Chambre des Députés
GRAND-DUCHÉ DE LUXEMBOURG

N°8364

PROJET DE LOI

concernant des mesures destinées à assurer un niveau élevé de cybersécurité et portant modification de :
1° la loi modifiée du 14 août 2000 relative au commerce électronique ;
2° la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale ;
3° la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques

*

Chapitre 1er – Champ d'application et définitions

Art. 1er. (1) La présente loi 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 de la Commission des Communautés européennes du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises, ou qui dépassent les plafonds prévus au paragraphe 1er dudit article, et qui fournissent leurs services ou exercent leurs activités au sein de l'Union européenne.

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

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

1° les services sont fournis par :

a) des fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public ;
b) des prestataires de services de confiance ;
c) des registres des noms de domaine de premier niveau et des fournisseurs de services de système de noms de domaine ;

2° l'entité est, au Grand-Duché de Luxembourg, le seul prestataire d'un service qui est essentiel au maintien d'activités sociétales ou économiques critiques ;

3° une perturbation du service fourni par l'entité pourrait avoir un impact important sur la sécurité publique, la sûreté publique ou la santé publique ;

4° 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 ;

5° 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 au Grand-Duché de Luxembourg ;

6° l'entité est une entité de l'administration publique telle que définie à l'article 2, point 34°.

(3) La présente loi s'applique aux entités recensées en tant qu'entités critiques en vertu de la loi du XXX sur la résilience des entités critiques, quelle que soit leur taille.

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

(5) La présente loi ne s'applique pas aux entités exclues du champ d'application du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011 conformément à l'article 2, paragraphe 4, dudit règlement.

(6) Les articles 12, 13, 14 et 15 ainsi que le chapitre 6 ne s'appliquent pas :

1° au Service de renseignement de l'État visé par la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État ;
2° aux services du ministre ayant la Défense dans ses attributions ;
3° à l'Armée luxembourgeoise visée par la loi modifiée du 7 août 2023 sur l'organisation de l'Armée luxembourgeoise.

(7) La présente loi ne s'applique pas aux systèmes de communication et d'information où sont conservées ou traitées des pièces classifiées au sens de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité.

(8) Lorsque des actes juridiques sectoriels de l'Union européenne 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 loi, les dispositions pertinentes de la présente loi, y compris celles relatives à la supervision et à l'exécution prévues au chapitre 6, ne sont pas applicables auxdites entités. Lorsqu'un acte juridique sectoriel de l'Union européenne ne couvre pas toutes les entités d'un secteur spécifique relevant du champ d'application de la présente loi, les dispositions pertinentes de la présente loi continuent de s'appliquer aux entités non couvertes par cet acte juridique sectoriel de l'Union européenne.

Les exigences visées à l'alinéa 1er du présent paragraphe sont considérées comme ayant un effet équivalent aux obligations prévues par la présente loi lorsque :

1° les mesures de gestion des risques en matière de cybersécurité ont un effet au moins équivalent à celui des mesures prévues à l'article 12, paragraphes 1er et 2 ; ou

2° l'acte juridique sectoriel de l'Union européenne 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 loi, et lorsque les exigences relatives à la notification des incidents importants sont au moins équivalentes à celles prévues à l'article 14, paragraphes 1er à 6.

Art. 2. Pour l'application de la présente loi, on entend par :

1° « réseau et système d'information » :

a) un réseau de communications électroniques au sens de l'article 2, point 1°, de la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques ;
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 lettres 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 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité), tel que modifié ;

4° « 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 ;

5° « 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 ;

6° « incident de cybersécurité majeur » : un incident qui provoque des perturbations dépassant les capacités de réaction du seul État membre de l'Union européenne concerné ou qui a un impact important sur au moins deux États membres de l'Union européenne ;

7° « 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 ;

8° « 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 ;

9° « cybermenace » : une cybermenace au sens de l'article 2, point 8°, du règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité), tel que modifié ;

10° « 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 ;

11° « produit TIC » : un produit TIC au sens de l'article 2, point 12°, du règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité), tel que modifié ;

12° « service TIC » : un service TIC au sens de l'article 2, point 13°, du règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité), tel que modifié ;

13° « processus TIC » : un processus TIC au sens de l'article 2, point 14°, du règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité), tel que modifié ;

14° « vulnérabilité » : une faiblesse, susceptibilité ou faille de produits TIC ou de services TIC qui peut être exploitée par une cybermenace ;

15° « norme » : une norme au sens de l'article 2, point 1°, du 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, tel que modifié ;

16° « spécification technique » : une spécification technique au sens de l'article 2, point 4°, du 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, tel que modifié ;

17° « 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 ;

18° « 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 ;

19° « 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 ;

20° « 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 ;

21° « 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 ;

22° « service numérique » : un service au sens de l'article 1er, paragraphe 1er, lettre b), de la loi du 8 novembre 2016 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information ;

23° « service de confiance » : un service de confiance au sens de l'article 3, point 16°, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE ;

24° « prestataire de services de confiance » : un prestataire de services de confiance au sens de l'article 3, point 19°, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE ;

25° « service de confiance qualifié » : un service de confiance qualifié au sens de l'article 3, point 17°, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE ;

26° « prestataire de services de confiance qualifié » : un prestataire de services de confiance qualifié au sens de l'article 3, point 20°, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE ;

27° « place de marché en ligne » : une place de marché en ligne au sens de l'article L. 010-1, point 15°, du Code de la consommation ;

28° « 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 du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne ;

29° « 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 ;

30° « service de centre de données » : un service qui englobe les structures, ou groupes de structures, dédiées à l'hébergement, l'interconnexion et l'exploitation centralisés 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 ;

31° « 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 ;

32° « 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 ;

33° « représentant » : une personne physique ou morale établie dans l'Union européenne 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 européenne, 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 loi ;

34° « entité de l'administration publique » : toute entité, à l'exclusion des cours et tribunaux, de la Chambre des députés et de la Banque centrale du Luxembourg, 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 ;

35° « réseau de communications électroniques public » : un réseau de communications électroniques public au sens de l'article 2, point 8°, de la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques ;

36° « service de communications électroniques » : un service de communications électroniques au sens de l'article 2, point 4°, de la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques ;

37° « 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 ;

38° « 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 ;

39° « 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 ;

40° « 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 ;

41° « CIRCL » : Computer Incident Response Center Luxembourg, opéré par le groupement d'intérêt économique Luxembourg House of Cybersecurity ;

42° « données de communications électroniques » : le contenu et les métadonnées de communications électroniques ;

43° « contenu de communications électroniques » : le contenu échangé au moyen de services de communications électroniques, notamment sous forme de texte, de voix, de documents vidéo, d'images et de son ;

44° « métadonnées de communications électroniques » : les données traitées dans un réseau de communications électroniques aux fins de la transmission, la distribution ou l'échange de contenu de communications électroniques, y compris les données permettant de retracer une communication et d'en déterminer l'origine et la destination ainsi que les données relatives à la localisation de l'appareil produites dans le cadre de la fourniture de services de communications électroniques, et la date, l'heure, la durée et le type de communication.

Chapitre 2 – Autorités en matière de cybersécurité

Art. 3. L'Institut luxembourgeois de régulation est l'autorité compétente chargée de la cybersécurité dans le cadre de la présente loi et des tâches de supervision et d'exécution visées au chapitre 6 pour les secteurs visés aux annexes I et II et les entités critiques telles que visées par la loi du XXX sur la résilience des entités critiques.

Par dérogation à l'alinéa 1er, la Commission de surveillance du secteur financier est l'autorité compétente chargée de la cybersécurité dans le cadre de la présente loi et des tâches de supervision et d'exécution visées au chapitre 6 pour le secteur bancaire et le secteur des infrastructures des marchés financiers, figurant aux points 3° et 4° du tableau de l'annexe I. Elle est par ailleurs l'autorité compétente pour le secteur des infrastructures numériques et le secteur de la gestion des services TIC, figurant aux points 8° et 9° du tableau de l'annexe I, en ce qui concerne les activités qui tombent sous la surveillance de la Commission de surveillance du secteur financier.

L'obligation au secret professionnel prévue par l'article 16 de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier et l'article 15 de la loi modifiée du 30 mai 2005 portant : 1) organisation de l'Institut Luxembourgeois de Régulation ; 2) modification de la loi modifiée du 22 juin 1963 fixant le régime des traitements des fonctionnaires de l'État ne fait pas obstacle à l'échange d'informations confidentielles entre les autorités compétentes, les CSIRT et le point de contact unique tels que visés aux articles 5 et 7, dans le cadre et aux seules fins de la présente loi et des mesures prises pour son exécution.

Art. 4. L'Institut luxembourgeois de régulation bénéficie d'une contribution financière à charge du budget de l'État afin de couvrir l'intégralité des frais de fonctionnement qui résultent de l'exercice des missions prévues par la présente loi.

Art. 5. Le Haut-Commissariat à la Protection nationale constitue le point de contact unique chargé d'exercer une fonction de liaison afin d'assurer la coopération transfrontière des autorités compétentes avec les autorités compétentes des autres États membres de l'Union européenne et, le cas échéant, avec la Commission européenne et l'Agence de l'Union européenne pour la cybersécurité, ci-après « ENISA », ainsi qu'à garantir la coopération intersectorielle avec les autres autorités compétentes nationales.

Art. 6. Le Haut-Commissariat à la Protection nationale est l'autorité compétente chargée de la gestion des incidents de cybersécurité majeurs et des crises, ci-après « autorité de gestion des crises cyber » et représente le Grand-Duché de Luxembourg au sein du réseau européen pour la préparation et la gestion des crises cyber, dénommé « EU-CyCLONe », institué par l'article 16 de la 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).

Art. 7. (1) Le Haut-Commissariat à la Protection nationale, dans sa fonction de GOVCERT.LU, constitue le centre de réponse aux incidents de sécurité informatique, ci-après « CSIRT », pour les administrations et services de l'État, les établissements publics et les entités critiques en vertu de la loi du XXX sur la résilience des entités critiques.

Le CIRCL constitue le CSIRT pour tous les autres cas, pour lesquels le Haut-Commissariat à la Protection nationale, dans sa fonction de GOVCERT.LU, n'est pas compétent.

(2) Les CSIRT 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.

(3) Les CSIRT coopèrent et, le cas échéant, échangent des informations pertinentes conformément à l'article 19 avec des communautés sectorielles ou intersectorielles d'entités essentielles et importantes.

Art. 8. (1) Les CSIRT satisfont aux exigences suivantes :

1° ils 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 ;

2° leurs locaux et les systèmes d'information utilisés se trouvent sur des sites sécurisés ;

3° ils sont dotés d'un système approprié de gestion et de routage des demandes afin, notamment, de faciliter les transferts effectifs et efficaces ;

4° ils garantissent la confidentialité et la fiabilité de leurs opérations ;

5° ils 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 ;

6° ils 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 CSIRT assument les tâches suivantes :

1° 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 ;

2° 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 ;

3° réagir aux incidents et apporter une assistance aux entités essentielles et importantes concernées, le cas échéant ;

4° 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 ;

5° 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 ;

6° participer au réseau des CSIRT, tel que visé par la 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) et apporter une assistance mutuelle en fonction de leurs capacités et de leurs compétences aux autres membres du réseau des CSIRT à leur demande ;

7° le cas échéant, agir en qualité de coordinateur aux fins du processus de divulgation coordonnée des vulnérabilités en vertu de l'article 9, paragraphe 1er ;

8° contribuer au déploiement d'outils de partage d'informations sécurisés conformément à l'article 10, paragraphe 3, de la 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).

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 à l'alinéa 1er, les CSIRT peuvent donner la priorité à certaines tâches sur la base d'une approche basée sur les risques.

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

Art. 9. Le CIRCL est le coordinateur aux fins de la divulgation coordonnée des vulnérabilités. Il 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 coordinateur consistent :

1° à identifier et contacter les entités concernées ;
2° à apporter une assistance aux personnes physiques ou morales signalant une vulnérabilité ;
3° à négocier des délais de divulgation et gérer les vulnérabilités qui touchent plusieurs entités.

Les personnes physiques ou morales sont en mesure de signaler une vulnérabilité, de manière anonyme lorsqu'elles le demandent, au CIRCL. Le CIRCL 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 de l'Union européenne, le CIRCL coopère, le cas échéant, avec les autres CSIRT désignés comme coordinateurs au sein du réseau des CSIRT tel que visé par la 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).

Art. 10. (1) Les autorités compétentes, le point de contact unique et les CSIRT coopèrent les uns avec les autres afin de respecter les obligations énoncées dans la présente loi.

(2) Les informations et notifications relatives aux incidents importants et aux incidents, aux cybermenaces et aux incidents évités notifiées à l'autorité compétente en application des articles 14 et 20, sont transmises au CSIRT concerné et au point de contact unique.

(3) Afin de veiller à ce que les tâches et obligations des autorités compétentes, du point de contact unique et des CSIRT soient exécutées efficacement, 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 du Parlement européen et du Conseil du 11 mars 2008 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile et abrogeant le règlement (CE) n° 2320/2002, tel que modifié, et (UE) 2018/1139 du Parlement européen et du Conseil du 4 juillet 2018 concernant des règles communes dans le domaine de l'aviation civile et instituant une Agence de l'Union européenne pour la sécurité aérienne, et modifiant les règlements (CE) n° 2111/2005, (CE) n° 1008/2008, (UE) n° 996/2010, (UE) n° 376/2014 et les directives 2014/30/UE et 2014/53/UE du Parlement européen et du Conseil, et abrogeant les règlements (CE) n° 552/2004 et (CE) n° 216/2008 du Parlement européen et du Conseil ainsi que le règlement (CEE) n° 3922/91 du Conseil, tel que modifié, les organes de contrôle au titre du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, les autorités compétentes en vertu du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011, les autorités de régulation nationales en vertu de la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques, les autorités compétentes en vertu de la loi du XXX sur la résilience des entités critiques, ainsi que les autorités compétentes en vertu d'autres actes juridiques sectoriels de l'Union européenne coopèrent de façon appropriée.

(4) Les autorités compétentes en vertu de la présente loi et les autorités compétentes en vertu de la loi du XXX sur la résilience des entités critiques 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 loi du XXX sur la résilience des entités critiques, et sur les mesures prises pour faire face à ces risques, menaces et incidents. Les autorités compétentes en vertu de la présente loi et les autorités compétentes en vertu du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011 et de la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques échangent régulièrement des informations pertinentes, y compris en ce qui concerne les incidents et les cybermenaces concernés.

(5) L'obligation au secret professionnel prévue par l'article 16 de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier et l'article 15 de la loi modifiée du 30 mai 2005 portant : 1) organisation de l'Institut Luxembourgeois de Régulation ; 2) modification de la loi modifiée du 22 juin 1963 fixant le régime des traitements des fonctionnaires de l'État ne fait pas obstacle aux différents types de coopération du présent article dans le cadre et aux seules fins de la présente loi et des mesures prises pour son exécution.

Chapitre 3 – Entités essentielles et importantes

Art. 11. (1) Les entités suivantes sont considérées comme étant des entités essentielles :

1° les entités d'un type visé à l'annexe I qui dépassent les plafonds applicables aux moyennes entreprises prévus à l'article 2, paragraphe 1er, de l'annexe de la recommandation 2003/361/CE de la Commission des Communautés européennes du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises ;

2° 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 ;

3° les fournisseurs de réseaux 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 de la Commission des Communautés européennes du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises ;

4° les entités de l'administration publique visées à l'article 1er, paragraphe 2, point 6° ;

5° toute autre entité d'un type visé à l'annexe I ou II qui est identifiée par le biais d'une décision de l'autorité compétente en tant qu'entité essentielle en vertu de l'article 1er, paragraphe 2, points 2° à 5° ;

6° les entités recensées en tant qu'entités critiques en vertu de la loi du XXX sur la résilience des entités critiques, visées à l'article 1er, paragraphe 3 ;

7° les entités que les autorités compétentes ont identifiées avant l'entrée en vigueur de la présente loi comme des opérateurs de services essentiels conformément à la loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne et modifiant 1° la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'État et 2° la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale.

(2) Aux fins de la présente loi, les entités d'un type visé à l'annexe I ou II qui ne constituent pas des entités essentielles en vertu du paragraphe 1er du présent article sont considérées comme des entités importantes. Celles-ci incluent les entités identifiées par l'autorité compétente en tant qu'entités importantes en vertu de l'article 1er, paragraphe 2, points 2° à 5°.

(3) Les autorités compétentes établissent une liste des entités essentielles et importantes ainsi que des entités fournissant des services d'enregistrement de noms de domaine. Les autorités compétentes réexaminent cette liste et, le cas échéant, la mettent à jour régulièrement et au moins tous les deux ans par la suite. Ces listes sont transmises par l'autorité compétente au CSIRT compétent et au point de contact unique.

(4) Aux fins de l'établissement de la liste visée au paragraphe 3, les entités visées audit paragraphe communiquent aux autorités compétentes, dans un délai de deux mois à compter de l'entrée en vigueur de la présente loi, au moins les informations suivantes :

1° le nom de l'entité ;

2° l'adresse et les coordonnées actualisées, y compris les adresses électroniques, les plages d'IP et les numéros de téléphone ;

3° le cas échéant, le secteur et le sous-secteur concernés visés à l'annexe I ou II ;

4° le cas échéant, une liste des États membres de l'Union européenne dans lesquels elles fournissent des services relevant du champ d'application de la présente loi ;

5° la taille de l'entité et, le cas échéant, celle du groupe d'entités auquel l'entité concernée appartient.

Les entités visées au paragraphe 3 notifient sans tarder toute modification des informations qu'elles ont communiquées conformément à l'alinéa 1er du présent paragraphe et, en tout état de cause, dans un délai de deux semaines à compter de la date de la modification.

Les autorités compétentes mettent en place des mécanismes nationaux permettant aux entités de s'enregistrer elles-mêmes. L'autorité compétente concernée confirme à ces entités concernées leur désignation en tant qu'entité essentielle ou importante.

Art. 12. (1) 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 à l'alinéa 1er 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.

Afin d'identifier les risques, les entités essentielles et importantes utilisent un cadre d'analyse de risques approprié pouvant être précisé par l'autorité compétente concernée par voie de règlement ou de circulaire.

(2) Les mesures visées au paragraphe 1er 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 :

1° les politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information ;

2° la gestion des incidents ;

3° la continuité des activités, par exemple la gestion des sauvegardes et la reprise des activités, et la gestion des crises ;

4° 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 ;

5° 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 ;

6° des politiques et des procédures pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité ;

7° les pratiques de base en matière de cyberhygiène et la formation à la cybersécurité ;

8° des politiques et des procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement ;

9° la sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs ;

10° 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 mesures prises par les entités essentielles sur base des paragraphes 1er et 2 sont notifiées à l'autorité compétente. Les modalités de cette notification, le format et le délai, sont déterminées par l'autorité compétente concernée par voie de règlement ou de circulaire.

(4) Les autorités compétentes veillent à ce que, lorsqu'elles examinent lesquelles des mesures visées au paragraphe 2, point 4°, 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 autorités compétentes 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 1er, de la 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).

(5) Les autorités compétentes 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.

Art. 13. (1) 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 12, supervisent leur mise en œuvre et peuvent être tenus responsables de la violation dudit article par ces entités.

(2) Les membres des organes de direction des entités essentielles et importantes sont tenus de suivre régulièrement une formation et les entités essentielles et importantes offrent 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.

Art. 14. (1) Les entités essentielles et importantes notifient, sans retard injustifié, à l'autorité compétente concernée, conformément au paragraphe 4, tout incident ayant un impact important sur leur fourniture des services visé au paragraphe 3, ci-après « 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. Ces entités signalent, entre autres, toute information permettant 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.

L'autorité compétente transmet la notification au CSIRT concerné et au point de contact unique dès qu'elle la reçoit.

(2) Le cas échéant, 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 :

1° il a causé ou est susceptible de causer une perturbation opérationnelle grave des services ou des pertes financières pour l'entité concernée ;

2° il a affecté ou est susceptible d'affecter d'autres personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables.

L'autorité compétente concernée peut préciser, par voie de règlement ou de circulaire, les paramètres et les modalités des notifications des incidents ayant un impact important sur leur fourniture des services.

(4) Aux fins de la notification visée au paragraphe 1er, les entités concernées soumettent à l'autorité compétente :

1° sans retard injustifié et en tout état de cause dans les vingt-quatre heures après avoir eu connaissance de l'incident important, une notification préliminaire 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 ;

2° sans retard injustifié et en tout état de cause dans les soixante-douze 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 1° 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 ;

3° 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 ;

4° un rapport final au plus tard un mois après la présentation de la notification d'incident visée au point 2°, comprenant les éléments suivants :

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

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

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

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

5° en cas d'incident en cours au moment de la présentation du rapport final visé au point 4°, 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.

Par dérogation à l'alinéa 1er, point 2°, un prestataire de services de confiance notifie 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 vingt-quatre heures après avoir eu connaissance de l'incident important.

(5) L'autorité compétente fournit, sans retard injustifié et si possible dans les vingt-quatre heures suivant la réception de la notification préliminaire visée au paragraphe 4, point 1°, 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. L'orientation est émise par l'autorité compétente en coopération avec le CSIRT concerné. 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 de l'Union européenne ou plus, le point de contact unique informe, sans retard injustifié, les autres États membres de l'Union européenne 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 point de contact unique doit préserver la sécurité et les intérêts commerciaux de l'entité ainsi que la confidentialité des informations communiquées.

(7) Lorsque la sensibilisation du public est nécessaire pour prévenir un incident 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, l'autorité compétente et, le cas échéant, les CSIRT ou les autorités compétentes des autres États membres de l'Union européenne 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 de l'autorité compétente, le point de contact unique transmet les notifications reçues en vertu du paragraphe 1er aux points de contact uniques des autres États membres de l'Union européenne 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 1er et à l'article 20.

(10) L'autorité compétente fournit aux autorités compétentes en vertu de la loi du XXX sur la résilience des entités critiques des informations sur les incidents importants, les incidents, les cybermenaces et les incidents évités notifiés conformément au paragraphe 1er et à l'article 20 par les entités identifiées comme des entités critiques en vertu de la loi du XXX sur la résilience des entités critiques.

Art. 15. Afin de démontrer la conformité à certaines exigences visées à l'article 12, l'autorité compétente peut prescrire, par voie de règlement et en prenant en considération les actes délégués adoptés par la Commission européenne en vertu de l'article 24, paragraphe 2, de la 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), 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 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité), tel que modifié. En outre, l'autorité compétente encourage les entités essentielles et importantes à utiliser des services de confiance qualifiés.

Chapitre 4 – Compétence et enregistrement

Art. 16. (1) Les entités relevant du champ d'application de la présente loi sont considérées comme relevant de la compétence du Grand-Duché de Luxembourg lorsqu'elles y sont établies, à l'exception des cas suivants :

1° 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 de l'Union européenne dans lequel ils fournissent leurs services ;

2° 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 de l'Union européenne dans lequel ils ont leur établissement principal dans l'Union européenne en application du paragraphe 2 ;

3° les entités de l'administration publique, qui sont considérées comme relevant de la compétence de l'État membre de l'Union européenne qui les a établies.

(2) Aux fins de la présente loi, une entité visée au paragraphe 1er, point 2°, est considérée avoir son établissement principal dans l'Union européenne 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 de l'Union européenne ne peut être déterminé ou si ces décisions ne sont pas prises dans l'Union européenne, l'établissement principal est considéré comme se trouvant dans l'État membre de l'Union européenne où les opérations de cybersécurité sont effectuées. Si un tel État membre de l'Union européenne ne peut être déterminé, l'établissement principal est considéré comme se trouvant dans l'État membre de l'Union européenne où l'entité concernée possède l'établissement comptant le plus grand nombre de salariés dans l'Union européenne.

(3) Si une entité visée au paragraphe 1er, point 2°, n'est pas établie dans l'Union européenne mais offre des services sur le territoire du Grand-Duché de Luxembourg, elle désigne un représentant dans l'Union européenne. Le représentant est établi dans l'un des États membres de l'Union européenne dans lesquels les services sont fournis. Une telle entité est considérée comme relevant de la compétence du Grand-Duché de Luxembourg si le représentant y est établi. En l'absence d'un représentant dans l'Union européenne désigné en vertu du présent paragraphe et si l'entité fournit des services au Grand-Duché de Luxembourg, l'autorité compétente peut assigner l'entité à comparaître devant le président du Tribunal d'arrondissement de Luxembourg statuant comme en matière de référé aux fins d'ordonner la désignation d'un représentant dans l'Union européenne.

(4) La désignation d'un représentant par une entité visée au paragraphe 1er, point 2°, est sans préjudice d'actions en justice qui pourraient être intentées contre l'entité elle-même.

(5) L'autorité compétente qui a reçu une demande d'assistance mutuelle en lien avec une entité visée au paragraphe 1er, point 2°, peut, 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 le territoire luxembourgeois.

Art. 17. (1) 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 soumettent les informations suivantes à l'autorité compétente au plus tard le 17 janvier 2025 :

1° le nom de l'entité ;

2° les secteur, sous-secteur et type d'entité concernés, visés à l'annexe I ou II, le cas échéant ;

3° l'adresse de l'établissement principal de l'entité et de ses autres établissements légaux dans l'Union européenne ou, si elle n'est pas établie dans l'Union européenne, de son représentant désigné conformément à l'article 16, paragraphe 3 ;

4° 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 16, paragraphe 3 ;

5° les États membres de l'Union européenne dans lesquels l'entité fournit des services ;

6° les plages d'IP de l'entité.

Le point de contact unique transmet ces informations, à l'exception de celles visées au paragraphe 1er, point 6°, à l'ENISA, afin de permettre à l'ENISA de mettre en place le registre visé à l'article 27 de la directive 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).

(2) Les entités visées au paragraphe 1er notifient à l'autorité compétente toute modification des informations qu'elles ont communiquées en vertu dudit paragraphe sans tarder et, en tout état de cause, dans un délai de trois mois à compter de la date de la modification.

Art. 18. (1) Afin de contribuer à la sécurité, à la stabilité et à la résilience du DNS, les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine collectent les données d'enregistrement de noms de domaine et les maintiennent exactes et complètes au sein d'une base de données spécialisée avec la diligence requise par la législation sur la protection des données à caractère personnel.

(2) Aux fins du paragraphe 1er, la base de données d'enregistrement des noms de domaine contient 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 :

1° le nom de domaine ;

2° la date d'enregistrement ;

3° le nom du titulaire, l'adresse de courrier électronique et le numéro de téléphone permettant de le contacter ;

4° 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 registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine mettent en place des politiques et des procédures, notamment des procédures de vérification, visant à garantir que les bases de données visées au paragraphe 1er contiennent des informations exactes et complètes. Ces politiques et procédures sont mises à la disposition du public.

(4) 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 registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine donnent accès aux données spécifiques d'enregistrement de noms de domaine sur demande légitime et dûment motivée des demandeurs d'accès légitimes, dans le respect de la législation sur la protection des données. 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 soixante-douze heures après réception de toute demande d'accès. Les politiques et procédures de divulgation de ces données sont rendues publiques.

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

Chapitre 5 – Partage d'informations

Art. 19. (1) Les entités relevant du champ d'application de la présente loi et, le cas échéant, les autres entités concernées ne relevant pas du champ d'application de la présente loi peuvent 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 :

1° vise à prévenir et à détecter les incidents, à y réagir, à s'en rétablir ou à atténuer leur impact ;

2° 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) Cet échange d'informations a lieu au sein de communautés d'entités essentielles et importantes ainsi que, le cas échéant, de leurs fournisseurs ou prestataires de services et 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 entités essentielles et importantes notifient à l'autorité compétente 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.

Art. 20. (1) Outre l'obligation de notification prévue à l'article 14, des notifications peuvent être transmises à titre volontaire :

1° aux autorités compétentes par les entités essentielles et importantes en ce qui concerne les incidents, les cybermenaces et les incidents évités ;

2° à l'Institut luxembourgeois de régulation par les entités autres que celles visées au point 1°, indépendamment du fait qu'elles relèvent ou non du champ d'application de la présente loi, en ce qui concerne les incidents importants, les cybermenaces ou les incidents évités.

(2) L'autorité compétente traite les notifications visées au paragraphe 1er conformément à la procédure énoncée à l'article 14. L'autorité compétente peut traiter les notifications obligatoires en leur donnant la priorité par rapport aux notifications volontaires.

Lorsque cela est nécessaire, l'autorité compétente fournit au CSIRT concerné et au point de contact unique 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 6 – Supervision et exécution

Art. 21. (1) Lorsque les autorités compétentes accomplissent leurs tâches de supervision prévues aux articles 22 et 23, elles peuvent mettre au point des méthodes de supervision permettant de fixer des priorités concernant ces tâches selon une approche basée sur les risques.

(2) 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 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), tel que modifié, sans préjudice de la compétence et des missions des autorités de contrôle.

Art. 22. (1) Les mesures de supervision ou d'exécution imposées aux entités essentielles à l'égard des obligations prévues par la présente loi doivent être effectives, proportionnées et dissuasives, compte tenu des circonstances de chaque cas.

(2) Les autorités compétentes, lorsqu'elles accomplissent leurs tâches de supervision à l'égard d'entités essentielles, ont le pouvoir de soumettre ces entités à :

1° des inspections sur place et des contrôles à distance, y compris des contrôles aléatoires effectués par des professionnels formés ;

2° des audits de sécurité réguliers et ciblés réalisés par un organisme indépendant ou l'autorité compétente ;

3° des audits ad hoc, notamment lorsqu'ils sont justifiés en raison d'un incident important ou d'une violation de la présente loi par l'entité essentielle ;

4° 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 ;

5° 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 17 ;

6° des demandes d'accès à des données, à des documents et à toutes informations nécessaires à l'accomplissement de leurs tâches de supervision ;

7° 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 à l'alinéa 1er, point 2°, 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, points 5°, 6° ou 7°, les autorités compétentes mentionnent la finalité de la demande et précisent quelles sont les informations exigées.

(4) Les autorités compétentes, lorsqu'elles exercent leurs pouvoirs d'exécution à l'égard d'entités essentielles, ont le pouvoir :

1° d'émettre des avertissements concernant les violations de la présente loi par les entités concernées ;

2° 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 loi ;

3° d'ordonner aux entités concernées de mettre un terme à un comportement qui viole la présente loi et de ne pas le réitérer ;

4° d'ordonner aux entités concernées de garantir la conformité de leurs mesures de gestion des risques en matière de cybersécurité avec l'article 12 ou de respecter les obligations d'information énoncées à l'article 14, de manière spécifique et dans un délai déterminé ;

5° 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 affectés 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 ;

6° d'ordonner aux entités concernées de mettre en œuvre les recommandations formulées à la suite d'un audit de sécurité dans un délai raisonnable ;

7° 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 12 et 14 ;

8° d'ordonner aux entités concernées de rendre publics les aspects de violations de la présente loi de manière spécifique ;

9° d'imposer une amende administrative en vertu de l'article 26 en plus de l'une ou l'autre des mesures visées aux points 1° à 8° du présent paragraphe.

(5) Lorsque les mesures d'exécution adoptées en vertu du paragraphe 4, points 1° à 4° et point 6°, sont inefficaces, les autorités compétentes peuvent 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 autorités compétentes ont le pouvoir :

1° de demander au président du Tribunal d'arrondissement de Luxembourg statuant comme en matière de référé 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 ;

2° de demander au président du Tribunal d'arrondissement de Luxembourg statuant comme en matière de référé 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.

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. La mainlevée de ces suspensions ou interdictions temporaires est prononcée par le président du Tribunal d'arrondissement de Luxembourg statuant comme en matière de référé.

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

(6) 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 a le pouvoir de veiller au respect, par l'entité, de la présente loi. Ces personnes physiques peuvent être tenues responsables des manquements à leur devoir de veiller au respect de la présente loi.

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 :

1° 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 :

a) les violations répétées ;

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

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

d) 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 ;

e) 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 12 et 14 ;

2° de la durée de la violation ;

3° de toute violation antérieure pertinente commise par l'entité concernée ;

4° 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 ;

5° du fait que l'auteur de la violation a agi délibérément ou par négligence ;

6° des mesures prises par l'entité pour prévenir ou atténuer les dommages matériels, corporels ou moraux ;

7° de l'application de codes de conduite approuvés ou de mécanismes de certification approuvés ;

8° 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 autorités compétentes en vertu de la présente loi informent les autorités compétentes concernées en vertu de la loi du XXX sur la résilience des entités critiques 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 loi du XXX sur la résilience des entités critiques respecte la présente loi. S'il y a lieu, les autorités compétentes en vertu de la loi du XXX sur la résilience des entités critiques peuvent demander aux autorités compétentes en vertu de la présente loi 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 loi du XXX sur la résilience des entités critiques.

(10) Les autorités compétentes en vertu de la présente loi coopèrent avec les autorités compétentes pertinentes de l'État membre de l'Union européenne concerné au titre du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011. Les autorités compétentes en vertu de la présente loi informent le forum de supervision institué en vertu de l'article 32, paragraphe 1er, du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011 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 dudit règlement respecte la présente loi.

Art. 23. (1) Au vu d'éléments de preuve, d'indications ou d'informations selon lesquels une entité importante ne respecterait pas la présente loi, et notamment ses articles 12 et 14, les autorités compétentes prennent des mesures, le cas échéant, dans le cadre de mesures de contrôle ex post. Ces mesures doivent être effectives, proportionnées et dissuasives, compte tenu des circonstances propres à chaque cas d'espèce.

(2) Les autorités compétentes, lorsqu'elles accomplissent leurs tâches de supervision à l'égard d'entités importantes, ont le pouvoir de soumettre ces entités à :

1° des inspections sur place et des contrôles à distance ex post, effectués par des professionnels formés ;

2° des audits de sécurité ciblés réalisés par un organisme indépendant ou l'autorité compétente ;

3° 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 ;

4° 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 17 ;

5° des demandes d'accès à des données, à des documents et à des informations nécessaires à l'accomplissement de leurs tâches de supervision ;

6° 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 à l'alinéa 1er, point 2°, 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, points 4°, 5° ou 6°, les autorités compétentes mentionnent la finalité de la demande et précisent quelles sont les informations exigées.

(4) Les autorités compétentes, lorsqu'elles exercent leurs pouvoirs d'exécution à l'égard d'entités importantes, ont le pouvoir :

1° d'émettre des avertissements concernant des violations de la présente loi par les entités concernées ;

2° d'adopter des instructions contraignantes ou une injonction exigeant des entités concernées qu'elles pallient les insuffisances constatées ou les violations de la présente loi ;

3° d'ordonner aux entités concernées de mettre un terme à un comportement qui viole la présente loi et de ne pas le réitérer ;

4° d'ordonner aux entités concernées de garantir la conformité de leurs mesures de gestion des risques en matière de cybersécurité avec l'article 12 ou de respecter les obligations d'information prévues à l'article 14, de manière spécifique et dans un délai déterminé ;

5° 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 ;

6° d'ordonner aux entités concernées de mettre en œuvre les recommandations formulées à la suite d'un audit de sécurité dans un délai raisonnable ;

7° d'ordonner aux entités concernées de rendre publics des aspects de violations de la présente loi de manière spécifique ;

8° d'imposer une amende administrative en vertu de l'article 26 en plus de l'une ou l'autre des mesures visées aux points 1° à 7°.

(5) L'article 22, 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 autorités compétentes en vertu de la présente loi coopèrent avec les autorités compétentes pertinentes de l'État membre de l'Union européenne concerné au titre du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011. Les autorités compétentes au titre de la présente loi informent le forum de supervision établi en vertu de l'article 32, paragraphe 1er, du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011 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 dudit règlement respecte la présente loi.

Art. 24. (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 12 et 14 peut donner lieu à une violation de données à caractère personnel au sens de l'article 4, point 12°, du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), tel que modifié, 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 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), tel que modifié, 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 26 pour une violation visée au paragraphe 1er 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 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), tel que modifié. Les autorités compétentes peuvent toutefois imposer les mesures d'exécution prévues à l'article 22, paragraphe 4, points 1° à 8°, à l'article 22, paragraphe 5, et à l'article 23, paragraphe 4, points 1° à 7°.

(3) Lorsque l'autorité de contrôle compétente en vertu du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), tel que modifié, est établie dans un autre État membre de l'Union européenne que l'autorité compétente, l'autorité compétente informe l'autorité de contrôle luxembourgeoise de la violation potentielle de données à caractère personnel visée au paragraphe 1er.

Art. 25. (1) Lorsque l'autorité compétente concernée constate une violation des obligations prévues par les articles 11, paragraphe 4, 13, paragraphes 1er et 2, 15, 17, paragraphes 1er, alinéa 1er, et 2, et 18, paragraphes 1er à 6, elle peut frapper l'entité essentielle ou importante concernée d'une ou de plusieurs des sanctions suivantes :

1° un avertissement ;
2° un blâme ;
3° une amende administrative, dont le montant est proportionné à la gravité du manquement, à la situation de l'intéressé, à l'ampleur du dommage et aux avantages qui en sont tirés sans pouvoir excéder 250 000 euros.

(2) En cas de constatation d'un fait susceptible de constituer un manquement visé au paragraphe 1er, l'autorité compétente concernée engage une procédure contradictoire dans laquelle l'entité essentielle ou importante concernée a la possibilité de consulter le dossier et de présenter ses observations. L'entité essentielle ou importante concernée peut se faire assister ou représenter par une personne de son choix. À l'issue de la procédure contradictoire, l'autorité compétente concernée peut prononcer à l'encontre de l'entité essentielle ou importante concernée une ou plusieurs des sanctions visées au paragraphe 1er.

(3) Les décisions prises par l'autorité compétente concernée à l'issue de la procédure contradictoire sont motivées et notifiées à l'entité essentielle ou importante concernée.

(4) Contre les décisions visées au paragraphe 3 un recours en réformation est ouvert devant le tribunal administratif.

(5) L'Administration de l'enregistrement, des domaines et de la TVA est chargée du recouvrement des amendes administratives qui lui sont communiquées par l'Institut luxembourgeois de régulation moyennant la transmission d'une copie des décisions de fixation. Le recouvrement est poursuivi comme en matière d'enregistrement.

Art. 26. (1) Les amendes administratives imposées aux entités essentielles et importantes pour des violations de la présente loi sont 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 22, paragraphe 4, points 1° à 8°, à l'article 22, paragraphe 5, et à l'article 23, paragraphe 4, points 1° à 7°.

(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 22, paragraphe 7.

(4) Lorsqu'elles violent l'article 12 ou 14, paragraphes 1er à 4, les entités essentielles sont soumises, conformément aux paragraphes 2 et 3, à des amendes administratives d'un montant maximal s'élevant à 10 000 000 EUR ou à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle l'entité essentielle appartient, le montant le plus élevé étant retenu.

(5) Lorsqu'elles violent l'article 12 ou 14, paragraphes 1er à 4, les entités importantes sont soumises, conformément aux paragraphes 2 et 3, à des amendes administratives d'un montant maximal s'élevant à 7 000 000 EUR ou à 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 amendes administratives prévues aux paragraphes 4 et 5 sont prononcées dans le respect de la procédure prévue à l'article 25, paragraphes 2 à 5.

(7) Les autorités compétentes ont le pouvoir d'assortir leur décision de sanction d'une astreinte pour contraindre une entité essentielle ou importante à mettre un terme à une violation de la présente loi.

Le montant de l'astreinte par jour à raison du manquement constaté ne peut être supérieur à 1 250 euros, sans que le montant total imposé à raison du manquement constaté ne puisse dépasser 25 000 euros.

Art. 27. (1) Lorsqu'une entité fournit des services dans plusieurs États membres de l'Union européenne, ou fournit des services dans un ou plusieurs États membres de l'Union européenne alors que ses réseaux et systèmes d'information sont situés dans un ou plusieurs autres États membres de l'Union européenne, les autorités compétentes des États membres de l'Union européenne concernés coopèrent et se prêtent mutuellement assistance si nécessaire. Cette coopération suppose, au minimum :

1° que les autorités compétentes appliquant des mesures de supervision ou d'exécution dans un État membre de l'Union européenne informent et consultent, par l'intermédiaire du point de contact unique, les autorités compétentes des autres États membres de l'Union européenne concernés en ce qui concerne les mesures de supervision et d'exécution prises ;

2° qu'une autorité compétente puisse demander à une autre autorité compétente de prendre des mesures de supervision ou d'exécution ;

3° 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 à l'alinéa 1er, point 3°, 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 de l'Union européenne. 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 de l'Union européenne concernés, la Commission européenne et l'ENISA.

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

Chapitre 7 – Dispositions modificatives

Art. 28. À l'article 45*bis*, paragraphe 3, de la loi modifiée du 14 août 2000 relative au commerce électronique, les lettres a) et b) sont abrogées.

Art. 29. La loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale est modifiée comme suit :

1° À l'article 2, le point 5° est remplacé comme suit :

« 5. « réseau et système d'information » : le réseau et système d'information au sens de l'article 2, point 1°, de la loi du XXXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité ;

6. « cybersécurité » : la cybersécurité au sens de l'article 2, point 3°, de la loi du XXXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité ;

7. « stratégie nationale en matière de cybersécurité » : un cadre cohérent fournissant des objectifs et des priorités stratégiques dans le domaine de la cybersécurité et de la gouvernance en vue de les réaliser au niveau national ;

8. « incident » : l'incident au sens de l'article 2, point 5°, de la loi du XXXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité ;

9. « gestion des incidents » : gestion des incidents au sens de l'article 2, point 7°, de la loi du XXXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité ;

10. « cybermenace » : la cybermenace au sens de l'article 2, point 9°, de la loi du XXXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité ;

11. « vulnérabilité » : la vulnérabilité au sens de l'article 2, point 14°, de la loi du XXXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité. » ;

2° L'article 3 est modifié comme suit :

a) au paragraphe 1er, lettre b), point 4°, les termes « stratégie nationale en matière de sécurité des réseaux et des systèmes d'information » sont remplacés par ceux de « stratégie nationale en matière de cybersécurité » ;

b) au paragraphe 1er, lettre c), après le point 1°, il est inséré un nouveau point 1*bis*°, libellé comme suit :

« 1*bis*. de coordonner la communication de crise en situation de crise ; »

c) au paragraphe 1er*bis*, la lettre b) est remplacée par la disposition suivante :

« b) attributions dans sa fonction de Centre gouvernemental de réponse aux incidents de sécurité informatique (CSIRT), ci-après « GOVCERT.LU ». » ;

d) au paragraphe 1er*bis*, la lettre c) est abrogée ;

e) le paragraphe 1er*quater* est remplacé par le libellé suivant :

« (1*quater*) Dans sa fonction de GOVCERT.LU, le Haut-Commissariat à la Protection nationale a pour missions :

a) de constituer le point de contact unique dédié à la gestion des incidents affectant les réseaux et systèmes d'information des administrations et services de l'État et des établissements publics ;

b) d'assurer un service de veille, de détection, d'alerte et de réaction aux cybermenaces et aux vulnérabilités affectant les réseaux et systèmes d'information des administrations et services de l'État et, à leur demande, des établissements publics ;

c) d'assurer la fonction de centre national de réponse aux incidents de sécurité informatique, dénommé « CSIRT National », en

1. opérant comme le point de contact officiel national pour les CSIRT nationaux et gouvernementaux étrangers ;
2. opérant comme le point de contact officiel national pour la collecte, l'analyse et la distribution d'informations relatives aux cybermenaces et incidents qui concernent les réseaux et systèmes d'information implantés au Grand-Duché de Luxembourg ;
3. relayant les informations collectées aux CSIRT sectoriels en charge de la cible d'une attaque ou, à défaut de CSIRT sectoriel, directement à la cible ;
4. assurant un service de veille aux cybermenaces et aux vulnérabilités et en réagissant aux incidents et en apportant une assistance aux entités critiques, le cas échéant.

d) d'assurer la fonction de centre militaire de réponse aux incidents de sécurité informatique, dénommé « MILCERT.LU », en

1. opérant comme le point de contact officiel national pour les CSIRT militaires étrangers ;
2. assurant, à partir du territoire du Grand-Duché de Luxembourg, un service de veille, de détection, d'alerte et de réaction aux cybermenaces,

vulnérabilités et incidents affectant les réseaux et les systèmes d'information de l'armée ;

3. opérant, à partir du territoire du Grand-Duché de Luxembourg, une équipe d'intervention spécialisée capable de prendre en charge la réponse aux incidents liés à ces réseaux et systèmes d'information.

Le Haut-Commissaire à la Protection nationale peut, dans l'intérêt de l'exécution des missions du GOVCERT.LU, demander leur concours aux agents des administrations et services de l'État. »

f) le paragraphe 1er*quinquies* est abrogé.

3° Le chapitre 4*bis* est remplacé par la disposition suivante :

« **Chapitre 4*bis* – La stratégie nationale en matière de cybersécurité**

Art. 9*bis*. (1) Le Haut-Commissariat à la Protection nationale 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 en matière de cybersécurité, couvrant en particulier les secteurs visés aux annexes I et II de la loi du XXXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité ;

b) un cadre de gouvernance visant à atteindre les objectifs et priorités visés à la lettre 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, et sur lequel reposent la coopération et la coordination entre les autorités compétentes, le point de contact unique et les CSIRT en vertu de la loi du XXXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité, ainsi que la coordination et la coopération entre ces organismes et les autorités compétentes en vertu d'actes juridiques sectoriels de l'Union européenne ;

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

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 loi et de la loi du XXX sur la résilience des entités critiques 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, le Haut-Commissariat à la Protection nationale adopte 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 9, paragraphe 1er, de la loi du XXXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité ;

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 ;

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 européenne ;

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 loi, en fournissant des orientations et un soutien facilement accessibles pour répondre à leurs besoins spécifiques ;

j) la promotion d'une cyberprotection active.

Le Haut-Commissariat à la Protection nationale évalue régulièrement la 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. » ;

4° Après l'article 9*bis,* il est inséré un nouveau chapitre 4*ter*, libellé comme suit :

« **Chapitre 4*ter* – Le plan national de réaction aux crises et incidents de cybersécurité majeurs**

Art. 9*ter*. Le Haut-Commissariat à la Protection nationale 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 de l'autorité de gestion des crises cyber en vertu de la loi du XXXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité ;

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 à la gestion coordonnée des incidents de cybersécurité majeurs et des crises au niveau de l'Union européenne. » ;

5° A l'article 15*bis*, les termes « Le personnel de l'ANSSI, du CERT Gouvernemental et du SCC » sont remplacés par ceux de « Le personnel de l'ANSSI et du GOVCERT.LU ».

Art. 30. La loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne et modifiant 1° la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'État et 2° la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale est abrogée.

Art. 31. Les articles 42 et 43 de la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques sont abrogés.

Chapitre 8 – Intitulé de citation

Art. 32. La référence à la présente loi se fait sous la forme suivante : « loi du XXXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité ».

ANNEXE I

Secteurs hautement critiques

Secteur	Sous-secteur	Type d'entité
1. Énergie	a) Électricité	- Entreprises d'électricité au sens de l'article 1er, point 14°, de la loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité, qui remplissent la fonction de « fourniture » au sens de l'article 1er, point 21°, de ladite loi
		- Gestionnaires de réseau de distribution au sens de l'article 1er, point 24°, de la loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité
		- Gestionnaires de réseau de transport au sens de l'article 1er, point 25°, de la loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité
		- Producteurs au sens de l'article 1er, point 39°, de la loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité
		- 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 du 5 juin 2019 sur le marché intérieur de l'électricité, tel que modifié - Acteurs du marché au sens de l'article 2, point 25°, du règlement (UE) 2019/943 du Parlement européen et du Conseil du 5 juin 2019 sur le marché intérieur de l'électricité, tel que modifié, fournissant des services d'agrégation, de participation active de la demande ou de stockage d'énergie au sens de l'article 1er, points 1*quindecies*°, 31*quater*° et 49*ter*°, de la loi modifiée du 1er août

		2007 relative à l'organisation du marché de l'électricité - 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 du 11 décembre 2018 relative à la promotion de l'utilisation de l'énergie produite à partir de sources renouvelables
	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 1er, lettre g), de la loi modifiée du 10 février 2015 relative à l'organisation du marché de produits pétroliers
	d) Gaz	- Entreprises de fourniture au sens de l'article 1er, point 14°, de la loi modifiée du 1er août 2007 relative à l'organisation du marché du gaz naturel
		- Gestionnaires de réseau de distribution au sens de l'article 1er, point 22°, de la loi modifiée du 1er août 2007 relative à l'organisation du marché du gaz naturel
		- Gestionnaires de réseau de transport au sens de l'article 1er, point 24°, de la loi modifiée du 1er août 2007 relative à l'organisation du marché du gaz naturel
		- Gestionnaires d'installation de stockage au sens de l'article 1er, point 25°, de la loi modifiée du 1er août 2007 relative à l'organisation du marché du gaz naturel
		- Gestionnaires d'installation de GNL au sens de l'article 1er, point 23°, de la loi modifiée du 1er août 2007 relative à l'organisation du marché du gaz naturel

		- Entreprises de gaz naturel au sens de l'article 1er, point 15°, de la loi modifiée du 1er août 2007 relative à l'organisation du marché du gaz naturel
		- 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) no 300/2008 du Parlement européen et du Conseil du 11 mars 2008 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile et abrogeant le règlement (CE) n°2320/2002, tel que modifié, utilisés à des fins commerciales
		- Entités gestionnaires d'aéroports au sens de l'article 2, point 1°, de la loi modifiée du 23 mai 2012 portant transposition de la directive 2009/12/CE du Parlement européen et du Conseil du 11 mars 2009 sur les redevances aéroportuaires et portant modification : 1) de la loi modifiée du 31 janvier 1948 relative à la réglementation de la navigation aérienne ; 2) de la loi modifiée du 19 mai 1999 ayant pour objet a) de réglementer l'accès au marché de l'assistance en escale à l'aéroport de Luxembourg, b) de créer un cadre réglementaire dans le domaine de la sûreté de l'aviation civile, et c) d'instituer une Direction de l'Aviation Civile, aéroports au sens de l'article 2, point 1°, de la directive 2009/12/CE du Parlement européen et du Conseil du 11 mars 2009 sur les redevances aéroportuaires, 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 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, tel que modifié, 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 du 10 mars 2004 fixant le cadre pour la réalisation du ciel unique européen (« règlement-cadre »), tel que modifié
	b) Transports ferroviaires	- Gestionnaires de l'infrastructure au sens de l'article 2, point 31°, de la loi du 5 février 2021 relative à l'interopérabilité ferroviaire, à la sécurité ferroviaire et à la certification des conducteurs de train
		- Entreprises ferroviaires au sens de l'article 2, point 15°, de la loi modifiée du 6 juin 2019 portant transposition de la directive (UE) 2016/2370 du Parlement européen et du Conseil du 14 décembre 2016 modifiant la directive 2012/34/UE en ce qui concerne l'ouverture du marché des services nationaux de transport de voyageurs par chemin de fer et la gouvernance de l'infrastructure ferroviaire, y compris les exploitants d'installation de service au sens de l'article 2, point 18°, de la même loi
	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 du 31 mars 2004 relatif à l'amélioration de la sûreté des navires et des installations portuaires, tel que modifié, à l'exclusion des navires exploités à titre individuel par ces sociétés
		- Entités gestionnaires des ports au sens de l'article 3, point 1°, de la directive 2005/65/CE du Parlement européen et du Conseil du 26 octobre 2005 relative à l'amélioration de la sûreté des ports, y compris les installations portuaires au sens de l'article 2, point 11°, du 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, tel que modifié, 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 2, lettre o, du règlement grand-ducal modifié du 27 février 2011 relatif à la mise en place d'un système communautaire de suivi du trafic des navires et d'information
	d) Transports routiers	- Autorités routières au sens de l'article 2, point 12°, du 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, 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 la lettre circulaire du 22 février 2012 concernant la 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
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 du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement et modifiant le règlement (UE) n°648/2012, tel que modifié
4. Infrastructures des marchés financiers		- Exploitants de plates-formes de négociation au sens de l'article 1er, point 43°, de la loi modifiée du 30 mai 2018 relative aux marchés d'instruments financiers
		- Contreparties centrales au sens de l'article 2, point 1°, du 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, tel que modifié
5. Santé		- Prestataires de soins de santé au sens de l'article 2, lettre e), de la loi modifiée du 24 juillet 2014 relative aux droits et obligations du patient
		- Laboratoires de référence de l'Union européenne visés à l'article 15 du 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 n°1082/2013/UE
		- Laboratoires nationaux de référence désignés en vertu de l'article 10 de la loi modifiée du 1er août 2018 sur la déclaration obligatoire de certaines maladies dans le cadre de la protection de la santé publique
		- 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 du 6 novembre 2001 instituant un code communautaire relatif aux médicaments à usage humain - Entités fabriquant des produits pharmaceutiques de base et des préparations pharmaceutiques au sens de la NACE Rév. 2 Nomenclature statistique des activités économiques dans la Communauté européenne, 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 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, tel que modifié

6. Eau potable		Fournisseurs et distributeurs d'eaux destinées à la consommation humaine au sens de l'article 2, point 1°, lettre a), de la loi du 23 décembre 2022 relative à la qualité des eaux destinées à la consommation humaine et modifiant la loi modifiée du 19 décembre 2008 relative à l'eau, 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°, du règlement grand-ducal modifié du 13 mai 1994 relatif au traitement des eaux urbaines résiduaires, 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 telle que définie à l'article 2, point 34°
11. Espace		Exploitants d'infrastructures terrestres, détenues, gérées et exploitées par des États membres de l'Union européenne ou

		par des parties privées, qui soutiennent la fourniture de services spatiaux, à l'exclusion des fournisseurs de réseaux de communications électroniques publics

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 1er, point 12°, de la loi modifiée du 26 décembre 2012 sur les services postaux, 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 4, point 22°, de la loi modifiée du 21 mars 2012 relative aux déchets, 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 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, tel que modifié, 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 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, tel que modifié, 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 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, tel que modifié, 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 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, tel que modifié, à l'exception des entités fabriquant des dispositifs médicaux mentionnés à l'annexe I, point 5°, cinquième tiret
	b) Fabrication de produits informatiques, électroniques et optiques	Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2 Nomenclature statistique des activités économiques dans la Communauté européenne, section C, division 26
	c) Fabrication d'équipements électriques	Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2 Nomenclature statistique des activités économiques dans la Communauté européenne, section C, division 27
	d) Fabrication de machines et équipements n.c.a.	Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2 Nomenclature statistique des activités économiques dans la Communauté européenne, 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 Nomenclature statistique des activités économiques dans la Communauté européenne, section C, division 29
	f) Fabrication d'autres matériels de transport	Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2 Nomenclature statistique des activités économiques dans la Communauté européenne, 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

Projet de loi adopté par la Chambre des Députés
en sa séance publique du 28 avril 2026

Le Secrétaire général,

Laurent Scheeck

Pour le Président,

André Bauler
Vice-Président de la Chambre des Députés