►**B**

DIRECTIVE (UE) 2022/2555 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 14 décembre 2022

concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2)

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

(JO L 333 du 27.12.2022, p. 80)

Rectifiée par:

►**C1** Rectificatif, JO L 90613 du 24.7.2025, p. 1 (2022/2555)

▼B

DIRECTIVE (UE) 2022/2555 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 14 décembre 2022

concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2)

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

CHAPITRE I

DISPOSITIONS GÉNÉRALES

Article premier

Objet

1. La présente directive établit des mesures qui ont pour but d'obtenir un niveau commun élevé de cybersécurité dans l'ensemble de l'Union, afin d'améliorer le fonctionnement du marché intérieur.

2. À cette fin, la présente directive fixe:

a) des obligations qui imposent aux États membres d'adopter des stratégies nationales en matière de cybersécurité, de désigner ou de mettre en place des autorités compétentes, des autorités chargées de la gestion des cybercrises, des points de contact uniques en matière de cybersécurité (ci-après dénommés «points de contact uniques») et des centres de réponse aux incidents de sécurité informatique (CSIRT);

b) des mesures de gestion des risques en matière de cybersécurité et des obligations d'information pour les entités d'un type visé à l'annexe I ou II, ainsi que pour les entités recensées en tant qu'entités critiques en vertu de la directive (UE) 2022/2557;

c) des règles et des obligations pour le partage d'informations en matière de cybersécurité;

d) les obligations des États membres en matière de supervision et d'exécution.

Article 2

Champ d'application

1. La présente directive s'applique aux entités publiques ou privées d'un type visé à l'annexe I ou II qui constituent des entreprises moyennes en vertu de l'article 2 de l'annexe de la recommandation 2003/361/CE, ou qui dépassent les plafonds prévus au paragraphe 1 dudit article, et qui fournissent leurs services ou exercent leurs activités au sein de l'Union.

▼B

L'article 3, paragraphe 4, de l'annexe de ladite recommandation ne s'applique pas aux fins de la présente directive.

2. La présente directive s'applique également aux entités d'un type visé à l'annexe I ou II, quelle que soit leur taille, dans les cas suivants:

a) les services sont fournis par:

   i) des fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public;

   ii) des prestataires de services de confiance;

   iii) des registres des noms de domaine de premier niveau et des fournisseurs de services de système de noms de domaine;

b) l'entité est, dans un État membre, le seul prestataire d'un service qui est essentiel au maintien d'activités sociétales ou économiques critiques;

c) une perturbation du service fourni par l'entité pourrait avoir un impact important sur la sécurité publique, la sûreté publique ou la santé publique;

d) une perturbation du service fourni par l'entité pourrait induire un risque systémique important, en particulier pour les secteurs où cette perturbation pourrait avoir un impact transfrontière;

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

f) l'entité est une entité de l'administration publique:

   i) des pouvoirs publics centraux tels qu'ils sont définis par un État membre conformément au droit national; ou

   ii) au niveau régional, tel qu'il est défini par un État membre conformément au droit national, qui, à la suite d'une évaluation basée sur les risques, fournit des services dont la perturbation pourrait avoir un impact important sur des activités sociétales ou économiques critiques.

3. La présente directive s'applique aux entités recensées en tant qu'entités critiques en vertu de la directive (UE) 2022/2557, quelle que soit leur taille.

▼B

4. La présente directive s'applique aux entités fournissant des services d'enregistrement de noms de domaine, quelle que soit leur taille.

5. Les États membres peuvent prévoir que la présente directive s'applique:

a) aux entités de l'administration publique au niveau local;

b) aux établissements d'enseignement, en particulier lorsqu'ils mènent des activités de recherche critiques.

6. La présente directive est sans préjudice de la responsabilité des États membres en matière de sauvegarde de la sécurité nationale et de leur pouvoir de garantir d'autres fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer l'intégrité territoriale de l'État et de maintenir l'ordre public.

7. La présente directive ne s'applique pas aux entités de l'administration publique qui exercent leurs activités dans les domaines de la sécurité nationale, de la sécurité publique, de la défense ou de l'application de la loi, y compris la prévention et la détection des infractions pénales, ainsi que les enquêtes et les poursuites en la matière.

8. Les États membres peuvent exempter des entités spécifiques qui exercent des activités dans les domaines de la sécurité nationale, de la sécurité publique, de la défense ou de l'application de la loi, y compris la prévention et la détection des infractions pénales, ainsi que les enquêtes et les poursuites en la matière, ou qui fournissent des services exclusivement aux entités de l'administration publique visées au paragraphe 7 du présent article, des obligations prévues à l'article 21 ou 23 en ce qui concerne ces activités ou services. Dans de tels cas, les mesures de supervision et d'exécution visées au chapitre VII ne s'appliquent pas à ces activités ou services spécifiques. Lorsque les entités exercent des activités ou fournissent des services exclusivement du type visé au présent paragraphe, les États membres peuvent également décider d'exempter ces entités des obligations prévues aux articles 3 et 27.

9. Les paragraphes 7 et 8 ne s'appliquent pas lorsqu'une entité agit en tant que prestataire de services de confiance.

10. La présente directive ne s'applique pas aux entités que les États membres ont exclues du champ d'application du règlement (UE) 2022/2554 conformément à l'article 2, paragraphe 4, dudit règlement.

11. Les obligations énoncées dans la présente directive n'impliquent pas la fourniture d'informations dont la divulgation serait contraire aux intérêts essentiels des États membres en matière de sécurité nationale, de sécurité publique ou de défense.

12. La présente directive est sans préjudice du règlement (UE) 2016/679, de la directive 2002/58/CE, des directives 2011/93/UE ([1]) et 2013/40/UE ([2]) du Parlement européen et du Conseil et de la directive (UE) 2022/2557.

([1]) 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).

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

▼B

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

14. Les entités, les autorités compétentes, les points de contact uniques et les CSIRT traitent les données à caractère personnel dans la mesure nécessaire aux fins de la présente directive et conformément au règlement (UE) 2016/679; ce traitement est fondé en particulier sur l'article 6 dudit règlement.

Le traitement des données à caractère personnel en vertu de la présente directive par les fournisseurs de réseaux de communications électroniques publics ou les fournisseurs de services de communications électroniques accessibles au public est effectué conformément au droit de l'Union en matière de protection des données et au droit de l'Union en matière de protection de la vie privée, en particulier la directive 2002/58/CE.

Article 3

Entités essentielles et importantes

1. Aux fins de la présente directive, les entités suivantes sont considérées comme étant des entités essentielles:

a) les entités d'un type visé à l'annexe I qui dépassent les plafonds applicables aux moyennes entreprises prévus à l'article 2, paragraphe 1, de l'annexe de la recommandation 2003/361/CE;

b) les prestataires de services de confiance qualifiés et les registres de noms de domaine de premier niveau ainsi que les fournisseurs de services DNS, quelle que soit leur taille;

c) les fournisseurs de réseaux publics de communications électroniques publics ou de services de communications électroniques accessibles au public qui constituent des moyennes entreprises en vertu de l'article 2 de l'annexe de la recommandation 2003/361/CE;

d) les entités de l'administration publique visées à l'article 2, paragraphe 2, point f) i);

e) toute autre entité d'un type visé à l'annexe I ou II qui est identifiée par un État membre en tant qu'entité essentielle en vertu de l'article 2, paragraphe 2, points b) à e);

f) les entités recensées en tant qu'entités critiques en vertu de la directive (UE) 2022/2557, visées à l'article 2, paragraphe 3, de la présente directive;

g) si l'État membre en dispose ainsi, les entités que cet État membre a identifiées avant le 16 janvier 2023 comme des opérateurs de services essentiels conformément à la directive (UE) 2016/1148 ou au droit national.

▼B

2. Aux fins de la présente directive, les entités d'un type visé à l'annexe I ou II qui ne constituent pas des entités essentielles en vertu du paragraphe 1 du présent article sont considérées comme des entités importantes. Celles-ci incluent les entités identifiées par un État membre en tant qu'entités importantes en vertu de l'article 2, paragraphe 2, points b) à e).

3. Au plus tard le 17 avril 2025, les États membres établissent une liste des entités essentielles et importantes ainsi que des entités fournissant des services d'enregistrement de noms de domaine. Les États membres réexaminent cette liste et, le cas échéant, la mettent à jour régulièrement et au moins tous les deux ans par la suite.

4. Aux fins de l'établissement de la liste visée au paragraphe 3, les États membres exigent des entités visées audit paragraphe qu'elles communiquent aux autorités compétentes au moins les informations suivantes:

a) le nom de l'entité;

b) l'adresse et les coordonnées actualisées, y compris les adresses électroniques, les plages d'IP et les numéros de téléphone;

c) le cas échéant, le secteur et le sous-secteur concernés visés à l'annexe I ou II; et

d) le cas échéant, une liste des États membres dans lesquels elles fournissent des services relevant du champ d'application de la présente directive.

Les entités visées au paragraphe 3 notifient sans tarder toute modification des informations qu'elles ont communiquées conformément au premier alinéa du présent paragraphe et, en tout état de cause, dans un délai de deux semaines à compter de la date de la modification.

La Commission, avec l'aide de l'Agence de l'Union européenne pour la cybersécurité (ENISA), fournit sans retard injustifié des lignes directrices et des modèles concernant les obligations prévues au présent paragraphe.

Les États membres peuvent mettre en place des mécanismes nationaux permettant aux entités de s'enregistrer elles-mêmes.

5. Au plus tard le 17 avril 2025, puis tous les deux ans par la suite, les autorités compétentes notifient:

a) à la Commission et au groupe de coopération le nombre des entités essentielles et importantes identifiées conformément au paragraphe 3 pour chaque secteur et sous-secteur visé à l'annexe I ou II; et

b) à la Commission les informations pertinentes sur le nombre d'entités essentielles et importantes identifiées en vertu de l'article 2, paragraphe 2, points b) à e), le secteur et le sous-secteur visés à l'annexe I ou II auxquels elles appartiennent, le type de service qu'elles fournissent et la disposition, parmi celles figurant à l'article 2, paragraphe 2, points b) à e), en vertu de laquelle elles ont été identifiées.

▼B

6. Jusqu'au 17 avril 2025 et à la demande de la Commission, les États membres peuvent notifier à la Commission le nom des entités essentielles et importantes visées au paragraphe 5, point b).

Article 4

Actes juridiques sectoriels de l'Union

1. Lorsque des actes juridiques sectoriels de l'Union imposent à des entités essentielles ou importantes d'adopter des mesures de gestion des risques en matière de cybersécurité ou de notifier des incidents importants, et lorsque ces exigences ont un effet au moins équivalent à celui des obligations prévues par la présente directive, les dispositions pertinentes de la présente directive, y compris celles relatives à la supervision et à l'exécution prévues au chapitre VII, ne sont pas applicables auxdites entités. Lorsque des actes juridiques sectoriels de l'Union ne couvrent pas toutes les entités d'un secteur spécifique relevant du champ d'application de la présente directive, les dispositions pertinentes de la présente directive continuent de s'appliquer aux entités non couvertes par ces actes juridiques sectoriels de l'Union.

2. Les exigences visées au paragraphe 1 du présent article sont considérées comme ayant un effet équivalent aux obligations prévues par la présente directive lorsque:

a) les mesures de gestion des risques en matière de cybersécurité ont un effet au moins équivalent à celui des mesures prévues à l'article 21, paragraphes 1 et 2; ou

b) l'acte juridique sectoriel de l'Union prévoit un accès immédiat, s'il y a lieu, automatique et direct, aux notifications d'incidents par les CSIRT, les autorités compétentes ou les points de contact uniques en vertu de la présente directive, et lorsque les exigences relatives à la notification des incidents importants sont au moins équivalentes à celles prévues à l'article 23, paragraphes 1 à 6, de la présente directive.

3. Au plus tard le 17 juillet 2023, la Commission fournit des lignes directrices clarifiant l'application des paragraphes 1 et 2. La Commission réexamine ces lignes directrices à intervalles réguliers. Lors de la préparation de ces lignes directrices, la Commission tient compte de toutes les observations du groupe de coopération et de l'ENISA.

Article 5

Harmonisation minimale

La présente directive ne fait pas obstacle à l'adoption ou au maintien par les États membres de dispositions assurant un niveau plus élevé de cybersécurité, à condition que ces dispositions soient compatibles avec les obligations des États membres prévues par le droit de l'Union.

Article 6

Définitions

Aux fins de la présente directive, on entend par:

▼B

1) «réseau et système d'information»:

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

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

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

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

3) «cybersécurité»: la cybersécurité au sens de l'article 2, point 1), du règlement (UE) 2019/881;

4) «stratégie nationale en matière de cybersécurité»: le cadre cohérent d'un État membre fournissant des objectifs et des priorités stratégiques dans le domaine de la cybersécurité et de la gouvernance en vue de les réaliser dans cet État membre;

5) «incident évité»: un événement qui aurait pu compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles, mais dont la réalisation a pu être empêchée ou ne s'est pas produite;

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

7) «incident de cybersécurité majeur»: un incident qui provoque des perturbations dépassant les capacités de réaction du seul État membre concerné ou qui a un impact important sur au moins deux États membres;

▼C1

8) «gestion des incidents»: toutes les actions et procédures visant à prévenir, détecter, analyser et contenir un incident ou à y répondre et à y remédier;

▼B

9) «risque»: le potentiel de perte ou de perturbation causé par un incident, à exprimer comme la combinaison de l'ampleur de cette perte ou de cette perturbation et de la probabilité qu'un tel incident se produise;

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

11) «cybermenace importante»: une cybermenace qui, compte tenu de ses caractéristiques techniques, peut être considérée comme susceptible d'avoir un impact grave sur les réseaux et les systèmes d'information d'une entité ou les utilisateurs des services de l'entité, en causant un dommage matériel, corporel ou moral considérable;

12) «produit TIC»: un produit TIC au sens de l'article 2, point 12), du règlement (UE) 2019/881;

13) «service TIC»: un service TIC au sens de l'article 2, point 13), du règlement (UE) 2019/881;

14) «processus TIC»: un processus TIC au sens de l'article 2, point 14), du règlement (UE) 2019/881;

15) «vulnérabilité»: une faiblesse, susceptibilité ou faille de produits TIC ou de services TIC qui peut être exploitée par une cybermenace;

16) «norme»: une norme au sens de l'article 2, point 1), du règlement (UE) n° 1025/2012 du Parlement européen et du Conseil ([3]);

17) «spécification technique»: une spécification technique au sens de l'article 2, point 4), du règlement (UE) n° 1025/2012;

18) «point d'échange internet»: une structure de réseau qui permet l'interconnexion de plus de deux réseaux indépendants (systèmes autonomes), essentiellement aux fins de faciliter l'échange de trafic internet, qui n'assure l'interconnexion que pour des systèmes autonomes et qui n'exige pas que le trafic internet passant entre une paire quelconque de systèmes autonomes participants transite par un système autonome tiers, pas plus qu'il ne modifie ou n'altère par ailleurs un tel trafic;

19) «système de noms de domaine» ou «DNS»: un système hiérarchique et distribué d'affectation de noms qui permet l'identification des services et des ressources internet, ce qui rend possible l'utilisation de services de routage et de connectivité internet par les dispositifs des utilisateurs finaux pour accéder à ces services et ressources;

([3]) 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).

▼B

20) «fournisseur de services DNS»: une entité qui fournit:

a) des services de résolution de noms de domaine récursifs accessibles au public destinés aux utilisateurs finaux de l'internet; ou

b) des services de résolution de noms de domaine faisant autorité pour une utilisation par des tiers, à l'exception des serveurs de noms de racines;

21) «registre de noms de domaine de premier niveau»: une entité à laquelle un domaine de premier niveau spécifique a été délégué et qui est responsable de l'administration du domaine de premier niveau, y compris de l'enregistrement des noms de domaine relevant du domaine de premier niveau et du fonctionnement technique du domaine de premier niveau, notamment l'exploitation de ses serveurs de noms, la maintenance de ses bases de données et la distribution des fichiers de zone du domaine de premier niveau sur les serveurs de noms, que ces opérations soient effectuées par l'entité elle-même ou qu'elles soient sous-traitées, mais à l'exclusion des situations où les noms de domaine de premier niveau sont utilisés par un registre uniquement pour son propre usage;

22) «entité fournissant des services d'enregistrement de noms de domaine»: un bureau d'enregistrement ou un agent agissant pour le compte de bureaux d'enregistrement, tel qu'un fournisseur ou revendeur de services d'anonymisation ou d'enregistrement fiduciaire;

23) «service numérique»: un service au sens de l'article 1er, paragraphe 1, point b), de la directive (UE) 2015/1535 du Parlement européen et du Conseil ([4]);

24) «service de confiance»: un service de confiance au sens de l'article 3, point 16, du règlement (UE) no 910/2014;

25) «prestataire de services de confiance»: un prestataire de services de confiance au sens de l'article 3, point 19, du règlement (UE) no 910/2014;

26) «service de confiance qualifié»: un service de confiance qualifié au sens de l'article 3, point 17, du règlement (UE) no 910/2014;

27) «prestataire de services de confiance qualifié»: un prestataire de services de confiance qualifié au sens de l'article 3, point 20, du règlement (UE) no 910/2014;

28) «place de marché en ligne»: une place de marché en ligne au sens de l'article 2, point n), de la directive 2005/29/CE du Parlement européen et du Conseil ([5]);

29) «moteur de recherche en ligne»: un moteur de recherche en ligne au sens de l'article 2, point 5), du règlement (UE) 2019/1150 du Parlement européen et du Conseil ([6]);

([4]) 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).

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

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

▼B

30) «service d'informatique en nuage»: un service numérique qui permet l'administration à la demande et l'accès large à distance à un ensemble modulable et variable de ressources informatiques pouvant être partagées, y compris lorsque ces ressources sont réparties à différents endroits;

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

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

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

34) «représentant»: une personne physique ou morale établie dans l'Union qui est expressément désignée pour agir pour le compte d'un fournisseur de services DNS, d'un registre de noms de domaine de premier niveau, d'une entité fournissant des services d'enregistrement de noms de domaine, d'un fournisseur d'informatique en nuage, d'un fournisseur de services de centre de données, d'un fournisseur de réseau de diffusion de contenu, d'un fournisseur de services gérés, d'un fournisseur de services de sécurité gérés ou d'un fournisseur de places de marché en ligne, de moteurs de recherche en ligne ou de plateformes de services de réseaux sociaux non établi dans l'Union, qui peut être contactée par une autorité compétente ou un CSIRT à la place de l'entité elle-même concernant les obligations incombant à ladite entité en vertu de la présente directive;

35) «entité de l'administration publique»: une entité reconnue comme telle dans un État membre conformément au droit national, à l'exclusion de la justice, des parlements et des banques centrales, qui satisfait aux critères suivants:

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

   b) elle est dotée de la personnalité juridique ou est juridiquement habilitée à agir pour le compte d'une autre entité dotée de la personnalité juridique;

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

   d) elle a le pouvoir d'adresser à des personnes physiques ou morales des décisions administratives ou réglementaires affectant leurs droits en matière de mouvements transfrontières des personnes, des biens, des services ou des capitaux;

▼B

36) «réseau de communications électroniques public»: un réseau de communications électroniques public au sens de l'article 2, point 8), de la directive (UE) 2018/1972;

37) «service de communications électroniques»: un service de communications électroniques au sens de l'article 2, point 4), de la directive (UE) 2018/1972;

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

39) «fournisseur de services gérés»: une entité qui fournit des services liés à l'installation, à la gestion, à l'exploitation ou à l'entretien de produits, de réseaux, d'infrastructures ou d'applications TIC ou d'autres réseaux et systèmes d'information, par l'intermédiaire d'une assistance ou d'une administration active, soit dans les locaux des clients, soit à distance;

40) «fournisseur de services de sécurité gérés»: un fournisseur de services gérés qui effectue ou fournit une assistance pour des activités liées à la gestion des risques en matière de cybersécurité;

41) «organisme de recherche»: une entité dont l'objectif premier est de mener des activités de recherche appliquée ou de développement expérimental en vue d'exploiter les résultats de cette recherche à des fins commerciales, à l'exclusion des établissements d'enseignement.

CHAPITRE II

CADRES COORDONNÉS EN MATIÈRE DE CYBERSÉCURITÉ

Article 7

Stratégie nationale en matière de cybersécurité

1. Chaque État membre adopte une stratégie nationale en matière de cybersécurité qui détermine les objectifs stratégiques, les ressources nécessaires pour atteindre ces objectifs ainsi que les mesures politiques et réglementaires appropriées, en vue de parvenir à un niveau élevé de cybersécurité et de le maintenir. La stratégie nationale en matière de cybersécurité comprend:

a) les objectifs et priorités de la stratégie de l'État membre en matière de cybersécurité, couvrant en particulier les secteurs visés aux annexes I et II;

b) un cadre de gouvernance visant à atteindre les objectifs et priorités visés au point a) du présent paragraphe, y compris les politiques visées au paragraphe 2;

c) un cadre de gouvernance précisant les rôles et les responsabilités des parties prenantes concernées au niveau national, et sur lequel reposent la coopération et la coordination au niveau national entre les autorités compétentes, les points de contact uniques et les CSIRT en vertu de la présente directive, ainsi que la coordination et la coopération entre ces organismes et les autorités compétentes en vertu d'actes juridiques sectoriels de l'Union;

▼B

d) un mécanisme visant à déterminer les actifs pertinents et une évaluation des risques dans cet État membre;

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

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

g) un cadre politique visant une coordination renforcée entre les autorités compétentes en vertu de la présente directive et de la directive (UE) 2022/2557 aux fins du partage d'informations relatives aux risques, aux menaces et aux incidents dans les domaines cyber et non cyber et de l'exercice des tâches de supervision, le cas échéant;

h) un plan comprenant les mesures nécessaires en vue d'améliorer le niveau général de sensibilisation des citoyens à la cybersécurité.

2. Dans le cadre de la stratégie nationale en matière de cybersécurité, les États membres adoptent notamment des politiques portant sur les éléments suivants:

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

b) l'inclusion et la spécification d'exigences liées à la cybersécurité pour les produits et services TIC dans les marchés publics, y compris concernant la certification de cybersécurité, le chiffrement et l'utilisation de produits de cybersécurité en sources ouvertes;

c) la gestion des vulnérabilités, y compris la promotion et la facilitation de la divulgation coordonnée des vulnérabilités en vertu de l'article 12, paragraphe 1;

d) le maintien de la disponibilité générale, de l'intégrité et de la confidentialité du noyau public de l'internet ouvert, y compris, le cas échéant, la cybersécurité des câbles de communication sous-marins;

e) la promotion du développement et de l'intégration de technologies avancées pertinentes visant à mettre en œuvre des mesures de pointe dans la gestion des risques en matière de cybersécurité;

f) la promotion et le développement de l'éducation et de la formation en matière de cybersécurité, des compétences en matière de cybersécurité, des initiatives de sensibilisation et de recherche et développement en matière de cybersécurité, ainsi que des orientations sur les bonnes pratiques de cyberhygiène et les contrôles, à l'intention des citoyens, des parties prenantes et des entités;

g) le soutien aux institutions universitaires et de recherche visant à développer, améliorer et promouvoir le déploiement des outils de cybersécurité et à sécuriser les infrastructures de réseau;

▼B

h) la mise en place de procédures pertinentes et d'outils de partage d'informations appropriés visant à soutenir le partage volontaire d'informations sur la cybersécurité entre les entités conformément au droit de l'Union;

i) le renforcement des valeurs de cyberrésilience et de cyberhygiène des petites et moyennes entreprises, en particulier celles qui sont exclues du champ d'application de la présente directive, en fournissant des orientations et un soutien facilement accessibles pour répondre à leurs besoins spécifiques;

j) la promotion d'une cyberprotection active.

3. Les États membres notifient leur stratégie nationale en matière de cybersécurité à la Commission dans un délai de trois mois suivant leur adoption. Les États membres peuvent exclure de ces notifications les informations relatives à leur sécurité nationale.

4. Les États membres évaluent régulièrement leur stratégie nationale en matière de cybersécurité, et au moins tous les cinq ans, sur la base d'indicateurs clés de performance et, le cas échéant, les modifient. L'ENISA aide les États membres, à leur demande, à élaborer ou actualiser une stratégie nationale en matière de cybersécurité et des indicateurs clés de performance aux fins de l'évaluation de cette stratégie, afin de l'aligner sur les exigences et les obligations prévues par la présente directive.

Article 8

Autorités compétentes et points de contact uniques

1. Chaque État membre désigne ou établit une ou plusieurs autorités compétentes chargées de la cybersécurité et des tâches de supervision visées au chapitre VII (ci-après dénommées «autorités compétentes»).

2. Les autorités compétentes visées au paragraphe 1 contrôlent la mise en œuvre de la présente directive au niveau national.

3. Chaque État membre désigne ou établit un point de contact unique. Lorsqu'un État membre désigne ou établit une seule autorité compétente conformément au paragraphe 1, cette dernière fait aussi fonction de point de contact unique dudit État membre.

4. Chaque point de contact unique exerce une fonction de liaison visant à assurer la coopération transfrontière des autorités de son État membre avec les autorités compétentes des autres États membres et, le cas échéant, avec la Commission et l'ENISA, ainsi qu'à garantir la coopération intersectorielle avec les autres autorités compétentes de son État membre.

5. Les États membres veillent à ce que leurs autorités compétentes et points de contact uniques disposent de ressources suffisantes pour pouvoir s'acquitter de leurs tâches de manière effective et efficace et atteindre ainsi les objectifs de la présente directive.

6. Chaque État membre notifie à la Commission, sans retard injustifié, l'identité de l'autorité compétente visée au paragraphe 1 et du point de contact unique visé au paragraphe 3, les tâches qui sont confiées à ces autorités et toute modification ultérieure dans ce cadre. Chaque État membre rend publique l'identité de son autorité compétente. La Commission publie une liste des points de contact uniques.

▼B

Article 9

Cadres nationaux de gestion des crises cyber

1. Chaque État membre désigne ou établit une ou plusieurs autorités compétentes qui sont chargées de la gestion des incidents de cybersécurité majeurs et des crises (ci-après dénommées «autorités de gestion des crises cyber»). Les États membres veillent à ce que ces autorités disposent de ressources suffisantes pour s'acquitter, de manière effective et efficace, des tâches qui leur sont dévolues. Les États membres veillent à la cohérence avec les cadres nationaux existants pour la gestion générale des crises.

2. Lorsqu'un État membre désigne ou établit plus d'une autorité de gestion des crises cyber conformément au paragraphe 1, il indique clairement laquelle de ces autorités fera office de coordinateur pour la gestion des incidents de cybersécurité majeurs et des crises.

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

4. Chaque État membre adopte un plan national de réaction aux crises et incidents de cybersécurité majeurs dans lequel sont définis les objectifs et les modalités de gestion des incidents de cybersécurité majeurs et des crises. Ce plan établit notamment les éléments suivants:

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

b) les tâches et responsabilités des autorités de gestion des crises cyber;

c) les procédures de gestion des crises cyber, y compris leur intégration dans le cadre national général de gestion des crises et les canaux d'échange d'informations;

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

e) les parties prenantes et les infrastructures des secteurs public et privé concernées;

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

5. Dans un délai de trois mois à compter de la désignation ou de la mise en place de l'autorité de gestion des crises cyber visée au paragraphe 1, chaque État membre notifie à la Commission l'identité de son autorité et toute modification ultérieure dans ce cadre. Les États membres soumettent à la Commission et au réseau européen pour la préparation et la gestion des crises cyber (EU-CyCLONe) les informations pertinentes relatives aux prescriptions du paragraphe 4 concernant leurs plans nationaux d'intervention en cas d'incident de cybersécurité majeurs et de crise dans un délai de trois mois suivant l'adoption de ces plans. Les États membres peuvent exclure certaines informations si et dans la mesure où cette exclusion est nécessaire pour préserver la sécurité nationale.

▼B

Article 10

Centres de réponse aux incidents de sécurité informatique (CSIRT)

1. Chaque État membre désigne ou met en place un ou plusieurs CSIRT. Les CSIRT peuvent être désignés ou établis au sein d'une autorité compétente. Les CSIRT se conforment aux exigences énumérées à l'article 11, paragraphe 1, couvrent au moins les secteurs, les sous-secteurs et les types d'entités visés aux annexes I et II, et sont chargés de la gestion des incidents selon un processus bien défini.

2. Les États membres veillent à ce que chaque CSIRT dispose de ressources suffisantes pour pouvoir s'acquitter efficacement de ses tâches énumérées à l'article 11, paragraphe 3.

3. Les États membres veillent à ce que chaque CSIRT dispose d'une infrastructure de communication et d'information adaptée, sécurisée et résiliente leur permettant d'échanger des informations avec les entités essentielles et importantes et les autres parties prenantes. À cette fin, les États membres veillent à ce que chaque CSIRT contribue au déploiement d'outils sécurisés de partage d'informations.

4. Les CSIRT coopèrent et, le cas échéant, échangent des informations pertinentes conformément à l'article 29 avec des communautés sectorielles ou intersectorielles d'entités essentielles et importantes.

5. Les CSIRT participent aux évaluations par les pairs organisées conformément à l'article 19.

6. Les États membres veillent à ce que leurs CSIRT coopèrent de manière effective, efficace et sécurisée au sein du réseau des CSIRT.

7. Les CSIRT peuvent établir des relations de coopération avec les centres de réponse aux incidents de sécurité informatique nationaux de pays tiers. Dans le cadre de ces relations de coopération, les États membres facilitent un échange d'informations effectif, efficace et sécurisé avec ces centres de réponse aux incidents de sécurité informatique nationaux de pays tiers, en utilisant les protocoles d'échange d'informations appropriés, y compris le «Traffic Light Protocol». Les CSIRT peuvent échanger des informations pertinentes avec des centres de réponse aux incidents de sécurité informatique nationaux de pays tiers, y compris des données à caractère personnel, dans le respect du droit de l'Union en matière de protection des données.

8. Les CSIRT peuvent coopérer avec des centres de réponse aux incidents de sécurité informatique nationaux de pays tiers ou des organismes équivalents de pays tiers, notamment dans le but de leur fournir une assistance en matière de cybersécurité.

9. Chaque État membre notifie à la Commission, sans retard injustifié, l'identité des CSIRT visés au paragraphe 1 du présent article et du CSIRT désigné comme coordinateur conformément à l'article 12, paragraphe 1, leurs tâches respectives à l'égard des entités essentielles et importantes, et toute modification ultérieure dans ce cadre.

10. Les États membres peuvent solliciter l'assistance de l'ENISA pour la mise en place de leurs CSIRT.

▼B

Article 11

Obligations, capacités techniques et tâches des CSIRT

1. Les CSIRT satisfont aux exigences suivantes:

a) les CSIRT veillent à un niveau élevé de disponibilité de leurs canaux de communication en évitant les points uniques de défaillance et disposent de plusieurs moyens pour être contactés et contacter autrui à tout moment; ils spécifient clairement les canaux de communication et les font connaître aux partenaires et collaborateurs;

b) les locaux des CSIRT et les systèmes d'information utilisés se trouvent sur des sites sécurisés;

c) les CSIRT sont dotés d'un système approprié de gestion et de routage des demandes afin, notamment, de faciliter les transferts effectifs et efficaces;

d) les CSIRT garantissent la confidentialité et la fiabilité de leurs opérations;

e) les CSIRT sont dotés des effectifs adéquats afin de pouvoir garantir une disponibilité permanente de leurs services et ils veillent à ce que leur personnel reçoive une formation appropriée;

f) les CSIRT sont dotés de systèmes redondants et d'un espace de travail de secours pour assurer la continuité de leurs services.

Les CSIRT peuvent participer à des réseaux de coopération internationale.

2. Les États membres veillent à ce que leurs CSIRT disposent conjointement des capacités techniques nécessaires pour pouvoir s'acquitter des tâches visées au paragraphe 3. Les États membres veillent à ce que des ressources suffisantes soient allouées à leurs CSIRT pour garantir des effectifs suffisants leur permettant de développer leurs capacités techniques.

3. Les CSIRT assument les tâches suivantes:

a) surveiller et analyser les cybermenaces, les vulnérabilités et les incidents au niveau national et, sur demande, apporter une assistance aux entités essentielles et importantes concernées pour surveiller en temps réel ou quasi réel leurs réseaux et systèmes d'information;

b) activer le mécanisme d'alerte précoce, la diffusion de messages d'alerte, les annonces et la diffusion d'informations sur les cybermenaces, les vulnérabilités et les incidents auprès des entités essentielles et importantes concernées ainsi qu'auprès des autorités compétentes et des autres parties prenantes concernées, si possible en temps quasi réel;

c) réagir aux incidents et apporter une assistance aux entités essentielles et importantes concernées, le cas échéant;

▼B

d) rassembler et analyser des données de police scientifique, et assurer une analyse dynamique des risques et incidents et une appréciation de la situation en matière de cybersécurité;

e) réaliser, à la demande d'une entité essentielle ou importante, un scan proactif du réseau et des systèmes d'information de l'entité concernée afin de détecter les vulnérabilités susceptibles d'avoir un impact important;

f) participer au réseau des CSIRT et apporter une assistance mutuelle en fonction de leurs capacités et de leurs compétences aux autres membres du réseau des CSIRT à leur demande;

g) le cas échéant, agir en qualité de coordinateur aux fins du processus de divulgation coordonnée des vulnérabilités en vertu de l'article 12, paragraphe 1;

h) contribuer au déploiement d'outils de partage d'informations sécurisés conformément à l'article 10, paragraphe 3.

Les CSIRT peuvent procéder à un scan proactif et non intrusif des réseaux et systèmes d'information accessibles au public d'entités essentielles et importantes. Ce scan est effectué dans le but de détecter les réseaux et systèmes d'information vulnérables ou configurés de façon peu sûre et d'informer les entités concernées. Ce scan n'a pas d'effet négatif sur le fonctionnement des services des entités.

Lorsqu'ils exécutent les tâches visées au premier alinéa, les CSIRT peuvent donner la priorité à certaines tâches sur la base d'une approche basée sur les risques.

4. Les CSIRT établissent des relations de coopération avec les acteurs concernés du secteur privé, en vue d'atteindre les objectifs de la présente directive.

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

a) les procédures de gestion des incidents;

b) la gestion de crise; et

c) la divulgation coordonnée des vulnérabilités en vertu de l'article 12, paragraphe 1.

Article 12

Divulgation coordonnée des vulnérabilités et base de données européenne des vulnérabilités

1. Chaque État membre désigne l'un de ses CSIRT comme coordinateur aux fins de la divulgation coordonnée des vulnérabilités. Le CSIRT désigné comme coordinateur fait office d'intermédiaire de confiance en facilitant, si nécessaire, les interactions entre la personne physique ou morale qui signale une vulnérabilité et le fabricant ou le fournisseur des produits TIC ou des services TIC potentiellement vulnérables, à la demande de l'une des deux parties. Les tâches du CSIRT désigné comme coordinateur consistent:

▼B

a) à identifier et contacter les entités concernées;

b) à apporter une assistance aux personnes physiques ou morales signalant une vulnérabilité; et

c) à négocier des délais de divulgation et gérer les vulnérabilités qui touchent plusieurs entités.

Les États membres veillent à ce que les personnes physiques ou morales soient en mesure de signaler une vulnérabilité, de manière anonyme lorsqu'elles le demandent, au CSIRT désigné comme coordinateur. Le CSIRT désigné comme coordinateur veille à ce que des mesures de suivi diligentes soient prises en ce qui concerne la vulnérabilité signalée et veille à l'anonymat de la personne physique ou morale signalant la vulnérabilité. Lorsque la vulnérabilité signalée est susceptible d'avoir un impact important sur des entités dans plusieurs États membres, le CSIRT désigné comme coordinateur de chaque État membre concerné coopère, le cas échéant, avec les autres CSIRT désignés comme coordinateurs au sein du réseau des CSIRT.

2. L'ENISA élabore et tient à jour, après consultation du groupe de coopération, une base de données européenne des vulnérabilités. À cette fin, l'ENISA établit et gère les systèmes d'information, les politiques et les procédures appropriés, et adopte les mesures techniques et organisationnelles nécessaires pour assurer la sécurité et l'intégrité de la base de données européenne des vulnérabilités, en vue notamment de permettre aux entités, indépendamment du fait qu'elles relèvent ou non du champ d'application de la présente directive, et à leurs fournisseurs de réseaux et de systèmes d'information, de divulguer et d'enregistrer, à titre volontaire, les vulnérabilités publiquement connues présentes dans les produits TIC ou les services TIC. Toutes les parties prenantes ont accès aux informations sur les vulnérabilités contenues dans la base de données européenne sur les vulnérabilités. Cette base de données comprend:

a) des informations décrivant la vulnérabilité;

b) les produits TIC ou les services TIC affectés ainsi que la gravité de la vulnérabilité rapportée aux circonstances dans lesquelles elle peut être exploitée;

c) la disponibilité des correctifs correspondants et, en l'absence de correctifs disponibles, des orientations fournies par les autorités compétentes ou les CSIRT, adressées aux utilisateurs des produits TIC et des services TIC vulnérables, sur la manière dont les risques résultant des vulnérabilités divulguées peuvent être atténués.

Article 13

Coopération au niveau national

1. Lorsqu'ils sont distincts, les autorités compétentes, le point de contact unique et les CSIRT d'un même État membre coopèrent les uns avec les autres afin de respecter les obligations énoncées dans la présente directive.

▼B

2. Les États membres veillent à ce que leurs CSIRT ou, le cas échéant, leurs autorités compétentes reçoivent les notifications relatives aux incidents importants conformément à l'article 23, et aux incidents, aux cybermenaces et aux incidents évités conformément à l'article 30.

3. Les États membres veillent à ce que leurs CSIRT ou, le cas échéant, leurs autorités compétentes informent leurs points de contact uniques des notifications d'incidents, de cybermenaces et d'incidents évités soumises en application de la présente directive.

4. Afin de veiller à ce que les tâches et obligations des autorités compétentes, des points de contact uniques et des CSIRT soient exécutées efficacement, les États membres assurent, dans la mesure du possible, une coopération appropriée entre ces organes et les autorités répressives, les autorités chargées de la protection des données, les autorités nationales en vertu des règlements (CE) n° 300/2008 et (UE) 2018/1139, les organes de contrôle au titre du règlement (UE) n° 910/2014, les autorités compétentes en vertu du règlement (UE) 2022/2554, les autorités de régulation nationales en vertu de la directive (UE) 2018/1972, les autorités compétentes en vertu de la directive (UE) 2022/2557, ainsi que les autorités compétentes en vertu d'autres actes juridiques sectoriels de l'Union, dans cet État membre.

5. Les États membres veillent à ce que leurs autorités compétentes en vertu de la présente directive et leurs autorités compétentes en vertu de la directive (UE) 2022/2557 coopèrent et échangent régulièrement des informations sur le recensement des entités critiques, les risques, les cybermenaces et les incidents, ainsi que sur les risques, menaces et incidents non cyber qui touchent les entités essentielles recensées en tant qu'entités critiques en vertu de la directive (UE) 2022/2557, et sur les mesures prises pour faire face à ces risques, menaces et incidents. Les États membres veillent également à ce que leurs autorités compétentes en vertu de la présente directive et leurs autorités compétentes en vertu du règlement (UE) n° 910/2014, du règlement (UE) 2022/2554 et de la directive (UE) 2018/1972 échangent régulièrement des informations pertinentes, y compris en ce qui concerne les incidents et les cybermenaces concernés.

6. Les États membres simplifient la communication d'informations par des moyens techniques pour les notifications visées aux articles 23 et 30.

CHAPITRE III

COOPÉRATION AU NIVEAU DE L'UNION ET AU NIVEAU INTERNATIONAL

Article 14

Groupe de coopération

1. Un groupe de coopération est institué afin de soutenir et de faciliter la coopération stratégique et l'échange d'informations entre les États membres et de renforcer la confiance.

2. Le groupe de coopération exécute ses tâches en s'appuyant sur les programmes de travail bisannuels visés au paragraphe 7.

▼B

3. Le groupe de coopération est composé de représentants des États membres, de la Commission et de l'ENISA. Le Service européen pour l'action extérieure participe aux activités du groupe de coopération en qualité d'observateur. Les autorités européennes de surveillance (AES) et les autorités compétentes en vertu du règlement (UE) 2022/2554 peuvent participer aux activités du groupe de coopération conformément à l'article 47, paragraphe 1, dudit règlement.

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

Le secrétariat est assuré par la Commission.

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

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

b) la fourniture d'orientations aux autorités compétentes en ce qui concerne l'élaboration et la mise en œuvre des politiques de divulgation coordonnée des vulnérabilités visées à l'article 7, paragraphe 2, point c);

c) l'échange des meilleures pratiques et d'informations relatives à la mise en œuvre de la présente directive, notamment en ce qui concerne les cybermenaces, les incidents, les vulnérabilités, les incidents évités, les initiatives de sensibilisation, les formations, les exercices et les compétences, le renforcement des capacités, les normes et les spécifications techniques ainsi que l'identification des entités essentielles et importantes en vertu de l'article 2, paragraphe 2, points b) à e);

d) l'échange de conseils et la coopération avec la Commission sur les initiatives politiques émergentes en matière de cybersécurité et la cohérence globale des exigences sectorielles en matière de cybersécurité;

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

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

g) l'échange de vues sur la mise en œuvre d'actes juridiques sectoriels de l'Union contenant des dispositions en matière de cybersécurité;

h) le cas échéant, la discussion portant sur les rapports relatifs à l'évaluation par les pairs visés à l'article 19, paragraphe 9, et l'élaboration de conclusions et de recommandations;

i) la réalisation d'évaluations coordonnées des risques pour la sécurité des chaînes d'approvisionnement critiques, conformément à l'article 22, paragraphe 1;

▼B

j) la discussion portant sur les cas d'assistance mutuelle, y compris les expériences et les résultats des activités de contrôle transfrontières visées à l'article 37;

k) à la demande d'un ou de plusieurs États membres concernés, la discussion portant sur les demandes spécifiques d'assistance mutuelle visées à l'article 37;

l) l'indication d'une orientation stratégique au réseau des CSIRT et au réseau UE-CyCLONe sur des questions spécifiques émergentes;

m) l'échange de vues sur la politique relative aux mesures prises à la suite d'incidents de cybersécurité majeurs et de crises, sur la base des enseignements tirés du réseau des CSIRT et d'EU-CyCLONe;

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

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

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

q) la mise au point de la méthodologie et des aspects organisationnels des évaluations par les pairs visées à l'article 19, paragraphe 1, ainsi que la définition de la méthode d'autoévaluation pour les États membres conformément à l'article 19, paragraphe 4, avec l'aide de la Commission et de l'ENISA, et l'élaboration, en coopération avec la Commission et l'ENISA, des codes de conduite sous-tendant les méthodes de travail des experts en cybersécurité désignés conformément à l'article 19, paragraphe 6;

r) l'élaboration, aux fins de la révision visée à l'article 40, de rapports sur l'expérience acquise au niveau stratégique et à partir des évaluations par les pairs;

s) l'examen et l'évaluation, de manière régulière, de l'état de la situation en matière de cybermenaces ou d'incidents, comme les rançongiciels.

Le groupe de coopération soumet les rapports visés au premier alinéa, point r), à la Commission, au Parlement européen et au Conseil.

5. Les États membres font en sorte que leurs représentants au sein du groupe de coopération puissent coopérer de manière effective, efficace et sécurisée.

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

7. Au plus tard le 1er février 2024, puis tous les deux ans, le groupe de coopération établit un programme de travail concernant les actions à entreprendre pour mettre en œuvre ses objectifs et ses tâches.

▼B

8. La Commission peut adopter des actes d'exécution fixant les modalités de procédure nécessaires au fonctionnement du groupe de coopération.

Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 39, paragraphe 2.

La Commission échange des conseils et coopère avec le groupe de coopération sur les projets d'actes d'exécution visés au premier alinéa du présent paragraphe conformément au paragraphe 4, point e).

9. Le groupe de coopération se réunit régulièrement et en tout état de cause au moins une fois par an avec le groupe sur la résilience des entités critiques institué par la directive (UE) 2022/2557 afin de promouvoir et de faciliter la coopération stratégique et l'échange d'informations.

Article 15

Réseau des CSIRT

1. Un réseau des CSIRT nationaux est institué afin de contribuer au renforcement de la confiance et de promouvoir une coopération opérationnelle rapide et effective entre les États membres.

2. Le réseau des CSIRT est composé de représentants des CSIRT, désignés ou mis en place en vertu de l'article 10, et de l'équipe d'intervention en cas d'urgence informatique pour les institutions, organes et agences de l'Union (CERT-UE). La Commission participe au réseau des CSIRT en qualité d'observateur. L'ENISA assure le secrétariat et apporte une aide active à la coopération entre les CSIRT.

3. Le réseau des CSIRT est chargé des tâches suivantes:

a) l'échange d'informations sur les capacités des CSIRT;

b) la facilitation du partage, du transfert et de l'échange, entre les CSIRT, des technologies et des mesures, politiques, outils, processus, meilleures pratiques et cadres pertinents;

c) l'échange d'informations pertinentes sur les incidents, les incidents évités, les cybermenaces, les risques et les vulnérabilités;

d) l'échange d'informations en ce qui concerne les publications et les recommandations en matière de cybersécurité;

e) l'assurance de l'interopérabilité en ce qui concerne les spécifications et les protocoles relatifs au partage d'informations;

f) à la demande d'un membre du réseau des CSIRT potentiellement affecté par un incident, l'échange et la discussion portant sur les informations en rapport avec cet incident et les cybermenaces, risques et vulnérabilités connexes;

g) à la demande d'un membre du réseau des CSIRT, la discussion et, si possible, la mise en œuvre d'une réponse coordonnée à un incident déterminé qui relève de la compétence de l'État membre concerné;

▼B

h) la fourniture aux États membres d'une assistance face aux incidents transfrontières en application de la présente directive;

i) la coopération, l'échange des meilleures pratiques et la fourniture d'une assistance aux CSIRT désignés comme coordinateurs conformément à l'article 12, paragraphe 1, en ce qui concerne la gestion de la divulgation coordonnée des vulnérabilités susceptibles d'avoir un impact important sur des entités de plusieurs États membres;

j) la discussion et l'identification d'autres formes de coopération opérationnelle, notamment en rapport avec:

   i) les catégories de cybermenaces et d'incidents;

   ii) les alertes précoces;

   iii) l'assistance mutuelle;

   iv) les principes et modalités d'une coordination en réponse à des risques et incidents transfrontières;

   v) la contribution au plan national de réaction aux crises et incidents de cybersécurité majeurs visé à l'article 9, paragraphe 4, à la demande d'un État membre;

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

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

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

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

o) s'il y a lieu, l'examen des rapports de l'évaluation par les pairs visés à l'article 19, paragraphe 9;

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

4. Au plus tard le 17 janvier 2025, puis tous les deux ans, le réseau des CSIRT évalue, aux fins du réexamen visé à l'article 40, les progrès réalisés en matière de coopération opérationnelle et adopte un rapport. Le rapport formule notamment des conclusions et des recommandations à partir des résultats des évaluations par les pairs visées à l'article 19 et concernant les CSIRT nationaux. Ce rapport est aussi transmis au groupe de coopération.

5. Le réseau des CSIRT adopte son règlement intérieur.

6. Le réseau des CSIRT et EU-CyCLONe fixent ensemble les modalités procédurales et coopèrent sur la base de ces modalités.

▼B

Article 16

Le réseau européen pour la préparation et la gestion des crises cyber (EU-CyCLONe)

1. EU-CyCLONe est institué afin de contribuer à la gestion coordonnée, au niveau opérationnel, des incidents de cybersécurité majeurs et des crises, et de garantir l'échange régulier d'informations pertinentes entre les États membres et les institutions, organes et organismes de l'Union.

2. EU-CyCLONe est composé des représentants des autorités des États membres chargées de la gestion des crises de cybersécurité, ainsi que de la Commission lorsqu'un incident de cybersécurité majeur, potentiel ou en cours, a ou est susceptible d'avoir un impact important sur les services et les activités relevant du champ d'application de la présente directive. Dans les autres situations, la Commission participe aux activités d'EU-CyCLONe en qualité d'observateur.

L'ENISA assure le secrétariat d'EU-CyCLONe et soutient l'échange sécurisé d'informations, et fournit également les outils nécessaires pour soutenir la coopération entre États membres en garantissant un échange sécurisé d'informations.

Si besoin est, EU-CyCLONe peut inviter des représentants des acteurs concernés à participer à ses travaux en qualité d'observateurs.

3. EU-CyCLONe a pour tâches:

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

b) de développer une connaissance situationnelle partagée des incidents de cybersécurité majeurs et des crises;

c) d'évaluer les conséquences et l'impact des incidents de cybersécurité majeurs et des crises en question et de proposer d'éventuelles mesures d'atténuation;

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

e) d'examiner, à la demande de l'État membre concerné, le plan national de réaction aux crises et aux incidents de cybersécurité majeurs visé à l'article 9, paragraphe 4.

4. EU-CyCLONe adopte son règlement intérieur.

5. EU-CyCLONe rend régulièrement compte au groupe de coopération de la gestion des incidents de cybersécurité majeurs et des crises, ainsi que des tendances, en mettant notamment l'accent sur leur impact sur les entités essentielles et importantes.

▼B

6. EU-CyCLONe coopère avec le réseau des CSIRT sur la base des modalités procédurales convenues conformément à l'article 15, paragraphe 6.

7. Au plus tard le 17 juillet 2024 et tous les 18 mois par la suite, EU-CyCLONe soumet au Parlement européen et au Conseil un rapport évaluant ses travaux.

Article 17

Coopération internationale

L'Union peut, conformément à l'article 218 du traité sur le fonctionnement de l'Union européenne et lorsque cela est pertinent, conclure avec des pays tiers ou des organisations internationales des accords internationaux qui permettent et organisent leur participation à certaines activités du groupe de coopération, du réseau des CSIRT et d'EU-CyCLONe. Ces accords sont conformes au droit de l'Union en matière de protection des données.

Article 18

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

1. L'ENISA adopte, en coopération avec la Commission et le groupe de coopération, un rapport bisannuel sur l'état de la cybersécurité dans l'Union et le soumet et le présente au Parlement européen. Le rapport est notamment mis à disposition dans un format lisible par machine et comporte les éléments suivants:

a) une évaluation des risques en matière de cybersécurité à l'échelle de l'Union, qui tient compte du panorama des cybermenaces;

b) une évaluation du développement des capacités de cybersécurité dans les secteurs public et privé dans l'ensemble de l'Union;

c) une évaluation du degré général de sensibilisation à la cybersécurité et de cyberhygiène des citoyens et des entités, y compris les petites et moyennes entreprises;

d) une évaluation agrégée du résultat des évaluations par les pairs visées à l'article 19;

e) une évaluation agrégée du niveau de maturité des capacités de cybersécurité et des ressources en la matière dans l'ensemble de l'Union, notamment au niveau sectoriel, ainsi que du degré d'harmonisation des stratégies nationales en matière de cybersécurité des États membres.

2. Le rapport comprend des recommandations politiques spécifiques visant à remédier aux lacunes et à accroître le niveau de cybersécurité dans l'Union, ainsi qu'un résumé des conclusions pour la période concernée des rapports de situation technique en matière de cybersécurité de l'Union européenne sur les incidents et cybermenaces, élaborés par l'ENISA conformément à l'article 7, paragraphe 6, du règlement (UE) 2019/881.

3. L'ENISA, en coopération avec la Commission, le groupe de coopération et le réseau des CSIRT, élabore la méthodologie, y compris les variables pertinentes, telles que les indicateurs quantitatifs et qualitatifs, de l'évaluation agrégée visée au paragraphe 1, point e).

▼B

Article 19

Évaluations par les pairs

1. Le groupe de coopération établit, au plus tard le 17 janvier 2025, avec l'aide de la Commission et de l'ENISA et, s'il y a lieu, du réseau des CSIRT, la méthodologie et les aspects organisationnels des évaluations par les pairs en vue de tirer des enseignements des expériences partagées, de renforcer la confiance mutuelle, de parvenir à un niveau élevé commun de cybersécurité, ainsi que de renforcer les capacités et les politiques des États membres en matière de cybersécurité qui sont nécessaires à la mise en œuvre de la présente directive. La participation aux évaluations par les pairs s'effectue à titre volontaire. Les évaluations par les pairs sont effectuées par des experts en cybersécurité. Ces experts en cybersécurité sont désignés par au moins deux États membres différents de l'État membre faisant l'objet de l'évaluation.

Les évaluations par les pairs portent au moins sur l'un des points suivants:

a) le niveau de mise en œuvre des mesures de gestion des risques en matière de cybersécurité et des obligations d'information prévues aux articles 21 et 23;

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

c) les capacités opérationnelles des CSIRT;

d) le niveau de mise en œuvre de l'assistance mutuelle visée à l'article 37;

e) le niveau de mise en œuvre des accords de partage d'informations en matière de cybersécurité visés à l'article 29;

f) des questions spécifiques de nature transfrontière ou transsectorielle.

2. La méthodologie visée au paragraphe 1 comprend des critères objectifs, non discriminatoires, équitables et transparents sur la base desquels les États membres désignent les experts en cybersécurité habilités à effectuer les évaluations par les pairs. La Commission et l'ENISA participent en tant qu'observateurs aux évaluations par les pairs.

3. Les États membres peuvent définir des questions spécifiques visées au paragraphe 1, point f), aux fins d'une évaluation par les pairs.

4. Avant d'entamer l'évaluation par les pairs visée au paragraphe 1, les États membres en notifient la portée, en ce compris les questions définies en vertu du paragraphe 3, aux États membres qui y participent.

5. Avant le début de l'évaluation par les pairs, les États membres peuvent procéder à une autoévaluation des aspects évalués et fournir celle-ci aux experts en cybersécurité désignés. Le groupe de coopération établit, avec l'aide de la Commission et de l'ENISA, la méthode pour l'autoévaluation des États membres.

▼B

6. Les évaluations par les pairs comportent des visites sur place physiques ou virtuelles et des échanges d'information hors site. Conformément au principe de bonne coopération, l'État membre faisant l'objet de l'évaluation par les pairs fournit aux experts en cybersécurité désignés les informations nécessaires à l'évaluation, sans préjudice du droit de l'Union ou du droit national concernant la protection des informations confidentielles ou classifiées, ni de la préservation des fonctions essentielles de l'État, telles que la sécurité nationale. Le groupe de coopération, en coopération avec la Commission et l'ENISA, élabore des codes de conduite appropriés qui sous-tendent les méthodes de travail des experts en cybersécurité désignés. Toute information obtenue durant l'évaluation par les pairs n'est utilisée qu'à cet effet. Les experts en cybersécurité participant à l'évaluation par les pairs ne divulguent à aucun tiers les informations sensibles ou confidentielles obtenues au cours de cette évaluation par les pairs.

7. Une fois qu'ils ont fait l'objet d'une évaluation par les pairs dans un État membre, les mêmes aspects ne font pas l'objet d'une nouvelle évaluation par les pairs dans cet État membre au cours des deux années suivant la conclusion de l'évaluation par les pairs, sauf si l'État membre le demande ou si une proposition en ce sens du groupe de coopération est approuvée.

8. Les États membres veillent à ce que tout risque de conflit d'intérêts concernant les experts en cybersécurité désignés soit révélé aux autres États membres, au groupe de coopération, à la Commission et à l'ENISA, avant le début de l'évaluation par les pairs. L'État membre faisant l'objet de l'évaluation par les pairs peut s'opposer à la désignation de certains experts en cybersécurité pour des raisons dûment motivées communiquées à l'État membre qui les a désignés.

9. Les experts en cybersécurité participant aux évaluations par les pairs rédigent des rapports sur les résultats et les conclusions des évaluations par les pairs. Les États membres qui font l'objet d'une évaluation par les pairs peuvent formuler des observations sur les projets de rapport les concernant et ces observations sont jointes aux rapports. Les rapports contiennent des recommandations permettant d'améliorer les aspects sur lesquels l'évaluation par les pairs a porté. Les rapports sont soumis, s'il y a lieu, au groupe de coopération et au réseau des CSIRT. Un État membre qui a fait l'objet d'une évaluation par les pairs peut décider de rendre public le rapport le concernant ou une version expurgée de celui-ci.

CHAPITRE IV

MESURES DE GESTION DES RISQUES EN MATIÈRE DE CYBERSÉCURITÉ ET OBLIGATIONS D'INFORMATION

Article 20

Gouvernance

1. Les États membres veillent à ce que les organes de direction des entités essentielles et importantes approuvent les mesures de gestion des risques en matière de cybersécurité prises par ces entités afin de se conformer à l'article 21, supervisent sa mise en œuvre et puissent être tenus responsables de la violation dudit article par ces entités.

L'application du présent paragraphe est sans préjudice du droit national en ce qui concerne les règles en matière de responsabilité applicables aux institutions publiques, ainsi que de responsabilité des agents de la fonction publique et des responsables élus ou nommés.

▼B

2. Les États membres veillent à ce que les membres des organes de direction des entités essentielles et importantes soient tenus de suivre une formation et ils encouragent les entités essentielles et importantes à offrir régulièrement une formation similaire aux membres de leur personnel afin que ceux-ci acquièrent des connaissances et des compétences suffisantes pour déterminer les risques et évaluer les pratiques de gestion des risques en matière de cybersécurité et leur impact sur les services fournis par l'entité.

Article 21

Mesures de gestion des risques en matière de cybersécurité

1. Les États membres veillent à ce que les entités essentielles et importantes prennent les mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information que ces entités utilisent dans le cadre de leurs activités ou de la fourniture de leurs services, ainsi que pour éliminer ou réduire les conséquences que les incidents ont sur les destinataires de leurs services et sur d'autres services.

Les mesures visées au premier alinéa garantissent, pour les réseaux et les systèmes d'information, un niveau de sécurité adapté au risque existant, en tenant compte de l'état des connaissances et, s'il y a lieu, des normes européennes et internationales applicables, ainsi que du coût de mise en œuvre. Lors de l'évaluation de la proportionnalité de ces mesures, il convient de tenir dûment compte du degré d'exposition de l'entité aux risques, de la taille de l'entité et de la probabilité de survenance d'incidents et de leur gravité, y compris leurs conséquences sociétales et économiques.

2. Les mesures visées au paragraphe 1 sont fondées sur une approche «tous risques» qui vise à protéger les réseaux et les systèmes d'information ainsi que leur environnement physique contre les incidents, et elles comprennent au moins:

a) les politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information;

b) la gestion des incidents;

c) la continuité des activités, par exemple la gestion des sauvegardes et la reprise des activités, et la gestion des crises;

d) la sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services directs;

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

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

g) les pratiques de base en matière de cyberhygiène et la formation à la cybersécurité;

▼B

h) des politiques et des procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement;

i) la sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs;

j) l'utilisation de solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence au sein de l'entité, selon les besoins.

3. Les États membres veillent à ce que, lorsqu'elles examinent lesquelles des mesures visées au paragraphe 2, point d), du présent article sont appropriées, les entités tiennent compte des vulnérabilités propres à chaque fournisseur et prestataire de services direct et de la qualité globale des produits et des pratiques de cybersécurité de leurs fournisseurs et prestataires de services, y compris de leurs procédures de développement sécurisé. Les États membres veillent également à ce que, lorsqu'elles examinent lesquelles des mesures visées audit point sont appropriées, les entités soient tenues de prendre en compte les résultats des évaluations coordonnées des risques pour la sécurité des chaînes d'approvisionnement critiques, effectuées conformément à l'article 22, paragraphe 1.

4. Les États membres veillent à ce que, lorsqu'une entité constate qu'elle ne se conforme pas aux mesures prévues au paragraphe 2, elle prenne, sans retard injustifié, toutes les mesures correctives nécessaires appropriées et proportionnées.

5. Au plus tard le 17 octobre 2024, la Commission adopte des actes d'exécution établissant les exigences techniques et méthodologiques liées aux mesures visées au paragraphe 2 en ce qui concerne les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés, ainsi que les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux, et les prestataires de services de confiance.

La Commission peut adopter des actes d'exécution établissant les exigences techniques et méthodologiques ainsi que les exigences sectorielles, si nécessaire, liées aux mesures visées au paragraphe 2 concernant les entités essentielles et importantes autres que celles visées au premier alinéa du présent paragraphe.

Lorsqu'elle prépare les actes d'exécution visés aux premier et deuxième alinéas du présent paragraphe, la Commission suit, dans la mesure du possible, les normes européennes et internationales ainsi que les spécifications techniques pertinentes. La Commission échange des conseils et coopère avec le groupe de coopération et l'ENISA sur les projets d'actes d'exécution conformément à l'article 14, paragraphe 4, point e).

Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 39, paragraphe 2.

Article 22

Évaluations coordonnées au niveau de l'Union des risques pour la sécurité des chaînes d'approvisionnement critiques

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

▼B

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

Article 23

Obligations d'information

1. Chaque État membre veille à ce que les entités essentielles et importantes notifient, sans retard injustifié, à son CSIRT ou, selon le cas, à son autorité compétente, conformément au paragraphe 4, tout incident ayant un impact important sur leur fourniture des services visés au paragraphe 3 (ci-après dénommé «incident important»). Le cas échéant, les entités concernées notifient, sans retard injustifié, aux destinataires de leurs services les incidents importants susceptibles de nuire à la fourniture de ces services. Chaque État membre veille à ce que ces entités signalent, entre autres, toute information permettant au CSIRT ou, le cas échéant, à l'autorité compétente de déterminer si l'incident a un impact transfrontière. Le simple fait de notifier un incident n'accroît pas la responsabilité de l'entité qui est à l'origine de la notification.

Lorsque les entités concernées notifient un incident important à l'autorité compétente en application du premier alinéa, l'État membre veille à ce que cette autorité compétente transmette la notification au CSIRT dès qu'elle la reçoit.

En cas d'incident important transfrontière ou transsectoriel, les États membres veillent à ce que leurs points de contact uniques reçoivent en temps utile les informations notifiées conformément au paragraphe 4.

2. Le cas échéant, les États membres veillent à ce que les entités essentielles et importantes communiquent, sans retard injustifié, aux destinataires de leurs services qui sont potentiellement affectés par une cybermenace importante toutes les mesures ou corrections que ces destinataires peuvent appliquer en réponse à cette menace. Le cas échéant, les entités informent également ces destinataires de la cybermenace importante elle-même.

3. Un incident est considéré comme important si:

a) il a causé ou est susceptible de causer une perturbation opérationnelle grave des services ou des pertes financières pour l'entité concernée;

b) il a affecté ou est susceptible d'affecter d'autres personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables.

4. Les États membres veillent à ce que, aux fins de la notification visée au paragraphe 1, les entités concernées soumettent au CSIRT ou, selon le cas, à l'autorité compétente:

a) sans retard injustifié et en tout état de cause dans les 24 heures après avoir eu connaissance de l'incident important, une alerte précoce qui, le cas échéant, indique si l'on suspecte l'incident important d'avoir été causé par des actes illicites ou malveillants ou s'il pourrait avoir un impact transfrontière;

▼B

b) sans retard injustifié et en tout état de cause dans les 72 heures après avoir eu connaissance de l'incident important, une notification d'incident qui, le cas échéant, met à jour les informations visées au point a) et fournit une évaluation initiale de l'incident important, y compris de sa gravité et de son impact, ainsi que des indicateurs de compromission, lorsqu'ils sont disponibles;

c) à la demande d'un CSIRT ou, selon le cas, de l'autorité compétente, un rapport intermédiaire sur les mises à jour pertinentes de la situation;

d) un rapport final au plus tard un mois après la présentation de la notification d'incident visée au point b), comprenant les éléments suivants:

i) une description détaillée de l'incident, y compris de sa gravité et de son impact;

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

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

iv) le cas échéant, l'impact transfrontière de l'incident;

▼C1

e) en cas d'incident en cours au moment de la présentation du rapport final visé au point d), les États membres veillent à ce que les entités concernées fournissent à ce moment-là un rapport d'avancement puis un rapport final dans un délai d'un mois à compter de la gestion de l'incident.

▼B

Par dérogation au premier alinéa, point b), un prestataire de services de confiance notifie au CSIRT ou, selon le cas, à l'autorité compétente les incidents importants qui ont un impact sur la fourniture de ses services de confiance, sans retard injustifié et en tout état de cause dans les 24 heures après avoir eu connaissance de l'incident important.

5. Le CSIRT ou l'autorité compétente fournissent, sans retard injustifié et si possible dans les 24 heures suivant la réception de l'alerte précoce visée au paragraphe 4, point a), une réponse à l'entité émettrice de la notification, y compris un retour d'information initial sur l'incident important et, à la demande de l'entité, des orientations ou des conseils opérationnels sur la mise en œuvre d'éventuelles mesures d'atténuation. Lorsque le CSIRT n'est pas le premier destinataire de la notification visée au paragraphe 1, l'orientation est émise par l'autorité compétente en coopération avec le CSIRT. Le CSIRT fournit un soutien technique supplémentaire si l'entité concernée le demande. Lorsqu'il y a lieu de suspecter que l'incident est de nature criminelle, le CSIRT ou l'autorité compétente fournit également des orientations sur les modalités de notification de l'incident important aux autorités répressives.

6. Lorsque c'est approprié, et notamment si l'incident important concerne deux États membres ou plus, le CSIRT, l'autorité compétente ou le point de contact unique informent sans retard injustifié les autres États membres touchés et l'ENISA de l'incident important. Sont alors partagées des informations du type de celles reçues conformément au paragraphe 4. Ce faisant, le CSIRT, l'autorité compétente ou le point de contact unique doivent, dans le respect du droit de l'Union ou du droit national, préserver la sécurité et les intérêts commerciaux de l'entité ainsi que la confidentialité des informations communiquées.

▼B

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

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

9. Le point de contact unique soumet tous les trois mois à l'ENISA un rapport de synthèse comprenant des données anonymisées et agrégées sur les incidents importants, les incidents, les cybermenaces et les incidents évités notifiés conformément au paragraphe 1 du présent article et à l'article 30. Afin de contribuer à la fourniture d'informations comparables, l'ENISA peut adopter des orientations techniques sur les paramètres des informations à inclure dans le rapport de synthèse. L'ENISA informe le groupe de coopération et le réseau des CSIRT de ses conclusions concernant les notifications reçues tous les six mois.

10. Les CSIRT ou, selon le cas, les autorités compétentes fournissent aux autorités compétentes en vertu de la directive (UE) 2022/2557 des informations sur les incidents importants, les incidents, les cybermenaces et les incidents évités notifiés conformément au paragraphe 1 du présent article et à l'article 30 par les entités identifiées comme des entités critiques en vertu de la directive (UE) 2022/2557.

11. La Commission peut adopter des actes d'exécution précisant plus en détail le type d'informations, le format et la procédure des notifications présentées en vertu du paragraphe 1 du présent article et de l'article 30 ainsi que des communications présentées en vertu du paragraphe 2 du présent article.

Au plus tard le 17 octobre 2024, la Commission adopte, en ce qui concerne les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés, ainsi que les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux, des actes d'exécution précisant plus en détail les cas dans lesquels un incident est considéré comme important au sens du paragraphe 3. La Commission peut adopter de tels actes d'exécution pour d'autres entités essentielles et importantes.

La Commission échange des conseils et coopère avec le groupe de coopération sur les projets d'actes d'exécution visés aux premier et deuxième alinéas du présent paragraphe conformément à l'article 14, paragraphe 4, point e).

Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 39, paragraphe 2.

▼B

Article 24

Recours aux schémas européens de certification de cybersécurité

1. Afin de démontrer la conformité à certaines exigences visées à l'article 21, les États membres peuvent prescrire aux entités essentielles et importantes d'utiliser des produits TIC, services TIC et processus TIC particuliers qui, mis au point par l'entité essentielle ou importante ou acquis auprès de tiers, sont certifiés dans le cadre de schémas européens de certification de cybersécurité adoptés conformément à l'article 49 du règlement (UE) 2019/881. En outre, les États membres encouragent les entités essentielles et importantes à utiliser des services de confiance qualifiés.

2. La Commission est habilitée à adopter des actes délégués, conformément à l'article 38, pour compléter la présente directive en précisant quelles catégories d'entités essentielles et importantes sont tenues d'utiliser certains produits TIC, services TIC et processus TIC certifiés ou d'obtenir un certificat dans le cadre d'un schéma européen de certification de cybersécurité adopté conformément à l'article 49 du règlement (UE) 2019/881. Ces actes délégués sont adoptés lorsque des niveaux insuffisants de cybersécurité ont été constatés et ils prévoient une période de mise en œuvre.

Avant d'adopter de tels actes délégués, la Commission procède à une analyse d'impact et mène des consultations conformément à l'article 56 du règlement (UE) 2019/881.

3. Lorsqu'il n'existe pas de schéma européen de certification de cybersécurité approprié aux fins du paragraphe 2 du présent article, la Commission peut, après consultation du groupe de coopération et du groupe européen de certification de cybersécurité, demander à l'ENISA de préparer un schéma candidat conformément à l'article 48, paragraphe 2, du règlement (UE) 2019/881.

Article 25

Normalisation

1. Afin de favoriser la mise en œuvre convergente de l'article 21, paragraphes 1 et 2, les États membres encouragent, sans imposer l'utilisation d'un type particulier de technologies ni créer de discrimination en faveur d'un tel type particulier de technologies, le recours à des normes et des spécifications techniques européennes et internationales pour la sécurité des réseaux et des systèmes d'information.

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

CHAPITRE V

COMPÉTENCE ET ENREGISTREMENT

Article 26

Compétence et territorialité

1. Les entités relevant du champ d'application de la présente directive sont considérées comme relevant de la compétence de l'État membre dans lequel elles sont établies, à l'exception des cas suivants:

▼B

a) les fournisseurs de réseaux de communications électroniques publics ou les fournisseurs de services de communications électroniques accessibles au public, qui sont considérés comme relevant de la compétence de l'État membre dans lequel ils fournissent leurs services;

b) les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les entités fournissant des services d'enregistrement de noms de domaine, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés, ainsi que les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne ou de plateformes de services de réseaux sociaux, qui sont considérés comme relevant de la compétence de l'État membre dans lequel ils ont leur établissement principal dans l'Union en application du paragraphe 2;

c) les entités de l'administration publique, qui sont considérées comme relevant de la compétence de l'État membre qui les a établies.

2. Aux fins de la présente directive, un entité visée au paragraphe 1, point b), est considérée avoir son établissement principal dans l'Union dans l'État membre où sont principalement prises les décisions relatives aux mesures de gestion des risques en matière de cybersécurité. Si un tel État membre ne peut être déterminé ou si ces décisions ne sont pas prises dans l'Union, l'établissement principal est considéré comme se trouvant dans l'État membre où les opérations de cybersécurité sont effectuées. Si un tel État membre ne peut être déterminé, l'établissement principal est considéré comme se trouvant dans l'État membre où l'entité concernée possède l'établissement comptant le plus grand nombre de salariés dans l'Union.

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

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

5. Les États membres qui ont reçu une demande d'assistance mutuelle en lien avec une entité visée au paragraphe 1, point b), peuvent, dans les limites de cette demande, prendre des mesures de supervision et d'exécution appropriées à l'égard de l'entité concernée qui fournit des services ou qui dispose d'un réseau et d'un système d'information sur leur territoire.

Article 27

Registre des entités

1. L'ENISA crée et tient, sur la base des informations reçues des points de contact uniques conformément au paragraphe 4, un registre des fournisseurs de services DNS, des registres des noms de domaine de premier niveau, des entités qui fournissent des services d'enregistrement de noms de domaine, des fournisseurs de services d'informatique en nuage, des fournisseurs de services de centres de données, des

▼B

fournisseurs de réseaux de diffusion de contenu, des fournisseurs de services gérés, des fournisseurs de services de sécurité gérés, ainsi que des fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux. Sur demande, l'ENISA permet aux autorités compétentes d'accéder à ce registre, tout en veillant à ce que la confidentialité des informations soit protégée, s'il y a lieu.

2. Les États membres demandent aux entités visées au paragraphe 1 de soumettre les informations suivantes aux autorités compétentes au plus tard le 17 janvier 2025:

a) le nom de l'entité;

b) les secteur, sous-secteur et type d'entité concernés, visés à l'annexe I ou II, le cas échéant;

c) l'adresse de l'établissement principal de l'entité et de ses autres établissements légaux dans l'Union ou, si elle n'est pas établie dans l'Union, de son représentant désigné conformément à l'article 26, paragraphe 3;

d) les coordonnées actualisées, y compris les adresses de courrier électronique et les numéros de téléphone de l'entité et, le cas échéant, de son représentant désigné conformément à l'article 26, paragraphe 3;

e) les États membres dans lesquels l'entité fournit des services; et

f) les plages d'IP de l'entité.

3. Les États membres veillent à ce que les entités visées au paragraphe 1 notifient à l'autorité compétente toute modification des informations qu'elles ont communiquées en vertu du paragraphe 2 sans tarder et, en tout état de cause, dans un délai de trois mois à compter de la date de la modification.

4. À la réception des informations visées aux paragraphes 2 et 3, à l'exception des informations visées au paragraphe 2, point f), le point de contact unique de l'État membre concerné les transmet sans retard injustifié à l'ENISA.

5. S'il y a lieu, les informations visées aux paragraphes 2 et 3 du présent article sont communiquées via le mécanisme national visé à l'article 3, paragraphe 4, quatrième alinéa.

Article 28

Base des données d'enregistrement des noms de domaine

1. Afin de contribuer à la sécurité, à la stabilité et à la résilience du DNS, les États membres imposent aux registres des noms de domaine de premier niveau et aux entités fournissant des services d'enregistrement de noms de domaine de collecter les données d'enregistrement de noms de domaine et de les maintenir exactes et complètes au sein d'une base de données spécialisée avec la diligence requise par le droit de l'Union en matière de protection des données pour ce qui concerne les données à caractère personnel.

2. Aux fins du paragraphe 1, les États membres exigent que la base des données d'enregistrement des noms de domaine contienne les informations nécessaires pour identifier et contacter les titulaires des noms de domaine et les points de contact qui gèrent les noms de domaine relevant des domaines de premier niveau. Ces informations comprennent notamment les éléments suivants:

▼B

a) le nom de domaine;

b) la date d'enregistrement;

c) le nom du titulaire, l'adresse de courrier électronique et le numéro de téléphone permettant de le contacter;

d) l'adresse de courrier électronique et le numéro de téléphone permettant de contacter le point de contact qui gère le nom de domaine, si ces coordonnées sont différentes de celles du titulaire.

3. Les États membres exigent que les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine aient mis en place des politiques et des procédures, notamment des procédures de vérification, visant à garantir que les bases de données visées au paragraphe 1 contiennent des informations exactes et complètes. Les États membres imposent que ces politiques et procédures soient mises à la disposition du public.

4. Les États membres exigent que les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine rendent publiques, sans retard injustifié après l'enregistrement d'un nom de domaine, les données d'enregistrement du nom de domaine qui ne sont pas des données à caractère personnel.

5. Les États membres imposent aux registres des noms de domaine de premier niveau et aux entités fournissant des services d'enregistrement de noms de domaine de donner accès aux données spécifiques d'enregistrement de noms de domaine sur demande légitime et dûment motivée des demandeurs d'accès légitimes, dans le respect du droit de l'Union en matière de protection des données. Les États membres exigent que les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine répondent sans retard injustifié et en tout état de cause dans un délai de 72 heures après réception de toute demande d'accès. Les États membres imposent que les politiques et procédures de divulgation de ces données soient rendues publiques.

6. Le respect des obligations énoncées aux paragraphes 1 à 5 ne saurait entraîner de répétition inutile de la collecte des données d'enregistrement de noms de domaine. À cet effet, les États membres imposent aux registres des noms de domaine de premier niveau et aux entités fournissant des services d'enregistrement de noms de domaine de coopérer entre eux.

CHAPITRE VI

PARTAGE D'INFORMATIONS

Article 29

Accords de partage d'informations en matière de cybersécurité

1. Les États membres veillent à ce que les entités relevant du champ d'application de la présente directive et, le cas échéant, les autres entités concernées ne relevant pas du champ d'application de la présente directive puissent échanger entre elles, à titre volontaire, des informations pertinentes en matière de cybersécurité, y compris des informations relatives aux cybermenaces, aux incidents évités, aux vulnérabilités, aux techniques et procédures, aux indicateurs de compromission, aux tactiques adverses, ainsi que des informations spécifiques sur les acteurs de la menace, des alertes de cybersécurité et des recommandations concernant la configuration des outils de cybersécurité pour détecter les cyberattaques, lorsque ce partage d'informations:

▼B

a) vise à prévenir et à détecter les incidents, à y réagir, à s'en rétablir ou à atténuer leur impact;

b) renforce le niveau de cybersécurité, notamment en sensibilisant aux cybermenaces, en limitant ou en empêchant leur capacité de se propager, en soutenant une série de capacités de défense, en remédiant aux vulnérabilités et en les révélant, en mettant en œuvre des techniques de détection, d'endiguement et de prévention des menaces, des stratégies d'atténuation ou des étapes de réaction et de rétablissement, ou en encourageant la recherche collaborative en matière de cybermenaces entre les entités publiques et privées.

2. Les États membres veillent à ce que l'échange d'informations ait lieu au sein de communautés d'entités essentielles et importantes ainsi que, le cas échéant, de leurs fournisseurs ou prestataires de services. Cet échange est mis en œuvre au moyen d'accords de partage d'informations en matière de cybersécurité, compte tenu de la nature potentiellement sensible des informations partagées.

3. Les États membres facilitent la mise en place des accords de partage d'informations en matière de cybersécurité visés au paragraphe 2 du présent article. Ces accords peuvent préciser les éléments opérationnels, y compris l'utilisation de plateformes TIC spécialisées et d'outils d'automatisation, le contenu et les conditions des accords de partage d'informations. Lorsqu'ils précisent la participation des autorités publiques à ces accords, les États membres peuvent imposer des conditions en ce qui concerne les informations mises à disposition par les autorités compétentes ou les CSIRT. Les États membres offrent un soutien à l'application de ces accords conformément à leurs politiques visées à l'article 7, paragraphe 2, point h).

4. Les États membres veillent à ce que les entités essentielles et importantes notifient aux autorités compétentes leur participation aux accords de partage d'informations en matière de cybersécurité visés au paragraphe 2, lorsqu'elles concluent de tels accords ou, le cas échéant, lorsqu'elles se retirent de ces accords, une fois que le retrait prend effet.

5. L'ENISA fournit une assistance pour la mise en place des accords de partage d'informations en matière de cybersécurité visés au paragraphe 2 par l'échange de bonnes pratiques et l'apport d'orientations.

Article 30

Notification volontaire d'informations pertinentes

1. Les États membres veillent à ce que, outre l'obligation de notification prévue à l'article 23, des notifications puissent être transmises à titre volontaire aux CSIRT ou, s'il y a lieu, aux autorités compétentes par:

a) les entités essentielles et importantes en ce qui concerne les incidents, les cybermenaces et les incidents évités;

▼B

b) les entités autres que celles visées au point a), indépendamment du fait qu'elles relèvent ou non du champ d'application de la présente directive, en ce qui concerne les incidents importants, les cybermenaces ou les incidents évités.

2. Les États membres traitent les notifications visées au paragraphe 1 du présent article conformément à la procédure énoncée à l'article 23. Les États membres peuvent traiter les notifications obligatoires en leur donnant la priorité par rapport aux notifications volontaires.

Lorsque cela est nécessaire, les CSIRT et, le cas échéant, les autorités compétentes fournissent aux points de contact uniques les informations relatives aux notifications reçues en vertu du présent article, tout en garantissant la confidentialité et une protection appropriée des informations fournies par l'entité à l'origine de la notification. Sans préjudice de la prévention et de la détection d'infractions pénales et des enquêtes et poursuites en la matière, un signalement volontaire n'a pas pour effet d'imposer à l'entité ayant effectué la notification des obligations supplémentaires auxquelles elle n'aurait pas été soumise si elle n'avait pas transmis la notification.

CHAPITRE VII

SUPERVISION ET EXÉCUTION

Article 31

Aspects généraux concernant la supervision et l'exécution

1. Les États membres veillent à ce que leurs autorités compétentes procèdent à une supervision efficace et prennent les mesures nécessaires pour assurer le respect de la présente directive.

2. Les États membres peuvent autoriser leurs autorités compétentes à fixer des priorités en ce qui concerne les tâches de supervision. La définition de ces priorités suit une approche basée sur les risques. À cet effet, lorsqu'elles accomplissent leurs tâches de supervision prévues aux articles 32 et 33, les autorités compétentes peuvent mettre au point des méthodes de supervision permettant de fixer des priorités concernant ces tâches selon une approche basée sur les risques.

3. Lorsqu'elles traitent des incidents donnant lieu à des violations de données à caractère personnel, les autorités compétentes coopèrent étroitement avec les autorités de contrôle en vertu du règlement (UE) 2016/679, sans préjudice de la compétence et des missions des autorités de contrôle.

4. Sans préjudice des cadres législatifs et institutionnels nationaux, les États membres veillent à ce que, dans le cadre de la supervision du respect de la présente directive par les entités de l'administration publique et de l'imposition d'éventuelles mesures d'exécution en cas de violation de la présente directive, les autorités compétentes disposent de pouvoirs appropriés pour mener à bien ces tâches en jouissant d'une indépendance opérationnelle vis-à-vis des entités de l'administration publique supervisées. Les États membres peuvent décider d'imposer des mesures de supervision et d'exécution appropriées, proportionnées et efficaces à l'égard de ces entités, conformément aux cadres législatifs et institutionnels nationaux.

▼B

Article 32

Mesures de supervision et d'exécution en ce qui concerne les entités essentielles

1. Les États membres veillent à ce que les mesures de supervision ou d'exécution imposées aux entités essentielles à l'égard des obligations prévues par la présente directive soient effectives, proportionnées et dissuasives, compte tenu des circonstances de chaque cas.

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

a) des inspections sur place et des contrôles à distance, y compris des contrôles aléatoires effectués par des professionnels formés;

b) des audits de sécurité réguliers et ciblés réalisés par un organisme indépendant ou une autorité compétente;

c) des audits ad hoc, notamment lorsqu'ils sont justifiés en raison d'un incident important ou d'une violation de la présente directive par l'entité essentielle;

d) des scans de sécurité fondés sur des critères d'évaluation des risques objectifs, non discriminatoires, équitables et transparents, si nécessaire avec la coopération de l'entité concernée;

e) des demandes d'informations nécessaires à l'évaluation des mesures de gestion des risques en matière de cybersécurité adoptées par l'entité concernée, notamment les politiques de cybersécurité consignées par écrit, ainsi que du respect de l'obligation de soumettre des informations aux autorités compétentes conformément à l'article 27;

f) des demandes d'accès à des données, à des documents et à toutes informations nécessaires à l'accomplissement de leurs tâches de supervision;

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

Les audits de sécurité ciblés visés au premier alinéa, point b), sont basés sur des évaluations des risques effectuées par l'autorité compétente ou l'entité contrôlée, ou sur d'autres informations disponibles relatives aux risques.

Les résultats de tout audit de sécurité ciblé sont mis à la disposition de l'autorité compétente. Les coûts de cet audit de sécurité ciblé effectué par un organisme indépendant sont à la charge de l'entité contrôlée, sauf lorsque l'autorité compétente en décide autrement dans des cas dûment motivés.

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

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

▼B

a) d'émettre des avertissements concernant les violations de la présente directive par les entités concernées;

b) d'adopter des instructions contraignantes, y compris en ce qui concerne les mesures nécessaires pour éviter un incident ou y remédier, ainsi que les délais pour mettre en œuvre ces mesures et rendre compte de cette mise en œuvre, ou une injonction exigeant des entités concernées qu'elles remédient aux insuffisances constatées ou aux violations de la présente directive;

c) d'ordonner aux entités concernées de mettre un terme à un comportement qui viole la présente directive et de ne pas le réitérer;

d) d'ordonner aux entités concernées de garantir la conformité de leurs mesures de gestion des risques en matière de cybersécurité avec l'article 21 ou de respecter les obligations d'information énoncées à l'article 23, de manière spécifique et dans un délai déterminé;

e) d'ordonner aux entités concernées d'informer les personnes physiques ou morales à l'égard desquelles elles fournissent des services ou exercent des activités susceptibles d'être affectées par une cybermenace importante de la nature de la menace, ainsi que de toutes mesures préventives ou réparatrices que ces personnes physiques ou morales pourraient prendre en réponse à cette menace;

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

g) de désigner, pour une période déterminée, un responsable du contrôle ayant des tâches bien définies pour superviser le respect, par les entités concernées, des articles 21 et 23;

h) d'ordonner aux entités concernées de rendre publics les aspects de violations de la présente directive de manière spécifique;

i) d'imposer ou de demander aux organes compétents ou aux juridictions d'imposer, conformément au droit national, une amende administrative en vertu de l'article 34 en plus de l'une ou l'autre des mesures visées aux points a) à h) du présent paragraphe.

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

a) de suspendre temporairement ou de demander à un organisme de certification ou d'autorisation, ou à une juridiction, conformément au droit national, de suspendre temporairement une certification ou une autorisation concernant tout ou partie des services pertinents fournis ou des activités pertinentes menées par l'entité essentielle;

b) de demander aux organes compétents ou aux juridictions compétentes, conformément au droit national, d'interdire temporairement à toute personne physique exerçant des responsabilités dirigeantes à un niveau de directeur général ou de représentant légal dans l'entité essentielle d'exercer des responsabilités dirigeantes dans cette entité.

▼B

Les suspensions ou interdictions temporaires imposées au titre du présent paragraphe sont uniquement appliquées jusqu'à ce que l'entité concernée prenne les mesures nécessaires pour remédier aux insuffisances ou se conformer aux exigences de l'autorité compétente à l'origine de l'application de ces mesures d'exécution. L'imposition de ces suspensions ou interdictions temporaires est soumise à des garanties procédurales appropriées conformément aux principes généraux du droit de l'Union et à la Charte, y compris le droit à un recours effectif et à accéder à un tribunal impartial, la présomption d'innocence et les droits de la défense.

Les mesures d'exécution prévues au présent paragraphe ne peuvent pas être appliquées aux entités de l'administration publiques qui relèvent de la présente directive.

6. Les États membres veillent à ce que toute personne physique responsable d'une entité essentielle ou agissant en qualité de représentant légal d'une entité essentielle sur la base du pouvoir de la représenter, de prendre des décisions en son nom ou d'exercer son contrôle ait le pouvoir de veiller au respect, par l'entité, de la présente directive. Les États membres veillent à ce que ces personnes physiques puissent être tenues responsables des manquements à leur devoir de veiller au respect de la présente directive.

En ce qui concerne les entités de l'administration publique, le présent paragraphe est sans préjudice du droit national en ce qui concerne la responsabilité des agents de la fonction publique et des responsables élus ou nommés.

7. Lorsqu'elles prennent toute mesure d'exécution visée au paragraphe 4 ou 5, les autorités compétentes respectent les droits de la défense et tiennent compte des circonstances propres à chaque cas et, au minimum, tiennent dûment compte:

a) de la gravité de la violation et de l'importance des dispositions enfreintes, les faits suivants, entre autres, devant être considérés en tout état de cause comme graves:

   i) les violations répétées;

   ii) le fait de ne pas notifier des incidents importants ou de ne pas y remédier;

   iii) le fait de ne pas pallier les insuffisances à la suite d'instructions contraignantes des autorités compétentes;

   iv) le fait d'entraver des audits ou des activités de contrôle ordonnées par l'autorité compétente à la suite de la constatation d'une violation;

   v) la fourniture d'informations fausses ou manifestement inexactes relatives aux mesures de gestion des risques en matière de cybersécurité ou aux obligations d'information prévues aux articles 21 et 23;

b) de la durée de la violation;

c) de toute violation antérieure pertinente commise par l'entité concernée;

d) des dommages matériels, corporels ou moraux causés, y compris des pertes financières ou économiques, des effets sur d'autres services et du nombre d'utilisateurs touchés;

▼B

e) du fait que l'auteur de la violation a agi délibérément ou par négligence;

f) des mesures prises par l'entité pour prévenir ou atténuer les dommages matériels, corporels ou moraux;

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

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

8. Les autorités compétentes exposent en détail les motifs de leurs mesures d'exécution. Avant de prendre de telles mesures, les autorités compétentes informent les entités concernées de leurs conclusions préliminaires. Elles laissent en outre à ces entités un délai raisonnable pour communiquer leurs observations, sauf dans des cas exceptionnels dûment motivés où cela empêcherait une intervention immédiate pour prévenir un incident ou y répondre.

9. Les États membres veillent à ce que leurs autorités compétentes en vertu de la présente directive informent les autorités compétentes concernées au sein du même État membre en vertu de la directive (UE) 2022/2557 lorsqu'elles exercent leurs pouvoirs de supervision et d'exécution dans le but de garantir qu'une entité définie comme critique en vertu de la directive (UE) 2022/2557 respecte la présente directive. S'il y a lieu, les autorités compétentes en vertu de la directive (UE) 2022/2557 peuvent demander aux autorités compétentes en vertu de la présente directive d'exercer leurs pouvoirs de supervision et d'exécution à l'égard d'une entité qui est définie comme entité critique en vertu de la directive (UE) 2022/2557.

10. Les États membres veillent à ce que leurs autorités compétentes en vertu de la présente directive coopèrent avec les autorités compétentes pertinentes de l'État membre concerné au titre du règlement (UE) 2022/2554. Les États membres veillent, en particulier, à ce que leurs autorités compétentes en vertu de la présente directive informent le forum de supervision institué en vertu de l'article 32, paragraphe 1, du règlement (UE) 2022/2554 lorsqu'elles exercent leurs pouvoirs de supervision et d'exécution dans le but de garantir qu'une entité essentielle qui a été désignée comme étant un prestataire tiers critique de services TIC au titre de l'article 31 du règlement (UE) 2022/2554 respecte la présente directive.

Article 33

Mesures de supervision et d'exécution en ce qui concerne les entités importantes

1. Au vu d'éléments de preuve, d'indications ou d'informations selon lesquels une entité importante ne respecterait pas la présente directive, et notamment ses articles 21 et 23, les États membres veillent à ce que les autorités compétentes prennent des mesures, le cas échéant, dans le cadre de mesures de contrôle ex post. Les États membres veillent à ce que ces mesures soient effectives, proportionnées et dissuasives, compte tenu des circonstances propres à chaque cas d'espèce.

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

▼B

a) des inspections sur place et des contrôles à distance ex post, effectués par des professionnels formés;

b) des audits de sécurité ciblés réalisés par un organisme indépendant ou une autorité compétente;

c) des scans de sécurité fondés sur des critères d'évaluation des risques objectifs, non discriminatoires, équitables et transparents, si nécessaire avec la coopération de l'entité concernée;

d) des demandes d'informations nécessaires à l'évaluation ex post des mesures de gestion des risques en matière de cybersécurité adoptées par l'entité concernée, notamment les politiques de cybersécurité consignées par écrit, ainsi que du respect de l'obligation de soumettre des informations aux autorités compétentes conformément à l'article 27;

e) des demandes d'accès à des données, à des documents et à des informations nécessaires à l'accomplissement de leurs tâches de supervision;

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

Les audits de sécurité ciblés visés au premier alinéa, point b), sont fondés sur des évaluations des risques effectuées par l'autorité compétente ou l'entité contrôlée, ou sur d'autres informations disponibles relatives aux risques.

Les résultats de tout audit de sécurité ciblé sont mis à la disposition de l'autorité compétente. Les coûts de cet audit de sécurité ciblé effectué par un organisme indépendant sont à la charge de l'entité contrôlée, sauf lorsque l'autorité compétente en décide autrement dans des cas dûment motivés.

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

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

a) d'émettre des avertissements concernant des violations de la présente directive par les entités concernées;

b) d'adopter des instructions contraignantes ou une injonction exigeant des entités concernées qu'elles pallient les insuffisances constatées ou les violations de la présente directive;

c) d'ordonner aux entités concernées de mettre un terme à un comportement qui viole la présente directive et de ne pas le réitérer;

d) d'ordonner aux entités concernées de garantir la conformité de leurs mesures de gestion des risques en matière de cybersécurité avec l'article 21 ou de respecter les obligations d'information prévues à l'article 23, de manière spécifique et dans un délai déterminé;

▼B

e) d'ordonner aux entités concernées d'informer les personnes physiques ou morales à l'égard desquelles elles fournissent des services ou exercent des activités susceptibles d'être affectées par une cybermenace importante de la nature de la menace, ainsi que de toutes mesures préventives ou réparatrices que ces personnes physiques ou morales pourraient prendre en réponse à cette menace;

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

g) d'ordonner aux entités concernées de rendre publics des aspects de violations de la présente directive de manière spécifique;

h) d'imposer ou de demander aux organes compétents ou aux juridictions compétentes d'imposer, conformément au droit national, une amende administrative en vertu de l'article 34 en plus de l'une ou l'autre des mesures visées aux points a) à g) du présent paragraphe.

5. L'article 32, paragraphes 6, 7 et 8, s'applique mutatis mutandis aux mesures de supervision et d'exécution prévues au présent article pour les entités importantes.

6. Les États membres veillent à ce que leurs autorités compétentes en vertu de la présente directive coopèrent avec les autorités compétentes pertinentes de l'État membre concerné au titre du règlement (UE) 2022/2554. Les États membres veillent, en particulier, à ce que leurs autorités compétentes au titre de la présente directive informent le forum de supervision établi en vertu de l'article 32, paragraphe 1, du règlement (UE) 2022/2554 lorsqu'elles exercent leurs pouvoirs de supervision et d'exécution dans le but de garantir qu'une entité importante qui a été désignée comme étant un prestataire tiers critique de services TIC en vertu de l'article 31 du règlement (UE) 2022/2554 respecte la présente directive.

Article 34

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

1. Les États membres veillent à ce que les amendes administratives imposées aux entités essentielles et importantes en vertu du présent article pour des violations de la présente directive soient effectives, proportionnées et dissuasives, compte tenu des circonstances de chaque cas.

2. Les amendes administratives sont imposées en complément de l'une ou l'autre des mesures visées à l'article 32, paragraphe 4, points a) à h), à l'article 32, paragraphe 5, et à l'article 33, paragraphe 4, points a) à g).

3. Au moment de décider s'il y a lieu d'imposer une amende administrative et de décider de son montant, dans chaque cas d'espèce, il est dûment tenu compte, au minimum, des éléments prévus à l'article 32, paragraphe 7.

4. Les États membres veillent à ce que, lorsqu'elles violent l'article 21 ou 23, les entités essentielles soient soumises, conformément aux paragraphes 2 et 3 du présent article, à des amendes administratives d'un montant maximal s'élevant à au moins 10 000 000 EUR ou à au moins 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle l'entité essentielle appartient, le montant le plus élevé étant retenu.

▼B

5. Les États membres veillent à ce que, lorsqu'elles violent l'article 21 ou 23, les entités importantes soient soumises, conformément aux paragraphes 2 et 3 du présent article, à des amendes administratives d'un montant maximal s'élevant à au moins 7 000 000 EUR ou à au moins 1,4 % du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle l'entité importante appartient, le montant le plus élevé étant retenu.

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

7. Sans préjudice des pouvoirs des autorités compétentes en vertu des articles 32 et 33, chaque État membre peut établir les règles déterminant si et dans quelle mesure des amendes administratives peuvent être imposées à des entités de l'administration publique.

8. Si le système juridique d'un État membre ne prévoit pas d'amendes administratives, cet État membre veille à ce que le présent article soit appliqué de telle sorte que l'amende soit déterminée par l'autorité compétente et imposée par les juridictions nationales compétentes, tout en veillant à ce que ces voies de droit soit effectives et aient un effet équivalent aux amendes administratives imposées par les autorités compétentes. En tout état de cause, les amendes imposées sont effectives, proportionnées et dissuasives. L'État membre notifie à la Commission les dispositions légales qu'il adopte en vertu du présent paragraphe au plus tard le 17 octobre 2024 et, sans tarder, toute disposition légale modificative ou modification ultérieure les concernant.

Article 35

Infractions donnant lieu à une violation de données à caractère personnel

1. Lorsque les autorités compétentes prennent connaissance, dans le cadre de la supervision ou de l'exécution, du fait que la violation commise par une entité essentielle ou importante à l'égard des obligations énoncées aux articles 21 et 23 de la présente directive peut donner lieu à une violation de données à caractère personnel au sens de l'article 4, point 12, du règlement (UE) 2016/679, devant être notifiée en vertu de l'article 33 dudit règlement, elles en informent sans retard injustifié les autorités de contrôle visées à l'article 55 ou 56 dudit règlement.

2. Lorsque les autorités de contrôle visées à l'article 55 ou 56 du règlement (UE) 2016/679 imposent une amende administrative en vertu de l'article 58, paragraphe 2, point i), dudit règlement, les autorités compétentes n'imposent pas d'amende administrative au titre de l'article 34 de la présente directive pour une violation visée au paragraphe 1 du présent article et découlant du même comportement que celui qui a fait l'objet d'une amende administrative au titre de l'article 58, paragraphe 2, point i), du règlement (UE) 2016/679. Les autorités compétentes peuvent toutefois imposer les mesures d'exécution prévues à l'article 32, paragraphe 4, points a) à h), à l'article 32, paragraphe 5, et à l'article 33, paragraphe 4, points a) à g), de la présente directive.

3. Lorsque l'autorité de contrôle compétente en vertu du règlement (UE) 2016/679 est établie dans un autre État membre que l'autorité compétente, l'autorité compétente informe l'autorité de contrôle établie dans son propre État membre de la violation potentielle de données à caractère personnel visée au paragraphe 1.

▼B

Article 36

Sanctions

Les États membres déterminent le régime des sanctions applicables aux violations des dispositions nationales adoptées conformément à la présente directive et prennent toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions. Les sanctions prévues sont effectives, proportionnées et dissuasives. Les États membres informent la Commission, au plus tard le 17 janvier 2025, des règles et mesures adoptées à cet égard, ainsi que, sans retard, de toute modification qui y serait apportée ultérieurement.

Article 37

Assistance mutuelle

1. Lorsqu'une entité fournit des services dans plusieurs États membres, ou fournit des services dans un ou plusieurs États membres alors que ses réseaux et systèmes d'information sont situés dans un ou plusieurs autres États membres, les autorités compétentes des États membres concernés coopèrent et se prêtent mutuellement assistance si nécessaire. Cette coopération suppose, au minimum:

a) que les autorités compétentes appliquant des mesures de supervision ou d'exécution dans un État membre informent et consultent, par l'intermédiaire du point de contact unique, les autorités compétentes des autres États membres concernés en ce qui concerne les mesures de supervision et d'exécution prises;

b) qu'une autorité compétente puisse demander à une autre autorité compétente de prendre des mesures de supervision ou d'exécution;

c) qu'une autorité compétente, dès réception d'une demande motivée d'une autre autorité compétente, fournisse à l'autre autorité compétente une assistance mutuelle proportionnée à ses propres ressources afin que les mesures de supervision ou d'exécution puissent être mises en œuvre de manière effective, efficace et cohérente.

L'assistance mutuelle visée au premier alinéa, point c), peut porter sur des demandes d'informations et des mesures de contrôle, y compris des demandes de procéder à des inspections sur place, à des contrôles à distance ou à des audits de sécurité ciblés. Une autorité compétente à laquelle une demande d'assistance est adressée ne peut refuser cette demande que s'il est établi que l'autorité n'est pas compétente pour fournir l'assistance demandée, que l'assistance demandée n'est pas proportionnée aux tâches de supervision de l'autorité compétente ou que la demande concerne des informations ou implique des activités dont la divulgation ou l'exercice seraient contraires aux intérêts essentiels de la sécurité nationale, la sécurité publique ou la défense de cet État membre. Avant de refuser une telle demande, l'autorité compétente consulte les autres autorités compétentes concernées ainsi que, à la demande de l'un des États membres concernés, la Commission et l'ENISA.

▼B

2. Le cas échéant et d'un commun accord, les autorités compétentes de différents États membres peuvent mener à bien des actions communes de supervision.

CHAPITRE VIII

ACTES DÉLÉGUÉS ET ACTES D'EXÉCUTION

Article 38

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 24, paragraphe 2, est conféré à la Commission pour une période de cinq ans à compter du 16 janvier 2023.

3. La délégation de pouvoir visée à l'article 24, paragraphe 2, peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au *Journal officiel de l'Union européenne* ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

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

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

6. Un acte délégué adopté en vertu de l'article 24, paragraphe 2, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de deux mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de deux mois à l'initiative du Parlement européen ou du Conseil.

Article 39

Comité

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

▼B

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

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

CHAPITRE IX

DISPOSITIONS FINALES

Article 40

Réexamen

Au plus tard le 17 octobre 2027 et tous les 36 mois par la suite, la Commission réexamine le fonctionnement de la présente directive et en fait rapport au Parlement européen et au Conseil. Le rapport évalue notamment la pertinence de la taille des entités concernées et des secteurs, sous-secteurs et types d'entité visés aux annexes I et II pour le fonctionnement de l'économie et de la société en ce qui concerne la cybersécurité. À cette fin et en vue de faire progresser la coopération stratégique et opérationnelle, la Commission tient compte des rapports du groupe de coopération et du réseau des CSIRT sur l'expérience acquise au niveau stratégique et opérationnel. Le rapport est accompagné, si nécessaire, d'une proposition législative.

Article 41

Transposition

1. Les États membres adoptent et publient, au plus tard le 17 octobre 2024, les dispositions nécessaires pour se conformer à la présente directive. Ils en informent immédiatement la Commission.

Ils appliquent ces dispositions à partir du 18 octobre 2024.

2. Lorsque les États membres adoptent les dispositions visées au paragraphe 1, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication officielle. Les modalités de cette référence sont arrêtées par les États membres.

Article 42

Modification du règlement (UE) nº 910/2014

Dans le règlement (UE) nº 910/2014, l'article 19 est supprimé avec effet au 18 octobre 2024.

Article 43

Modification de la directive (UE) 2018/1972

Dans la directive (UE) 2018/1972, les articles 40 et 41 sont supprimés avec effet au 18 octobre 2024.

▼B

Article 44

Abrogation

La directive (UE) 2016/1148 est abrogée avec effet au 18 octobre 2024.

Les références à la directive abrogée s'entendent comme faites à la présente directive et sont à lire selon le tableau de correspondance figurant à l'annexe III.

Article 45

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 46

Destinataires

Les États membres sont destinataires de la présente directive.

▼B

ANNEXE I

SECTEURS HAUTEMENT CRITIQUES

Secteur	Sous-secteur	Type d'entité
1. Énergie	a) Électricité	— Entreprises d'électricité au sens de l'article 2, point 57), de la directive (UE) 2019/944 du Parlement européen et du Conseil ([1]), qui remplissent la fonction de «fourniture» au sens de l'article 2, point 12), de ladite directive
		— Gestionnaires de réseau de distribution au sens de l'article 2, point 29), de la directive (UE) 2019/944
		— Gestionnaires de réseau de transport au sens de l'article 2, point 35), de la directive (UE) 2019/944
		— Producteurs au sens de l'article 2, point 38), de la directive (UE) 2019/944
		— Opérateurs désignés du marché de l'électricité au sens de l'article 2, point 8), du règlement (UE) 2019/943 du Parlement européen et du Conseil ([2]) — Acteurs du marché au sens de l'article 2, point 25), du règlement (UE) 2019/943 fournissant des services d'agrégation, de participation active de la demande ou de stockage d'énergie au sens de l'article 2, points 18), 20) et 59), de la directive (UE) 2019/944 — Exploitants d'un point de recharge qui sont responsables de la gestion et de l'exploitation d'un point de recharge, lequel fournit un service de recharge aux utilisateurs finals, y compris au nom et pour le compte d'un prestataire de services de mobilité
	b) Réseaux de chaleur et de froid	— Opérateurs de réseaux de chaleur ou de réseaux de froid au sens de l'article 2, point 19), de la directive (UE) 2018/2001 du Parlement européen et du Conseil ([3])
	c) Pétrole	— Exploitants d'oléoducs
		— Exploitants d'installations de production, de raffinage, de traitement, de stockage et de transport de pétrole
		— Entités centrales de stockage au sens de l'article 2, point f), de la directive 2009/119/CE du Conseil ([4])
	d) Gaz	— Entreprises de fourniture au sens de l'article 2, point 8, de la directive 2009/73/CE du Parlement européen et du Conseil ([5])
		— Gestionnaires de réseau de distribution au sens de l'article 2, point 6, de la directive 2009/73/CE
		— Gestionnaires de réseau de transport au sens de l'article 2, point 4, de la directive 2009/73/CE
		— Gestionnaires d'installation de stockage au sens de l'article 2, point 10, de la directive 2009/73/CE

▼B

Secteur	Sous-secteur	Type d'entité
		— Gestionnaires d'installation de GNL au sens de l'article 2, point 12, de la directive 2009/73/CE
		— Entreprises de gaz naturel au sens de l'article 2, point 1, de la directive 2009/73/CE
		— Exploitants d'installations de raffinage et de traitement de gaz naturel
	e) Hydrogène	— Exploitants de systèmes de production, de stockage et de transport d'hydrogène
2. Transports	a) Transports aériens	— Transporteurs aériens au sens de l'article 3, point 4), du règlement (CE) n° 300/2008 utilisés à des fins commerciales
		— Entités gestionnaires d'aéroports au sens de l'article 2, point 2), de la directive 2009/12/CE du Parlement européen et du Conseil ([6]), aéroports au sens de l'article 2, point 1), de ladite directive, y compris les aéroports du réseau central énumérés à l'annexe II, section 2, du règlement (UE) n° 1315/2013 du Parlement européen et du Conseil ([7]), et entités exploitant les installations annexes se trouvant dans les aéroports
		— Services du contrôle de la circulation aérienne au sens de l'article 2, point 1), du règlement (CE) n° 549/2004 du Parlement européen et du Conseil ([8])
	b) Transports ferroviaires	— Gestionnaires de l'infrastructure au sens de l'article 3, point 2), de la directive 2012/34/UE du Parlement européen et du Conseil ([9])
		— Entreprises ferroviaires au sens de l'article 3, point 1), de la directive 2012/34/UE, y compris les exploitants d'installation de service au sens de l'article 3, point 12), de ladite directive
	c) Transports par eau	— Sociétés de transport par voie d'eau intérieure, maritime et côtier de passagers et de fret, telles qu'elles sont définies pour le domaine du transport maritime à l'annexe I du règlement (CE) n° 725/2004 du Parlement européen et du Conseil ([10]), à l'exclusion des navires exploités à titre individuel par ces sociétés

▼B

Secteur	Sous-secteur	Type d'entité
		— Entités gestionnaires des ports au sens de l'article 3, point 1), de la directive 2005/65/CE du Parlement européen et du Conseil ([11]), y compris les installations portuaires au sens de l'article 2, point 11), du règlement (CE) n° 725/2004, ainsi que les entités exploitant des infrastructures et des équipements à l'intérieur des ports
		— Exploitants de services de trafic maritime (STM) au sens de l'article 3, point o), de la directive 2002/59/CE du Parlement européen et du Conseil ([12])
	d) Transports routiers	— Autorités routières au sens de l'article 2, point 12), du règlement délégué (UE) 2015/962 de la Commission ([13]) chargées du contrôle de la gestion de la circulation, à l'exclusion des entités publiques pour lesquelles la gestion de la circulation ou l'exploitation de systèmes de transport intelligents constituent une partie non essentielle de leur activité générale
		— Exploitants de systèmes de transport intelligents au sens de l'article 4, point 1), de la directive 2010/40/UE du Parlement européen et du Conseil ([14])
3. Secteur bancaire		Établissements de crédit au sens de l'article 4, point 1), du règlement (UE) n° 575/2013 du Parlement européen et du Conseil ([15])
4. Infrastructures des marchés financiers		— Exploitants de plates-formes de négociation au sens de l'article 4, point 24), de la directive 2014/65/UE du Parlement européen et du Conseil ([16])
		— Contreparties centrales au sens de l'article 2, point 1), du règlement (UE) n° 648/2012 du Parlement européen et du Conseil ([17])
5. Santé		— Prestataires de soins de santé au sens de l'article 3, point g), de la directive 2011/24/UE du Parlement européen et du Conseil ([18])
		— Laboratoires de référence de l'Union européenne visés à l'article 15 du règlement (UE) 2022/2371 du Parlement européen et du Conseil ([19])
		— Entités exerçant des activités de recherche et de développement dans le domaine des médicaments au sens de l'article 1er, point 2, de la directive 2001/83/CE du Parlement européen et du Conseil ([20]) — Entités fabriquant des produits pharmaceutiques de base et des préparations pharmaceutiques au sens de la NACE Rév. 2, section C, division 21 — Entités fabriquant des dispositifs médicaux considérés comme critiques en cas d'urgence de santé publique (liste des dispositifs médicaux critiques en cas d'urgence de santé publique) au sens de l'article 22 du règlement (UE) 2022/123 du Parlement européen et du Conseil ([21])

▼B

Secteur	Sous-secteur	Type d'entité
6. Eau potable		Fournisseurs et distributeurs d'eaux destinées à la consommation humaine au sens de l'article 2, point 1) a), de la directive (UE) 2020/2184 du Parlement européen et du Conseil ([22]), à l'exclusion des distributeurs pour lesquels la distribution d'eaux destinées à la consommation humaine constitue une partie non essentielle de leur activité générale de distribution d'autres produits et biens
7. Eaux usées		Entreprises collectant, évacuant ou traitant les eaux urbaines résiduaires, les eaux ménagères usées ou les eaux industrielles usées au sens de l'article 2, points 1), 2) et 3), de la directive 91/271/CEE du Conseil ([23]), à l'exclusion des entreprises pour lesquelles la collecte, l'évacuation ou le traitement des eaux urbaines résiduaires, des eaux ménagères usées ou des eaux industrielles usées constituent une partie non essentielle de leur activité générale
8. Infrastructure numérique		— Fournisseurs de points d'échange internet
		— Fournisseurs de services DNS, à l'exclusion des opérateurs de serveurs racines de noms de domaine
		— Registres de noms de domaine de premier niveau
		— Fournisseurs de services d'informatique en nuage
		— Fournisseurs de services de centres de données
		— Fournisseurs de réseaux de diffusion de contenu
		— Prestataires de services de confiance
		— Fournisseurs de réseaux de communications électroniques publics
		— Fournisseurs de services de communications électroniques accessibles au public
9. Gestion des services TIC (interentreprises)		— Fournisseurs de services gérés — Fournisseurs de services de sécurité gérés
10. Administration publique		— Entités de l'administration publique des pouvoirs publics centraux définies comme telles par un État membre conformément au droit national
		— Entités de l'administration publique au niveau régional définies comme telles par un État membre conformément au droit national

▼B

Secteur	Sous-secteur	Type d'entité
11. Espace		Exploitants d'infrastructures terrestres, détenues, gérées et exploitées par des États membres ou par des parties privées, qui soutiennent la fourniture de services spatiaux, à l'exclusion des fournisseurs de réseaux de communications électroniques publics

(1) Directive (UE) 2019/944 du Parlement européen et du Conseil du 5 juin 2019 concernant des règles communes pour le marché intérieur de l'électricité et modifiant la directive 2012/27/UE (JO L 158 du 14.6.2019, p. 125).
(2) Règlement (UE) 2019/943 du Parlement européen et du Conseil du 5 juin 2019 sur le marché intérieur de l'électricité (JO L 158 du 14.6.2019, p. 54).
(3) Directive (UE) 2018/2001 du Parlement européen et du Conseil du 11 décembre 2018 relative à la promotion de l'utilisation de l'énergie produite à partir de sources renouvelables (JO L 328 du 21.12.2018, p. 82).
(4) Directive 2009/119/CE du Conseil du 14 septembre 2009 faisant obligation aux États membres de maintenir un niveau minimal de stocks de pétrole brut et/ou de produits pétroliers (JO L 265 du 9.10.2009, p. 9).
(5) Directive 2009/73/CE du Parlement européen et du Conseil du 13 juillet 2009 concernant des règles communes pour le marché intérieur du gaz naturel et abrogeant la directive 2003/55/CE (JO L 211 du 14.8.2009, p. 94).
(6) Directive 2009/12/CE du Parlement européen et du Conseil du 11 mars 2009 sur les redevances aéroportuaires (JO L 70 du 14.3.2009, p. 11).
(7) Règlement (UE) n° 1315/2013 du Parlement européen et du Conseil du 11 décembre 2013 sur les orientations de l'Union pour le développement du réseau transeuropéen de transport et abrogeant la décision n° 661/2010/UE (JO L 348 du 20.12.2013, p. 1).
(8) Règlement (CE) n° 549/2004 du Parlement européen et du Conseil du 10 mars 2004 fixant le cadre pour la réalisation du ciel unique européen («règlement-cadre») (JO L 96 du 31.3.2004, p. 1).
(9) 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).
(10) Règlement (CE) n° 725/2004 du Parlement européen et du Conseil du 31 mars 2004 relatif à l'amélioration de la sûreté des navires et des installations portuaires (JO L 129 du 29.4.2004, p. 6).
(11) Directive 2005/65/CE du Parlement européen et du Conseil du 26 octobre 2005 relative à l'amélioration de la sûreté des ports (JO L 310 du 25.11.2005, p. 28).
(12) 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).
(13) Règlement délégué (UE) 2015/962 de la Commission du 18 décembre 2014 complétant la directive 2010/40/UE du Parlement européen et du Conseil en ce qui concerne la mise à disposition, dans l'ensemble de l'Union, de services d'informations en temps réel sur la circulation (JO L 157 du 23.6.2015, p. 21).
(14) Directive 2010/40/UE du Parlement européen et du Conseil du 7 juillet 2010 concernant le cadre pour le déploiement de systèmes de transport intelligents dans le domaine du transport routier et d'interfaces avec d'autres modes de transport (JO L 207 du 6.8.2010, p. 1).
(15) Règlement (UE) n° 575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et modifiant le règlement (UE) n° 648/2012 (JO L 176 du 27.6.2013, p. 1).
(16) 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).
(17) Règlement (UE) n° 648/2012 du Parlement européen et du Conseil du 4 juillet 2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux (JO L 201 du 27.7.2012, p. 1).
(18) Directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers (JO L 88 du 4.4.2011, p. 45).
(19) Règlement (UE) 2022/2371 du Parlement européen et du Conseil du 23 novembre 2022 concernant les menaces transfrontières graves pour la santé et abrogeant la décision no 1082/2013/UE (JO L 314 du 6.12.2022, p. 26).
(20) Directive 2001/83/CE du Parlement européen et du Conseil du 6 novembre 2001 instituant un code communautaire relatif aux médicaments à usage humain (JO L 311 du 28.11.2001, p. 67).
(21) Règlement (UE) 2022/123 du Parlement européen et du Conseil du 25 janvier 2022 relatif à un rôle renforcé de l'Agence européenne des médicaments dans la préparation aux crises et la gestion de celles-ci en ce qui concerne les médicaments et les dispositifs médicaux (JO L 20 du 31.1.2022, p. 1).
(22) Directive (UE) 2020/2184 du Parlement européen et du Conseil du 16 décembre 2020 relative à la qualité des eaux destinées à la consommation humaine (JO L 435 du 23.12.2020, p. 1).
(23) Directive 91/271/CEE du Conseil du 21 mai 1991 relative au traitement des eaux urbaines résiduaires (JO L 135 du 30.5.1991, p. 40).

▼B

ANNEXE II

AUTRES SECTEURS CRITIQUES

Secteur	Sous-secteur	Type d'entité
1. Services postaux et d'expédition		Prestataires de services postaux au sens de l'article 2, point 1 *bis*), de la directive 97/67/CE, y compris les prestataires de services d'expédition
2. Gestion des déchets		Entreprises exécutant des opérations de gestion des déchets au sens de l'article 3, point 9), de la directive 2008/98/CE du Parlement européen et du Conseil ([1]), à l'exclusion des entreprises pour lesquelles la gestion des déchets n'est pas la principale activité économique
3. Fabrication, production et distribution de produits chimiques		Entreprises procédant à la fabrication de substances et à la distribution de substances ou de mélanges au sens de l'article 3, points 9 et 14, du règlement (CE) n° 1907/2006 du Parlement européen et du Conseil ([2]) et entreprises procédant à la production d'articles au sens de l'article 3, point 3), dudit règlement, à partir de substances ou de mélanges
4. Production, transformation et distribution des denrées alimentaires		Entreprises du secteur alimentaire au sens de l'article 3, point 2), du règlement (CE) n° 178/2002 du Parlement européen et du Conseil ([3]) qui exercent des activités de distribution en gros ainsi que de production et de transformation industrielles
5. Fabrication	a) Fabrication de dispositifs médicaux et de dispositifs médicaux de diagnostic in vitro	Entités fabriquant des dispositifs médicaux au sens de l'article 2, point 1), du règlement (UE) 2017/745 du Parlement européen et du Conseil ([4]) et entités fabriquant des dispositifs médicaux de diagnostic in vitro au sens de l'article 2, point 2), du règlement (UE) 2017/746 du Parlement européen et du Conseil ([5]), à l'exception des entités fabriquant des dispositifs médicaux mentionnés à l'annexe I, point 5, cinquième tiret, de la présente directive
	b) Fabrication de produits informatiques, électroniques et optiques	Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2, section C, division 26
	c) Fabrication d'équipements électriques	Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2, section C, division 27

▼B

Secteur	Sous-secteur	Type d'entité
	d) Fabrication de machines et équipements n.c.a.	Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2, section C, division 28
	e) Construction de véhicules automobiles, remorques et semi-remorques	Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2, section C, division 29
	f) Fabrication d'autres matériels de transport	Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2, section C, division 30
6. Fournisseurs numériques		— Fournisseurs de places de marché en ligne
		— Fournisseurs de moteurs de recherche en ligne
		— Fournisseurs de plateformes de services de réseaux sociaux
7. Recherche		Organismes de recherche

([1]) 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).
([2]) Règlement (CE) n° 1907/2006 du Parlement européen et du Conseil du 18 décembre 2006 concernant l'enregistrement, l'évaluation et l'autorisation des substances chimiques, ainsi que les restrictions applicables à ces substances (REACH), instituant une agence européenne des produits chimiques, modifiant la directive 1999/45/CE et abrogeant le règlement (CEE) n° 793/93 du Conseil et le règlement (CE) n° 1488/94 de la Commission ainsi que la directive 76/769/CEE du Conseil et les directives 91/155/CEE, 93/67/CEE, 93/105/CE et 2000/21/CE de la Commission (JO L 396 du 30.12.2006, p. 1).
([3]) Règlement (CE) n° 178/2002 du Parlement européen et du Conseil du 28 janvier 2002 établissant les principes généraux et les prescriptions générales de la législation alimentaire, instituant l'Autorité européenne de sécurité des aliments et fixant des procédures relatives à la sécurité des denrées alimentaires (JO L 31 du 1.2.2002, p. 1).
([4]) Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) n° 178/2002 et le règlement (CE) n° 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE (JO L 117 du 5.5.2017, p. 1).
([5]) Règlement (UE) 2017/746 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux de diagnostic in vitro et abrogeant la directive 98/79/CE et la décision 2010/227/UE de la Commission (JO L 117 du 5.5.2017, p. 176).

▼B

ANNEXE III

TABLEAU DE CORRESPONDANCE

Directive (UE) 2016/1148	Présente directive
Article 1er, paragraphe 1	Article 1er, paragraphe 1
Article 1er, paragraphe 2	Article 1er, paragraphe 2
Article 1er, paragraphe 3	—
Article 1er, paragraphe 4	Article 2, paragraphe 12
Article 1er, paragraphe 5	Article 2, paragraphe 13
Article 1er, paragraphe 6	Article 2, paragraphes 6 et 11
Article 1er, paragraphe 7	Article 4
Article 2	Article 2, paragraphe 14
Article 3	Article 5
Article 4	Article 6
Article 5	—
Article 6	—
Article 7, paragraphe 1	Article 7, paragraphes 1 et 2
Article 7, paragraphe 2	Article 7, paragraphe 4
Article 7, paragraphe 3	Article 7, paragraphe 3
Article 8, paragraphes 1 à 5	Article 8, paragraphes 1 à 5
Article 8, paragraphe 6	Article 13, paragraphe 4
Article 8, paragraphe 7	Article 8, paragraphe 6
Article 9, paragraphes 1, 2 et 3	Article 10, paragraphes 1, 2 et 3
Article 9, paragraphe 4	Article 10, paragraphe 9
Article 9, paragraphe 5	Article 10, paragraphe 10
Article 10, paragraphes 1 et 2 et paragraphe 3, premier alinéa	Article 13, paragraphes 1, 2 et 3
Article 10, paragraphe 3, deuxième alinéa	Article 23, paragraphe 9
Article 11, paragraphe 1	Article 14, paragraphes 1 et 2
Article 11, paragraphe 2	Article 14, paragraphe 3
Article 11, paragraphe 3	Article 14, paragraphe 4, premier alinéa, points a) à r) et s), et paragraphe 7

▼B

Directive (UE) 2016/1148	Présente directive
Article 11, paragraphe 4	Article 14, paragraphe 4, premier alinéa, point r), et deuxième alinéa
Article 11, paragraphe 5	Article 14, paragraphe 8
Article 12, paragraphes 1 à 5	Article 15, paragraphes 1 à 5
Article 13	Article 17
Article 14, paragraphes 1 et 2	Article 21, paragraphes 1 à 4
Article 14, paragraphe 3	Article 23, paragraphe 1
Article 14, paragraphe 4	Article 23, paragraphe 3
Article 14, paragraphe 5	Article 23, paragraphes 5, 6 et 8
Article 14, paragraphe 6	Article 23, paragraphe 7
Article 14, paragraphe 7	Article 23, paragraphe 11
Article 15, paragraphe 1	Article 31, paragraphe 1
Article 15, paragraphe 2, premier alinéa, point a)	Article 32, paragraphe 2, point e)
Article 15, paragraphe 2, premier alinéa, point b)	Article 32, paragraphe 2, point g)
Article 15, paragraphe 2, deuxième alinéa	Article 32, paragraphe 3
Article 15, paragraphe 3	Article 32, paragraphe 4, point b)
Article 15, paragraphe 4	Article 31, paragraphe 3
Article 16, paragraphes 1 et 2	Article 21, paragraphes 1 à 4
Article 16, paragraphe 3	Article 23, paragraphe 1
Article 16, paragraphe 4	Article 23, paragraphe 3
Article 16, paragraphe 5	—
Article 16, paragraphe 6	Article 23, paragraphe 6
Article 16, paragraphe 7	Article 23, paragraphe 7
Article 16, paragraphes 8 et 9	Article 21, paragraphe 5, et article 23, paragraphe 11
Article 16, paragraphe 10	—
Article 16, paragraphe 11	Article 2, paragraphes 1, 2 et 3
Article 17, paragraphe 1	Article 33, paragraphe 1
Article 17, paragraphe 2, point a)	Article 32, paragraphe 2, point e)
Article 17, paragraphe 2, point b)	Article 32, paragraphe 4, point b)

▼B

Directive (UE) 2016/1148	Présente directive
Article 17, paragraphe 3	Article 37, paragraphe 1, points a) et b)
Article 18, paragraphe 1	Article 26, paragraphe 1, point b), et paragraphe 2
Article 18, paragraphe 2	Article 26, paragraphe 3
Article 18, paragraphe 3	Article 26, paragraphe 4
Article 19	Article 25
Article 20	Article 30
Article 21	Article 36
Article 22	Article 39
Article 23	Article 40
Article 24	—
Article 25	Article 41
Article 26	Article 45
Article 27	Article 46
Annexe I, point 1)	Article 11, paragraphe 1
Annexe I, points 2 a) i) à iv)	Article 11, paragraphe 2, points a) à d)
Annexe I, point 2) a) v)	Article 11, paragraphe 2, point f)
Annexe I, point 2) b)	Article 11, paragraphe 4
Annexe I, points 2) c) i) et ii)	Article 11, paragraphe 5, point a)
Annexe II	Annexe I
Annexe III, points 1) et 2)	Annexe II, point 6)
Annexe III, point 3)	Annexe I, point 8)