, en fournissant des précisions, notamment, sur la non-conformité et sur toute mesure corrective prise. Dans de tels cas, les importateurs tiennent un registre des produits non conformes aux exigences applicables en matière d'accessibilité et des plaintes y afférentes.

9. Sur demande motivée d'une autorité nationale compétente, les importateurs lui communiquent toutes les informations et tous les documents nécessaires pour démontrer la conformité d'un produit, dans une langue aisément compréhensible par cette autorité. Ils coopèrent avec l'autorité en question, à sa demande, à toute mesure prise en vue d'éliminer la non-conformité avec les exigences applicables en matière d'accessibilité des produits qu'ils ont mis sur le marché.

Article 10

Obligations des distributeurs

1. Lorsqu'ils mettent un produit à disposition sur le marché, les distributeurs agissent avec la diligence requise en ce qui concerne les exigences de la présente directive.

2. Avant de mettre un produit à disposition sur le marché, les distributeurs vérifient qu'il porte le marquage CE, qu'il est accompagné des documents requis ainsi que d'instructions et d'informations de sécurité fournies dans une langue aisément compréhensible par les consommateurs et autres utilisateurs finals de l'État membre dans lequel le produit doit être mis à disposition et que le fabricant et l'importateur se sont conformés aux exigences prévues respectivement à l'article 7, paragraphes 5 et 6, et à l'article 9, paragraphe 4.

3. Lorsqu'un distributeur considère ou a des raisons de croire qu'un produit n'est pas conforme aux exigences applicables en matière d'accessibilité énoncées dans la présente directive, le distributeur ne met pas le produit à disposition sur le marché tant que ce produit n'a pas été mis en conformité. En outre, lorsque le produit n'est pas conforme aux exigences applicables en matière d'accessibilité, le distributeur en informe le fabricant ou l'importateur ainsi que les autorités de surveillance du marché.

4. Tant qu'un produit est sous leur responsabilité, les distributeurs s'assurent que les conditions de stockage ou de transport ne compromettent pas sa conformité avec les exigences applicables en matière d'accessibilité.

5. Les distributeurs qui considèrent ou ont des raisons de croire qu'un produit qu'ils ont mis à disposition sur le marché n'est pas conforme à la présente directive veillent à ce que soient prises les mesures correctives nécessaires pour le mettre en conformité ou, le cas échéant, pour le retirer. En outre, lorsque le produit n'est pas conforme aux exigences applicables en matière d'accessibilité, les distributeurs en informent immédiatement les autorités nationales compétentes des États membres dans lesquels ils ont mis le produit à disposition, en fournissant des précisions, notamment, sur la non-conformité et sur toute mesure corrective prise.

6. Sur demande motivée d'une autorité nationale compétente, les distributeurs lui communiquent toutes les informations et tous les documents nécessaires pour démontrer la conformité d'un produit. Ils coopèrent avec l'autorité en question, à sa demande, à toute mesure prise en vue d'éliminer la non-conformité avec les exigences applicables en matière d'accessibilité des produits qu'ils ont mis à disposition sur le marché.

Article 11

Cas dans lesquels les obligations des fabricants s'appliquent aux importateurs et aux distributeurs

Un importateur ou un distributeur est considéré comme un fabricant aux fins de la présente directive et est soumis aux obligations incombant au fabricant en vertu de l'article 7 lorsqu'il met un produit sur le marché sous son propre nom ou sa propre marque ou modifie un produit déjà mis sur le marché de telle sorte que la conformité avec les exigences de la présente directive peut être compromise.

Article 12

Identification des opérateurs économiques dans le secteur des produits

1. Les opérateurs économiques visés aux articles 7 à 10, sur demande, identifient à l'intention des autorités de surveillance du marché:

a) tout autre opérateur économique qui leur a fourni un produit;

b) tout autre opérateur économique auquel ils ont fourni un produit.

2. Les opérateurs économiques visés aux articles 7 à 10 sont en mesure de communiquer les informations visées au paragraphe 1 du présent article pendant une durée de cinq ans à compter de la date à laquelle le produit leur a été fourni et pendant une durée de cinq ans à compter de la date à laquelle ils ont fourni le produit.

3. La Commission est habilitée à adopter des actes délégués conformément à l'article 26, modifiant la présente directive afin de changer la période visée au paragraphe 2 du présent article pour des produits spécifiques. Cette période modifiée est supérieure à cinq ans et est proportionnée à la durée de vie économiquement utile du produit concerné.

CHAPITRE IV

Obligations des prestataires de services

Article 13

Obligations des prestataires de services

1. Les prestataires de services veillent à concevoir et à fournir des services conformément aux exigences en matière d'accessibilité énoncées dans la présente directive.

2. Les prestataires de services établissent les informations nécessaires conformément à l'annexe V, et expliquent comment les services satisfont aux exigences applicables en matière d'accessibilité. Les informations sont mises à la disposition du public sous forme écrite et orale, y compris d'une façon qui est accessible aux personnes handicapées. Les prestataires de services conservent ces informations aussi longtemps que le service est disponible.

3. Sans préjudice de l'article 32, les prestataires de services veillent à ce que des procédures soient en place afin que la fourniture des services reste conforme aux exigences applicables en matière d'accessibilité. Toute modification des caractéristiques de la fourniture du service, des exigences applicables en matière d'accessibilité et des normes harmonisées ou des spécifications techniques par rapport auxquelles est déclarée la conformité d'un service aux exigences en matière d'accessibilité, est dûment prise en considération par les prestataires de services.

4. En cas de non-conformité du service, les prestataires prennent les mesures correctives nécessaires pour le mettre en conformité avec les exigences applicables en matière d'accessibilité. En outre, lorsque le service n'est pas conforme aux exigences applicables en matière d'accessibilité, les prestataires de services en informent immédiatement les autorités nationales compétentes des États membres dans lesquels ils fournissent le service, en fournissant des précisions, notamment, sur la non-conformité et sur toute mesure corrective prise.

5. Sur demande motivée d'une autorité compétente, les prestataires de services lui communiquent toutes les informations nécessaires pour démontrer la conformité du service avec les exigences applicables en matière d'accessibilité. Ils coopèrent avec cette autorité, à la demande de celle-ci, à toute mesure prise en vue de rendre le service conforme à ces exigences.

CHAPITRE V

Modification fondamentale des produits ou services et charge disproportionnée pour les opérateurs économiques

Article 14

Modification fondamentale et charge disproportionnée

1. Les exigences en matière d'accessibilité visées à l'article 4 s'appliquent uniquement dans la mesure où la conformité:

a) n'exige pas de modification significative d'un produit ou d'un service qui entraîne une modification fondamentale de la nature de celui-ci; et

b) n'entraîne pas l'imposition d'une charge disproportionnée aux opérateurs économiques concernés.

2. Les opérateurs économiques effectuent une évaluation afin de déterminer si la conformité avec les exigences en matière d'accessibilité visées à l'article 4 introduirait une modification fondamentale ou, sur la base des critères pertinents énoncés à l'annexe VI, imposerait une charge disproportionnée, conformément au paragraphe 1 du présent article.

3. Les opérateurs économiques apportent des preuves à l'appui de l'évaluation visée au paragraphe 2. Les opérateurs économiques conservent tous les résultats pertinents pendant une période de cinq ans à compter de la date de dernière mise à disposition d'un produit sur le marché, ou de dernière fourniture d'un service, selon le cas. À la demande des autorités de surveillance du marché ou des autorités chargées du contrôle de la conformité des services, selon le cas, les opérateurs économiques leur fournissent une copie de l'évaluation visée au paragraphe 2.

4. Par dérogation au paragraphe 3, les microentreprises exerçant leur activité dans le domaine des produits sont exonérées de l'obligation d'apporter des preuves à l'appui de leur évaluation. Toutefois, si une autorité de surveillance du marché le demande, les microentreprises qui exercent leur activité dans le domaine des produits et qui ont choisi d'invoquer le paragraphe 1 lui communiquent les faits pertinents pour l'évaluation visée au paragraphe 2.

5. Les prestataires de services qui invoquent le paragraphe 1, point b), renouvellent, pour chaque catégorie ou type de service, l'évaluation du caractère disproportionné ou non de la charge:

a) lorsque le service proposé est modifié; ou

b) à la demande des autorités chargées du contrôle de la conformité des services; et

c) en tout état de cause, au moins tous les cinq ans.

6. Lorsqu'ils perçoivent, aux fins de l'amélioration de l'accessibilité, un financement provenant d'autres sources que leurs ressources propres, qu'elles soient d'origine publique ou privée, les opérateurs économiques ne peuvent invoquer le paragraphe 1, point b).

7. La Commission est habilitée à adopter des actes délégués conformément à l'article 26 afin de compléter l'annexe VI en précisant davantage les critères pertinents que l'opérateur économique doit prendre en compte pour effectuer l'évaluation visée au paragraphe 2 du présent article. Lorsqu'elle précise davantage lesdits critères, la Commission ne tient pas compte des avantages estimés pour les personnes handicapées uniquement, mais pour les personnes présentant des limitations fonctionnelles également.

La Commission adopte le cas échéant le premier de ces actes délégués au plus tard le 28 juin 2020. Cet acte commence à s'appliquer au plus tôt le 28 juin 2025.

8. Lorsque les opérateurs économiques invoquent le paragraphe 1 pour un produit ou service spécifique, ils en informent les autorités de surveillance du marché ou les autorités chargées du contrôle de la conformité des services de l'État membre dans lequel le produit spécifique est mis sur le marché ou dans lequel le service spécifique est fourni.

Le premier alinéa ne s'applique pas aux microentreprises.

CHAPITRE VI

Normes harmonisées et spécifications techniques pour les produits et services

Article 15

Présomption de conformité

1. Les produits et services conformes aux normes harmonisées ou à des parties de normes harmonisées dont les références ont été publiées au *Journal officiel de l'Union européenne* sont présumés conformes aux exigences en matière d'accessibilité énoncées dans la présente directive dans la mesure où ces normes ou parties de normes couvrent ces exigences.

2. Conformément à l'article 10 du règlement (UE) n° 1025/2012, la Commission demande à une ou plusieurs organisations européennes de normalisation d'élaborer des normes harmonisées pour les exigences en matière d'accessibilité des produits énoncées à l'annexe I. La Commission présente le premier projet de demande au comité concerné au plus tard 28 juin 2021.

3. La Commission peut adopter des actes d'exécution établissant des spécifications techniques conformes aux exigences en matière d'accessibilité énoncées dans la présente directive lorsque les conditions ci-après sont satisfaites:

a) aucune référence à des normes harmonisées n'a été publiée au *Journal officiel de l'Union européenne* conformément au règlement (UE) n° 1025/2012; et

b) soit:

   i) la Commission a demandé à une ou plusieurs organisations européennes de normalisation d'élaborer une norme harmonisée, et la procédure de normalisation rencontre un retard injustifié ou aucune organisation européenne de normalisation n'a accepté la demande; ou

ii) la Commission peut démontrer qu'une spécification technique satisfait aux exigences visées à l'annexe II du règlement (UE) n° 1025/2012, sauf pour ce qui est de l'exigence selon laquelle les spécifications techniques doivent être élaborées par un organisme à but non lucratif.

Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 27, paragraphe 2.

4. Les produits et services conformes aux spécifications techniques ou à des parties de spécifications techniques sont présumés conformes aux exigences en matière d'accessibilité énoncées dans la présente directive dans la mesure où ces spécifications techniques ou parties de spécifications techniques couvrent ces exigences.

CHAPITRE VII

Conformité des produits et marquage CE

Article 16

Déclaration UE de conformité de produits

1. La déclaration UE de conformité atteste que le respect des exigences en matière d'accessibilité applicables a été démontré. Lorsqu'à titre exceptionnel, l'article 14 a été appliqué, la déclaration UE de conformité précise les exigences en matière d'accessibilité concernées par cette exception.

2. La déclaration UE de conformité est établie selon le modèle figurant à l'annexe III de la décision n° 768/2008/CE. Elle contient les éléments précisés à l'annexe IV de la présente directive et est mise à jour de façon continue. Les exigences concernant la documentation technique évitent d'imposer une charge indue aux microentreprises et aux PME. Cette documentation est traduite dans la (les) langue(s) requise(s) par l'État membre sur le territoire duquel le produit est mis sur le marché ou mis à disposition sur le marché.

3. Lorsqu'un produit relève de plusieurs actes de l'Union imposant une déclaration UE de conformité, une seule déclaration UE de conformité est établie pour l'ensemble de ces actes. La déclaration mentionne les titres des actes concernés, ainsi que les références de publication.

4. En établissant la déclaration UE de conformité, le fabricant assume la responsabilité de la conformité du produit avec les exigences de la présente directive.

Article 17

Principes généraux du marquage CE des produits

Le marquage CE est soumis aux principes généraux énoncés à l'article 30 du règlement (CE) n° 765/2008.

Article 18

Règles et conditions d'apposition du marquage CE

1. Le marquage CE est apposé de manière visible, lisible et indélébile sur le produit ou sur sa plaque signalétique. Lorsque la nature du produit ne le permet pas ou ne le justifie pas, il est apposé sur son emballage et sur les documents d'accompagnement.

2. Le marquage CE est apposé avant que le produit ne soit mis sur le marché.

3. Les États membres s'appuient sur les mécanismes existants pour assurer la bonne application du régime régissant le marquage CE et prennent les mesures nécessaires en cas d'usage abusif du marquage.

Chapitre VIII

Surveillance du marché pour les produits et procédure de sauvegarde de l'Union

Article 19

Surveillance du marché pour les produits

1. L'article 15, paragraphe 3, les articles 16 à 19, l'article 21, les articles 23 à 28 et l'article 29, paragraphes 2 et 3, du règlement (CE) n° 765/2008 s'appliquent aux produits.

2. Lorsqu'elles effectuent la surveillance d'un produit sur le marché et lorsque l'opérateur économique a invoqué l'article 14, les autorités de surveillance du marché compétentes:

a) vérifient si l'évaluation visée à l'article 14 a été effectuée par l'opérateur économique;

b) examinent cette évaluation et ses résultats, y compris l'utilisation correcte des critères énoncés à l'annexe VI; et

c) contrôlent la conformité avec les exigences applicables en matière d'accessibilité.

3. Les États membres veillent à ce que les informations détenues par les autorités de surveillance du marché en ce qui concerne la conformité des opérateurs économiques avec les exigences applicables en matière d'accessibilité énoncées dans la présente directive et l'évaluation prévue à l'article 14, soient mises à la disposition des consommateurs, sur demande, dans un format accessible, sauf lorsque ces informations ne peuvent être fournies pour des raisons de confidentialité conformément aux dispositions de l'article 19, paragraphe 5, du règlement (CE) n° 765/2008.

Article 20

Procédure applicable au niveau national aux produits qui ne sont pas conformes aux exigences applicables en matière d'accessibilité

1. Lorsque les autorités de surveillance du marché d'un État membre ont des raisons suffisantes de croire qu'un produit relevant de la présente directive n'est pas conforme aux exigences applicables en matière d'accessibilité, elles effectuent une évaluation du produit concerné en tenant compte de toutes les exigences énoncées dans la présente directive. À cet effet, les opérateurs économiques concernés coopèrent pleinement avec les autorités de surveillance du marché.

Lorsque, au cours de l'évaluation visée au premier alinéa, les autorités de surveillance du marché constatent que le produit n'est pas conforme aux exigences énoncées dans la présente directive, elles demandent sans retard à l'opérateur économique en cause de prendre toutes les mesures correctives appropriées pour mettre le produit en conformité avec ces exigences dans le délai raisonnable, proportionné à la nature de la non-conformité, qu'elles prescrivent.

Les autorités de surveillance du marché demandent à l'opérateur économique en cause de retirer le produit du marché, dans un délai supplémentaire raisonnable, uniquement si ledit opérateur économique n'a pas pris les mesures correctives adéquates dans le délai visé au deuxième alinéa.

L'article 21 du règlement (CE) n° 765/2008 s'applique aux mesures visées aux deuxième et troisième alinéas du présent paragraphe.

2. Lorsque les autorités de surveillance du marché considèrent que la non-conformité n'est pas limitée au territoire national, elles informent la Commission et les autres États membres des résultats de l'évaluation et des mesures qu'elles ont prescrites à l'opérateur économique.

3. L'opérateur économique s'assure que toutes les mesures correctives appropriées sont prises pour tous les produits concernés qu'il a mis à disposition sur le marché dans toute l'Union.

4. Lorsque l'opérateur économique en cause ne prend pas des mesures correctives adéquates dans le délai visé au paragraphe 1, troisième alinéa, les autorités de surveillance du marché prennent toutes les mesures provisoires appropriées pour interdire ou restreindre la mise à disposition du produit sur leur marché national ou pour le retirer de ce marché.

Les autorités de surveillance du marché en informent sans retard la Commission et les autres États membres.

5. Les informations visées au paragraphe 4, deuxième alinéa, contiennent tous les détails disponibles, notamment en ce qui concerne les données nécessaires pour identifier le produit non conforme, son origine, la nature de la non-conformité alléguée et les exigences en matière d'accessibilité auxquelles le produit n'est pas conforme, ainsi que la nature et la durée des mesures nationales prises et les arguments avancés par l'opérateur économique en cause. En particulier, les autorités de surveillance du marché indiquent si la non-conformité est imputable à l'un des éléments suivants:

a) non-conformité du produit avec les exigences applicables en matière d'accessibilité;

b) lacunes dans les normes harmonisées ou dans les spécifications techniques visées à l'article 15, qui confèrent une présomption de conformité.

6. Les États membres autres que celui qui a entamé la procédure au titre du présent article informent sans retard la Commission et les autres États membres de toute mesure prise et de toute information supplémentaire dont ils disposent à propos de la non-conformité du produit concerné et, dans l'éventualité où ils s'opposent à la mesure nationale notifiée, de leurs objections.

7. Lorsque, dans un délai de trois mois à compter de la réception des informations visées au paragraphe 4, deuxième alinéa, aucune objection n'a été émise par un État membre ou par la Commission à l'encontre de la mesure provisoire d'un État membre, cette mesure est réputée justifiée.

8. Les États membres veillent à ce que des mesures restrictives appropriées, telles que le retrait du produit de leur marché, soient prises sans retard à l'égard du produit concerné.

Article 21

Procédure de sauvegarde de l'Union

1. Lorsque, au terme de la procédure prévue à l'article 20, paragraphes 3 et 4, des objections sont émises à l'encontre d'une mesure prise par un État membre ou lorsque la Commission détient des preuves suffisantes indiquant qu'une mesure nationale est contraire au droit de l'Union, la Commission entame sans retard des consultations avec les États membres et le ou les opérateurs économiques en cause et procède à l'évaluation de la mesure nationale. En fonction des résultats de cette évaluation, la Commission décide si la mesure nationale est ou non justifiée.

La Commission adresse sa décision à tous les États membres et la communique immédiatement à ceux-ci ainsi qu'au ou aux opérateurs économiques en cause.

2. Lorsque la mesure nationale visée au paragraphe 1, est considérée comme justifiée, tous les États membres prennent les mesures nécessaires pour garantir le retrait du produit non conforme de leur marché et ils en informent la Commission. Lorsque la mesure nationale est considérée comme injustifiée, l'État membre concerné la retire.

3. Lorsque la mesure nationale visée au paragraphe 1 du présent article est considérée comme justifiée et que la non-conformité du produit est attribuée à des lacunes dans les normes harmonisées visées à l'article 20, paragraphe 5, point b), la Commission applique la procédure prévue à l'article 11 du règlement (UE) n° 1025/2012.

4. Lorsque la mesure nationale visée au paragraphe 1 du présent article est considérée comme justifiée et que la non-conformité du produit est attribuée à des lacunes dans les spécifications techniques visées à l'article 20, paragraphe 5, point b), la Commission adopte sans retard un acte d'exécution modifiant ou abrogeant la spécification technique en question. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 27, paragraphe 2.

Article 22

Non-conformité formelle

1. Sans préjudice de l'article 20, lorsqu'un État membre fait l'une des constatations ci-après, il invite l'opérateur économique en cause à mettre un terme à la non-conformité en question:

a) le marquage CE a été apposé en violation de l'article 30 du règlement (CE) n° 765/2008 ou de l'article 18 de la présente directive;

b) le marquage CE n'a pas été apposé;

c) la déclaration UE de conformité n'a pas été établie;

d) la déclaration UE de conformité n'a pas été établie correctement;

e) la documentation technique n'est pas disponible ou n'est pas complète;

f) les informations visées à l'article 7, paragraphe 6, ou à l'article 9, paragraphe 4, sont absentes, fausses ou incomplètes;

g) une autre obligation administrative prévue à l'article 7 ou à l'article 9 n'est pas respectée.

2. Lorsque la non-conformité visée au paragraphe 1 persiste, l'État membre concerné prend toutes les mesures appropriées pour restreindre ou interdire la mise à disposition du produit sur le marché ou pour assurer son retrait du marché.

CHAPITRE IX

Conformité des services

Article 23

Conformité des services

1. Les États membres établissent, appliquent et mettent à jour régulièrement des procédures appropriées en vue:

a) de vérifier la conformité des services avec les exigences de la présente directive, y compris l'évaluation visée à l'article 14, à laquelle l'article 19, paragraphe 2, s'applique mutatis mutandis;

b) d'assurer le suivi des plaintes ou des rapports sur des aspects liés à la non-conformité de services avec les exigences en matière d'accessibilité énoncées dans la présente directive;

c) de vérifier que l'opérateur économique a pris les mesures correctives nécessaires.

2. Les États membres désignent les autorités responsables de la mise en œuvre des procédures visées au paragraphe 1 en ce qui concerne la conformité des services.

Chaque État membre veille à ce que le public soit informé de l'existence, des responsabilités, de l'identité, du travail et des décisions des autorités visées au premier alinéa. Ces autorités mettent ces informations à disposition sur demande dans des formats appropriés.

CHAPITRE X

Exigences en matière d'accessibilité figurant dans d'autres actes de l'Union

Article 24

Exigences en matière d'accessibilité figurant dans d'autres actes de l'Union

1. En ce qui concerne les produits et services visés à l'article 2 de la présente directive, les exigences en matière d'accessibilité énoncées à l'annexe I de la présente directive constituent des exigences d'accessibilité contraignantes au sens de l'article 42, paragraphe 1, de la directive 2014/24/UE et de l'article 60, paragraphe 1, de la directive 2014/25/UE.

2. Tout produit ou service dont les caractéristiques, éléments ou fonctions sont conformes aux exigences en matière d'accessibilité énoncées à l'annexe I de la présente directive conformément à la section VI de ladite annexe est présumé satisfaire aux obligations pertinentes en matière d'accessibilité figurant dans des actes de l'Union autres que la présente directive, pour ce qui est de ces caractéristiques, éléments ou fonctions, sauf mention contraire dans ces autres actes.

Article 25

Normes harmonisées et spécifications techniques pour d'autres actes de l'Union

La conformité avec des normes harmonisées et des spécifications techniques ou avec des parties de normes harmonisées et de spécifications techniques adoptées conformément à l'article 15 établit une présomption de conformité avec l'article 24 dans la mesure où ces normes et spécifications techniques ou ces parties de normes et de spécifications techniques satisfont aux exigences en matière d'accessibilité énoncées dans la présente directive.

CHAPITRE XI

Actes délégués, compétences d'exécution et dispositions finales

Article 26

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 4, paragraphe 9, est conféré à la Commission pour une durée indéterminée à compter du 27 juin 2019.

Le pouvoir d'adopter des actes délégués visé à l'article 12, paragraphe 3, et à l'article 14, paragraphe 7, est conféré à la Commission pour une période de cinq ans à compter du 27 juin 2019. La Commission élabore un rapport relatif à la délégation de pouvoir, au plus tard neuf mois avant la fin de la période de cinq ans. La délégation de pouvoir est tacitement prorogée pour des périodes d'une durée identique, sauf si le Parlement européen ou le Conseil s'oppose à cette prorogation trois mois au plus tard avant la fin de chaque période.

3. La délégation de pouvoir visée à l'article 4, paragraphe 9, à l'article 12, paragraphe 3, et à l'article 14, paragraphe 7, 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 au Parlement européen et au Conseil simultanément.

6. Un acte délégué adopté en vertu de l'article 4, paragraphe 9, de l'article 12, paragraphe 3, et de l'article 14, paragraphe 7, 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 27

Comité

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

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

Article 28

Groupe de travail

La Commission établit un groupe de travail constitué des représentants des autorités de surveillance du marché, des autorités chargées de la conformité des services et des parties prenantes concernées, y compris des représentants des organisations qui représentent les personnes handicapées.

Le groupe de travail:

a) facilite l'échange d'informations et de bonnes pratiques entre les autorités et les parties prenantes concernées;

b) favorise la coopération entre les autorités et les parties prenantes concernées sur les questions relatives à la mise en œuvre de la présente directive afin d'améliorer la cohérence dans l'application des exigences en matière d'accessibilité énoncées dans la présente directive et de suivre étroitement la mise en œuvre de l'article 14; et

c) fournit des conseils, en particulier à la Commission, en ce qui concerne notamment la mise en œuvre des articles 4 et 14.

Article 29

Mesures d'exécution

1. Les États membres veillent à ce qu'il existe des moyens adéquats et efficaces permettant de faire respecter la présente directive.

2. Les moyens visés au paragraphe 1 comprennent:

a) des dispositions permettant à un consommateur de saisir les tribunaux ou les organes administratifs compétents en vertu du droit national, afin de garantir le respect des dispositions nationales transposant la présente directive;

b) des dispositions permettant à des organismes publics ou des associations privées, des organisations ou autres entités juridiques ayant un intérêt légitime à l'application de la présente directive d'agir devant les tribunaux ou les organes administratifs compétents en vertu du droit national, au nom ou au soutien du requérant et avec son accord, dans toute procédure judiciaire ou administrative prévue aux fins de l'exécution des obligations énoncées par la présente directive.

3. Le présent article ne s'applique pas aux procédures de passation de marchés relevant des directives 2014/24/UE et 2014/25/UE.

Article 30

Sanctions

1. Les États membres déterminent le régime des sanctions applicables aux violations des dispositions nationales adoptées en application de la présente directive et prennent toute mesure nécessaire pour assurer la mise en œuvre de celles-ci.

2. Les sanctions ainsi prévues sont effectives, proportionnées et dissuasives. Ces sanctions s'accompagnent de mesures correctives efficaces au cas où les opérateurs économiques ne se conforment pas à ces dispositions.

3. Les États membres informent sans retard la Commission du régime des sanctions et des mesures qu'ils ont adoptés et de toute modification apportée ultérieurement.

4. Les sanctions tiennent compte de l'étendue du cas de non-conformité, notamment de sa gravité et du nombre d'unités de produits ou services non conformes mais aussi du nombre de personnes concernées.

5. Le présent article ne s'applique pas aux procédures de passation de marchés relevant des directives 2014/24/UE et 2014/25/UE.

Article 31

Transposition

1. Les États membres adoptent et publient, au plus tard le 28 juin 2022, les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive. Ils communiquent immédiatement à la Commission le texte de ces dispositions.

2. Ils appliquent ces dispositions à partir du 28 juin 2025.

3. Par dérogation au paragraphe 2 du présent article, les États membres peuvent décider d'appliquer les mesures relatives aux obligations prévues à l'article 4, paragraphe 8, au plus tard le 28 juin 2027.

4. 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.

5. Les États membres communiquent à la Commission le texte des dispositions essentielles de droit interne qu'ils adoptent dans le domaine régi par la présente directive.

6. Les États membres qui font usage de la possibilité prévue à l'article 4, paragraphe 4, communiquent à la Commission le texte des dispositions essentielles de droit interne qu'ils adoptent à cette fin et présentent à la Commission un rapport sur les progrès réalisés dans leur mise en œuvre.

Article 32

Mesures transitoires

1. Sans préjudice du paragraphe 2 du présent article, les États membres prévoient une période transitoire s'achevant le 28 juin 2030, au cours de laquelle les prestataires de services ont la possibilité de continuer à fournir leurs services en utilisant des produits qu'ils utilisaient légalement pour fournir des services similaires avant cette date.

Les contrats de services convenus avant le 28 juin 2025 peuvent courir sans modification jusqu'à expiration, mais pas plus que cinq ans à compter de ladite date.

2. Les États membres peuvent prévoir que les terminaux en libre-service utilisés légalement par les prestataires de services pour fournir des services avant le 28 juin 2025 peuvent continuer à être utilisés pour fournir des services similaires jusqu'à la fin de leur durée de vie économiquement utile, cette période ne pouvant dépasser vingt ans après leur mise en service.

Article 33

Rapports et réexamen

1. Au plus tard le 28 juin 2030 et tous les cinq ans par la suite, la Commission soumet au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions un rapport sur l'application de la présente directive.

2. Les rapports décrivent entre autres, à la lumière de l'évolution sociale, économique et technologique, les développements en matière d'accessibilité des produits et des services, le verrouillage technologique éventuel ou les possibles obstacles à l'innovation et les incidences de la présente directive sur les opérateurs économiques et sur les personnes handicapées. Les rapports évaluent également si l'application de l'article 4, paragraphe 4, a contribué à rapprocher les exigences divergentes en matière d'accessibilité de l'environnement bâti lié aux services de transport de passagers et de voyageurs, aux services bancaires aux consommateurs et aux centres de services à la clientèle des magasins gérés par des prestataires de services de communications électroniques, le cas échéant, en vue de permettre l'alignement progressif sur les exigences en matière d'accessibilité énoncées à l'annexe III.

Les rapports évaluent également si l'application de la présente directive, et en particulier ses dispositions facultatives, a contribué à rapprocher les exigences en matière d'accessibilité de l'environnement bâti constituant des travaux relevant du champ d'application de la directive 2014/23/UE du Parlement européen et du Conseil ([35]), de la directive 2014/24/UE et de la directive 2014/25/UE.

Les rapports traitent également des effets sur le fonctionnement du marché intérieur de l'application de l'article 14 de la présente directive, y compris, le cas échéant, sur la base des informations reçues en application de l'article 14, paragraphe 8, ainsi que de l'exemption accordée aux microentreprises. Les rapports déterminent si la présente directive a atteint ses objectifs et s'il serait approprié d'inclure de nouveaux produits et services dans son champ d'application, ou d'en exclure certains produits et services, et ils recensent, si possible, les domaines dans lesquels la charge devrait être réduite, en vue d'une possible révision de la présente directive.

La Commission propose s'il y a lieu des mesures appropriées, notamment des mesures législatives.

([35]) Directive 2014/23/UE du Parlement européen et du Conseil du 26 février 2014 sur l'attribution de contrats de concession (JO L 94 du 28.3.2014, p. 1).

3. Les États membres communiquent en temps utile à la Commission toutes les informations dont elle a besoin pour établir de tels rapports.

4. Les rapports de la Commission prennent en considération le point de vue des acteurs économiques et des organisations non gouvernementales concernées, notamment les organisations représentant les personnes handicapées.

Article 34

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

Article 35

Les États membres sont destinataires de la présente directive.

Fait à Strasbourg, le 17 avril 2019.

Par le Parlement européen	*Par le Conseil*
Le président	*Le président*
A. TAJANI	G. CIAMBA

ANNEXE I

EXIGENCES EN MATIÈRE D'ACCESSIBILITÉ POUR LES PRODUITS ET SERVICES

Section I

Exigences générales en matière d'accessibilité liées à tous les produits relevant de la présente directive conformément à l'article 2, paragraphe 1

Les produits doivent être conçus et fabriqués de manière à garantir une utilisation prévisible optimale par les personnes handicapées et sont accompagnés d'informations accessibles sur leur fonctionnement et leurs caractéristiques d'accessibilité, figurant dans la mesure du possible dans ou sur le produit.

1. Exigences relatives à la fourniture d'informations

   a) informations sur l'utilisation du produit, figurant sur le produit lui-même (étiquetage, instructions et avertissement). Ces informations sont:

      i) disponibles au moyen de plusieurs canaux sensoriels;

      ii) présentées de façon compréhensible;

      iii) présentées aux utilisateurs de manière à ce qu'ils les perçoivent;

      iv) présentées en utilisant une police de caractères de taille et de forme appropriées compte tenu des conditions d'utilisation prévisibles, ainsi qu'un contraste suffisant, et en ménageant un espace ajustable entre les lettres, les lignes et les paragraphes;

   b) instructions concernant l'utilisation d'un produit lorsqu'elles ne sont pas fournies sur le produit lui-même, mais sont disponibles lors de l'utilisation du produit ou par d'autres moyens comme un site internet, notamment les fonctions d'accessibilité du produit, leur activation et leur interopérabilité avec des solutions d'assistance. Ces instructions sont mises à la disposition du public lorsque le produit est mis sur le marché et:

      i) sont disponibles au moyen de plusieurs canaux sensoriels;

      ii) sont présentées de façon compréhensible;

      iii) sont présentées aux utilisateurs de manière à ce qu'ils les perçoivent;

      iv) sont présentées en utilisant une police de caractères de taille et de forme appropriées compte tenu des conditions d'utilisation prévisibles, ainsi qu'un contraste suffisant, et en ménageant un espace ajustable entre les lettres, les lignes et les paragraphes;

      v) sont disponibles, en ce qui concerne leur contenu, dans des formats texte permettant de générer d'autres formats auxiliaires pouvant être présentés de différentes manières et par l'intermédiaire de plusieurs canaux sensoriels;

      vi) sont accompagnées d'une présentation de substitution de tout contenu non textuel;

      vii) comprennent une description de l'interface utilisateur du produit (manipulation, commande et retour d'informations, entrée-sortie) conformément au point 2; la description indique, pour chacun des éléments énumérés au point 2, si le produit présente ces caractéristiques;

      viii) comprennent une description des fonctionnalités du produit. Des fonctions adaptées aux besoins des personnes handicapées sont proposées conformément au point 2; la description indique, pour chacun des éléments énumérés au point 2, si le produit présente ces caractéristiques;

      ix) comprennent une description de l'interfaçage logiciel et matériel du produit avec des dispositifs d'assistance; la description inclut une liste des dispositifs d'assistance qui ont été testés avec le produit.

2. Conception de l'interface utilisateur et des fonctionnalités

   Le produit, y compris son interface utilisateur, comporte des caractéristiques, des éléments et des fonctions permettant aux personnes handicapées d'accéder au produit, de le percevoir, de l'utiliser, de le comprendre et de le commander, en veillant aux aspects suivants:

   a) lorsque le produit permet la communication, y compris la communication interpersonnelle, l'utilisation, la fourniture d'informations, la commande et l'orientation, ces fonctions sont disponibles au moyen de plusieurs canaux sensoriels, notamment en proposant des solutions de substitution à la vision, à l'audition, à la parole et au toucher;

   b) lorsque le produit utilise la parole, des solutions de substitution à la parole et à l'intervention vocale sont proposées pour la communication, l'utilisation, la commande et l'orientation;

c) lorsque le produit utilise des éléments visuels, des fonctions flexibles d'agrandissement, de réglage de la luminosité et de contraste sont proposées pour la communication, la fourniture d'informations et l'utilisation et il est veillé à l'interopérabilité avec des programmes et des dispositifs d'assistance pour explorer l'interface;

d) lorsque le produit utilise des couleurs pour transmettre des informations, indiquer une action, demander une réponse ou signaler des éléments, une solution de substitution à la couleur est proposée;

e) lorsque le produit utilise des signaux auditifs pour transmettre des informations, indiquer une action, demander une réponse ou signaler des éléments, une solution de substitution aux signaux auditifs est proposée;

f) lorsque le produit utilise des éléments visuels, des fonctions flexibles sont proposées pour améliorer la clarté visuelle;

g) lorsque le produit utilise des sons, une fonction de réglage du volume et de la vitesse est proposée, ainsi que des caractéristiques audio avancées, notamment de réduction des interférences provenant de produits proches et de clarté auditive;

h) lorsque le produit nécessite une utilisation et une commande manuelles, une commande séquentielle et des possibilités de commande autres que fondées sur la motricité fine sont proposées, en évitant que des commandes simultanées soient nécessaires pour la manipulation, et des éléments perceptibles au toucher sont disponibles;

i) le produit est conçu pour éviter les modes de fonctionnement exigeant une forte amplitude de mouvements et une grande force;

j) le produit est conçu pour éviter le déclenchement de réactions photosensibles;

k) le produit préserve la vie privée de l'utilisateur lors de son utilisation des caractéristiques d'accessibilité;

l) le produit offre une solution de substitution à l'identification et à la commande biométriques;

m) le produit garantit la cohérence des fonctionnalités et prévoit un laps de temps suffisant et flexible pour l'interaction;

n) le produit prévoit un interfaçage logiciel et matériel avec les technologies d'assistance;

o) le produit satisfait aux exigences sectorielles suivantes:

i) les terminaux en libre-service:

— intègrent une technologie de synthèse vocale de texte,

— permettent l'utilisation d'un casque personnel,

— lorsque le temps de réponse est limité, transmettent à l'utilisateur un signal par l'intermédiaire de plusieurs canaux sensoriels,

— donnent la possibilité de prolonger le temps de réponse,

— lorsque des touches et boutons de commande sont disponibles, présentent un contraste suffisant et des touches et boutons de commande perceptibles au toucher,

— n'exigent pas, pour qu'un utilisateur puisse s'en servir, qu'une caractéristique d'accessibilité soit activée,

— lorsque le produit utilise des signaux audio ou auditifs, il est compatible avec des dispositifs et technologies d'assistance disponibles au niveau de l'Union, y compris des technologies auditives, telles que des appareils auditifs, boucles auditives, implants cochléaires et dispositifs d'aide à l'audition;

ii) les liseuses numériques intègrent une technologie de synthèse vocale de texte;

iii) les équipements terminaux grand public avec des capacités informatiques interactives utilisés pour la fourniture de services de communications électroniques:

— permettent, lorsqu'ils ont des capacités textuelles en complément des capacités vocales, le traitement de texte en temps réel, et supportent un son haute fidélité,

— permettent, lorsqu'ils ont des capacités vidéo en complément du texte et de la voix ou en association avec ces deux canaux, l'utilisation de la conversation totale, y compris la synchronisation vocale, le texte en temps réel et la vidéo avec une résolution permettant une communication en langue des signes,

— assurent une connexion sans fil efficace aux technologies auditives,

— évitent les interférences avec les dispositifs d'assistance;

iv) les équipements terminaux grand public avec des capacités informatiques interactives utilisés pour accéder à des services de médias audiovisuels mettent à disposition des personnes handicapées les éléments en matière d'accessibilité fournis par le prestataire de services de médias audiovisuels en ce qui concerne l'accès, la sélection, la commande et la personnalisation par l'utilisateur ainsi que la transmission aux dispositifs d'assistance.

3. Services d'assistance:

Le cas échéant, les services d'assistance (services d'aide, centres d'appel, assistance technique, services de relais et services de formation) fournissent des informations sur l'accessibilité du produit et sur sa compatibilité avec les technologies d'assistance, via des modes de communication accessibles.

Section II

Exigences en matière d'accessibilité liées aux produits visés à l'article 2, paragraphe 1, à l'exception des terminaux en libre-service visés à l'article 2, paragraphe 1, point b)

Outre les exigences de la section I, afin de garantir une utilisation prévisible optimale par les personnes handicapées, les emballages des produits relevant de la présente section et les instructions doivent être rendus accessibles. Cela signifie que:

a) l'emballage du produit, y compris les informations contenues dans celui-ci (par exemple concernant l'ouverture, la fermeture, l'utilisation, l'élimination), notamment, le cas échéant, les informations sur les caractéristiques du produit en matière d'accessibilité, est rendu accessible; et, dans la mesure du possible, ces informations accessibles sont mentionnées sur l'emballage;

b) les instructions concernant l'installation, l'entretien, le stockage et l'élimination du produit qui ne sont pas fournies sur le produit lui-même, mais sont disponibles par d'autres moyens comme un site internet, sont mises à la disposition du public lorsque le produit est mis sur le marché et sont conformes aux exigences suivantes:

i) elles sont disponibles au moyen de plusieurs canaux sensoriels;

ii) elles sont présentées de façon compréhensible;

iii) elles sont présentées aux utilisateurs de manière à ce qu'ils les perçoivent;

iv) elles sont présentées en utilisant une police de caractères de taille et de forme appropriées compte tenu des conditions d'utilisation prévisibles, ainsi qu'un contraste suffisant, et ménagent un espace ajustable entre les lettres, les lignes et les paragraphes;

v) leur contenu est disponible dans des formats texte permettant de générer d'autres formats auxiliaires pouvant être présentés de différentes manières et par l'intermédiaire de plusieurs canaux sensoriels; et

vi) elles sont accompagnées d'une présentation de substitution du contenu lorsqu'elles contiennent du contenu non textuel.

Section III

Exigences générales en matière d'accessibilité liées à tous les services relevant de la présente directive conformément à l'article 2, paragraphe 2

Afin de garantir une utilisation prévisible optimale par les personnes handicapées, les services proposés doivent être conformes aux exigences suivantes:

a) veiller à ce que les produits utilisés dans la fourniture du service soient accessibles, conformément à la section I et, le cas échéant, à la section II;

b) fournir des informations sur le fonctionnement du service et, lorsque des produits sont utilisés dans la fourniture du service, sur son lien avec ces produits, ainsi que des informations sur leurs caractéristiques en matière d'accessibilité et sur leur interopérabilité avec des dispositifs et fonctionnalités d'assistance:

i) en mettant à disposition les informations au moyen de plusieurs canaux sensoriels;

ii) en présentant les informations de façon compréhensible;

iii) en présentant les informations aux utilisateurs de manière à ce qu'ils les perçoivent;

iv) en mettant à disposition le contenu informatif dans des formats texte permettant de générer d'autres formats auxiliaires pouvant être présentés de différentes manières par les utilisateurs et par l'intermédiaire de plusieurs canaux sensoriels;

v) en utilisant une police de caractères de taille et de forme appropriées compte tenu des conditions d'utilisation prévisibles, ainsi qu'un contraste suffisant, et en ménageant un espace ajustable entre les lettres, les lignes et les paragraphes;

vi) en accompagnant tout contenu non textuel d'une présentation de substitution dudit contenu; et

vii) en fournissant les informations électroniques nécessaires à la fourniture du service d'une manière cohérente et adéquate en les rendant perceptibles, utilisables, compréhensibles et robustes;

c) rendre les sites internet, y compris les applications en ligne connexes, et les services intégrés sur appareils mobiles, y compris les applications mobiles, accessibles d'une manière cohérente et appropriée en les rendant perceptibles, utilisables, compréhensibles et robustes;

d) le cas échéant, veiller à ce que les services d'assistance (services d'aide, centres d'appel, assistance technique, services de relais et services de formation) fournissent des informations sur l'accessibilité du service et sur sa compatibilité avec les technologies d'assistance, via des modes de communication accessibles.

Section IV

Exigences supplémentaires en matière d'accessibilité liées à des services spécifiques

Afin de garantir une utilisation prévisible optimale par les personnes handicapées, les services proposés doivent inclure des fonctions, des pratiques, des stratégies et des procédures ainsi que des modifications du fonctionnement du service visant à répondre aux besoins des personnes handicapées et à garantir l'interopérabilité avec les technologies d'assistance, selon les modalités suivantes:

a) pour les services de communications électroniques, y compris les communications d'urgence visées à l'article 109, paragraphe 2, de la directive (UE) 2018/1972:

i) fournir du texte en temps réel en plus de la communication vocale;

ii) fournir la conversation totale lorsque de la vidéo est proposée en plus de la communication vocale;

iii) veiller à ce que les communications d'urgence utilisant la voix et du texte (y compris du texte en temps réel) soient synchronisées et, lorsque de la vidéo est proposée, qu'elles soient également synchronisées en mode conversation totale et transmises par les prestataires de services de communications électroniques au PSAP le plus approprié;

b) pour les services fournissant un accès à des services de médias audiovisuels:

i) fournir des guides électroniques de programme perceptibles, utilisables, compréhensibles et robustes et fournir des informations sur la disponibilité des caractéristiques d'accessibilité;

ii) veiller à ce que les éléments d'accessibilité (services d'accès) des services de médias audiovisuels, tels que le sous-titrage pour les personnes sourdes ou malentendantes, l'audiodescription, le sous-titrage audio et l'interprétation en langue des signes, soient entièrement transmis avec une qualité appropriée à un affichage net et synchronisés avec le son et la vidéo, tout en permettant à l'utilisateur de régler leur affichage et leur utilisation;

c) pour les services de transport aérien, ferroviaire, par voie de navigation intérieure et par autobus de voyageurs et de passagers, à l'exception des services de transport urbains et suburbains et des services de transport régionaux:

i) veiller à fournir des informations sur l'accessibilité des véhicules, des infrastructures avoisinantes et de l'environnement bâti ainsi que sur l'assistance pour les personnes handicapées;

ii) veiller à fournir des informations sur les systèmes de billetterie intelligents (réservation électronique, réservation de billets, etc.) ou la communication d'informations en temps réel sur le voyage (horaires, informations relatives aux perturbations du trafic, services de liaison, connexion avec d'autres modes de transport, etc.) et d'informations supplémentaires concernant le service (par exemple sur le personnel présent en gare, les ascenseurs hors service ou les services momentanément indisponibles);

d) pour les services de transport urbains et suburbains et les services de transport régionaux: veiller à ce que les terminaux en libre-service utilisés pour la fourniture du service soient accessibles, conformément à la section I;

e) pour les services bancaires aux consommateurs:

i) fournir des méthodes d'identification, des signatures électroniques et des services de sécurité et de paiement perceptibles, utilisables, compréhensibles et robustes;

ii) veiller à ce que les informations soient compréhensibles, sans dépasser un niveau de complexité supérieur au niveau B2 (avancé) du cadre européen commun de référence pour les langues du Conseil de l'Europe;

f) pour les livres numériques:

i) veiller à ce qu'un livre numérique contenant des éléments audio en plus du texte fournisse des contenus textuels et audio synchronisés;

ii) veiller à ce que les fichiers numériques n'empêchent pas les technologies d'assistance de fonctionner correctement;

iii) garantir l'accès au contenu, la navigation dans le contenu et dans la mise en page du fichier, y compris la mise en page dynamique, la mise à disposition de la structure du fichier, la flexibilité et le choix de la présentation du contenu;

iv) permettre des restitutions alternatives du contenu et son interopérabilité avec diverses technologies d'assistance, de manière à ce qu'il soit perceptible, utilisable, compréhensible et robuste;

v) permettre la découverte en fournissant des informations, via les métadonnées, sur les caractéristiques d'accessibilité;

vi) s'assurer que les mesures de gestion des droits numériques ne bloquent pas les caractéristiques d'accessibilité;

g) pour les services de commerce électronique:

i) fournir les informations relatives à l'accessibilité des produits et services mis en vente lorsque ces informations sont fournies par l'opérateur économique responsable;

ii) veiller à l'accessibilité des fonctionnalités relatives à l'identification, à la sécurité et au paiement lorsqu'elles sont fournies en tant qu'éléments d'un service plutôt que d'un produit, en les rendant perceptibles, utilisables, compréhensibles et robustes;

iii) fournir des méthodes d'identification, des signatures électroniques et des services de paiement perceptibles, utilisables, compréhensibles et robustes.

Section V

Exigences spécifiques en matière d'accessibilité liées à la réception, par le PSAP le plus approprié, des communications d'urgence dirigées vers le numéro d'urgence unique européen «112»

Afin de garantir une utilisation prévisible optimale par les personnes handicapées, la réception, par le PSAP le plus approprié, des communications d'urgence dirigées vers le numéro d'urgence unique européen «112» doit inclure des fonctions, des pratiques, des stratégies et des procédures ainsi que des modifications visant à répondre aux besoins des personnes handicapées.

Les communications d'urgence dirigées vers le numéro d'urgence unique européen «112» reçoivent, de la façon la mieux adaptée à l'organisation nationale des systèmes d'urgence, une réponse appropriée de la part du PSAP le plus approprié, en utilisant les mêmes moyens de communication que ceux réceptionnés, notamment en synchronisant la voix avec du texte (y compris du texte en temps réel), ou, lorsque de la vidéo est proposée, en synchronisant en mode conversation totale la voix avec du texte (y compris du texte en temps réel) et de la vidéo.

Section VI

Exigences en matière d'accessibilité applicables aux caractéristiques, éléments ou fonctions des produits et services conformément à l'article 24, paragraphe 2

Pour qu'il soit présumé que les obligations pertinentes énoncées dans d'autres actes de l'Union en ce qui concerne les caractéristiques, éléments ou fonctions des produits et services sont satisfaites, les conditions ci-après doivent être remplies:

1. Produits:

a) L'accessibilité des informations relatives au fonctionnement et aux caractéristiques d'accessibilité liées aux produits est conforme aux éléments correspondants figurant à la section I, point 1, de la présente annexe, à savoir les informations sur l'utilisation du produit figurant sur le produit lui-même et les instructions concernant l'utilisation du produit qui ne sont pas fournies sur le produit lui-même, mais sont disponibles lors de l'utilisation du produit ou par d'autres moyens comme un site internet.

b) L'accessibilité des caractéristiques, éléments et fonctions de la conception de l'interface utilisateur et des fonctionnalités des produits est conforme aux exigences en matière d'accessibilité correspondantes énoncées à la section I, point 2, de la présente annexe.

c) L'accessibilité de l'emballage, y compris les informations contenues dans celui-ci, et des instructions concernant l'installation, l'entretien, le stockage et l'élimination du produit qui ne sont pas fournies sur le produit lui-même, mais sont disponibles par d'autres moyens comme un site internet, sauf en ce qui concerne les terminaux en libre-service, est conforme aux exigences en matière d'accessibilité correspondantes énoncées à la section II de la présente annexe.

2. Services:

L'accessibilité des caractéristiques, éléments et fonctions des services est conforme aux exigences en matière d'accessibilité correspondantes en ce qui concerne ces caractéristiques, éléments et fonctions énoncées dans les sections relatives aux services de la présente annexe.

Section VII

Critères en matière de performances fonctionnelles

Afin de garantir une utilisation prévisible optimale par les personnes handicapées, lorsque les exigences en matière d'accessibilité énoncées dans les sections I à VI ne traitent pas d'une ou plusieurs fonctions de la conception et de la fabrication des produits ou de la fourniture des services, ces fonctions ou moyens sont rendus accessibles par le respect des critères en matière de performances fonctionnelles qui y sont liés.

Lorsque les exigences en matière d'accessibilité comportent des exigences techniques spécifiques, les critères en matière de performances fonctionnelles ne peuvent se substituer à une ou plusieurs exigences techniques spécifiques que si et seulement si l'application des critères pertinents en matière de performances fonctionnelles est conforme aux exigences en matière d'accessibilité et qu'il est déterminé que la conception et la fabrication des produits et la fourniture des services donnent lieu à une accessibilité équivalente ou accrue dans le cadre d'une utilisation prévisible par les personnes handicapées.

a) Utilisation en l'absence de vision

Lorsque le produit ou service prévoit des modes visuels d'utilisation, il prévoit au moins un mode d'utilisation pour lequel la vue n'est pas nécessaire.

b) Utilisation en cas de vision limitée

Lorsque le produit ou service prévoit des modes visuels d'utilisation, il prévoit au moins un mode d'utilisation permettant aux utilisateurs d'utiliser le produit avec des capacités visuelles limitées.

c) Utilisation en l'absence de perception des couleurs

Lorsque le produit ou service prévoit des modes visuels d'utilisation, il prévoit au moins un mode d'utilisation pour lequel il n'est pas nécessaire que l'utilisateur perçoive les couleurs.

d) Utilisation en l'absence d'audition

Lorsque le produit ou service prévoit des modes auditifs d'utilisation, il prévoit au moins un mode d'utilisation pour lequel l'audition n'est pas nécessaire.

e) Utilisation en cas d'audition limitée

Lorsque le produit ou service prévoit des modes auditifs d'utilisation, il prévoit au moins un mode d'utilisation disposant de caractéristiques audio avancées, permettant aux utilisateurs ayant une audition limitée d'utiliser le produit.

f) Utilisation en l'absence de capacité vocale

Lorsque le produit ou service fonctionne via l'intervention vocale des utilisateurs, il prévoit au moins un mode d'utilisation ne nécessitant pas d'intervention vocale. L'intervention vocale fait référence à l'ensemble des sons générés oralement tels que des paroles, des sifflements ou des claquements de langue.

g) Utilisation en cas de capacités de manipulation ou de force limitées

Lorsque le produit ou service requiert des actions manuelles, il prévoit au moins un mode d'utilisation permettant aux utilisateurs d'utiliser le produit à l'aide d'autres actions ne nécessitant pas de commande fondée sur la motricité fine, la manipulation ou la force manuelle, ni l'utilisation de plus d'une commande au même moment.

h) Utilisation en cas d'amplitude de mouvements limitée

Les éléments servant au fonctionnement des produits sont à la portée de tous les utilisateurs. Lorsque le produit ou service prévoit un mode manuel d'utilisation, il prévoit au moins un mode d'utilisation permettant aux utilisateurs ayant une amplitude de mouvements et une force limitées d'utiliser le produit.

i) Réduction du risque de déclenchement de réactions photosensibles

Lorsque le produit prévoit des modes visuels d'utilisation, il évite les modes d'utilisation déclenchant des réactions photosensibles.

j) Utilisation en cas de capacités cognitives limitées

Le produit ou service prévoit au moins un mode d'utilisation intégrant des caractéristiques qui en rendent l'utilisation plus simple et plus facile.

k) Protection de la vie privée

Lorsque le produit ou service comporte des caractéristiques permettant l'accessibilité, il prévoit au moins un mode d'utilisation qui préserve la vie privée lors de l'utilisation de ces caractéristiques.

ANNEXE II

EXEMPLES INDICATIFS NON CONTRAIGNANTS DE SOLUTIONS POSSIBLES CONTRIBUANT À RESPECTER LES EXIGENCES EN MATIÈRE D'ACCESSIBILITÉ ÉNONCÉES À L'ANNEXE I

SECTION I:

EXEMPLES LIÉS AUX EXIGENCES GÉNÉRALES EN MATIÈRE D'ACCESSIBILITÉ APPLICABLES À TOUS LES PRODUITS RELEVANT DE LA PRÉSENTE DIRECTIVE CONFORMÉMENT À L'ARTICLE 2, PARAGRAPHE 1

EXIGENCES ÉNONCÉES À LA SECTION I DE L'ANNEXE I	EXEMPLES
1. Fourniture d'informations	
a)	
i)	Fournir des informations visuelles et tactiles ou des informations visuelles et auditives concernant l'endroit où il convient d'introduire une carte dans un terminal en libre-service, pour que les personnes aveugles et les personnes sourdes puissent utiliser le terminal.
ii)	Utiliser les mêmes termes de façon cohérente ou selon une structure claire et logique, pour que les personnes atteintes de déficience intellectuelle puissent mieux comprendre les informations.
iii)	Doubler un avertissement écrit d'une écriture tactile ou d'un son, pour que les personnes aveugles puissent le percevoir.
iv)	Faire en sorte que le texte puisse être lu par des personnes atteintes de déficience visuelle.
b)	
i)	Fournir des fichiers électroniques pouvant être lus par un ordinateur au moyen d'un logiciel de lecture d'écran pour que les personnes aveugles puissent utiliser les informations.
ii)	Utiliser les mêmes termes de façon cohérente ou selon une structure claire et logique, pour que les personnes atteintes de déficience intellectuelle puissent mieux comprendre les informations.
iii)	Fournir des sous-titres lorsque les instructions sont présentées dans une vidéo.
iv)	Faire en sorte que le texte puisse être lu par des personnes atteintes de déficience visuelle.
v)	Imprimer en braille, pour qu'une personne aveugle puisse utiliser les informations.
vi)	Doubler un diagramme d'une description textuelle précisant les principaux éléments ou décrivant les principales actions.
vii)	Aucun exemple fourni.
viii)	Aucun exemple fourni.
ix)	Inclure dans un guichet de banque automatique un connecteur logiciel et un logiciel permettant de brancher un casque qui retransmettra le texte apparaissant sur l'écran sous forme sonore.

2. Conception de l'interface utilisateur et des fonctionnalités	
a)	Fournir les instructions sous forme vocale et textuelle, ou prévoir des signes tactiles sur un clavier, pour que les personnes aveugles ou les personnes malentendantes puissent interagir avec le produit.
b)	Fournir, en plus des instructions vocales données par un terminal en libre-service, des instructions sous forme de texte ou d'images, pour que les personnes sourdes puissent elles aussi effectuer les actions requises.
c)	Permettre aux utilisateurs d'agrandir un texte, de zoomer sur un pictogramme précis ou de renforcer le contraste, pour que les personnes atteintes de déficience visuelle puissent percevoir les informations.
d)	En plus de donner la possibilité de presser le bouton vert ou le bouton rouge pour sélectionner une option, inscrire les options sur les boutons, pour que les personnes daltoniennes puissent faire leur choix.
e)	Lorsqu'un ordinateur émet un signal d'erreur, afficher un texte ou une image indiquant l'erreur, permettant ainsi aux personnes sourdes de savoir qu'une erreur se produit.
f)	Renforcer le contraste des images en avant-plan, pour que les personnes atteintes de déficience visuelle puissent les voir.
g)	Permettre à l'utilisateur d'un téléphone de sélectionner le volume et de réduire les interférences avec des appareils auditifs, pour que les personnes malentendantes puissent utiliser le téléphone.
h)	Agrandir et bien séparer les boutons de l'écran tactile, pour que les personnes atteintes de tremblement puissent les presser.
i)	Veiller à ce que les boutons à presser ne nécessitent pas une grande force, pour que les personnes atteintes de déficience motrice puissent les utiliser.
j)	Éviter les images qui clignotent, pour que les personnes atteintes d'épilepsie ne soient pas mises en danger.
k)	Permettre l'utilisation d'un casque lorsque des informations vocales sont communiquées par un guichet de banque automatique.
l)	Comme solution de substitution à la reconnaissance des empreintes digitales, permettre à des personnes qui ne peuvent pas faire usage de leurs mains de sélectionner un mot de passe pour bloquer ou débloquer un téléphone.
m)	Faire en sorte que le logiciel réagisse de manière prévisible lorsqu'une certaine action est effectuée et laisser suffisamment de temps pour saisir un mot de passe, pour que le produit soit aisé à utiliser pour des personnes atteintes de déficience mentale.
n)	Proposer une connexion à un afficheur braille actualisable pour que les personnes aveugles puissent utiliser l'ordinateur.
o)	Exemples d'exigences sectorielles
i)	Aucun exemple fourni.
ii)	Aucun exemple fourni.
iii) Premier tiret	Veiller à ce qu'un téléphone mobile soit en mesure de traiter des conversations par texte en temps réel, pour que les personnes malentendantes puissent échanger des informations de manière interactive.
iii) Quatrième tiret	Permettre l'utilisation simultanée de la vidéo pour afficher le langage des signes et du texte pour écrire un message, pour que deux personnes sourdes puissent communiquer entre elles ou avec une personne qui n'est pas sourde.

iv)	Veiller à ce que les sous-titres soient transmis via le décodeur, pour que les personnes sourdes puissent en faire usage.

3. Services d'assistance: Aucun exemple fourni.

SECTION II:

EXEMPLES LIÉS AUX EXIGENCES EN MATIÈRE D'ACCESSIBILITÉ APPLICABLES AUX PRODUITS VISÉS À L'ARTICLE 2, PARAGRAPHE 1, À L'EXCEPTION DES TERMINAUX EN LIBRE-SERVICE VISÉS À L'ARTICLE 2, PARAGRAPHE 1, POINT b)

EXIGENCES ÉNONCÉES À LA SECTION II DE L'ANNEXE I	EXEMPLES
Emballages des produits et instructions	
a)	Indiquer sur l'emballage que le téléphone contient des caractéristiques d'accessibilité pour les personnes handicapées.
b)	
i)	Fournir des fichiers électroniques pouvant être lus par un ordinateur au moyen d'un logiciel de lecture d'écran pour que les personnes aveugles puissent utiliser les informations.
ii)	Utiliser les mêmes termes de façon cohérente ou selon une structure claire et logique, pour que les personnes atteintes de déficience intellectuelle puissent mieux comprendre les informations.
iii)	Doubler un avertissement écrit d'une écriture tactile ou d'un son, pour que les personnes aveugles aient connaissance du message.
iv)	Faire en sorte que le texte puisse être lu par des personnes atteintes de déficience visuelle.
v)	Imprimer en braille, pour qu'une personne aveugle puisse lire les informations.
vi)	Doubler un diagramme d'une description textuelle précisant les principaux éléments ou décrivant les principales actions.

SECTION III:

EXEMPLES LIÉS AUX EXIGENCES GÉNÉRALES EN MATIÈRE D'ACCESSIBILITÉ APPLICABLES À TOUS LES SERVICES RELEVANT DE LA PRÉSENTE DIRECTIVE CONFORMÉMENT À L'ARTICLE 2, PARAGRAPHE 2

EXIGENCES ÉNONCÉES À LA SECTION III DE L'ANNEXE I	EXEMPLES
Fourniture de services	
a)	Aucun exemple fourni.
b)	
i)	Fournir des fichiers électroniques pouvant être lus par un ordinateur au moyen d'un logiciel de lecture d'écran pour que les personnes aveugles puissent utiliser les informations.
ii)	Utiliser les mêmes termes de façon cohérente ou selon une structure claire et logique, pour que les personnes atteintes de déficience intellectuelle puissent mieux comprendre les informations.
iii)	Fournir des sous-titres lorsque les instructions sont présentées dans une vidéo.

iv)	Veiller à ce qu'une personne aveugle puisse utiliser un fichier en l'imprimant en braille.
v)	Faire en sorte que le texte puisse être lu par des personnes atteintes de déficience visuelle.
vi)	Doubler un diagramme d'une description textuelle précisant les principaux éléments ou décrivant les principales actions.
vii)	Lorsqu'un prestataire de services propose une clé USB contenant des informations sur le service, veiller à ce que ces informations soient accessibles.
c)	Prévoir des descriptions textuelles des images, rendre toutes les fonctionnalités accessibles depuis un clavier, laisser suffisamment de temps aux utilisateurs pour lire les messages, faire apparaître le contenu et le faire fonctionner de manière prévisible, et veiller à la compatibilité avec les technologies d'assistance, pour que les personnes atteintes de diverses déficiences puissent consulter un site internet et interagir avec ce site.
d)	Aucun exemple fourni.

SECTION IV:

EXEMPLES LIÉS AUX EXIGENCES SUPPLÉMENTAIRES EN MATIÈRE D'ACCESSIBILITÉ APPLICABLES À DES SERVICES SPÉCIFIQUES

EXIGENCES ÉNONCÉES À LA SECTION IV DE L'ANNEXE I	EXEMPLES
Services spécifiques	
a)	
i)	Faire en sorte que les personnes malentendantes puissent écrire et recevoir un texte de manière interactive et en temps réel.
ii)	Faire en sorte que des personnes sourdes puissent utiliser le langage des signes pour communiquer entre elles.
iii)	Faire en sorte qu'une personne atteinte de déficience de la parole et de l'ouïe qui choisit d'utiliser une combinaison de texte, de voix et de vidéo sache que la communication est transmise par le réseau à un service d'urgence.
b)	
i)	Faire en sorte qu'une personne aveugle puisse sélectionner des programmes à la télévision.
ii)	Offrir la possibilité de sélectionner, de personnaliser et d'afficher des services d'accès tels que le sous-titrage pour les personnes sourdes ou malentendantes, l'audiodescription, le sous-titrage audio et l'interprétation en langue des signes, en proposant des moyens permettant une connexion sans fil efficace aux technologies auditives ou en fournissant à l'utilisateur des commandes permettant d'activer des services d'accès pour les services de médias audiovisuels, au même niveau que les commandes primaires.
c)	
i)	Aucun exemple fourni.
ii)	Aucun exemple fourni.
d)	Aucun exemple fourni.
e)	
i)	Faire en sorte que les dialogues d'identification soient lisibles au moyen d'un logiciel de lecture d'écran, pour que les personnes aveugles puissent les utiliser.

ii)	Aucun exemple fourni.
f)	
i)	Faire en sorte qu'une personne atteinte de dyslexie puisse lire et entendre le texte en même temps.
ii)	Permettre une restitution textuelle et audio synchronisée ou une transcription braille actualisable.
iii)	Faire en sorte qu'une personne aveugle puisse accéder à l'index ou changer de chapitre.
iv)	Aucun exemple fourni.
v)	Veiller à ce que les informations sur les caractéristiques d'accessibilité soient disponibles dans le fichier électronique, pour que les personnes handicapées puissent être informées.
vi)	Veiller, par exemple, à ce que la lecture à haute voix du texte par des dispositifs d'assistance ne soit pas empêchée par des mesures de protection technique, des informations sur la gestion des droits ou des problèmes d'interopérabilité, de manière que les utilisateurs aveugles puissent lire le livre.
g)	
i)	Veiller à ce que les informations disponibles sur les caractéristiques d'accessibilité d'un produit ne soient pas supprimées.
ii)	Faire en sorte que l'interface utilisateur d'un service de paiement soit accessible par la voix, pour que les personnes aveugles puissent effectuer des achats en ligne en toute indépendance.
iii)	Faire en sorte que les dialogues d'identification soient lisibles au moyen d'un logiciel de lecture d'écran, pour que les personnes aveugles puissent les utiliser.

ANNEXE III

EXIGENCES EN MATIÈRE D'ACCESSIBILITÉ AUX FINS DE L'ARTICLE 4, PARAGRAPHE 4, EN CE QUI CONCERNE L'ENVIRONNEMENT BÂTI À L'ENDROIT OÙ LES SERVICES RELEVANT DE LA PRÉSENTE DIRECTIVE SONT FOURNIS

Afin de garantir une utilisation prévisible optimale et indépendante, par les personnes handicapées, de l'environnement bâti visé à l'article 4, paragraphe 4, à l'endroit où un service est fourni sous la responsabilité du prestataire de services, l'accessibilité des zones destinées au public, comprend les éléments suivants:

a) utilisation des zones et installations extérieures;

b) abords des bâtiments;

c) utilisation des entrées;

d) utilisation des voies de circulation horizontale;

e) utilisation des voies de circulation verticale;

f) utilisation des salles ouvertes au public;

g) utilisation d'équipements et d'installations utilisés pour la fourniture du service;

h) utilisation des toilettes et autres installations sanitaires;

i) utilisation des sorties, des issues de secours et des éléments relevant de la planification des mesures d'urgence;

j) communications et orientations au moyen de plusieurs canaux sensoriels;

k) utilisation des installations et des bâtiments conformément à leur utilisation prévisible;

l) protection contre les dangers émanant de l'environnement intérieur et extérieur.

ANNEXE IV

PROCÉDURES D'ÉVALUATION DE LA CONFORMITÉ — PRODUITS

1. Contrôle interne de la fabrication

Le contrôle interne de la fabrication est la procédure d'évaluation de la conformité par laquelle le fabricant remplit les obligations définies aux points 2, 3 et 4 de la présente annexe, et assure et déclare sous sa seule responsabilité que les produits concernés satisfont aux exigences applicables de la présente directive.

2. Documentation technique

La documentation technique est établie par le fabricant. Elle permet d'évaluer la conformité du produit avec les exigences en matière d'accessibilité visées à l'article 4 ainsi que, dans le cas où le fabricant s'est fondé sur l'article 14, de démontrer que la conformité avec les exigences en matière d'accessibilité introduirait une modification fondamentale ou imposerait une charge disproportionnée. La documentation technique précise uniquement les exigences applicables et porte, dans la mesure nécessaire à l'évaluation, sur la conception, la fabrication et le fonctionnement du produit.

La documentation technique comporte, le cas échéant, au moins les éléments suivants:

a) une description générale du produit;

b) une liste des normes harmonisées et des spécifications techniques dont les références ont été publiées au *Journal officiel de l'Union européenne* et qui ont été intégralement ou partiellement appliquées, ainsi qu'une description des solutions adoptées pour satisfaire aux exigences en matière d'accessibilité visées à l'article 4 lorsque ces normes harmonisées ou ces spécifications techniques n'ont pas été appliquées. En cas d'application partielle de normes harmonisées ou de spécifications techniques, la documentation technique précise quelles parties ont été appliquées.

3. Fabrication

Le fabricant prend toutes les mesures nécessaires pour que le procédé de fabrication et le suivi de celui-ci assurent la conformité des produits avec la documentation technique visée au point 2 de la présente annexe et avec les exigences en matière d'accessibilité énoncées dans la présente directive.

4. Marquage CE et déclaration de conformité UE

4.1. Le fabricant appose le marquage CE visé dans la présente directive sur chaque produit qui est conforme aux exigences applicables de la présente directive.

4.2. Le fabricant établit une déclaration écrite de conformité UE concernant un modèle de produit. La déclaration de conformité UE précise le produit pour lequel elle a été établie.

Une copie de la déclaration de conformité UE est mise à la disposition des autorités compétentes sur demande.

5. Mandataire

Les obligations du fabricant énoncées au point 4 peuvent être remplies par son mandataire, en son nom et sous sa responsabilité, pour autant qu'elles soient spécifiées dans le mandat.

ANNEXE V

INFORMATIONS SUR LES SERVICES CONFORMES AUX EXIGENCES EN MATIÈRE D'ACCESSIBILITÉ

1. Le prestataire de services inclut les informations évaluant la façon dont le service respecte les exigences en matière d'accessibilité visées à l'article 4 dans les clauses et conditions générales ou dans un document équivalent. Ces informations décrivent les exigences applicables et portent, dans la mesure nécessaire à l'évaluation, sur la conception et le fonctionnement du service. Outre l'information du consommateur exigée en vertu de la directive 2011/83/UE, cette documentation comporte, le cas échéant, les éléments suivants:

   a) une description générale du service dans des formats accessibles;

   b) les descriptions et explications nécessaires pour comprendre le fonctionnement du service;

   c) une description de la manière dont les exigences en matière d'accessibilité prévues à l'annexe I sont remplies par le service.

2. Pour satisfaire aux exigences du point 1 de la présente annexe, le prestataire de services peut appliquer entièrement ou en partie les normes harmonisées et les spécifications techniques dont les références ont été publiées au *Journal officiel de l'Union européenne*.

3. Le prestataire de services fournit des informations démontrant que le procédé de prestation du service et le suivi de celui-ci assurent sa conformité avec le point 1 de la présente annexe et avec les exigences applicables de la présente directive.

ANNEXE VI

CRITÈRES D'ÉVALUATION DU CARACTÈRE DISPROPORTIONNÉ DE LA CHARGE

Critères pour l'évaluation et preuves à apporter à l'appui de cette évaluation:

1. Rapport entre les coûts nets de la conformité avec les exigences en matière d'accessibilité et les coûts totaux (dépenses opérationnelles et dépenses en capital) pour fabriquer, distribuer ou importer le produit ou fournir le service que supportent les opérateurs économiques.

   Éléments à appliquer pour évaluer les coûts nets de la conformité avec les exigences en matière d'accessibilité:

   a) critères liés à des coûts organisationnels ponctuels à prendre en considération dans l'évaluation:

      i) coûts liés à des ressources humaines supplémentaires spécialisées dans les questions d'accessibilité;

      ii) coûts liés à la formation des ressources humaines et à l'acquisition de compétences en matière d'accessibilité;

      iii) coûts liés à la mise au point d'un nouveau procédé pour inclure l'accessibilité dans le développement de produits ou la prestation de services;

      iv) coûts liés à la mise au point d'orientations concernant l'accessibilité;

      v) coûts ponctuels liés à l'examen de la législation sur l'accessibilité;

   b) critères liés aux coûts récurrents de développement et de production à prendre en considération dans l'évaluation:

      i) coûts liés à la conception des caractéristiques d'accessibilité pour le produit ou le service;

      ii) coûts supportés dans le cadre des procédés de fabrication;

      iii) coûts liés aux essais d'accessibilité concernant le produit ou le service;

      iv) coûts liés à l'établissement de la documentation.

2. Estimation des coûts et des avantages pour les opérateurs économiques, y compris en ce qui concerne les processus de production et les investissements, par rapport à l'avantage estimé pour les personnes handicapées, compte tenu de la quantité et de la fréquence d'utilisation d'un produit ou d'un service spécifique.

3. Rapport entre les coûts nets de la conformité avec les exigences en matière d'accessibilité et le chiffre d'affaires net de l'opérateur économique.

   Éléments à appliquer pour évaluer les coûts nets de la conformité avec les exigences en matière d'accessibilité:

   a) critères liés à des coûts organisationnels ponctuels à prendre en considération dans l'évaluation:

      i) coûts liés à des ressources humaines supplémentaires spécialisées dans les questions d'accessibilité;

      ii) coûts liés à la formation des ressources humaines et à l'acquisition de compétences en matière d'accessibilité;

      iii) coûts liés à la mise au point d'un nouveau procédé pour inclure l'accessibilité dans le développement de produits ou la prestation de services;

      iv) coûts liés à la mise au point d'orientations concernant l'accessibilité;

      v) coûts ponctuels liés à l'examen de la législation sur l'accessibilité;

   b) critères liés aux coûts récurrents de développement et de production à prendre en considération dans l'évaluation:

      i) coûts liés à la conception des caractéristiques d'accessibilité pour le produit ou le service;

      ii) coûts supportés dans le cadre des procédés de fabrication;

      iii) coûts liés aux essais d'accessibilité concernant le produit ou le service;

      iv) coûts liés à l'établissement de la documentation.

DIRECTIVE (UE) 2019/883 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 17 avril 2019

relative aux installations de réception portuaires pour le dépôt des déchets des navires, modifiant la directive 2010/65/UE et abrogeant la directive 2000/59/CE

(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 100, paragraphe 2,

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 ([1]),

vu l'avis du Comité des régions ([2]),

statuant conformément à la procédure législative ordinaire ([3]),

considérant ce qui suit:

(1) La politique maritime de l'Union vise à assurer un niveau élevé de sécurité et de protection de l'environnement. Cet objectif peut être atteint par le respect des conventions, codes et résolutions internationaux tout en maintenant la liberté de navigation prévue par la convention des Nations unies sur le droit de la mer (CNUDM).

(2) L'objectif de développement durable n° 14 des Nations unies attire l'attention sur les menaces que représentent la pollution marine et la pollution par les nutriments, l'épuisement des ressources et le changement climatique, lesquels sont tous causés principalement par des actions humaines. Ces menaces exercent une pression supplémentaire sur les systèmes environnementaux, tels que la biodiversité et les infrastructures naturelles, tout en entraînant des problèmes socio-économiques mondiaux, notamment des risques pour la santé et la sécurité et des risques financiers. L'Union doit œuvrer à la protection des espèces marines et soutenir les populations qui dépendent des océans, que ce soit pour l'emploi, les ressources ou les loisirs.

(3) La convention internationale pour la prévention de la pollution par les navires (ci-après dénommée «convention MARPOL») prévoit des interdictions générales en matière de rejets en mer des déchets des navires, mais régit aussi les conditions dans lesquelles certains types de déchets peuvent être déversés dans le milieu marin. La convention MARPOL exige des parties contractantes qu'elles garantissent la mise à disposition d'installations de réception adéquates dans les ports.

(4) L'Union a poursuivi la mise en œuvre de parties de la convention MARPOL par le biais de la directive 2000/59/CE du Parlement européen et du Conseil ([4]) et en suivant une approche fondée sur les ports. La directive 2000/59/CE vise à concilier les intérêts d'un bon fonctionnement des transports maritimes et la protection du milieu marin.

(5) Au cours des deux dernières décennies, la convention MARPOL et ses annexes ont fait l'objet d'amendements importants, qui ont permis de fixer des normes plus strictes et de poser des interdictions de rejets en mer de déchets des navires.

(6) L'annexe VI de la convention MARPOL a introduit des normes en matière de rejet pour de nouvelles catégories de déchets, notamment les résidus des systèmes d'épuration des gaz d'échappement, qui comprennent à la fois des boues et des eaux d'écoulement. Ces catégories de déchets devraient être incluses dans le champ d'application de la présente directive.

([1]) JO C 283 du 10.8.2018, p. 61.
([2]) JO C 461 du 21.12.2018, p. 220.
([3]) Position du Parlement européen du 13 mars 2019 (non encore parue au Journal officiel) et décision du Conseil du 9 avril 2019.
([4]) Directive 2000/59/CE du Parlement européen et du Conseil du 27 novembre 2000 sur les installations de réception portuaires pour les déchets d'exploitation des navires et les résidus de cargaison (JO L 332 du 28.12.2000, p. 81).

(7) Il convient que les États membres continuent à travailler au niveau de l'Organisation maritime internationale (OMI) pour envisager de manière globale les incidences environnementales des rejets d'eaux résiduaires provenant des scrubbers à circuit ouvert, y compris pour que des mesures soient prises en vue de lutter contre les incidences possibles.

(8) Il y a lieu d'encourager les États membres à prendre des mesures appropriées conformément à la directive 2000/60/CE du Parlement européen et du Conseil ([5]), y compris des interdictions de rejets d'eaux résiduaires provenant de scrubbers à circuit ouvert et de certains résidus de cargaisons dans leurs eaux territoriales.

(9) Le 1er mars 2018, l'OMI a adopté le guide récapitulatif à l'intention des fournisseurs et des utilisateurs d'installations de réception portuaires révisé (MEPC.1/Circ. 834/Rev.1) (ci-après dénommé «guide récapitulatif de l'OMI»), qui comprend des modèles types pour la notification des déchets, pour le reçu du dépôt des déchets et pour la notification de l'inadéquation présumée des installations de réception portuaires, ainsi que pour les prescriptions relatives à la soumission de rapports sur les installations portuaires de réception des déchets.

(10) Malgré ces évolutions réglementaires, les rejets de déchets en mer se poursuivent et leurs coûts environnementaux et socio-économiques sont considérables. Cela s'explique par une combinaison de facteurs, à savoir des installations de réception portuaires adéquates qui ne sont pas toujours disponibles dans les ports, le contrôle de l'application qui est souvent insuffisant et le manque d'incitations à déposer les déchets à terre.

(11) La directive 2000/59/CE a contribué à l'augmentation des volumes de déchets déposés dans les installations de réception portuaires, notamment en garantissant que les navires contribuent aux coûts de ces installations, indépendamment de leur utilisation effective de ces installations et, partant, elle a joué un rôle crucial dans la réduction des rejets de déchets en mer, comme l'atteste l'évaluation de ladite directive qui a été effectuée dans le cadre du programme pour une réglementation affûtée et performante (ci-après dénommée «évaluation REFIT»).

(12) L'évaluation REFIT a aussi démontré que la directive 2000/59/CE n'a pas été pleinement efficace en raison d'incohérences avec le cadre de la convention MARPOL. En outre, les États membres ont développé des interprétations divergentes des concepts clés de ladite directive, tels que l'adéquation des installations, la notification préalable des déchets, l'obligation de dépôt dans les installations de réception portuaires et les exemptions pour les navires exploités sur des lignes régulières. L'évaluation REFIT a mis en exergue la nécessité d'harmoniser davantage ces concepts et de s'aligner pleinement sur la convention MARPOL afin d'éviter une charge administrative inutile, tant pour les ports que pour les utilisateurs du port.

(13) Afin d'aligner la directive 2005/35/CE du Parlement européen et du Conseil ([6]) sur les dispositions pertinentes de la convention MARPOL en matière de normes de rejet, la Commission devrait évaluer l'opportunité d'un réexamen de cette directive, notamment par une extension de son champ d'application.

(14) La politique maritime de l'Union devrait avoir pour objectif un niveau élevé de protection de l'environnement marin qui tienne compte de la diversité des zones maritimes de l'Union. Il convient qu'elle repose sur les principes d'action préventive, de correction en priorité à la source des atteintes à l'environnement, et du pollueur-payeur.

(15) La présente directive devrait également être essentielle pour l'application des principaux textes législatifs et principes en matière d'environnement dans les ports et dans le cadre de la gestion des déchets des navires. En particulier, les directives 2008/56/CE ([7]) et 2008/98/CE ([8]) du Parlement européen et du Conseil sont des instruments pertinents à cet égard.

(16) La directive 2008/98/CE énonce les grands principes en matière de gestion des déchets, notamment le principe du «pollueur-payeur» et la hiérarchie des déchets, lequel prône le réemploi et le recyclage des déchets plutôt que d'autres formes de valorisation et d'élimination des déchets et exige la mise en place de systèmes de collecte séparée des déchets. En outre, la notion de responsabilité élargie du producteur est un principe directeur du droit de l'Union en matière de déchets, en vertu duquel les producteurs sont responsables des effets qu'ont leurs produits sur l'environnement tout au long de leur cycle de vie. Ces obligations s'appliquent aussi à la gestion des déchets des navires.

([5]) Directive 2000/60/CE du Parlement européen et du Conseil du 23 octobre 2000 établissant un cadre pour une politique communautaire dans le domaine de l'eau (JO L 327 du 22.12.2000, p. 1).

([6]) Directive 2005/35/CE du Parlement européen et du Conseil du 7 septembre 2005 relative à la pollution causée par les navires et à l'introduction de sanctions, notamment pénales, en cas d'infractions de pollution (JO L 255 du 30.9.2005, p. 11).

([7]) Directive 2008/56/CE du Parlement européen et du Conseil du 17 juin 2008 établissant un cadre d'action communautaire dans le domaine de la politique pour le milieu marin (directive-cadre «stratégie pour le milieu marin») (JO L 164 du 25.6.2008, p. 19).

([8]) Directive 2008/98/CE du Parlement européen et du Conseil du 19 novembre 2008 relative aux déchets et abrogeant certaines directives (JO L 312 du 22.11.2008, p. 3).

(17) La collecte séparée des déchets des navires, y compris des engins de pêche laissés à l'abandon, est nécessaire afin de garantir la poursuite de leur valorisation pour permettre leur préparation en vue du réemploi ou du recyclage dans le processus de gestion des déchets en aval et d'empêcher qu'ils ne nuisent aux organismes et aux milieux marins. Les déchets sont fréquemment triés à bord des navires conformément aux règles et normes internationales, et le droit de l'Union devrait garantir que ces efforts de tri des déchets à bord ne sont pas compromis par un manque de dispositifs de collecte séparée à terre.

(18) Chaque année, des quantités importantes de matières plastiques finissent dans les mers et les océans au sein de l'Union. Bien que, dans la plupart des zones maritimes, la majeure partie des déchets sauvages dans le milieu marin proviennent d'activités terrestres, le secteur des transports maritimes, y compris celui de la pêche et de la navigation de plaisance, joue un rôle non négligeable du fait du rejet direct de déchets dans la mer, y compris de matières plastiques et d'engins de pêche abandonnés.

(19) La directive 2008/98/CE invite les États membres à mettre fin à la production de déchets sauvages dans le milieu marin afin de contribuer à l'objectif de développement durable des Nations unies visant à prévenir et à réduire nettement la pollution marine de tous types.

(20) La communication de la Commission du 2 décembre 2015 intitulée «Boucler la boucle - Un plan d'action de l'Union européenne en faveur de l'économie circulaire» a reconnu le rôle spécifique que la directive 2000/59/CE a été amenée à jouer à cet égard, en garantissant la disponibilité d'installations adéquates pour la réception des déchets et en prévoyant à la fois le niveau approprié d'incitations et le contrôle de l'application de l'obligation de dépôt de déchets dans les installations à terre.

(21) Les installations offshore sont l'une des sources de production en mer de déchets sauvages dans le milieu marin. C'est la raison pour laquelle les États membres devraient adopter les mesures qui conviennent en matière de dépôt de déchets en provenance d'installations offshore battant leur pavillon ou opérant dans leurs eaux, ou les deux, et garantir le respect des normes rigoureuses relatives au rejet de déchets applicables aux installations offshore qui figurent dans la convention MARPOL.

(22) Les déchets, et en particulier les matières plastiques, provenant de cours d'eau figurent parmi les principales composantes des déchets sauvages dans le milieu marin, en ce compris les rejets des bateaux de navigation intérieure. Dès lors, il y a lieu de soumettre ces bateaux à des normes rigoureuses en matière de rejet et de dépôt de déchets. Aujourd'hui, ces règles sont établies par la commission fluviale compétente. Toutefois, les ports intérieurs sont couverts par le droit de l'Union en matière de déchets. Afin de poursuivre les efforts d'harmonisation du cadre législatif pour les voies de navigation intérieure de l'Union, la Commission est invitée à évaluer un régime de l'Union de normes de rejet et de dépôt pour les bateaux de navigation intérieure, en tenant compte de la convention relative à la collecte, au dépôt et à la réception des déchets survenant en navigation rhénane et intérieure du 9 septembre 1996 (CDNI).

(23) Le règlement (CE) n° 1224/2009 du Conseil ([9]) fait obligation aux navires de pêche de l'Union de disposer à bord de l'équipement nécessaire pour récupérer les engins perdus. En cas de perte d'un engin, le capitaine du navire est tenu d'essayer de le récupérer dès que possible. Si l'engin perdu ne peut être retrouvé, le capitaine du navire de pêche doit en informer les autorités de l'État membre de son pavillon dans les vingt-quatre heures. L'État membre de son pavillon doit en informer à son tour l'autorité compétente de l'État membre côtier. Les informations comprennent le numéro d'identification externe et le nom du navire de pêche, le type d'engin perdu et la position de celui-ci, ainsi que les mesures prises pour le récupérer. Les navires de pêche d'une longueur inférieure à douze mètres peuvent être exemptés. Aux termes de la proposition de règlement du Parlement et du Conseil modifiant le règlement (CE) n° 1224/2009 du Conseil, la déclaration par le navire de pêche doit être faite dans un journal de pêche électronique, et les États membres sont tenus de recueillir et de consigner les informations concernant les engins perdus et de communiquer ces informations à la Commission, sur demande. Les informations recueillies et figurant sur les reçus de dépôt des déchets concernant les déchets pêchés passivement, conformément à la présente directive, pourraient également être déclarées de cette façon.

(24) Conformément à la convention internationale pour le contrôle et la gestion des eaux de ballast et sédiments des navires, qui a été adoptée par l'OMI le 13 février 2004 et qui est entrée en vigueur le 8 septembre 2017, tous les navires sont tenus d'appliquer des procédures de gestion des eaux de ballast conformément aux normes de l'OMI, et les ports et les terminaux où ont lieu le nettoyage et les réparations des citernes à ballast sont tenus de fournir des installations adéquates pour la réception des sédiments.

([9]) Règlement (CE) n° 1224/2009 du Conseil du 20 novembre 2009 instituant un régime de l'Union de contrôle afin d'assurer le respect des règles de la politique commune de la pêche, modifiant les règlements (CE) n° 847/96, (CE) n° 2371/2002, (CE) n° 811/2004, (CE) n° 768/2005, (CE) n° 2115/2005, (CE) n° 2166/2005, (CE) n° 388/2006, (CE) n° 509/2007, (CE) n° 676/2007, (CE) n° 1098/2007, (CE) n° 1300/2008, (CE) n° 1342/2008 et abrogeant les règlements (CEE) n° 2847/93, (CE) n° 1627/94 et (CE) n° 1966/2006 (JO L 343 du 22.12.2009, p. 1).

(25) Une installation de réception portuaire est considérée comme adéquate si elle est en mesure de répondre aux besoins des navires utilisant habituellement le port sans causer de retards anormaux, comme cela est également indiqué dans le guide récapitulatif de l'OMI et dans les lignes directrices de l'OMI visant à garantir l'adéquation des installations portuaires de réception des déchets (résolution MEPC.83(44)]. Le caractère adéquat a trait à la fois aux conditions d'exploitation de l'installation au regard des besoins des utilisateurs et à la gestion environnementale des installations conformément au droit de l'Union en matière de déchets. Il pourrait s'avérer difficile, dans certains cas, d'évaluer si une installation de réception portuaire située en dehors de l'Union respecte une telle norme.

(26) Le règlement (CE) n° 1069/2009 du Parlement européen et du Conseil ([10]) exige que les déchets de cuisine et de table issus de voyages internationaux soient incinérés ou éliminés par enfouissement dans une décharge autorisée, y compris les déchets des navires faisant escale dans des ports de l'Union et qui sont susceptibles d'avoir été en contact avec des sous-produits animaux à bord. Afin que cette exigence ne limite pas la préparation en vue du réemploi et du recyclage ultérieurs des déchets des navires, il convient de s'efforcer, conformément au guide récapitulatif de l'OMI, de mieux trier les déchets afin d'éviter le risque de contamination des déchets, comme les déchets d'emballage.

(27) Ainsi que le prévoit le règlement (CE) n° 1069/2009, en liaison avec le règlement (UE) n° 142/2011 de la Commission ([11]), les voyages à l'intérieur de l'Union ne sont pas considérés comme du transport opérant au niveau international et les déchets de cuisine et de table provenant de ces voyages ne doivent pas obligatoirement être incinérés. Toutefois, ces voyages à l'intérieur de l'Union sont considérés comme des voyages internationaux au titre de la législation maritime internationale (la convention MARPOL et la convention internationale pour la sauvegarde de la vie humaine en mer (SOLAS)]. Afin d'assurer la cohérence du droit de l'Union, il convient de respecter les définitions énoncées dans le règlement (CE) n° 1069/2009 au moment de définir le champ d'application et le traitement des déchets de cuisine et de table internationaux dans le cadre de la présente directive, en liaison avec le règlement (UE) n° 142/2011.

(28) Pour garantir l'adéquation des installations de réception portuaires, il est indispensable d'élaborer, de mettre en œuvre et de réévaluer le plan de réception et de traitement des déchets sur la base de la consultation de toutes les parties concernées. Pour des raisons d'ordre pratique et organisationnel, les ports voisins d'une même région géographique pourraient souhaiter établir un plan conjoint portant sur la disponibilité des installations de réception portuaires dans chacun des ports couverts par le plan tout en offrant un cadre administratif commun.

(29) Il peut s'avérer difficile d'adopter et de contrôler des plans de réception et de traitement des déchets pour les petits ports non-commerciaux, tels que les zones d'amarrage et les marinas, dont le trafic - constitué uniquement de bateaux de plaisance - est faible, ou qui ne sont utilisés que pendant une partie de l'année. En règle générale, les déchets provenant de ces petits ports sont traités par le système municipal de gestion des déchets conformément aux principes énoncés dans la directive 2008/98/CE. Afin de ne pas surcharger les autorités locales et de faciliter la gestion des déchets dans ces petits ports, il devrait suffire que les déchets provenant de ces ports soient inclus dans le flux de déchets municipaux et gérés en conséquence, que le port communique aux utilisateurs du port les informations relatives à la réception des déchets, et que les ports exemptés soient signalés dans un système électronique afin de pouvoir réduire le contrôle au minimum.

(30) Pour résoudre le problème des déchets sauvages dans le milieu marin de manière efficace, il est essentiel de prévoir un niveau adéquat de mesures d'incitation au dépôt des déchets dans les installations de réception portuaires, en particulier des déchets définis à l'annexe V de la convention MARPOL (ci-après dénommés «déchets relevant de l'annexe V de MARPOL»). Il est possible d'y parvenir grâce à un système de recouvrement des coûts qui impose l'application d'une redevance indirecte. Il convient que cette redevance indirecte soit due indépendamment du fait que des déchets soient déposés ou non, et devrait donner le droit de déposer des déchets sans paiement de frais directs supplémentaires. Les secteurs de la pêche et de la navigation de plaisance devraient également être soumis à la redevance indirecte en raison de leur part dans le déversement en mer de déchets sauvages dans le milieu marin. Toutefois, lorsqu'un navire dépose un volume exceptionnel de déchets relevant de l'annexe V de MARPOL, en particulier des déchets d'exploitation, qui excède la capacité de stockage dédiée maximale indiquée dans le formulaire de notification préalable de dépôt de déchets, il devrait être possible de percevoir une redevance directe supplémentaire pour faire en sorte que les coûts liés à la réception de ce volume exceptionnel de déchets ne fassent pas peser une charge disproportionnée sur le système de recouvrement des coûts d'un port. Tel pourrait également être le cas lorsque la capacité de stockage dédiée déclarée est excessive ou déraisonnable.

([10]) Règlement (CE) n° 1069/2009 du Parlement européen et du Conseil du 21 octobre 2009 établissant des règles sanitaires applicables aux sous-produits animaux et produits dérivés non destinés à la consommation humaine et abrogeant le règlement (CE) n° 1774/2002 (règlement relatif aux sous-produits animaux) (JO L 300 du 14.11.2009, p. 1).

([11]) Règlement (UE) n° 142/2011 de la Commission du 25 février 2011 portant application du règlement (CE) n° 1069/2009 du Parlement européen et du Conseil établissant des règles sanitaires applicables aux sous-produits animaux et produits dérivés non destinés à la consommation humaine et portant application de la directive 97/78/CE du Conseil en ce qui concerne certains échantillons et articles exemptés des contrôles vétérinaires effectués aux frontières en vertu de cette directive (JO L 54 du 26.2.2011, p. 1).

(31) Dans certains États membres, des dispositifs ont été mis en place pour offrir d'autres modes de financement des coûts de collecte et de gestion à terre des déchets d'engins de pêche ou des déchets pêchés passivement, y compris les «systèmes de pêche aux déchets sauvages». Il convient d'accueillir positivement de telles initiatives et d'encourager les États membres à compléter les systèmes de recouvrement des coûts mis en place conformément à la présente directive par des systèmes de pêche aux déchets sauvages afin de couvrir les coûts des déchets pêchés passivement. En tant que tels, ces systèmes de recouvrement des coûts, qui s'appuient sur l'application d'une redevance indirecte de 100 % sur les déchets relevant de l'annexe V de MARPOL, à l'exclusion des résidus de cargaison, ne devraient pas dissuader les communautés portuaires de pêcheurs de participer aux systèmes existants de dépôt des déchets pêchés passivement.

(32) La redevance applicable à un navire devrait être réduite pour les navires qui sont conçus, équipés ou exploités de manière à réduire au minimum les déchets, dans le respect de certains critères dont l'élaboration est du ressort des compétences d'exécution conférées à la Commission, en conformité avec les lignes directrices de l'OMI pour la mise en œuvre de l'annexe V de MARPOL et avec les normes élaborées par l'Organisation internationale de normalisation. La réduction et le recyclage efficace des déchets peuvent être obtenus avant tout par un véritable tri des déchets à bord selon ces lignes directrices et ces normes.

(33) En raison du type de commerce auquel il est lié, qui se caractérise par des escales portuaires fréquentes, le transport maritime à courte distance est confronté à des coûts considérables dans le cadre du régime actuel de dépôt des déchets dans les installations de réception portuaires, une redevance étant due à chaque escale dans un port. Dans le même temps, le trafic n'est pas organisé de manière suffisamment régulière pour donner lieu à une exemption de paiement ou de dépôt de déchets pour ces motifs. Afin de limiter la charge financière pesant sur le secteur, il convient d'appliquer une redevance réduite aux navires en fonction du type de trafic pour lequel ils sont utilisés.

(34) Les résidus de cargaison restent la propriété du propriétaire de la cargaison après son déchargement au terminal et peuvent avoir une valeur économique. C'est pourquoi les résidus de cargaison ne devraient pas être inclus dans les systèmes de recouvrement des coûts qui prévoient l'application de la redevance indirecte. Les frais de dépôt de résidus de cargaison devraient être acquittés par l'utilisateur de l'installation de réception portuaire, comme précisé dans les arrangements contractuels entre les parties concernées ou dans d'autres arrangements locaux. Parmi les résidus de cargaison figurent également les restes de cargaisons liquides huileuses ou nocives après les opérations de nettoyage, auxquels s'appliquent les normes en matière de rejet figurant aux annexes I et II de la convention MARPOL et qui, sous certaines conditions énoncées auxdites annexes, ne doivent pas nécessairement être déposés au port afin d'éviter des coûts d'exploitation inutiles pour les navires et un engorgement des ports.

(35) Les États membres devraient encourager le dépôt de résidus de lavage de citernes contenant des substances flottantes persistantes à haute viscosité, éventuellement en octroyant des incitations financières appropriées.

(36) Le règlement (UE) 2017/352 du Parlement européen et du Conseil [12] prévoit que la mise à disposition d'installations de réception portuaires est un service qui relève de son champ d'application. Il contient des règles en matière de transparence des structures tarifaires appliquées à l'utilisation de services portuaires, de consultation des utilisateurs du port et de procédures de traitement des plaintes. La présente directive va au-delà du cadre offert par ledit règlement en prévoyant des exigences plus détaillées concernant la conception et le fonctionnement des systèmes de recouvrement des coûts applicables aux installations de réception portuaires pour les déchets des navires et la transparence de la structure des coûts.

(37) Outre la mise en place d'incitations au dépôt des déchets, le contrôle effectif du respect de l'obligation de dépôt est crucial et devrait suivre une approche fondée sur les risques pour laquelle il convient d'établir un mécanisme de ciblage de l'Union fondé sur les risques.

(38) Un des principaux freins au contrôle effectif de l'obligation de dépôt est que les États membres ont interprété et, partant, mis en œuvre de manière divergente l'exception fondée sur une capacité de stockage suffisante. Pour éviter que l'application de cette exception ne compromette le principal objectif de la présente directive, il convient de la définir plus précisément, notamment en ce qui concerne la notion de port d'escale suivant, et de déterminer une capacité de stockage suffisante de manière harmonisée, en s'appuyant sur une méthode et des critères communs. Dans les cas où il s'avère difficile d'établir si des installations de réception portuaires adéquates sont disponibles dans un port situé en dehors de l'Union, il est essentiel que l'autorité compétente examine avec soin l'application de l'exception.

[12] Règlement (UE) 2017/352 du Parlement européen et du Conseil du 15 février 2017 établissant un cadre pour la fourniture de services portuaires et des règles communes relatives à la transparence financière des ports (JO L 57 du 3.3.2017, p. 1).

(39) Il est nécessaire de poursuivre l'harmonisation du régime des exemptions pour les navires exploités sur des lignes régulières qui comportent des escales portuaires fréquentes et régulières, et plus particulièrement de clarifier les termes utilisés et les conditions régissant ces exemptions. L'évaluation REFIT et l'analyse d'impact ont fait apparaître que le manque d'harmonisation des conditions et de l'application des exemptions avait engendré une charge administrative indue pour les navires et les ports.

(40) La mise en place d'un système reposant sur la déclaration électronique et l'échange électronique d'informations devrait faciliter le suivi et le contrôle de l'application. À cette fin, il convient de développer plus avant le système d'information et de surveillance mis en place au titre de la directive 2000/59/CE et d'en poursuivre l'exploitation en s'appuyant sur des systèmes de données électroniques existants, en particulier le système d'échange d'informations maritimes de l'Union (SafeSeaNet) mis en place en vertu de la directive 2002/59/CE du Parlement européen et du Conseil ([13]) et la base de données sur les inspections créée par la directive 2009/16/CE du Parlement européen et du Conseil ([14]) (THETIS). Un tel système devrait également inclure les informations relatives aux installations de réception portuaires disponibles dans les différents ports.

(41) La directive 2010/65/UE du Parlement européen et du Conseil ([15]) simplifie et harmonise les procédures administratives appliquées au transport maritime en généralisant davantage la transmission électronique d'informations et en rationalisant les formalités déclaratives. La déclaration de La Valette sur les priorités en matière de politique du transport maritime de l'Union européenne jusqu'en 2020, entérinée par le Conseil dans ses conclusions du 8 juin 2017, invitait la Commission à proposer la suite qu'il convenait de donner au réexamen de cette directive. Du 25 octobre 2017 au 18 janvier 2018, la Commission a mené une consultation publique sur les formalités déclaratives applicables aux navires. Le 17 mai 2018, la Commission a transmis au Parlement européen et au Conseil une proposition de règlement établissant un guichet unique maritime européen et abrogeant la directive 2010/65/UE.

(42) La convention MARPOL exige des parties contractantes qu'elles tiennent à jour les informations concernant leurs installations de réception portuaires et qu'elles les communiquent à l'OMI. À cet effet, l'OMI a mis en place une base de données relative aux installations de réception portuaires dans le cadre de son système mondial intégré de renseignements maritimes (GISIS).

(43) Dans le guide récapitulatif de l'OMI, celle-ci prévoit la notification des inadéquations présumées des installations de réception portuaires. Dans le cadre de cette procédure, un navire devrait signaler de telles inadéquations à l'administration de l'État du pavillon, qui, à son tour, doit en informer l'OMI et l'État du port. L'État du port devrait examiner le rapport et apporter une réponse appropriée, en en informant l'OMI et l'État du pavillon signalant. Si ces informations relatives à des inadéquations présumées étaient directement consignées dans le système d'information, de suivi et de contrôle de l'application prévu par la présente directive, elles pourraient ensuite être transmises au GISIS, ce qui libérerait les États membres, qu'ils soient État du pavillon ou État du port, de leur obligation de notification à l'OMI.

(44) Le sous-groupe sur les installations de réception portuaires, qui a été créé dans le cadre du Forum européen du transport maritime durable et qui réunissait un large éventail d'experts dans le domaine de la lutte contre la pollution causée par les navires et de la gestion des déchets des navires, a été suspendu en décembre 2017 en raison du lancement de négociations interinstitutionnelles. Compte tenu des conseils précieux et de l'expertise que ce sous-groupe apportait à la Commission, il serait souhaitable de créer un groupe d'experts similaire chargé de procéder à un partage d'expérience sur la mise en œuvre de la présente directive.

(45) Il importe que les sanctions prévues par les États membres soient correctement mises en œuvre et soient effectives, proportionnées et dissuasives.

(46) De bonnes conditions de travail pour le personnel des installations de réception portuaires sont d'une importance primordiale pour que le secteur du transport maritime soit sûr, efficace et socialement responsable, qu'il puisse attirer des travailleurs qualifiés et garantir des conditions de concurrence égales dans toute l'Europe. La formation initiale ainsi que la formation continue du personnel sont indispensables pour garantir la qualité des services et protéger les travailleurs. Il convient que les autorités du port et les autorités de l'installation de réception portuaire veillent à ce que tous les membres de leur personnel bénéficient de la formation nécessaire pour acquérir les connaissances indispensables à leur travail, une attention particulière étant accordée aux aspects liés à la santé et à la sécurité en cas de manipulation de matériaux dangereux, et à ce que les exigences en matière de formation soient actualisées régulièrement de manière à relever les défis de l'innovation technologique.

([13]) Directive 2002/59/CE du Parlement européen et du Conseil du 27 juin 2002 relative à la mise en place d'un système communautaire de suivi du trafic des navires et d'information, et abrogeant la directive 93/75/CEE du Conseil (JO L 208 du 5.8.2002, p. 10).

([14]) Directive 2009/16/CE du Parlement européen et du Conseil du 23 avril 2009 relative au contrôle par l'État du port (JO L 131 du 28.5.2009, p. 57).

([15]) Directive 2010/65/UE du Parlement européen et du Conseil du 20 octobre 2010 concernant les formalités déclaratives applicables aux navires à l'entrée et/ou à la sortie des ports des États membres et abrogeant la directive 2002/6/CE (JO L 283 du 29.10.2010, p. 1).

(47) Les pouvoirs conférés à la Commission pour mettre en œuvre la directive 2000/59/CE devraient être mis à jour en conformité avec le traité sur le fonctionnement de l'Union européenne.

(48) Il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne, en ce qui concerne la modification des annexes de la présente directive et des références aux instruments internationaux dans la mesure nécessaire pour les aligner sur le droit de l'Union ou pour tenir compte des évolutions au niveau international, notamment à l'échelle de l'OMI; pour modifier les annexes de la présente directive lorsque cela est nécessaire pour améliorer les modalités de mise en œuvre et de suivi qu'elle établit, notamment pour ce qui est de l'efficacité de la notification et du dépôt des déchets et de la bonne application des exemptions; et, dans des circonstances exceptionnelles, lorsque cela est dûment justifié par une analyse appropriée de la Commission, et afin d'écarter une menace grave et inacceptable pour l'environnement marin, pour modifier la présente directive, dans la mesure nécessaire pour écarter une telle menace, ce afin d'empêcher, le cas échéant, que des modifications apportées à ces instruments internationaux ne s'appliquent aux fins de la présente directive. 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» ([16]). 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.

(49) Afin de fournir les méthodes de calcul de la capacité de stockage suffisante dédiée; d'élaborer des critères communs concernant la reconnaissance, aux fins de l'octroi d'une réduction de la redevance de dépôt des déchets aux navires, du fait que la conception, l'équipement et l'exploitation d'un navire démontrent que celui-ci génère une quantité réduite de déchets et qu'il gère ceux-ci de manière durable et respectueuse de l'environnement; de définir des méthodologies de collecte des données de suivi concernant le volume et la quantité de déchets pêchés passivement et le format de communication de ces données; de définir les éléments détaillés d'un mécanisme de ciblage de l'Union fondé sur les risques, il convient de conférer des compétences d'exécution à la Commission. Ces compétences devraient être exercées en conformité avec le règlement (UE) n° 182/2011 du Parlement européen et du Conseil ([17]).

(50) Étant donné que l'objectif de la présente directive, à savoir la protection du milieu marin contre les rejets de déchets en mer, ne peut pas être atteint de manière suffisante par les États membres mais peut, en raison des dimensions 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.

(51) L'Union se caractérise par d'importantes disparités régionales au niveau des ports, comme l'a également montré l'analyse d'impact territorial réalisée par la Commission. Les ports se différencient en fonction de leur position géographique, de leur taille, de leur structure administrative et de la propriété, et se caractérisent par le type de navires qui y font habituellement escale. En outre, les systèmes de gestion des déchets tiennent compte des différences au niveau des municipalités et des infrastructures de gestion des déchets en aval.

(52) L'article 349 du traité sur le fonctionnement de l'Union européenne dispose qu'il y a lieu de tenir compte des caractéristiques particulières des régions ultrapériphériques de l'Union, à savoir la Guadeloupe, la Guyane française, la Martinique, Mayotte, La Réunion, Saint-Martin, les Açores, Madère et les îles Canaries. Afin de garantir l'adéquation et la disponibilité des installations de réception portuaires, il pourrait être opportun que les États membres mettent une aide au fonctionnement à finalité régionale à la disposition des exploitants d'installations de réception portuaires ou des autorités portuaires dans ces régions de l'Union en vue de remédier aux effets des handicaps permanents visés dans cet article. L'aide au fonctionnement à finalité régionale octroyée par les États membres dans ce contexte est exemptée de l'obligation de notification visée à l'article 108, paragraphe 3, du traité sur le fonctionnement de l'Union européenne si, au moment où elle est octroyée, elle remplit les conditions fixées par le règlement (UE) n° 651/2014 de la Commission ([18]) adopté en vertu du règlement (CE) n° 994/98 du Conseil ([19]).

(53) Il y a donc lieu d'abroger la directive 2000/59/CE,

([16]) JO L 123 du 12.5.2016, p. 1.

([17]) Règlement (UE) n° 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).

([18]) Règlement (UE) n° 651/2014 de la Commission du 17 juin 2014 déclarant certaines catégories d'aides compatibles avec le marché intérieur en application des articles 107 et 108 du traité (JO L 187 du 26.6.2014, p. 1).

([19]) Règlement (CE) n° 994/98 du Conseil du 7 mai 1998 sur l'application des articles 107 et 108 du traité sur le fonctionnement de l'Union européenne à certaines catégories d'aides d'État horizontales (JO L 142 du 14.5.1998, p. 1).

ONT ADOPTÉ LA PRÉSENTE DIRECTIVE:

Partie 1

Dispositions générales

Article premier

Objet

La présente directive vise à protéger le milieu marin contre les conséquences néfastes des rejets des déchets des navires qui font escale dans les ports situés dans l'Union, tout en assurant la fluidité du trafic maritime, en améliorant la disponibilité et l'utilisation d'installations de réception portuaires adéquates et le dépôt des déchets dans ces installations.

Article 2

Définitions

Aux fins de la présente directive, on entend par:

1) «navire», un bâtiment de mer de tout type exploité en milieu marin, y compris les navires de pêche, les bateaux de plaisance, les hydroptères, les aéroglisseurs, les engins submersibles et les engins flottants;

2) «convention MARPOL», la convention internationale pour la prévention de la pollution par les navires, dans sa version actualisée;

3) «déchets des navires», tous les déchets, y compris les résidus de cargaison, qui sont générés durant l'exploitation d'un navire ou pendant les opérations de chargement, de déchargement et de nettoyage, et qui relèvent des annexes I, II, IV, V et VI de la convention MARPOL, ainsi que les déchets pêchés passivement;

4) «déchets pêchés passivement», les déchets collectés dans des filets au cours d'opérations de pêche;

5) «résidus de cargaison», les restes de cargaison à bord qui demeurent sur le pont, dans les cales ou dans des citernes après les opérations de chargement et de déchargement, y compris les excès ou les pertes de chargement et de déchargement, que ce soit à l'état sec ou humide, ou entraînés par les eaux de lavage, à l'exclusion de la poussière résiduelle sur le pont après balayage ou de la poussière provenant des surfaces extérieures du navire;

6) «installation de réception portuaire», toute installation fixe, flottante ou mobile pouvant assurer le service de réception des déchets des navires;

7) «navire de pêche», tout navire équipé ou utilisé à des fins commerciales pour la capture de poissons ou d'autres ressources vivantes de la mer;

8) «bateau de plaisance», un navire de tout type, dont la coque a une longueur égale ou supérieure à 2,5 m, quel que soit le moyen de propulsion, destiné à des fins sportives et de loisir, et à des fins non commerciales;

9) «port», un lieu ou une zone géographique comportant des aménagements et des équipements principalement conçus pour permettre la réception de navires, y compris une zone de mouillage relevant de la juridiction du port;

10) «capacité de stockage suffisante», une capacité suffisante pour stocker les déchets à bord à compter du moment du départ jusqu'au port d'escale suivant, y compris les déchets susceptibles d'être générés au cours du voyage;

11) «services réguliers», des services organisés sur la base d'horaires de départ et d'arrivée publiés ou planifiés entre deux ports déterminés ou des traversées récurrentes qui constituent un calendrier reconnu;

12) «escales portuaires régulières», des trajets répétés d'un même navire formant une constante entre des ports déterminés ou une série de voyages à destination et en provenance du même port sans escale intermédiaire;

13) «escales portuaires fréquentes», des visites effectuées par un navire dans le même port au moins une fois par quinzaine;

14) «GISIS», le système mondial intégré d'information sur les transports maritimes mis en place par l'OMI;

15) «traitement», toute opération de valorisation ou d'élimination, y compris la préparation qui précède la valorisation ou l'élimination;

16) «redevance indirecte», une redevance payée pour la fourniture des services d'une installation de réception portuaire, qu'il soit procédé ou non au dépôt effectif de déchets des navires.

Les «déchets des navires» visés au point 3) sont considérés comme des déchets au sens de l'article 3, point 1), de la directive 2008/98/CE.

Article 3

Champ d'application

1. La présente directive s'applique:

a) à tous les navires, quel que soit leur pavillon, faisant escale dans un port d'un État membre ou y opérant, à l'exception des navires affectés à des services portuaires au sens de l'article 1er, paragraphe 2, du règlement (UE) 2017/352, et à l'exception des navires de guerre et navires de guerre auxiliaires, ou des autres navires appartenant à un État ou exploités par un État tant que celui-ci les utilise exclusivement à des fins gouvernementales et non commerciales;

b) à tous les ports des États membres dans lesquels les navires relevant du point a) font habituellement escale.

Aux fins de la présente directive, et pour éviter de causer des retards anormaux aux navires, les États membres peuvent décider d'exclure de leurs ports la zone de mouillage aux fins de l'application des articles 6, 7 et 8.

2. Les États membres prennent des mesures pour faire en sorte que, lorsque cela est raisonnablement possible, les navires qui ne relèvent pas du champ d'application de la présente directive déposent leurs déchets d'une manière qui soit compatible avec cette dernière.

3. Les États membres n'ayant ni ports ni navires battant leur pavillon qui relèvent du champ d'application de la présente directive peuvent, à l'exception de l'obligation énoncée au troisième alinéa du présent paragraphe, déroger aux dispositions de la présente directive.

Les États membres n'ayant pas de ports qui relèvent du champ d'application de la présente directive peuvent déroger aux dispositions de cette dernière qui visent uniquement les ports.

Les États membres qui entendent se prévaloir des dérogations prévues au présent paragraphe font savoir à la Commission, au plus tard le 28 juin 2021, s'ils satisfont aux conditions applicables et informent la Commission, chaque année par la suite, de tout changement ultérieur. Tant qu'ils n'ont pas transposé et mis en œuvre la présente directive, ces États membres ne peuvent avoir de ports relevant du champ d'application de la présente directive et ils ne peuvent autoriser des navires, y compris des engins, qui relèvent du champ d'application de la présente directive à battre leur pavillon.

Partie 2

Mise à disposition d'installations de réception portuaires adéquates

Article 4

Installations de réception portuaires

1. Les États membres garantissent la disponibilité des installations de réception portuaires adéquates pour répondre aux besoins des navires qui utilisent habituellement le port sans causer de retards anormaux à ces navires.

2. Les États membres s'assurent de ce qui suit:

a) les installations de réception portuaires ont une capacité permettant de recueillir les types et les quantités de déchets des navires qui utilisent habituellement le port, compte tenu:

   i) des besoins opérationnels des utilisateurs du port;

   ii) de la taille et de la position géographique de ce port;

   iii) du type de navires qui font escale dans ce port; et

   iv) des exemptions prévues à l'article 9;

b) les formalités et modalités pratiques liées à l'utilisation des installations de réception portuaires sont simples et rapides pour éviter de causer des retards anormaux aux navires;

c) les redevances perçues pour le dépôt ne dissuadent pas les navires d'utiliser les installations de réception portuaires; et

d) les installations de réception portuaires permettent de gérer les déchets des navires d'une manière qui soit respectueuse de l'environnement, conformément à la directive 2008/98/CE et aux autres dispositions pertinentes du droit de l'Union et du droit national relatives aux déchets.

Aux fins du premier alinéa, point d), les États membres veillent à ce qu'une collecte séparée soit en place pour faciliter le réemploi et le recyclage des déchets des navires dans les ports, comme le requiert le droit de l'Union en matière de déchets, notamment la directive 2006/66/CE du Parlement européen et du Conseil ([20]), la directive 2008/98/CE et la directive 2012/19/UE du Parlement européen et du Conseil ([21]). Afin de faciliter ce processus, les installations de réception portuaires peuvent collecter des fractions séparées de déchets conformément aux catégories de déchets définies dans la convention MARPOL, en tenant compte des lignes directrices qu'elle contient.

Le premier alinéa, point d), s'applique sans préjudice des exigences plus strictes imposées par le règlement (CE) n° 1069/2009 en ce qui concerne la gestion des déchets de cuisine et de table issus de voyages internationaux.

3. Les États membres, en leur qualité d'États du pavillon, utilisent les formulaires et les procédures de l'OMI pour notifier à celle-ci, ainsi qu'aux autorités de l'État du port, des défauts présumés d'adéquation des installations de réception portuaires.

Les États membres, en leur qualité d'États du port, enquêtent sur tous les cas de défaut présumé d'adéquation signalés et utilisent les formulaires et les procédures de l'OMI pour notifier les conclusions de l'enquête à l'OMI et à l'État du pavillon signalant.

4. Les autorités portuaires compétentes, ou, à défaut, les autorités compétentes veillent à ce que les opérations de dépôt ou de réception des déchets s'accompagnent de mesures de sécurité suffisantes pour prévenir les risques pour les personnes et pour l'environnement dans les ports relevant de la présente directive.

5. Les États membres veillent à ce que toute partie concernée par le dépôt ou la réception de déchets des navires puisse demander une indemnisation pour tout dommage résultant d'un retard anormal.

([20]) Directive 2006/66/CE du Parlement européen et du Conseil du 6 septembre 2006 relative aux piles et accumulateurs ainsi qu'aux déchets de piles et d'accumulateurs et abrogeant la directive 91/157/CEE (JO L 266 du 26.9.2006, p. 1).

([21]) Directive 2012/19/UE du Parlement européen et du Conseil du 4 juillet 2012 relative aux déchets d'équipements électriques et électroniques (DEEE) (JO L 197 du 24.7.2012, p. 38).

Article 5

Plans de réception et de traitement des déchets

1. Les États membres veillent à ce qu'un plan approprié de réception et de traitement des déchets soit établi et ait été mis en œuvre pour chaque port à l'issue des consultations menées auprès des parties concernées, y compris - en particulier - les utilisateurs des ports ou leurs représentants et, le cas échéant, les autorités locales compétentes, les exploitants de l'installation de réception portuaire, des organisations mettant en œuvre les obligations découlant de la responsabilité élargie du producteur et des représentants de la société civile. Ces consultations devraient être organisées à la fois au cours de la phase initiale d'élaboration du plan de réception et de traitement des déchets et après son adoption, en particulier lorsque des changements importants ont eu lieu concernant les exigences prévues aux articles 4, 6 et 7.

Les prescriptions détaillées relatives à l'élaboration du plan de réception et de traitement des déchets figurent à l'annexe 1.

2. Les États membres s'assurent que les informations suivantes, tirées des plans de réception et de traitement des déchets et relatives à la disponibilité d'installations de réception portuaires adéquates dans leurs ports et à la structure des coûts, sont communiquées clairement aux exploitants de navires, sont rendues publiques et sont facilement accessibles, dans une langue officielle de l'État membre où le port est situé et, le cas échéant, dans une langue utilisée dans le monde entier:

a) l'emplacement des installations de réception portuaires correspondant à chaque poste de mouillage et, le cas échéant, leurs heures d'ouverture;

b) la liste des déchets des navires habituellement gérés par le port;

c) la liste des points de contact, des exploitants de l'installation de réception portuaire et des services proposés;

d) la description des procédures de dépôt des déchets;

e) la description des systèmes de recouvrement des coûts, y compris les systèmes et fonds de gestion des déchets tels qu'ils sont visés à l'annexe 4, le cas échéant.

Les informations mentionnées au premier alinéa du présent paragraphe sont également rendues accessibles par voie électronique et mises à jour dans la partie du système d'information, de suivi et de contrôle de l'application visée à l'article 13.

3. Lorsque cela s'impose pour des raisons d'efficacité, les plans de réception et de traitement des déchets peuvent être élaborés conjointement par deux ports voisins ou plus dans la même région géographique, chaque port y étant associé comme il se doit, pour autant qu'y soient précisés, pour chacun des ports, les besoins en installations de réception portuaires et la disponibilité de telles installations.

4. Les États membres évaluent et approuvent le plan de réception et de traitement des déchets et veillent à le soumettre à une nouvelle approbation au moins tous les cinq ans après qu'il a été approuvé ou nouvellement approuvé et après toute modification importante de l'exploitation du port. Ces modifications peuvent notamment comprendre des changements structurels dans le trafic du port, la création de nouvelles infrastructures, des changements dans la demande et l'offre d'installations de réception portuaires et de nouvelles techniques de traitement à bord.

Les États membres contrôlent la mise en œuvre par le port du plan de réception et de traitement des déchets. Si aucune modification significative n'est intervenue au cours de la période de cinq ans mentionnée au premier alinéa, la nouvelle approbation peut consister en la validation de plans existants.

5. Les petits ports non commerciaux, qui se caractérisent par un trafic très faible ou faible de bateaux de plaisance uniquement, peuvent être exemptés des paragraphes 1 à 4 si leurs installations de réception portuaires sont intégrées dans le système de traitement des déchets géré par ou pour le compte de la municipalité compétente, et si les États membres qui abritent de tels ports veillent à ce que les informations concernant le système de gestion des déchets soient mises à la disposition des utilisateurs de ces ports.

Les États membres qui abritent de tels ports en communiquent le nom et la localisation par voie électronique dans la partie du système d'information, de suivi et de contrôle de l'application visée à l'article 13.

Partie 3

Dépôt des déchets des navires

Article 6

Notification préalable des déchets

1. L'exploitant, l'agent ou le capitaine d'un navire relevant du champ d'application de la directive 2002/59/CE qui fait route vers un port de l'Union remplit fidèlement et minutieusement le formulaire figurant à l'annexe 2 de la présente directive (ci-après dénommé «notification préalable des déchets») et communique toutes les informations que celle-ci contient à l'autorité ou à l'organisme désigné à cet effet par l'État membre dans lequel ce port est situé:

a) au moins vingt-quatre heures avant l'arrivée, si le port d'escale est connu;

b) dès que le port d'escale est connu, si ces informations sont disponibles moins de vingt-quatre heures avant l'arrivée; ou

c) au plus tard au moment où le navire quitte le port précédent, si la durée du voyage est inférieure à vingt-quatre heures.

2. Les informations figurant sur la notification préalable des déchets sont communiquées par voie électronique pour être consignées dans la partie du système d'information, de suivi et de contrôle de l'application visée à l'article 13 de la présente directive, conformément aux directives 2002/59/CE et 2010/65/UE.

3. Les informations figurant sur la notification préalable des déchets sont disponibles à bord, de préférence sous forme électronique, au moins jusqu'au port d'escale suivant, et sont mises à la disposition des autorités compétentes des États membres qui en font la demande.

4. Les États membres veillent à ce que les informations qui sont communiquées en vertu du présent article soient examinées et partagées avec les autorités chargées du contrôle de l'application sans retard.

Article 7

Dépôt des déchets des navires

1. Avant de quitter un port de l'Union, le capitaine d'un navire faisant escale dans ce port dépose tous les déchets conservés à bord dans une installation de réception portuaire conformément aux normes relatives aux rejets pertinentes qui sont fixées dans la convention MARPOL.

2. Lors du dépôt, l'exploitant de l'installation de réception portuaire ou l'autorité du port où les déchets ont été déposés remplit fidèlement et minutieusement le formulaire figurant à l'annexe 3 (ci-après dénommé «reçu de dépôt des déchets») et il délivre et fournit sans retard indu le reçu de dépôt des déchets au capitaine du navire.

Les exigences énoncées au premier alinéa ne s'appliquent pas aux petits ports équipés d'installations sans personnel ou situés dans des régions éloignées, pour autant que l'État membre qui abrite ces ports ait déclaré le nom et le lieu de ces ports par voie électronique dans la partie du système d'information, de suivi et de contrôle de l'application visée à l'article 13.

3. L'exploitant, l'agent ou le capitaine d'un navire entrant dans le champ d'application de la directive 2002/59/CE consigne par voie électronique, avant le départ ou dès réception du reçu de dépôt des déchets, les informations figurant dans celui-ci dans la partie du système d'information, de suivi et de contrôle de l'application visée à l'article 13 de la présente directive, conformément aux directives 2002/59/CE et 2010/65/UE.

Les informations figurant sur le reçu de dépôt des déchets sont disponibles à bord pendant au moins deux ans, le cas échéant avec le registre des hydrocarbures, le registre de la cargaison, le registre des ordures ou le plan de gestion des ordures appropriés, et sont mises à la disposition des autorités des États membres qui en font la demande.

4. Sans préjudice du paragraphe 1, un navire peut continuer sa route jusqu'au port d'escale suivant sans déposer de déchets, si:

a) les informations fournies conformément aux annexes 2 et 3 montrent qu'il existe une capacité de stockage suffisante dédiée à bord du navire pour tous les déchets qui ont été et seront accumulés pendant le trajet prévu jusqu'au port d'escale suivant;

b) les informations disponibles à bord des navires ne relevant pas du champ d'application de la directive 2002/59/CE montrent qu'il existe une capacité de stockage suffisante dédiée à bord du navire pour tous les déchets qui ont été et seront accumulés pendant le trajet prévu jusqu'au port d'escale suivant; ou

c) le navire est uniquement au mouillage pendant moins de 24 heures ou en cas de mauvaises conditions météorologiques, à moins qu'une telle zone de mouillage n'ait été exclue conformément à l'article 3, paragraphe 1, second alinéa.

Afin d'assurer des conditions uniformes d'exécution de l'exception mentionnée au premier alinéa, points a) et b), la Commission adopte des actes d'exécution afin de définir les méthodes à utiliser pour calculer la capacité de stockage suffisante dédiée. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 20, paragraphe 2.

5. Un État membre exige du navire qu'il dépose tous ses déchets avant de repartir:

a) s'il ne peut être établi, sur la base des informations consignées par voie électronique dans la partie du système d'information, de suivi et de contrôle de l'application visée à l'article 13 ou dans le GISIS, que des installations de réception portuaires adéquates sont disponibles dans le port d'escale suivant; ou

b) si le port d'escale suivant n'est pas connu.

6. Le paragraphe 4 est applicable sans préjudice d'exigences plus strictes valables pour les navires, adoptées conformément au droit international.

Article 8

Systèmes de recouvrement des coûts

1. Les États membres veillent à ce que les coûts d'exploitation des installations portuaires pour la réception et le traitement des déchets des navires autres que les résidus de cargaison soient couverts par une redevance perçue sur les navires. Ces coûts comprennent les éléments énumérés à l'annexe 4.

2. Les systèmes de recouvrement des coûts ne constituent en aucune manière une incitation à déverser les déchets en mer. À cet effet, les États membres observent l'ensemble des principes suivants lorsqu'ils élaborent et appliquent les systèmes de recouvrement des coûts:

a) les navires s'acquittent d'une redevance indirecte, indépendamment du dépôt ou non de déchets dans une installation de réception portuaire;

b) la redevance indirecte couvre:

   i) les coûts administratifs indirects;

   ii) une partie significative des coûts d'exploitation directs, tels qu'ils sont fixés à l'annexe 4, qui représente au moins 30 % du total des coûts directs correspondant au dépôt effectif des déchets au cours de l'année précédente, avec la possibilité de prendre également en compte les coûts liés au volume de trafic prévu pour l'année à venir;

c) afin d'offrir une incitation la plus large possible au dépôt des déchets relevant de l'annexe V de MARPOL, autres que les résidus de cargaison, aucune redevance directe n'est perçue pour ces déchets, de manière à garantir un droit de dépôt sans frais supplémentaires fondés sur le volume de déchets déposés, sauf lorsque le volume des déchets excède la capacité de stockage dédiée maximale indiquée dans le formulaire figurant à l'annexe 2 de la présente directive; les déchets pêchés passivement sont couverts par ce régime, y compris le droit de dépôt;

d) afin d'éviter que les coûts de collecte et de traitement des déchets pêchés passivement ne soit supportés exclusivement par les utilisateurs des ports, les États membres couvrent, le cas échéant, ces coûts grâce aux recettes provenant d'autres mécanismes de financement, y compris les systèmes de gestion des déchets ainsi que les financements de l'Union, les financements nationaux ou les financements régionaux disponibles;

e) afin d'encourager le dépôt de résidus de lavage de citernes contenant des substances flottantes persistantes à haute viscosité, les États membres peuvent prévoir des incitations financières appropriées pour leur dépôt;

f) la redevance indirecte ne porte pas sur les résidus des systèmes d'épuration des gaz d'échappement, pour lesquels les coûts sont couverts sur la base des types et des quantités de déchets déposés.

3. La part des coûts qui n'est pas couverte par la redevance indirecte éventuelle est couverte sur la base des types et des quantités de déchets effectivement déposés par le navire.

4. Les redevances peuvent être différenciées selon les critères suivants:

a) la catégorie, le type et la taille du navire;

b) la fourniture de services aux navires en dehors des heures habituelles de fonctionnement du port; ou

c) le caractère dangereux des déchets.

5. Les redevances sont réduites selon les critères suivants:

a) le type d'activité du navire, en particulier lorsqu'il s'agit de transport maritime à courte distance;

b) la conception, l'équipement et l'exploitation du navire démontrent que le navire génère une quantité réduite de déchets et qu'il gère ceux-ci de manière durable et respectueuse de l'environnement.

Au plus tard le 28 juin 2020, la Commission adopte des actes d'exécution pour définir les critères permettant de déterminer qu'un navire satisfait aux exigences énoncées au premier alinéa, point b), en ce qui concerne la gestion des déchets à bord du navire. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 20, paragraphe 2.

6. Afin de garantir que les redevances sont équitables, transparentes, facilement identifiables et non discriminatoires et qu'elles reflètent les coûts des installations et des services proposés et, le cas échéant, utilisés, le montant des redevances et la base de calcul de celles-ci sont mis à la disposition des utilisateurs du port dans le plan de réception et de traitement des déchets, dans une langue officielle de l'État membre où le port est situé et, le cas échéant, dans une langue utilisée dans le monde entier.

7. Les États membres veillent à ce que des données de suivi concernant le volume et la quantité de déchets pêchés passivement soient recueillies et communiquent ces données de suivi à la Commission. Sur la base de ces données de suivi, la Commission publie un rapport pour le 31 décembre 2022, puis tous les deux ans par la suite.

La Commission adopte des actes d'exécution pour définir les méthodologies applicables aux données de suivi et le format de communication des données. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 20, paragraphe 2.

Article 9

Exemptions

1. Les États membres peuvent exempter un navire faisant escale dans leurs ports des obligations énoncées à l'article 6, à l'article 7, paragraphe 1, et à l'article 8 (ci-après dénommée «exemption») lorsqu'il existe des preuves suffisantes attestant que les conditions ci-après sont remplies:

a) le navire effectue des services réguliers qui comportent des escales portuaires fréquentes et régulières;

b) il existe un arrangement visant à garantir le dépôt des déchets et le paiement des redevances dans un port situé sur l'itinéraire du navire qui:

   i) est attesté par un contrat signé avec le port ou le gestionnaire de déchets et par des reçus de dépôt des déchets;

   ii) a été notifié à tous les ports situés sur l'itinéraire du navire; et

   iii) a été approuvé par le port où le dépôt et le paiement ont lieu, qu'il s'agisse d'un port de l'Union ou d'un autre port dans lequel des installations adéquates sont disponibles, ainsi que cela est établi sur la base des informations communiquées par voie électronique pour être consignées dans la partie du système d'information, de suivi et de contrôle de l'application visée à l'article 13 et dans le GISIS;

c) l'exemption n'entraîne pas de conséquences négatives pour la sécurité maritime, la santé, les conditions de vie ou de travail à bord ou pour l'environnement marin.

2. Si l'exemption est accordée, l'État membre qui abrite le port délivre un certificat d'exemption dans le format figurant à l'annexe 5, qui confirme que le navire satisfait aux conditions et exigences requises pour l'application de l'exemption et précise la durée de validité de celle-ci.

3. Les États membres communiquent par voie électronique les informations figurant sur le certificat d'exemption pour qu'elles soient consignées dans la partie du système d'information, de suivi et de contrôle de l'application visée à l'article 13.

4. Les États membres assurent de manière efficace le suivi et le contrôle de l'application des arrangements en matière de dépôt et de paiement existants pour les navires exemptés qui font escale dans leurs ports.

5. Nonobstant l'exemption accordée, un navire ne poursuit pas sa route jusqu'au port d'escale suivant s'il ne dispose pas d'une capacité de stockage suffisante dédiée pour tous les déchets qui ont été et qui seront accumulés pendant le trajet prévu du navire jusqu'au port d'escale suivant.

Partie 4

Contrôle de l'application

Article 10

Inspections

Les États membres veillent à ce que tout navire soit susceptible de faire l'objet d'inspections, y compris aléatoires, destinées à vérifier qu'il satisfait à la présente directive.

Article 11

Obligations en matière d'inspection

1. Chaque État membre procède à des inspections de navires faisant escale dans ses ports, en ce qui concerne au moins 15 % du nombre total de navires distincts faisant escale dans ses ports chaque année.

Le nombre total de navires distincts faisant escale dans un État membre est calculé comme étant le nombre moyen de navires distincts des trois années précédentes, tel qu'il a été communiqué par le biais de la partie du système d'information, de suivi et de contrôle de l'application visée à l'article 13.

2. Les États membres se conforment au paragraphe 1 du présent article en sélectionnant les navires sur la base d'un mécanisme de ciblage de l'Union fondé sur les risques.

Afin de garantir une harmonisation des inspections et d'assurer des conditions uniformes de sélection des navires aux fins d'inspection, la Commission adopte des actes d'exécution afin de définir les éléments détaillés du mécanisme de ciblage de l'Union fondé sur les risques. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 20, paragraphe 2.

3. Les États membres mettent en place des procédures pour les inspections des navires qui ne relèvent pas du champ d'application de la directive 2002/59/CE afin de garantir, dans toute la mesure du possible, le respect de la présente directive.

Lors de l'établissement de ces procédures, les États membres peuvent tenir compte du mécanisme de ciblage de l'Union fondé sur les risques visé au paragraphe 2.

4. Si l'autorité compétente de l'État membre n'est pas satisfaite des résultats de l'inspection, elle fait en sorte que le navire ne quitte pas le port avant d'avoir déposé ses déchets dans une installation de réception portuaire conformément à l'article 7, et ce sans préjudice de l'application des sanctions prévues à l'article 16.

Article 12

Système d'information, de suivi et de contrôle de l'application

La mise en œuvre et le contrôle de l'application de la présente directive sont facilités par la communication et l'échange d'informations par voie électronique entre les États membres conformément aux articles 13 et 14.

Article 13

Communication et échange d'informations

1. La communication et l'échange d'informations reposent sur le système d'échange d'informations maritimes de l'Union (ci-après dénommé «SafeSeaNet») visé à l'article 22 *bis*, paragraphe 3, de la directive 2002/59/CE et à son annexe III.

2. Les États membres veillent à ce que les informations suivantes soient communiquées par voie électronique et dans un délai raisonnable conformément à la directive 2010/65/UE:

a) les informations sur l'heure réelle d'arrivée et de départ de chaque navire relevant de la directive 2002/59/CE qui fait escale dans un port de l'Union, ainsi que l'identifiant du port en question;

b) les informations contenues dans la notification préalable des déchets figurant à l'annexe 2;

c) les informations contenues dans le reçu de dépôt des déchets figurant à l'annexe 3;

d) les informations contenues dans le certificat d'exemption figurant à l'annexe 5.

3. Les États membres veillent à ce que les informations énumérées à l'article 5, paragraphe 2, soient rendues accessibles par voie électronique par le biais du SafeSeaNet.

Article 14

Enregistrement des inspections

1. La Commission crée, gère et met à jour une base de données des inspections à laquelle tous les États membres sont connectés et qui contient toutes les informations requises pour la mise en œuvre du système d'inspection prévu par la présente directive (ci-après dénommée «base de données des inspections»). La base de données des inspections est créée sur le modèle de la base de données des inspections visée à l'article 24 de la directive 2009/16/CE et est dotée de fonctionnalités semblables à ladite base de données.

2. Les États membres veillent à ce que les informations relatives aux inspections effectuées au titre de la présente directive, notamment les informations relatives aux défauts de conformité et aux ordres d'interdiction de départ, soient transférées sans tarder vers la base de données des inspections dès:

a) que le rapport d'inspection a été établi;

b) que l'ordre d'interdiction de départ a été levé; ou

c) qu'une exemption a été accordée.

3. La Commission veille à ce qu'il soit possible d'extraire de la base des données des inspections toute donnée utile communiquée par les États membres aux fins du suivi de la mise en œuvre de la présente directive.

La Commission veille à ce que la base de données des inspections fournisse des informations pour le mécanisme de ciblage de l'Union fondé sur les risques visé à l'article 11, paragraphe 2.

La Commission réexamine régulièrement la base de données des inspections pour suivre la mise en œuvre de la présente directive et attire l'attention sur tout doute concernant sa mise en œuvre globale dans le but de susciter des mesures correctives.

4. Les États membres ont à tout moment accès aux informations enregistrées dans la base de données des inspections.

Article 15

Formation du personnel

Les autorités du port et les autorités de l'installation de réception portuaire veillent à ce que tous les membres de leur personnel bénéficient de la formation nécessaire pour acquérir les connaissances indispensables à leur travail pour ce qui concerne les déchets, une attention particulière étant accordée aux aspects liés à la santé et à la sécurité en cas de manipulation de matériaux dangereux, et à ce que les exigences en matière de formation soient actualisées régulièrement de manière à relever les défis de l'innovation technologique.

Article 16

Sanctions

Les États membres déterminent le régime des sanctions applicables aux violations des dispositions nationales adoptées en application de la présente directive et prennent toute mesure nécessaire pour en assurer la mise en œuvre. Les sanctions ainsi prévues sont effectives, proportionnées et dissuasives.

Partie 5

Dispositions finales

Article 17

Partage d'expérience

La Commission organise le partage d'expérience entre les autorités nationales et les experts des États membres, y compris en provenance du secteur privé, de la société civile et des organisations syndicales, en matière d'application de la présente directive dans les ports de l'Union.

Article 18

Procédure de modification

1. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 19 en vue de modifier les annexes de la présente directive et les références faites aux instruments de l'OMI dans la présente directive dans la mesure nécessaire pour les aligner sur le droit de l'Union ou pour tenir compte des évolutions au niveau international, notamment à l'échelle de l'OMI.

2. La Commission est également habilitée à adopter des actes délégués en conformité avec l'article 19 en vue de modifier les annexes lorsque cela est nécessaire pour améliorer les modalités de mise en œuvre et de suivi établies par la présente directive, notamment celles prévues aux articles 6, 7 et 9, de manière à garantir l'efficacité de la notification et du dépôt des déchets, ainsi que la bonne application des exemptions.

3. Dans des circonstances exceptionnelles, lorsque cela est dûment justifié par une analyse appropriée de la Commission, et afin d'écarter une menace grave et inacceptable pour l'environnement marin, la Commission est habilitée à adopter des actes délégués conformément à l'article 19 en vue de modifier la présente directive, dans la mesure nécessaire pour écarter une telle menace, afin que ne soit pas appliquée, aux fins de la présente directive, une modification apportée à la convention MARPOL.

4. Les actes délégués visés au présent article sont adoptés au moins trois mois avant l'expiration de la période fixée au niveau international pour l'acceptation tacite de la modification de la convention MARPOL ou avant la date envisagée pour l'entrée en vigueur de ladite modification.

Au cours de la période précédant l'entrée en vigueur de ces actes délégués, les États membres s'abstiennent de toute initiative visant à intégrer ladite modification dans le droit national ou à appliquer la modification de l'instrument international concerné.

Article 19

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, paragraphes 1, 2 et 3, est conféré à la Commission pour une période de cinq ans à compter du 27 juin 2019. La Commission élabore un rapport relatif à la délégation de pouvoir au plus tard neuf mois avant la fin de la période de cinq ans. La délégation de pouvoir est tacitement prorogée pour des périodes d'une durée identique, sauf si le Parlement européen ou le Conseil s'oppose à cette prorogation trois mois au plus tard avant la fin de chaque période.

3. La délégation de pouvoir visée à l'article 18, paragraphes 1, 2 et 3, 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 au Parlement européen et au Conseil simultanément.

6. Un acte délégué adopté en vertu de l'article 18, paragraphes 1, 2 et 3, 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 20

Comité

1. La Commission est assistée par le comité pour la sécurité maritime et la prévention de la pollution par les navires (COSS) institué par le règlement (CE) n° 2099/2002 du Parlement européen et du Conseil ([22]). Ledit comité est un comité au sens du règlement (UE) n° 182/2011.

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

Article 21

Modification de la directive 2010/65/UE

Au point A de l'annexe de la directive 2010/65/UE, le point 4) est remplacé par le texte suivant:

«4) Notification des déchets des navires, y compris les résidus

Articles 6, 7 et 9 de la directive (UE) 2019/883 du Parlement européen et du Conseil du 17 avril 2019 relative aux installations de réception portuaires pour le dépôt des déchets des navires, modifiant la directive 2010/65/UE et abrogeant la directive 2000/59/CE (JO L 151 du 7.6.2019, p. 116)».

Article 22

Abrogation

La directive 2000/59/CE est abrogée.

Les références faites à la directive abrogée s'entendent comme faites à la présente directive.

Article 23

Réexamen

1. La Commission évalue la présente directive et présente les résultats de l'évaluation au Parlement européen et au Conseil au plus tard le 28 juin 2026. L'évaluation comprend également un rapport détaillant les meilleures pratiques de prévention et de gestion des déchets à bord des navires.

2. Dans le cadre du règlement (UE) 2016/1625 du Parlement européen et du Conseil ([23]), à l'occasion du prochain réexamen du mandat de l'Agence européenne pour la sécurité maritime (AESM), la Commission évalue également s'il convient d'octroyer des compétences supplémentaires à l'AESM pour le contrôle de l'application de la présente directive.

([22]) Règlement (CE) n° 2099/2002 du Parlement européen et du Conseil du 5 novembre 2002 instituant un comité pour la sécurité maritime et la prévention de la pollution par les navires (COSS) et modifiant les règlements en matière de sécurité maritime et de prévention de la pollution par les navires (JO L 324 du 29.11.2002, p. 1).

([23]) Règlement (UE) 2016/1625 du Parlement européen et du Conseil du 14 septembre 2016 modifiant le règlement (CE) n° 1406/2002 instituant une Agence européenne pour la sécurité maritime (JO L 251 du 16.9.2016, p. 77).

Article 24

Transposition

1. Les États membres mettent en vigueur les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive au plus tard le 28 juin 2021. Ils communiquent immédiatement à la Commission le texte de ces dispositions.

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.

2. Les États membres communiquent à la Commission le texte des dispositions essentielles de droit interne qu'ils adoptent dans le domaine régi par la présente directive.

Article 25

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 26

Destinataires

Les États membres sont destinataires de la présente directive.

Fait à Strasbourg, le 17 avril 2019.

Par le Parlement européen	*Par le Conseil*
Le président	*Le président*
A. TAJANI	G. CIAMBA

ANNEXE 1

PRESCRIPTIONS CONCERNANT LES PLANS DE RÉCEPTION ET DE TRAITEMENT DES DÉCHETS

Les plans de réception et de traitement des déchets couvrent tous les types de déchets provenant des navires faisant escale dans le port et être élaborés en fonction de la taille du port et des catégories de navires qui y font escale.

Les plans de réception et de traitement des déchets doivent notamment comprendre les éléments suivants:

a) une évaluation des besoins en termes d'installations de réception portuaires, compte tenu des besoins des navires qui font habituellement escale dans le port;

b) une description du type et de la capacité des installations de réception portuaires;

c) une description des procédures de réception et de collecte des déchets des navires;

d) une description du système de recouvrement des coûts;

e) une description de la procédure à suivre pour signaler les inadéquations présumées dans les installations de réception portuaires;

f) une description de la procédure à suivre pour la consultation permanente des utilisateurs du port, des contractants du secteur des déchets, des exploitants de terminaux et des autres parties intéressées; et

g) un aperçu du type et des quantités de déchets reçus des navires et traités dans les installations.

Les plans de réception et de traitement des déchets peuvent comprendre:

a) un résumé du droit national applicable ainsi que la procédure et les formalités pour le dépôt des déchets dans des installations de réception portuaires;

b) l'identification d'un point de contact dans le port;

c) une description, le cas échéant, des équipements et procédés de prétraitement pour des flux de déchets spécifiques dans le port;

d) une description des méthodes employées pour enregistrer l'utilisation effective des installations de réception portuaires;

e) une description des méthodes employées pour enregistrer les quantités de déchets déposés par les navires;

f) une description des méthodes de gestion des différents flux de déchets dans le port.

Les procédures de réception, collecte, stockage, traitement et élimination devraient être à tous égards conformes à un programme de gestion de l'environnement conduisant à une réduction progressive de l'impact de ces activités sur l'environnement. Cette conformité est présumée si les procédures sont conformes au règlement (CE) n° 1221/2009 du Parlement européen et du Conseil ([1]).

([1]) Règlement (CE) n° 1221/2009 du Parlement européen et du Conseil du 25 novembre 2009 concernant la participation volontaire des organisations à un système communautaire de management environnemental et d'audit (EMAS), abrogeant le règlement (CE) n° 761/2001 et les décisions de la Commission 2001/681/CE et 2006/193/CE (JO L 342 du 22.12.2009, p. 1).

ANNEXE 2

MODÈLE NORMALISÉ POUR LA NOTIFICATION PRÉALABLE DE DÉPÔT DES DÉCHETS DANS DES INSTALLATIONS DE RÉCEPTION PORTUAIRES

Notification du dépôt de déchets à: *(indiquer le nom du port d'escale, tel qu'il est visé à l'article 6 de la directive (UE) 2019/883)*

Le présent formulaire devrait être conservé à bord du navire avec le registre des hydrocarbures, le registre de la cargaison, le registre des ordures ou le plan de gestion des ordures, comme l'exige la convention MARPOL.

1. RENSEIGNEMENTS CONCERNANT LE NAVIRE

1.1 Nom du navire:	1.5 Propriétaire ou exploitant:
1.2 Numéro OMI:	1.6 Numéro ou lettres distinctifs:
	Numéro MMSI (Maritime Mobile Service Identity):
1.3 Tonnage brut:	1.7 État du pavillon:
1.4 Type de navire: ☐ Pétrolier ☐ Navire-citerne pour produits chimiques ☐ Vraquier ☐ Porte-conteneurs ☐ Autre navire de charge ☐ Navires à passagers ☐ Navire roulier ☐ Autre type (préciser)	

2. RENSEIGNEMENTS CONCERNANT LE PORT ET LE VOYAGE

2.1 Position géographique/nom du terminal:	2.6 Dernier port où des déchets ont été déposés:
2.2 Date et heure d'arrivée:	2.7 Date du dernier dépôt:
2.3 Date et heure de départ:	2.8 Port de dépôt suivant:
2.4 Dernier port et pays:	2.9 Personne soumettant le présent formulaire (si autre que le capitaine):
2.5 Port suivant et pays (s'il est connu):	

3. TYPE ET VOLUME DE DÉCHETS ET CAPACITÉ DE STOCKAGE

Type	Quantités à déposer (m^3)	Capacité de stockage dédiée maximale (m^3)	Quantité de déchets restants à bord (m^3)	Port dans lequel les déchets restants seront déposés	Estimation de la quantité de déchets qui sera produite entre la notification et l'entrée dans le port d'escale suivant (m^3)
Annexe I de MARPOL – Hydrocarbures					
Eaux de cale polluées par les hydrocarbures					
Résidus d'hydrocarbures (boues)					
Eaux de lavage des citernes d'hydrocarbures					
Eaux de ballast sales					

Type	Quantités à déposer (m^3)	Capacité de stockage dédiée maximale (m^3)	Quantité de déchets restants à bord (m^3)	Port dans lequel les déchets restants seront déposés	Estimation de la quantité de déchets qui sera produite entre la notification et l'entrée dans le port d'escale suivant (m^3)
Tartre et boues provenant du nettoyage des citernes					
Autres (veuillez préciser)					
Annexe II de MARPOL – Substances liquides nocives (SLN) (1)					
Substance de catégorie X					
Substance de catégorie Y					
Substance de catégorie Z					
AS - Autres substances					
Annexe IV de MARPOL – Eaux usées					
Annexe V de MARPOL – Ordures					
A. Matières plastiques					
B. Déchets alimentaires					
C. Déchets domestiques (papier, chiffons, verre, métaux, bouteilles, vaisselle, etc.)					
D. Huiles de cuisson					
E. Cendres d'incinération					
F. Déchets d'exploitation					
G. Carcasse(s) d'animaux					
H. Engins de pêche					
I. Déchets électroniques					

(1) Indiquer la désignation officielle de transport des SLN concernés.

Type	Quantités à déposer (m^3)	Capacité de stockage dédiée maximale (m^3)	Quantité de déchets restants à bord (m^3)	Port dans lequel les déchets restants seront déposés	Estimation de la quantité de déchets qui sera produite entre la notification et l'entrée dans le port d'escale suivant (m^3)
J. Résidus de cargaison (1) (nocifs pour le milieu marin - HME)					
K. Résidus de cargaison (2) (non HME)					
Annexe VI de MARPOL – Pollution de l'atmosphère					
Substances appauvrissant la couche d'ozone et équipements contenant de telles substances (3)					
Résidus d'épuration des gaz d'échappement					

Autres déchets, non couverts par MARPOL					
Déchets pêchés passivement					

Remarques

1. Ces renseignements sont utilisés à des fins de contrôle par l'État du port ainsi qu'à d'autres fins d'inspection.
2. Le présent formulaire doit être rempli, sauf si le navire fait l'objet d'une exemption conformément à l'article 9 de la directive (UE) 2019/883

(1) Il peut s'agir d'estimations; indiquer la désignation officielle de transport des marchandises solides.
(2) Il peut s'agir d'estimations; indiquer la désignation officielle de transport des marchandises solides.
(3) Substances produites au cours des activités d'entretien normales à bord.

ANNEXE 3

MODÈLE NORMALISÉ DE REÇU DE DÉPÔT DES DÉCHETS

Le représentant désigné du fournisseur de l'installation de réception portuaire remet le formulaire suivant au capitaine d'un navire qui a déposé des déchets conformément à l'article 7 de la directive (UE) 2019/883.

Ce formulaire doit être conservé à bord du navire en même temps que le registre des hydrocarbures, le registre de la cargaison, le registre des ordures ou le plan de gestion des ordures, comme l'exige la convention MARPOL.

1. RENSEIGNEMENTS CONCERNANT L'INSTALLATION DE RÉCEPTION PORTUAIRE ET LE PORT

1.1. Position géographique/Nom du terminal:
1.2. Fournisseur(s) de l'installation de réception portuaire
1.3. Fournisseur(s) de l'installation de traitement — si autre que la personne susmentionnée:
1.4. Date et heure de dépôt des déchets à partir du: à:

2. RENSEIGNEMENTS CONCERNANT LE NAVIRE

2.1. Nom du navire:	2.5. Propriétaire ou exploitant:
2.2. Numéro OMI:	2.6. Numéro ou lettres distinctifs: Numéro MMSI (Maritime Mobile Service Identity):
2.3. Tonnage brut:	2.7. État du pavillon:
2.4. Type de navire:: ☐ Pétrolier ☐ Navire-citerne pour produits chimiques ☐ Vraquier ☐ Porte-conteneur ☐ Autre type de navire de charge ☐ Navire à passagers ☐ Navire roulier ☐ utre (veuillez préciser)	

3. TYPE ET VOLUME DE DÉCHETS REÇUS

Annexe I de MARPOL – Hydrocarbures	Quantité (m^3)
Eaux de cale polluées par les hydrocarbures	
Résidus d'hydrocarbures (boues)	
Eaux de lavage des citernes d'hydrocarbures	
Eaux de ballast sales	
Tartre et boues provenant du nettoyage des citernes	
Autres (veuillez préciser)	
Annexe II de MARPOL – SUBSTANCES LIQUIDES NOCIVES (SLN)	Quantité (m^3)/Nom [1]
Substance de catégorie X	
Substance de catégorie Y	
Substance de catégorie Z	
AS – Autres substances	
Annexe IV de MARPOL – Eaux usées	Quantité (m^3)

Annexe V de MARPOL – Ordures	Quantité (m^3)
A. Matières plastiques	
B. Déchets alimentaires	
C. Déchets domestiques (papier, chiffons, verre, métaux, bouteilles, vaisselle, etc.)	
D. Huile de cuisson	
E. Cendres d'incinération	
F. Déchets d'exploitation	
G. Carcasse(s) d'animaux	
H. Engins de pêche	
I. Déchets électroniques	
J. Résidus de cargaison [2] (nocifs pour le milieu marin)	
K. Résidus de cargaison [2] (non nocifs pour le milieu marin)	
Annexe VI de MARPOL – Pollution de l'atmosphère	Quantité (m^3)
Substances appauvrissant la couche d'ozone et équipements contenant de telles substances	
Résidus d'épuration des gaz d'échappement	
Autres déchets, non couverts par MARPOL	Quantité (m^3)
Déchets pêchés passivement	

[1] Indiquer la désignation officielle de transport des SLN concernés.
[2] Indiquer la désignation officielle de transport des marchandises solides.

ANNEXE 4

CATÉGORIES DE COÛTS ET DE RECETTES NETTES LIÉS À L'EXPLOITATION ET LA GESTION DES INSTALLATIONS DE RÉCEPTION PORTUAIRES

Coûts directs Coûts d'exploitation directs découlant du dépôt effectif de déchets des navires, y compris les éléments de coût énumérés ci-dessous.	Coûts indirects Coûts administratifs indirects découlant de la gestion du système dans le port, y compris les éléments de coût énumérés ci-dessous.	Recettes nettes Produits nets provenant des systèmes de gestion de déchets et du financement national/régional disponible, y compris les éléments de recettes énumérés ci-dessous.
— Fourniture d'infrastructures des installations de réception portuaires, y compris les conteneurs, citernes, outils de traitement, barges, camions, installations de réception des déchets, installations de traitement; — Concessions de location du site, le cas échéant, ou de location des équipements nécessaires pour l'exploitation des installations de réception portuaires; — Exploitation proprement dite des installations de réception portuaires: collecte des déchets des navires, transport des déchets depuis les installations de réception portuaires pour le traitement final, entretien et nettoyage des installations de réception portuaires, coûts de personnel, y compris les heures supplémentaires, approvisionnement en électricité, analyse des déchets et assurance; — Préparation au réemploi, au recyclage ou à l'élimination des déchets des navires, y compris la collecte sélective des déchets; — Administration: facturation, délivrance des reçus de dépôt des déchets aux navires, déclarations.	— Élaboration et approbation du plan de réception et de traitement des déchets, y compris les éventuels audits de ce plan et de sa mise en œuvre; — Mise à jour du plan de réception et de traitement des déchets, y compris les coûts de main-d'œuvre et les coûts de services de conseil, le cas échéant; — Organisation des procédures de consultation pour l'évaluation (ou réévaluation) du plan de réception et de traitement des déchets; — Gestion des systèmes de notification et de recouvrement des coûts, y compris la demande de réduction des redevances pour les «navires verts», la fourniture de systèmes informatiques au niveau des ports, l'analyse statistique et les coûts de main-d'œuvre connexes; — Organisation de procédures de passation de marchés publics pour la fourniture d'installations de réception portuaires, et délivrance des autorisations nécessaires pour la fourniture d'installations de réception portuaires dans les ports; — Communication d'informations aux utilisateurs du port en distribuant des brochures, en plaçant une signalisation et des affiches dans le port ou en publiant les informations sur le site internet du port, et communication électronique des informations requises à l'article 5; — Gestion des systèmes de gestion de déchets: régimes de responsabilité élargie des producteurs, recyclage, demande d'utilisation et mise en œuvre de fonds nationaux/régionaux; — Autres coûts administratifs: coûts de suivi et de communication électronique des exemptions requises à l'article 9.	— Bénéfices financiers nets provenant des régimes de responsabilité élargie des producteurs; — Autres recettes nettes provenant de la gestion de déchets, notamment des systèmes de recyclage; — Financement au titre du Fonds européen pour les affaires maritimes et la pêche (FEAMP); — Autres financements ou subventions à la disposition des ports en matière de gestion de déchets et de pêche.

ANNEXE 5

CERTIFICAT D'EXEMPTION EN VERTU DE L'ARTICLE 9 EN CE QUI CONCERNE LES EXIGENCES DE L'ARTICLES 6, DE L'ARTICLE 7, PARAGRAPHE 1, ET DE L'ARTICLE 8 DE LA DIRECTIVE (UE) 2019/883 DANS LE[S] PORT[S] DE [INSÉRER LE NOM DU/DES PORTS] [EN][AU][AUX] [INSÉRER L'ÉTAT MEMBRE] [1]

Nom du navire	Numéro ou lettres distinctifs	État du pavillon
[insérer le nom du navire]	*[insérer le numéro OMI]*	*[insérer le nom de l'État du pavillon]*

effectue des services réguliers qui comportent des escales portuaires fréquentes et régulières dans le(s) port(s) suivant(s) situé(s) [en][au][aux] [insérer le nom de l'État membre] conformément à un horaire ou un itinéraire prédéterminé:

[ ]

et fait escale dans ces ports au moins une fois par quinzaine:

[ ]

et a prévu des mesures pour garantir le paiement des redevances et le dépôt des déchets au port ou auprès d'une tierce partie dans le port:

[ ]

et est donc exempté, conformément à [*insérer la disposition pertinente dans la législation nationale du pays*], [des exigences relatives:

☐ *au dépôt obligatoire des déchets des navires*,

☐ *à la notification préalable des déchets, et*

☐ *au paiement de la redevance obligatoire, au(x) port(s) suivant(s)*]:

Le présent certificat est valable jusqu'au [insérer la date], sauf modification avant cette date des motifs de délivrance du certificat.

Lieu et date

.....

Nom
Titre

[1] Rayer la mention inutile.

DIRECTIVE (UE) 2019/884 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 17 avril 2019

modifiant la décision-cadre 2009/315/JAI du Conseil en ce qui concerne les échanges d'informations relatives aux ressortissants de pays tiers ainsi que le système européen d'information sur les casiers judiciaires (ECRIS), et remplaçant la décision 2009/316/JAI du Conseil

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

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 82, paragraphe 1, deuxième alinéa, point d),

vu la proposition de la Commission européenne,

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

statuant conformément à la procédure législative ordinaire ([1]),

considérant ce qui suit:

(1) L'Union s'est donné pour objectif d'offrir à ses citoyens un espace de liberté, de sécurité et de justice sans frontières intérieures, au sein duquel est assurée la libre circulation des personnes. Cet objectif devrait être réalisé au moyen, entre autres, de mesures appropriées visant à prévenir et à lutter contre la criminalité, y compris la criminalité organisée et le terrorisme.

(2) Cet objectif requiert que les informations relatives aux condamnations prononcées dans les États membres soient prises en compte en dehors de l'État membre de condamnation à l'occasion d'une nouvelle procédure pénale, conformément à la décision-cadre 2008/675/JAI du Conseil ([2]), ainsi que pour prévenir de nouvelles infractions.

(3) Cet objectif suppose des échanges d'informations extraites des casiers judiciaires entre les autorités compétentes des États membres. Ces échanges d'informations sont organisés et facilités par les règles énoncées dans la décision-cadre 2009/315/JAI du Conseil ([3]) et par le système européen d'information sur les casiers judiciaires (ECRIS), créé conformément à la décision 2009/316/JAI du Conseil ([4]).

(4) Toutefois, le cadre juridique actuel de l'ECRIS ne répond pas suffisamment aux particularités des demandes concernant des ressortissants de pays tiers. Bien qu'il soit déjà possible d'échanger des informations sur les ressortissants de pays tiers au moyen de l'ECRIS, il n'existe pas de procédure ni de mécanisme commun de l'Union permettant de le faire avec efficacité, rapidité et exactitude.

(5) Au sein de l'Union, les informations relatives aux ressortissants de pays tiers ne sont pas rassemblées, comme c'est le cas pour les ressortissants des États membres - dans l'État membre de nationalité -, mais seulement conservées dans les États membres où les condamnations ont été prononcées. Il n'est donc possible d'avoir un aperçu complet des antécédents judiciaires d'un ressortissant d'un pays tiers qu'en demandant ces informations à tous les États membres.

(6) De telles demandes générales imposent une charge administrative disproportionnée à tous les États membres, y compris à ceux qui ne détiennent pas d'informations sur le ressortissant d'un pays tiers concerné. Dans la pratique, cette charge dissuade les États membres de demander des informations sur les ressortissants de pays tiers à d'autres États membres, ce qui entrave considérablement l'échange d'informations entre eux, et a pour résultat que l'accès aux informations sur les casiers judiciaires est limité aux informations conservées dans leur registre national. Il existe dès lors un risque accru que les échanges d'informations entre États membres soient inefficaces et incomplets.

([1]) Position du Parlement européen du 12 mars 2019 (non encore parue au Journal officiel) et décision du Conseil du 9 avril 2019.
([2]) Décision-cadre 2008/675/JAI du Conseil du 24 juillet 2008 relative à la prise en compte des décisions de condamnation entre les États membres de l'Union européenne à l'occasion d'une nouvelle procédure pénale (JO L 220 du 15.8.2008, p. 32).
([3]) Décision-cadre 2009/315/JAI du Conseil du 26 février 2009 concernant l'organisation et le contenu des échanges d'informations extraites du casier judiciaire entre les États membres (JO L 93 du 7.4.2009, p. 23).
([4]) Décision 2009/316/JAI du Conseil du 6 avril 2009 relative à la création du système européen d'information sur les casiers judiciaires (ECRIS), en application de l'article 11 de la décision-cadre 2009/315/JAI (JO L 93 du 7.4.2009, p. 33).

(7) Afin d'améliorer la situation, la Commission a soumis une proposition, qui a conduit à l'adoption du règlement (UE) 2019/816du Parlement européen et du Conseil ([5]) portant création d'un système centralisé au niveau de l'Union, contenant les données à caractère personnel des ressortissants de pays tiers condamnés, permettant l'identification de l'État membre ou des États membres détenant des informations sur leurs condamnations antérieures (ci-après dénommé «ECRIS-TCN»).

(8) L'ECRIS-TCN permettra à l'autorité centrale d'un État membre de déterminer de manière rapide et efficace dans quels autres États membres des informations sur le casier judiciaire d'un ressortissant d'un pays tiers sont conservées, de manière que le cadre actuel de l'ECRIS puisse être utilisé pour demander à ces États membres des informations sur le casier judiciaire en question conformément à la décision-cadre 2009/315/JAI.

(9) L'échange d'informations sur les condamnations pénales est un aspect important de toute stratégie visant à lutter contre la criminalité et le terrorisme. L'utilisation, par les États membres, de toutes les possibilités qu'offre l'ECRIS contribuerait à la réponse de la justice pénale à la radicalisation conduisant au terrorisme et à l'extrémisme violent.

(10) Afin d'accroître l'utilité des informations relatives aux condamnations et aux mesures d'interdiction consécutives à des condamnations pour infractions sexuelles à l'encontre d'enfants, la directive 2011/93/UE du Parlement européen et du Conseil ([6]) a établi l'obligation, pour les États membres, de prendre les mesures nécessaires pour faire en sorte que, lors du recrutement d'une personne pour un poste impliquant des contacts directs et réguliers avec des enfants, des informations relatives à l'existence de condamnations pénales pour infractions sexuelles à l'encontre d'enfants inscrites au casier judiciaire ou de mesures d'interdiction consécutives auxdites condamnations pénales soient transmises conformément aux procédures prévues dans la décision-cadre 2009/315/JAI. Le but de ce mécanisme est de veiller à ce qu'une personne condamnée pour une infraction sexuelle commise à l'égard d'enfants ne puisse pas dissimuler cette condamnation ou cette mesure d'interdiction en vue d'exercer une activité professionnelle impliquant des contacts directs et réguliers avec des enfants dans un autre État membre.

(11) La présente directive vise à apporter à la décision-cadre 2009/315/JAI les modifications nécessaires pour permettre un échange d'informations efficace sur les condamnations de ressortissants de pays tiers au moyen de l'ECRIS. Elle oblige les États membres à prendre les mesures nécessaires pour faire en sorte que les condamnations soient accompagnées d'informations sur la nationalité, ou les nationalités, de la personne condamnée, dans la mesure où ils disposent de ces informations. Elle introduit également des procédures pour répondre aux demandes d'information, veille à ce qu'un extrait de casier judiciaire demandé par un ressortissant d'un pays tiers soit complété par des informations provenant d'autres États membres, et prévoit les modifications techniques requises pour assurer le bon fonctionnement du système d'échange d'informations.

(12) La directive (UE) 2016/680 du Parlement européen et du Conseil ([7]) devrait s'appliquer au traitement des données à caractère personnel par les autorités nationales compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. Le règlement (UE) 2016/679 du Parlement européen et du Conseil ([8]) devrait s'appliquer au traitement des données à caractère personnel par les autorités nationales lorsqu'un tel traitement ne relève pas du champ d'application de la directive (UE) 2016/680.

(13) Afin d'assurer des conditions uniformes d'exécution de la décision-cadre 2009/315/JAI, il convient d'intégrer les principes de la décision 2009/316/JAI dans ladite décision-cadre, et de conférer des compétences d'exécution à la Commission. Ces compétences devraient être exercées conformément au règlement (UE) nº 182/2011 du Parlement européen et du Conseil ([9]).

([5]) Règlement (UE) 2019/816 du Parlement européen et du Conseil du 17 avril 2019 portant création d'un système centralisé permettant d'identifier les États membres détenant des informations relatives aux condamnations concernant des ressortissants de pays tiers et des apatrides (ECRIS-TCN), qui vise à compléter le système européen d'information sur les casiers judiciaires et modifiant le règlement (UE) 2018/1726 (JO L 135 du 22.5.2019, p. 1).

([6]) 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).

([7]) Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016, p. 89).

([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).

([9]) 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).

(14) L'infrastructure de communication commune utilisée pour l'échange d'informations sur les casiers judiciaires devrait être constituée par les services télématiques transeuropéens sécurisés entre administrations (s-TESTA), toute nouvelle version de ces services ou tout autre réseau sécurisé.

(15) Nonobstant la possibilité de recourir aux programmes financiers de l'Union conformément à la réglementation applicable, chaque État membre devrait supporter ses propres frais résultant de la mise en œuvre, de la gestion, de l'utilisation et de la maintenance de sa base de données relative aux casiers judiciaires, ainsi que de la mise en œuvre, de la gestion, de l'utilisation et de la maintenance des adaptations techniques nécessaires pour pouvoir utiliser l'ECRIS.

(16) La présente directive respecte les droits et libertés fondamentaux consacrés, en particulier, dans la Charte des droits fondamentaux de l'Union européenne, tels que le droit à la protection des données à caractère personnel, les droits à des recours juridictionnel et administratif, le principe de l'égalité en droit, le droit à accéder à un tribunal impartial, la présomption d'innocence et l'interdiction générale de toute discrimination. La présente directive devrait être mise en œuvre conformément à ces droits et principes.

(17) Étant donné que l'objectif de la présente directive, à savoir permettre l'échange rapide et efficace d'informations précises sur les casiers judiciaires des ressortissants de pays tiers, ne peut pas être atteint de manière suffisante par les États membres mais peut, grâce à la mise en place de règles communes, 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.

(18) Conformément aux articles 1er et 2 du protocole nº 22 sur la position du Danemark annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Danemark ne participe pas à l'adoption de la présente directive et n'est pas lié par celle-ci ni soumis à son application.

(19) Conformément aux articles 1er et 2 ainsi qu'à l'article 4 *bis*, paragraphe 1, du protocole nº 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, et sans préjudice de l'article 4 dudit protocole, l'Irlande ne participe pas à l'adoption de la présente directive et n'est pas liée par celle-ci ni soumise à son application.

(20) Conformément à l'article 3 et à l'article 4 *bis*, paragraphe 1, du protocole nº 21, le Royaume-Uni a notifié son souhait de participer à l'adoption et à l'application de la présente directive.

(21) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 28, paragraphe 2, du règlement (CE) nº 45/2001 du Parlement européen et du Conseil ([10]) et a rendu un avis le 13 avril 2016 ([11]).

(22) Il convient dès lors de modifier la décision-cadre 2009/315/JAI en conséquence,

ONT ADOPTÉ LA PRÉSENTE DIRECTIVE:

Article premier

Modifications de la décision-cadre 2009/315/JAI

La décision-cadre 2009/315/JAI est modifiée comme suit:

1) l'article 1er est remplacé par le texte suivant:

«*Article premier*

Objet

La présente décision-cadre

a) définit les conditions dans lesquelles un État membre de condamnation communique aux autres États membres les informations relatives à des condamnations;

([10]) Règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO L 8 du 12.1.2001, p. 1).

([11]) JO C 186 du 25.5.2016, p. 7.

b) définit les obligations qui incombent à l'État membre de condamnation ainsi qu'à l'État membre de la nationalité de la personne condamnée (ci-après dénommé "État membre de nationalité"), et précise les modalités à respecter pour répondre à une demande d'informations extraites du casier judiciaire;

c) établit un système informatique décentralisé pour les échanges d'informations relatives aux condamnations, fondé sur les bases de données relatives aux casiers judiciaires de chaque État membre, le système européen d'information sur les casiers judiciaires (ECRIS).»;

2) à l'article 2, les points suivants sont ajoutés:

«d) "État membre de condamnation": l'État membre dans lequel une condamnation est prononcée;

e) "ressortissant d'un pays tiers": une personne qui n'est pas citoyen de l'Union au sens de l'article 20, paragraphe 1, du traité sur le fonctionnement de l'Union européenne, ou qui est une personne apatride ou dont la nationalité n'est pas connue;

f) "données dactyloscopiques": les données relatives aux impressions simultanées et roulées des empreintes digitales de chaque doigt d'une personne;

g) "image faciale": une image numérique du visage d'une personne;

h) "application de référence de l'ECRIS": le logiciel développé par la Commission et mis à la disposition des États membres pour les échanges d'informations sur les casiers judiciaires au moyen de l'ECRIS.»;

3) à l'article 4, le paragraphe 1 est remplacé par le texte suivant:

«1. Chaque État membre de condamnation prend toutes les mesures nécessaires pour que les condamnations prononcées sur son territoire soient accompagnées des informations relatives à la nationalité ou aux nationalités de la personne condamnée s'il s'agit d'un ressortissant d'un autre État membre ou d'un ressortissant d'un pays tiers. Si la nationalité de la personne condamnée n'est pas connue ou si cette personne est apatride, cela est mentionné dans le casier judiciaire.»;

4) l'article 6 est modifié comme suit:

a) le paragraphe 3 est remplacé par le texte suivant:

«3. Lorsqu'un ressortissant d'un État membre demande à l'autorité centrale d'un autre État membre des informations sur son propre casier judiciaire, cette autorité centrale adresse à l'autorité centrale de l'État membre de nationalité une demande d'informations et d'informations connexes extraites du casier judiciaire et les fait figurer dans l'extrait qui est fourni à la personne concernée.»;

b) le paragraphe suivant est inséré:

«3 *bis*. Lorsqu'un ressortissant d'un pays tiers demande à l'autorité centrale d'un État membre des informations sur son propre casier judiciaire, cette autorité centrale adresse aux seules autorités centrales des États membres qui détiennent des informations sur le casier judiciaire de cette personne une demande d'informations et d'informations connexes extraites du casier judiciaire et les fait figurer dans l'extrait qui est fourni à la personne concernée.»;

5) l'article 7 est modifié comme suit:

a) le paragraphe 4 est remplacé par le texte suivant:

«4. Lorsqu'une demande d'informations extraites du casier judiciaire et relatives aux condamnations prononcées à l'encontre d'un ressortissant d'un État membre est adressée, au titre de l'article 6, à l'autorité centrale d'un État membre autre que l'État membre de nationalité, l'État membre requis transmet ces informations dans les mêmes conditions que celles prévues à l'article 13 de la Convention européenne d'entraide judiciaire en matière pénale.»;

b) le paragraphe suivant est inséré:

«4 *bis*. Lorsqu'une demande d'informations extraites du casier judiciaire et relatives aux condamnations prononcées à l'encontre d'un ressortissant d'un pays tiers est adressée, au titre de l'article 6, aux fins d'une procédure pénale, l'État membre requis transmet les informations correspondant à toute condamnation prononcée dans l'État membre requis et inscrites dans le casier judiciaire ainsi qu'à toute condamnation prononcée dans des pays tiers qui lui ont été ultérieurement transmises et qui ont été inscrites dans le casier judiciaire.

Si ces informations sont demandées à des fins autres qu'une procédure pénale, le paragraphe 2 du présent article s'applique mutatis mutandis.»;

6) à l'article 8, le paragraphe 2 est remplacé par le texte suivant:

«2. Les réponses aux demandes visées à l'article 6, paragraphes 2, 3 et 3 *bis*, sont transmises dans un délai de 20 jours ouvrables à partir de la date de réception de la demande.»;

7) l'article 9 est modifié comme suit:

a) au paragraphe 1, les termes «l'article 7, paragraphes 1 et 4» sont remplacés par les termes «l'article 7, paragraphes 1, 4 et 4 *bis*»;

b) au paragraphe 2, les termes «l'article 7, paragraphes 2 et 4» sont remplacés par les termes «l'article 7, paragraphes 2, 4 et 4 *bis*»;

c) au paragraphe 3, les termes «l'article 7, paragraphes 1, 2 et 4» sont remplacés par les termes «l'article 7, paragraphes 1, 2, 4 et 4 *bis*»;

8) l'article 11 est modifié comme suit:

a) au paragraphe 1, premier alinéa, point c), le point suivant est ajouté:

«iv) l'image faciale;»;

b) les paragraphes 3 à 7 sont remplacés par le texte suivant:

«3. Les autorités centrales des États membres transmettent les informations suivantes par voie électronique au moyen de l'ECRIS et en utilisant un format standardisé conforme aux normes établies par des actes d'exécution:

a) les informations visées à l'article 4;

b) les demandes visées à l'article 6;

c) les réponses visées à l'article 7; et

d) les autres informations pertinentes.

4. En cas d'indisponibilité de la voie de transmission visée au paragraphe 3, les autorités centrales des États membres transmettent toutes les informations visées au paragraphe 3 par tout moyen permettant de laisser une trace écrite et dans des conditions permettant à l'autorité centrale de l'État membre qui les reçoit d'établir l'authenticité des informations, en prenant en considération la sécurité de la transmission.

Si la voie de transmission visée au paragraphe 3 est indisponible pendant une période prolongée, l'État membre concerné en informe les autres États membres et la Commission.

5. Chaque État membre procède aux adaptations techniques nécessaires à l'utilisation du format standardisé aux fins de la transmission par voie électronique, au moyen de l'ECRIS, de toutes les informations visées au paragraphe 3 aux autres États membres. Il notifie à la Commission la date à partir de laquelle il est en mesure de procéder à ces transmissions.»;

9) les articles suivants sont insérés:

«*Article 11* bis

Système européen d'information sur les casiers judiciaires (ECRIS)

1. Afin d'échanger des informations extraites des casiers judiciaires par voie électronique conformément à la présente décision-cadre, un système informatique décentralisé, fondé sur les bases de données relatives aux casiers judiciaires de chaque État membre, le système européen d'information sur les casiers judiciaires (ECRIS), est créé. Il est composé des éléments suivants:

a) l'application de référence de l'ECRIS;

b) une infrastructure de communication commune aux autorités centrales, fournissant un réseau crypté.

Afin de garantir la confidentialité et l'intégrité des informations sur les casiers judiciaires qui sont transmises aux autres États membres, des mesures techniques et organisationnelles appropriées sont utilisées, en tenant compte de l'état des connaissances, du coût de mise en œuvre et des risques posés par le traitement des informations.

2. Toutes les données issues des casiers judiciaires sont conservées exclusivement dans des bases de données gérées par les États membres.

3. Les autorités centrales des États membres ne disposent pas d'un accès direct aux bases de données relatives aux casiers judiciaires des autres États membres.

4. L'État membre concerné est responsable du fonctionnement de l'application de référence de l'ECRIS et des bases de données qui conservent, transmettent et reçoivent des informations extraites des casiers judiciaires. L'Agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA) créée par le règlement (UE) 2018/1726 du Parlement européen et du Conseil (*) soutient les États membres conformément à ses missions telles qu'elles sont énoncées dans le règlement (UE) 2019/816 du Parlement européen et du Conseil (**).

5. La Commission est responsable du fonctionnement de l'infrastructure de communication commune. Celle-ci remplit les conditions requises en matière de sécurité et répond pleinement aux besoins de l'ECRIS.

6. L'eu-LISA fournit, développe et gère l'application de référence de l'ECRIS.

7. Chaque État membre supporte ses propres frais résultant de la mise en œuvre, de la gestion, de l'utilisation et de la maintenance de sa base de données relative aux casiers judiciaires ainsi que de l'installation et de l'utilisation de l'application de référence de l'ECRIS.

La Commission supporte les frais résultant de la mise en œuvre, de la gestion, de l'utilisation, de la maintenance et des développements futurs de l'infrastructure de communication commune.

8. Les États membres qui utilisent leur logiciel d'application national de l'ECRIS conformément à l'article 4, paragraphes 4 à 8, du règlement (UE) 2019/816 peuvent continuer à utiliser leur logiciel d'application national de l'ECRIS au lieu de l'application de référence de l'ECRIS, pour autant qu'ils remplissent les conditions énoncées dans ces paragraphes.

Article 11 ter

Actes d'exécution

1. La Commission arrête les mesures ci-après au moyen d'actes d'exécution:

a) le format standardisé visé à l'article 11, paragraphe 3, y compris en ce qui concerne les informations relatives à l'infraction ayant donné lieu à la condamnation et les informations relatives au contenu de la condamnation;

b) les règles relatives à la mise en œuvre technique de l'ECRIS et à l'échange de données dactyloscopiques;

c) les autres modalités techniques d'organisation et de facilitation des échanges d'informations sur les condamnations entre les autorités centrales des États membres, et notamment:

i) les dispositifs facilitant la compréhension et la traduction automatique des informations transmises;

ii) les conditions de l'échange des informations par voie électronique, notamment en ce qui concerne les normes techniques à utiliser et, le cas échéant, les procédures d'échange applicables.

2. Les actes d'exécution visés au paragraphe 1 du présent article sont adoptés en conformité avec la procédure d'examen visée à l'article 12 *bis*, paragraphe 2.

(*) Règlement (UE) 2018/1726 du Parlement européen et du Conseil du 14 novembre 2018 relatif à l'Agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA), modifiant le règlement (CE) n° 1987/2006 et la décision 2007/533/JAI du Conseil et abrogeant le règlement (UE) n° 1077/2011 (JO L 295 du 21.11.2018, p. 99).

(**) Règlement (UE) 2019/816 du Parlement européen et du Conseil du 17 avril 2019 portant création d'un système centralisé permettant d'identifier les États membres détenant des informations relatives aux condamnations concernant des ressortissants de pays tiers et des apatrides (ECRIS-TCN), qui vise à compléter le système européen d'information sur les casiers judiciaires et modifiant le règlement (UE) 2018/1726 (JO L 135 du 22.5.2019, p. 1).»;

10) l'article suivant est inséré:

«*Article 12* bis

Comité

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

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

Lorsque le comité n'émet aucun avis, la Commission n'adopte pas le projet d'acte d'exécution, et l'article 5, paragraphe 4, troisième alinéa, du règlement (UE) n° 182/2011 s'applique.»;

11) l'article suivant est inséré:

«*Article 13* bis

Rapport de la Commission et réexamen

1. Au plus tard le 29 juin 2023, la Commission présente au Parlement européen et au Conseil un rapport sur l'application de la présente décision-cadre. Le rapport évalue dans quelle mesure les États membres ont pris les mesures nécessaires pour se conformer aux dispositions de la présente décision-cadre, y compris sa mise en œuvre technique.

2. Le rapport est accompagné, le cas échéant, de propositions législatives pertinentes.

3. La Commission publie régulièrement un rapport sur les échanges d'informations extraites du casier judiciaire au moyen de l'ECRIS ainsi que sur l'utilisation de l'ECRIS-TCN, fondé notamment sur les statistiques fournies par l'eu-LISA et par les États membres conformément au règlement (UE) 2019/816. Le rapport est publié pour la première fois un an après la présentation du rapport visé au paragraphe 1.

4. Le rapport de la Commission visé au paragraphe 3 porte en particulier sur le niveau des échanges d'informations entre les États membres, y compris ceux relatifs aux ressortissants de pays tiers, ainsi que sur la finalité des demandes et leur nombre respectif, y compris les demandes introduites à des fins autres qu'une procédure pénale, telles que la vérification des antécédents et les demandes d'informations introduites par des personnes concernées pour obtenir leur propre casier judiciaire.»

Article 2

Remplacement de la décision 2009/316/JAI

La décision 2009/316/JAI est remplacée à l'égard des États membres liés par la présente directive, sans préjudice des obligations desdits États membres en ce qui concerne la date de transposition de ladite décision.

Article 3

Transposition

1. Les États membres mettent en vigueur les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive au plus tard le 28 juin 2022. Ils communiquent immédiatement à la Commission le texte de ces dispositions.

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. Elles contiennent également une mention précisant que les références faites, dans les dispositions législatives, réglementaires et administratives en vigueur, à la décision remplacée par la présente directive s'entendent comme faites à la présente directive. Les modalités de cette référence et la formulation de cette mention sont arrêtées par les États membres.

2. Les États membres communiquent à la Commission le texte des dispositions essentielles de droit interne qu'ils adoptent dans le domaine régi par la présente directive.

3. Les États membres procèdent aux adaptations techniques visées à l'article 11, paragraphe 5, de la décision-cadre 2009/315/JAI, telle que modifiée par la présente directive, au plus tard le 28 juin 2022.

Article 4

Entrée en vigueur et application

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

L'article 2 s'applique à partir du 28 juin 2022.

Article 5

Destinataires

Les États membres sont destinataires de la présente directive conformément aux traités.

Fait à Strasbourg, le 17 avril 2019.

Par le Parlement européen	*Par le Conseil*
Le président	*Le président*
A. TAJANI	G. CIAMBA

ISSN 1977-0693 (édition électronique)
ISSN 1725-2563 (édition papier)

Office des publications de l'Union européenne
2985 Luxembourg
LUXEMBOURG

FR