N° 8364[3]

CHAMBRE DES DEPUTES

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 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'Etat et 2° la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale ;

4° la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques

* * *

AVIS DE LA CHAMBRE DES METIERS

(10.12.2024)

RESUME STRUCTURE

Le projet de loi sous avis a pour objet de transposer en droit national la directive 2022/2555 qui vise à établir des mesures pour atteindre un niveau élevé commun de cybersécurité dans l'ensemble de l'Union européenne.

La Chambre des Métiers se prononce en faveur d'un niveau élevé de sécurité des réseaux et des systèmes d'information, notamment au regard de l'existence de risques croissants de cybermenaces au sein de l'Union européenne. Néanmoins, la Chambre des Métiers souligne que l'élargissement du champ d'application et la mise en conformité avec les nouvelles dispositions entraînent une surcharge administrative et des défis de gestion pour les entités nouvellement incluses et engendre des coûts et le cas échéant des investissements conséquents. Elle demande donc aux autorités compétentes d'adopter une approche collaborative et de conseiller les entreprises en la matière. Il importe que les autorités apportent une assistance aux entreprises et que les coûts de la mise en conformité soient éligibles à des aides financières, notamment pour les moyennes entreprises artisanales qui tombent dans le champ d'application du projet de loi.

La Chambre des Métiers demande que les entreprises artisanales soient expressément exclues du champ d'application du projet de loi, étant donné qu'elles fabriquent généralement sur mesure et en petites quantités. Par conséquent, leur production ne peut pas être considérée comme une production industrielle et la distribution de leurs denrées alimentaires ne peut pas être comparée avec une distribution « en gros ». En raison de l'impact sociétal et économique restreint d'un incident potentiel, ces entités ne revêtent pas une « importance cruciale pour les activités économiques et sociétales essentielles dans le marché intérieur ».

La Chambre des Métiers se pose la question de savoir si les fournisseurs et prestataires de service de la chaîne d'approvisionnement des entités concernées doivent être pris en compte et si des obligations découlant du projet de loi s'appliquent également à eux. Elle estime par ailleurs que les listes des secteurs critiques figurant dans les annexes du projet de loi ne devraient pas être établies sur la base des codes NACE, mais sur la base des activités visées par le droit d'établissement luxembourgeois.

Par ailleurs, la Chambre des Métiers estime utile que les autorités compétentes contactent les entreprises concernées pour les informer des nouvelles obligations découlant du projet de loi sous avis.

Finalement, la Chambre des Métiers voit d'un œil critique l'application d'amendes administratives. Elle demande aux auteurs de prévoir une procédure de mise en demeure suivi d'un contrôle qui laisse la possibilité à l'entité contrôlée de remédier à des non-conformités dans un délai raisonnable avant un deuxième contrôle. Afin de ne pas laisser place à l'arbitraire administratif, la Chambre des Métiers demande d'établir des procédures et des listes de contrôle au sein des autorités compétentes pour définir le déroulement des inspections sur place ou des contrôles à distance.

*

En l'absence d'une demande d'avis formelle adressée à la Chambre des Métiers, elle juge utile et nécessaire de s'autosaisir du projet de loi sous avis, eu égard notamment à son importance et ses répercussions sur l'ensemble des entreprises luxembourgeoises, y compris les entreprises artisanales.

Le projet de loi sous avis a pour objet de transposer en droit national la directive (UE) 2022/2555 du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union[1], nommée « Directive NIS 2 ».

La Directive NIS 2 établit des mesures qui ont pour but d'atteindre un niveau élevé commun de cybersécurité dans l'ensemble de l'Union européenne. Ce dispositif vise à renforcer la cybersécurité des entités dites essentielles et importantes en imposant à ces entités des obligations en matière de gestion des risques et de notification des incidents. Il fixe des obligations à l'adresse des politiques nationales en matière de cybersécurité et il vise à renforcer la coopération européenne entre les autorités de cybersécurité. Par ailleurs, le champ d'application de ladite directive est considérablement élargi quant aux secteurs d'activités et aux types d'entités concernées par rapport à la directive précédente, la « Directive NIS 1 »[2], qui a été transposée en droit national par la loi du 28 mai 2019[3], nommée « Loi NIS 1 ».

Il est à noter que la Directive NIS 2 et sa transposition en droit national par le présent projet de loi est en étroite relation avec la directive (UE) 2022/2557[4] et le projet de loi n°8307 y relatif ainsi que le règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier.[5] Par conséquent, les dispositions de la Directive NIS 2 relatives à la gestion des risques de cybersécurité, aux obligations de notification et à la supervision et exécution ne s'appliquent pas aux entités financières relevant du règlement (UE) 2022/2554.

Le projet de loi sous avis reflète une transposition fidèle de la Directive NIS 2, garantissant ainsi à assurer une harmonisation maximale au niveau européen et favorable au développement du marché intérieur. Conformément à la directive, le projet de loi impose tout d'abord des obligations renforcées

---

1 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 ; nommée « Directive NIS 2 »

2 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, nommée « Directive NIS 1 »

3 Loi 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, loi nommée « Loi NIS 1 »

4 Directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil, nommée « Directive CER » (« Critical Entities Resilience Directive »)

5 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) no 1060/2009, (UE) no 648/2012, (UE) no 600/2014, (UE) no 909/2014 et (UE) 2016/1011 nommé « Règlement DORA » (« Digital Operational Resilience Act »)

aux entités essentielles et importantes spécifiées dans l'annexe I et II du projet de loi, telles que l'obligation de s'enregistrer auprès des autorités compétentes, la mise en place de mesures de gestion des risques en matière de cybersécurité, la notification des incidents importants aux autorités compétentes dans un certain délai, et les responsabilités des membres des organes de direction en termes d'approbation et de mise en œuvre des mesures de gestion des risques de cybersécurité, ainsi que leurs obligations de suivre une formation et d'offrir une formation aux membres de leur personnel afin d'acquérir des connaissances et des compétences suffisantes en la matière. Les micros et petites entreprises n'entrent pas dans le champ d'application du projet de loi à l'exception des entités visées par l'article 1er, paragraphe 2 du projet de loi.

Le projet de loi détermine, d'une part, le cadre institutionnel pour sa mise en œuvre, et donne, d'autre part, l'assise juridique pour une stratégie nationale en matière de cybersécurité. Il s'agit de déterminer les objectifs stratégiques, les ressources nécessaires pour atteindre les objectifs ainsi que les mesures politiques et réglementaires appropriées en vue de parvenir à un niveau élevé de cybersécurité et de le maintenir.

Ainsi, l'Institut luxembourgeois de régulation (ILR) et la Commission de surveillance du secteur financier (CSSF) sont les autorités compétentes chargées de la cybersécurité dans le cadre du présent projet de loi. Ils sont en charge des tâches de supervision et d'exécution pour les entités essentielles et importantes, dont la CSSF pour le secteur bancaire et le secteur des infrastructures des marchés financiers figurant aux points 3° et 4° du tableau de l'annexe I du projet de loi. La mission de point de contact unique est confiée au Haut-Commissariat à la Protection nationale (HCPN) qui assure la coopération transfrontière des autorités compétentes luxembourgeoises avec les autorités compétentes des autres États membres, et le cas échéant, avec la Commission européenne et l'Agence de l'Union européenne pour la cybersécurité (ENISA). Le HCPN garantit par ailleurs la coopération intersectorielle avec les autres autorités compétentes nationales.

En outre, le projet de loi prévoit un mécanisme d'évaluation régulière de la stratégie nationale en matière de cybersécurité, au moins tous les cinq ans, garantissant ainsi une adaptation aux évolutions technologiques et aux menaces émergentes. Le HCPN devient l'autorité compétente chargée de la gestion des crises « cyber », ce qui implique l'adoption d'un plan national de réaction aux crises et incidents de cybersécurité majeurs définissant les objectifs et les modalités de gestion des incidents de cybersécurité majeurs et des crises.

En plus de l'élaboration de la stratégie nationale en matière de cybersécurité, de la mission de point de contact unique et de la gestion des crises « cyber », le HCPN assure au niveau international l'interface avec le réseau européen pour la préparation et la gestion des crises « cyber » (EU-CyCLONe)[6] et il assure la fonction de centre national de réponse aux incidents de sécurité informatique (CSIRT)[7] dans sa fonction de GOVCERT.LU[8] pour les administrations et services de l'Etat, ainsi que les établissements publics et les entités critiques en vertu de la directive 2022/2557. Le CIRCL[9] 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.

Finalement le projet de loi sous avis prévoit une série de mesures de supervision et d'exécution que les autorités compétentes (ILR et CSSF) peuvent appliquer aux entités importantes et aux entités essentielles. Les entités essentielles sont soumises à un régime de supervision à part entière, ex ante et ex post. Les mesures de supervision ou d'exécution imposées aux entités essentielles doivent être effectives, proportionnées et dissuasives, compte tenu des circonstances de chaque cas. Les entités importantes sont soumises à un régime de supervision plus léger, uniquement ex post : elles ne sont

---

6 EU-CyCLONe est un nouveau réseau européen pour la préparation et la gestion des crises cyber institué par l'article 16 de la directive (UE) 2022/2555. Ce réseau tend à contribuer à la gestion coordonnée, au niveau opérationnel, des incidents de cybersécurité majeurs et des crises, à garantir l'échange régulier d'informations pertinentes entre les États membres et les institutions, organes et organismes de l'Union européenne.

7 Le projet de loi prévoit la mise en place de centres de réponse aux incidents de sécurité informatiques (« CSIRT »), dont leurs tâches sont précisées à l'article 8 du projet de loi. Selon l'article 8, (1), 1° du projet de loi, les « CSIRT » doivent, sur demande, fournir aux entités concernées une aide pour surveiller leur réseau.

8 « GOVCERT.LU » (Government Computer Emergency Response Team) est la désignation pour le CSIRT pour les administrations et services de l'Etat. Selon le commentaire de l'article 29 du projet de loi, cet acronyme GOVCERT(.LU) correspond à un standard internationale utilisé dans le monde entier pour désigner les CSIRT gouvernementaux nationaux.

9 Computer Incident Response Center Luxembourg, opéré par le groupement d'intérêt économique Luxembourg House of Cybersecurity.

pas tenues de notifier systématiquement leur conformité aux exigences en matière de gestion des risques de cybersécurité. En cas de violation des obligations, le projet de loi prévoit des sanctions telles qu'un avertissement, un blâme ou une amende administrative dont la dernière doit être effective, proportionnée et dissuasive, compte tenu des circonstances de chaque cas.

*

1. CONSIDERATIONS GENERALES

La Chambre des Métiers se prononce en faveur d'un niveau élevé de sécurité des réseaux et des systèmes d'information, notamment au regard de l'existence de risques croissants de cybermenaces au sein de l'Union européenne. En raison du fait que le champ d'application de la Directive NIS 2 a été sensiblement élargi par rapport à la Directive NIS 1 pour inclure un plus grand nombre d'entités et couvrir un éventail plus large de secteurs d'activités, la Chambre des Métiers souligne que la mise en conformité par rapport aux nouvelles dispositions risque d'engendrer des investissements conséquents pour les entreprises concernées qui sont un fardeau pour leur rentabilité, en particulier celles des entreprises qui dépassent tout juste les plafonds applicables aux petites entreprises[10].

Face à ces nouvelles charges, il importe que les autorités apportent une assistance aux entreprises et que les investissements soient éligibles à des aides financières, notamment pour les moyennes entreprises artisanales.

La Chambre des Métiers note avec satisfaction qu'il est prévu de transposer la Directive NIS 2 en droit national en suivant le principe « toute la directive, rien que la directive », ce qui permet non seulement d'éviter des divergences importantes entre les Etats membres en matière de cybersécurité, mais aussi des conditions concurrentielles inéquitables entre les Etats membres.

Même si les mesures techniques, opérationnelles et organisationnelles doivent être appropriées, proportionnées et adaptées aux risques existants tout en tenant compte du coût de mise en œuvre, la Chambre des Métiers pour sa part, souhaite une approche progressive concernant la mise en vigueur des obligations, avec la définition d'une feuille de route pour les entreprises. Aussi, elle donne à considérer que certains aspects relatifs à la mise en œuvre de la future loi devraient être précisés dans un souci de sécurité juridique et pour faciliter aux entités concernées la mise en conformité avec les obligations leur incombant. Elle s'interroge notamment sur l'absence de précisions dans le projet de loi quant aux délais endéans lesquels les entités vont devoir s'enregistrer auprès des autorités compétentes ainsi que le délai de réponse des autorités compétentes pour confirmer la désignation des entités.

Par ailleurs, la Chambre des Métiers estime que les listes des secteurs critiques figurant dans les annexes du projet de loi ne devraient pas être établies sur base des codes NACE[11], mais sur base du droit d'établissement luxembourgeois. Cela nécessiterait de définir plus précisément les secteurs critiques mentionnés dans l'annexe II du projet de loi, afin d'exclure les entités qui ne revêtent pas une « importance cruciale pour les activités économiques et sociétales essentielles dans le marché intérieur »[12]. En ce sens, la Chambre des Métiers demande que les entreprises artisanales soient expressément exclues du champ d'application du projet de loi, étant donné qu'elles fabriquent généralement sur mesure et en petites quantités. Par conséquent, leur production ne peut pas être considérée comme une production industrielle et la distribution de leurs denrées alimentaires ne peut pas être comparée avec une distribution « en gros ».

En outre, comme exposé plus en détail dans le chapitre « Considérations particulières », des précisions concernant la détermination des secteurs hautement critiques et autres secteurs critiques figurant dans les annexes I et II manquent et devraient être ajoutées.

*

---

10 Cf article 2 de l'annexe de la recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micros, petites et moyennes entreprises

11 Nomenclature statistique des activités économiques dans la Communauté Européenne (NACE). Au Luxembourg, le STATEC est responsable de la classification des unités statistiques par activité économique selon la nomenclature NACE.

12 Considérant n°6 de la Directive NIS 2

2. CONSIDERATIONS PARTICULIERES

2.1. Définition du champ d'application et des entités « essentielles » et des entités « importantes »

Conformément à la Directive NIS 2, le présent projet de loi prévoit une distinction entre les entités « essentielles » et les entités « importantes ». Cette détermination précise quelles entités tombent dans le champ d'application du projet de loi et sous quel régime de supervision et d'exécution chacune d'entre elles est soumise. En principe les micros et petites entreprises sont exclues du champ d'application du projet de loi à l'exception des entités visées par l'article 1er, paragraphe 2 du projet de loi.

Le tableau suivant montre la catégorisation des entreprises en vertu de l'annexe de la recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micros, petites et moyennes entreprises :

	Micro-entreprises	*Petites entreprises*	*Entreprises moyennes*	*Grandes entreprises*
Total du bilan	≤ 2 000 000€	≤ 10 000 000€	≤ 43 000 000€	> 43 000 000€
Chiffre d'affaires net	≤ 2 000 000€	≤ 10 000 000€	≤ 50 000 000€	> 50 000 000€
Nombre moyen de salariés	< 10	< 50	< 250	≥ 250

Seules les entités publiques ou privées d'un type visé à l'annexe I et II qui constituent des entreprises moyennes tombent dans le champ d'application, à savoir les entreprises qui occupent plus de 50 personnes ou dont le chiffre d'affaires annuel ou le total du bilan annuel excède 10 millions d'euros.[13]

Certaines entités sont toujours considérées comme « essentielles » peu importe la taille, tels :

- les prestataires de services de confiance[14]
- les registres de noms de domaine de premier niveau et les fournisseurs de services de système de noms de domaine (DNS)
- les entités de l'administration publique
- les entités recensées en tant qu'entités critiques en vertu de la directive (UE) 2022/2557[15]
- toute autre entité d'un type visé à l'annexe I ou II du projet de loi qui est identifiée par l'autorité compétente en tant qu'entité essentielle[16]

Sont également considérés comme entités « essentielles », les fournisseurs de réseau de communications électroniques publics ou de services de communications électroniques accessibles au public qui constituent des moyennes entreprises.

Les entités « essentielles » sont par ailleurs aussi les entités d'un type visé à l'annexe I du projet de loi qui dépassent les plafonds applicables aux moyennes entreprises dans des secteurs hautement critiques spécifiés, à savoir les secteurs suivants :

- Energie : Electricité, réseaux de chaleur et de froid, pétrole, gaz, hydrogène
- Transports : Transports aériens, transports ferroviaires, transports par eau, transports routiers
- Secteur bancaire
- Infrastructures des marchés financiers

---

13 Pour savoir quelles sont les données qu'il y a lieu de prendre en considération et d'apprécier en fonction des seuils, une entreprise doit d'abord établir si elle est une entreprise autonome, une entreprise partenaire ou une entreprise liée au sens de la recommandation 2003/361/CE. Voir le Guide de l'utilisateur pour la définition des PME, publié par la Commission européenne

14 Règlement (UE) no 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, modifié par le Règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique

15 L'article 1er, paragraphe 1er du projet de loi n°8307 portant transposition de la directive (UE) 2022/2557 prévoit que les autorités compétentes recensent les entités critiques pour les secteurs et sous-secteurs figurant à l'annexe du projet de loi n°8307. La désignation d'une entité critique fait l'objet d'un arrêté grand-ducal. Conformément à l'article 7 de la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale actuellement en vigueur, la désignation d'une infrastructure critique fait l'objet d'un arrêté grand-ducal.

16 En vertu de l'article 1er, paragraphe 2, points 2° à 5°

- Santé
- Eau potable
- Eaux usées
- Infrastructure numérique
- Gestion des services TIC (interentreprises)
- Administration publique
- Espace

La Chambre des Métiers demande de préciser pour tous les secteurs hautement critiques et les autres secteurs critiques si les fournisseurs et prestataires de service de la chaîne d'approvisionnement des entités doivent être pris en compte et si des obligations découlant du projet de loi s'appliquent également à eux, telles la mise en place de mesures de gestion des risques ou la notification d'incidents importants. Dans ce contexte, la Chambre des Métiers recommande de définir plus précisément le terme « exploitants d'un point de recharge » (cf. annexe 1 du projet de loi, secteur Energie) afin de préciser quelle entité dans la chaîne d'approvisionnement est concernée.

La Chambre des Métiers se pose la question de savoir si, le terme « prestataire de soins de santé »[17] (cf. annexe 1 du projet de loi, secteur Santé) inclut tout professionnel de santé, tout établissement hospitalier ainsi que tout prestataire de soins, exerçant légalement sa profession en dehors du secteur hospitalier, visé par l'alinéa second de l'article 61 du Code de la sécurité sociale ; incluant donc les fournisseurs de prothèses orthopédiques, d'orthèses et d'épithèses, ainsi que les opticiens qui sont des grandes entreprises (entités « essentielles ») ou des moyennes entreprises (entités « importantes »). La Chambre des Métiers se pose également la question de savoir si les audioprothésistes et les loueurs d'ambulance font partie des prestataires de soins de santé.

Elle s'interroge sur la disponibilité d'une liste des dispositifs médicaux critiques en cas d'urgence de santé publique au sens de l'article 22 du règlement (UE) 2022/123, dont l'existence est nécessaire pour identifier les entités essentielles d'un type visé à l'annexe I, point 5 du secteur de santé.

Les entités d'un type visé à l'annexe I qui constituent des entreprises de taille moyenne sont considérées comme des entités « importantes ».[18]

Les entités d'un type visé à l'annexe II du projet de loi qui constituent des entreprises moyennes, sont considérées comme « importantes », à savoir les secteurs suivants :

- Prestataires de services postaux et d'expédition 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.
- 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.
- 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 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.
- Entreprises du secteur alimentaire au sens de l'article 3, point 2°, du règlement (CE) n°178/2002 qui exercent des activités de distribution en gros ainsi que de production et de transformation industrielles.
- Entités fabriquant des dispositifs médicaux au sens de l'article 2, point 1°, du règlement (UE) 2017/745 et entités fabriquant des dispositifs médicaux de diagnostic in vitro au sens de l'article 2, point 2°, du règlement (UE) 2017/746 à l'exception des entités fabriquant des dispositifs médicaux mentionnés à l'annexe I, point 5°, cinquième tiret, à savoir des dispositifs médicaux critiques en cas d'urgence de santé publique.
- Fabrication de produits informatiques, électroniques et optiques (NACE Rév. 2 section C, division 26)[19].

---

17 Au sens de l'article 2, lettre e) de la loi du 24 juillet 2014 modifiée relative aux droits et obligations du patient

18 A l'exception des entités qui sont toujours considérées comme « essentielles » selon le projet de loi.

19 D'après la dernière publication « Répertoire des entreprises » du février 2021 disponible au Portail des Statistiques, ce code NACE a été attribué à 11 entreprises au Luxembourg.

- Fabrication d'équipements électriques (NACE Rév. 2 section C, division 27)[20].
- Fabrication de machines et équipements n.c.a. (NACE Rév. 2 section C, division 28)[21].
- Construction de véhicules automobiles, remorques et semi-remorques (NACE Rév. 2 section C, division 29)[22].
- Fabrication d'autres matériels de transport (NACE Rév. 2 section C, division 30)[23].
- Fournisseurs de places de marché en ligne, fournisseurs de moteurs de recherche en ligne, fournisseurs de plateforme de services de réseaux sociaux.
- Organismes de recherche.

Les entreprises de taille[24] moyenne et supérieure du secteur alimentaire au sens de l'article 3, point 2°, du règlement (CE) n°178/2002, qui exercent des activités de distribution en gros ainsi que de production et de transformation industrielles, entrent dans le champ d'application du projet de loi.

La Chambre des Métiers estime indispensable de définir plus précisément les termes « activités de distribution en gros » et « production et transformation industrielle » (cf. Annexe II du projet de loi, secteur 4. Production, transformation et distribution des denrées alimentaires), afin de préciser quelles entités du secteur alimentaire sont visées à l'annexe II du projet de loi. Étant donné que seulement la production et la transformation industrielles sont visées par la Directive NIS 2, la Chambre des Métiers demande à exclure le secteur artisanal du champ d'application.

Néanmoins, les entreprises artisanales alimentaires sans production industrielle pourraient relever de la notion de distribution en gros et donc du champ d'application du projet de loi, bien qu'elles ne représentent en aucun cas, par leur activité au sein de ce secteur et leur offre de services, une « importance cruciale pour les activités économiques et sociétales essentielles dans le marché intérieur »[25]. La Chambre des Métiers demande donc d'exclure notamment les entreprises de restauration et de traiteur, qui, à ses yeux, n'exercent pas des activités de distribution en gros, ainsi que tous les métiers alimentaires artisanaux (boulangeries, pâtisseries, etc.) du champ d'application du projet de loi.

Concernant le point 5 de l'annexe II relatif à la fabrication de machines et équipements n.c.a, de la construction de véhicules automobiles, de remorques et de semi-remorques ou de la fabrication de dispositifs médicaux[26], les entreprises artisanales concernées fabriquent en général des produits sur mesure et en petite quantité. Il est évident que la fabrication sur mesure ne peut avoir une « importance cruciale pour les activités économiques et sociétales essentielles dans le marché intérieur ». Selon l'appréciation de la Chambre des Métiers, seule la fabrication industrielle en série (en masse) et non la fabrication de produits en petite quantité ou sur mesure devrait tomber sous le champ d'application du projet de loi. La Chambre des Métiers demande donc l'exclusion de la fabrication sur mesure du champ d'application du projet de loi.

En ce qui concerne la fabrication de dispositifs médicaux, la Chambre des Métiers tient à souligner que des entreprises artisanales, telles que les entreprises de prothésistes dentaires, fabriquent en général des dispositifs sur mesure[27]. Comme ces dispositifs médicaux sur mesure sont fabriqués pour un patient spécifique, leur fabrication ne peut non plus être considérée comme faisant partie d'un secteur d'« importance cruciale pour les activités économiques et sociétales essentielles dans le marché intérieur ». La Chambre des Métiers demande donc l'exclusion du champ d'application du projet de loi de la fabrication de dispositifs médicaux sur mesure et des secteurs artisanaux qui fabriquent en petite quantité et dont la production ne peut être considérée comme industrielle.

---

20 D'après la dernière publication « Répertoire des entreprises » du février 2021 disponible au Portail des Statistiques, ce code NACE a été attribué à 11 entreprises au Luxembourg.

21 D'après la dernière publication « Répertoire des entreprises » du février 2021 disponible au Portail des Statistiques, ce code NACE a été attribué à 28 entreprises au Luxembourg.

22 D'après la dernière publication « Répertoire des entreprises » du février 2021 disponible au Portail des Statistiques, ce code NACE a été attribué à 8 entreprises au Luxembourg.

23 D'après la dernière publication « Répertoire des entreprises » du février 2021 disponible au Portail des Statistiques, ce code NACE a été attribué à 3 entreprises au Luxembourg.

24 Cf article 2 de l'annexe de la recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micros, petites et moyennes entreprises

25 Considérant n°6 de la directive (UE) 2022/2555

26 Au sens de l'article 2, point 1° du règlement (UE) 2017/745

27 Au sens de l'article 2, point 3° du règlement (UE) 2017/745

Enfin, la Chambre des Métiers demande aux autorités compétentes d'établir une liste des entreprises concernées et de les contacter pour les informer des nouvelles obligations découlant du projet de loi sous avis.

2.2. Les nouvelles obligations imposées aux entités visées

2.2.1. *Obligation de s'autoenregistrer auprès des autorités*

Conformément à l'article 11, paragraphe 4, dernier alinéa du projet de loi, les entreprises sont tenues de s'identifier et de s'enregistrer elles-mêmes auprès des autorités compétentes. Les informations qui doivent au moins être communiquées sont reprises au paragraphe 4, premier alinéa, point 1° à 5° dudit article.[28] Les autorités compétentes confirment ensuite aux entités concernées leur désignation en tant qu'entité essentielle ou importante. De plus, les entités visées sont obligées de notifier toute modification des informations qu'elles ont communiquées en tout état de cause dans un délai de deux semaines à compter de la date de la modification. Ce mécanisme est différent de celui prévu par la loi NIS 1 où les autorités compétentes devaient identifier les opérateurs de services essentiels concernés et leur notifier la décision d'identification. Selon l'article 3 de la Directive NIS 2, les Etats membres établissent au plus tard le 17 avril 2025 une liste des entités essentielles et importantes ainsi que des entités fournissant des services d'enregistrement de noms de domaine.[29] Les États membres réexaminent cette liste et, le cas échéant, la mettent à jour régulièrement et au moins tous les deux ans par la suite.

2.2.2. *Compétence territoriale des autorités compétentes luxembourgeoises*

L'article 16 du projet de loi traite la compétence territoriale des autorités luxembourgeoises en définissant les cas dans lesquels une entité relevant du champ d'application du présent projet de loi est considérée comme relevant de la compétence du Grand-Duché de Luxembourg.

D'après l'article 16, paragraphe 1er du projet de loi, qui transpose l'article 26 de la directive NIS 2, les entités relevant du champ d'application du présent projet de loi sont, en règle générale, soumises à la compétence du Grand-Duché de Luxembourg si elles y sont établies. Le commentaire de l'article 16 du projet de loi et le considérant 114 de la Directive NIS 2, indiquent que le fait d'être établi suppose l'exercice effectif d'une activité au moyen d'une installation stable. La forme juridique retenue pour un tel établissement, qu'il s'agisse d'une succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard.

Étant donné qu'il existe au Luxembourg des succursales ou des filiales d'entreprises étrangères considérées « importantes » ou « essentielles », la Chambre des Métiers demande aux auteurs de préciser au niveau de la loi les cas dans lesquels l'autorité luxembourgeoise est compétente pour les entités concernées et où celles-ci doivent s'autoenregistrer. La Chambre des Métiers estime également inévitable de définir plus précisément la notion d'« installation stable ».

L'article 16, paragraphe 1er du projet de loi prévoit trois exceptions à la règle générale énoncée ci-dessous pour les cas suivants :

- Règle du lieu de fourniture du service

  Les fournisseurs de réseaux de communications électroniques publics ou les fournisseurs de services de communications électroniques accessibles au public sont considérés comme relevant de la compétence de l'Etat membre dans lequel ils fournissent leurs services.

- Règle de l'établissement principal ou du représentant dans l'Union européenne

  Les fournisseurs de service 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

---

28 L'institut Luxembourgeois de Régulation a mis en place un formulaire en ligne aux fins d'enregistrement des entités visées.

29 Conformément à l'article 17 du projet de loi, les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les entités qui fournissent 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, des 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 doivent soumettre les informations reprises audit article au plus tard le 17 janvier 2025.

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 sont considérés comme relevant de la compétence de l'Etat membre dans lesquels ils ont leur établissement principal.[30]

- Compétence de l'Etat membre qui a établi les entités de l'administration publique

  Les entités de l'administration publique sont considérées comme relevant de la compétence de l'Etat membre qui les a établies.

2.2.3. *Mise en place de mesures de gestion des risques en matière de cybersécurité*

Conformément à l'article 12 du projet de loi, les entités essentielles et importantes doivent mettre en place des 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. D'après le commentaire dudit article et le considérant 83 de la Directive NIS 2, ces entités devront garantir la sécurité de tous les réseaux et systèmes d'information qu'elles utilisent, indépendamment du fait que ces entités effectuent la maintenance de ces réseaux en interne ou en externe. Aux yeux de la Chambre des Métiers il conviendrait également de préciser dans quelle mesure les fournisseurs et prestataires de services de la chaîne d'approvisionnement de ces entités sont concernés par cette obligation de mise en place de mesures de gestion des risques ou de la notification d'incidents importants.

Les mesures doivent garantir un niveau de sécurité adapté aux risques existant pour les réseaux et les systèmes d'information, en tenant compte de l'état des connaissances, des normes européennes et internationales applicables ainsi que du coût de mise en œuvre. Lors de l'évaluation de la proportionnalité de ces mesures, le degré d'exposition de l'entité aux risques, sa taille et la probabilité de survenance d'incidents ainsi que leur gravité, y compris leurs conséquences sociétales et économiques, doivent être pris en compte. 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.[31] [32]

Les mesures doivent être 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.

Les mesures comprennent au moins :

- Les politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information (« Risk analysis & information security »)
- La gestion des incidents (« Incident handling »)
- La continuité des activités, p.ex. la gestion des sauvegardes et la reprise des activités, et la gestion des crises (« Business continuity : backup management, disaster recovery & crisis management »)
- La sécurité de la chaine d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services directs[33]. (« Security in procurement »)
- 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. (« vulnerability handling & disclosure »)

---

30 Selon l'article 16, paragraphe 2, l'établissement principal est considéré comme se trouvant dans l'Etat membre où les opérations de cybersécurité sont effectuées. Si un tel État membre ne peut être déterminé, l'établissement principal est considéré comme se trouvant dans l'État membre où l'entité concernée possède l'établissement comptant le plus grand nombre de salariés dans l'Union européenne.

31 Par exemple le règlement ILR/N22/7 du 15 septembre 2022 portant sur la notification des mesures de sécurité à prendre par les opérateurs de services essentiels a été établie en vertu de la loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148.

32 Par exemple le règlement ILR/N22/8 du 26 septembre 2022 portant sur la notification des mesures de sécurité à prendre par les entreprises fournissant des réseaux de communications publics et/ou des services de communications électroniques au public a été établi en vertu de la loi du 17 décembre 2021 portant transposition de la directive (UE) 2018/1972.

33 Établir une liste de tous les fournisseurs serait certainement la première étape.

- Des politiques et des procédures pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité.
- Les pratiques de base en matière de cyber hygiène et la formation à la cybersécurité (« Training & hygiene »)
- Les politiques et les procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement
- La sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs (« Human ressources & Access Control »)
- 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.

La Chambre des Métiers fait appel aux autorités compétentes de publier une liste avec les mesures de sécurité exigées et les lignes directrices pour préciser « l'état de connaissance » pour chaque secteur indiquant aux entreprises quelles normes doivent être respectées et par rapport à quels termes une entreprise certifiée ISO/IEC 2700x est conforme aux dispositions du projet de loi.[34] De plus, la Chambre des Métiers demande aux autorités de préciser, pour chaque secteur et sous-secteur concerné, le cadre d'analyse des risques par voie de règlement ou de circulaire comme prévu par l'article 12, paragraphe 1er, 3e alinéa du projet de loi. Elle demande également aux autorités compétentes d'adopter une approche collaborative et de conseiller les entreprises en matière d'identification et de mise en place des mesures prévues à l'article 12 du projet de loi.

Dans une optique de « mieux légiférer » la Chambre des Métiers s'étonne du fait que les termes de cybersécurité et de cybermenace soient définis par des renvois en cascade ce qui rend la lecture du projet de loi particulièrement difficile. Plus grave encore est le fait que le terme « cyber hygiène » n'est pas du tout défini alors que c'est une des mesures introduites par l'article 12 et que même les grands dictionnaires de la langue française ne fournissent pas de définition.

Finalement, la Chambre des Métiers demande au législateur et aux autorités compétentes de prévoir un délai de mise en conformité prolongé pour les entreprises entrant dans le champ d'application du projet de loi et qui ont de peu dépassé les seuils relatifs aux petites entreprises et qui sont devenues ainsi des entreprises moyennes au sens de l'annexe de la recommandation 2003/361/CE[35]. En effet, elles disposent de capacités limitées pendant leur phase de transition et doivent avant tout développer les compétences en la matière.

2.2.4. *Obligations de notification*

Selon l'article 12, paragraphe 3 du projet de loi, les mesures de gestion des risques en matière de cybersécurité prises par les entités essentielles sur base de l'article 12, paragraphes 1er et 2 dudit projet doivent être notifiées à l'autorité compétente. Les modalités de cette notification, tel le format et le délai sont déterminées par l'autorité compétente concernée par voie de règlement ou de circulaire. Cette obligation de notification des mesures de gestion des risques ne s'applique pas aux entités importantes mais ces dernières peuvent néanmoins faire l'objet de contrôles ex post sur base d'éléments de preuve, d'indication ou d'information de violations avérées ou potentielles des obligations prévues par le projet de loi.

Conformément à l'article 14 du projet de loi, les entités essentielles et importantes sont soumises à une notification des incidents importants endéans certains délais.

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.

---

34 L'institut Luxembourgeois de Régulation a déjà publié une fiche contenant une liste de six mesures de sécurité fondamentales qui peuvent servir de point de départ pour se conformer à la directive NIS 2, sous le lien suivant : https://assets.ilr.lu/NISS/Documents/ILRLU-970684412-71.pdf

35 Par exemple pour les entreprises qui ont juste dépassé les seuils d'un maximum de 20 %

Les paramètres et les modalités des notifications des incidents ayant un impact important sur la fourniture de service peuvent être précisés par l'autorité compétente par voie de règlement ou de circulaire.

Le simple fait de notifier un incident n'accroît pas la responsabilité de l'entité qui est à l'origine de la notification.

Le tableau suivant résume les obligations de notification des entités importantes et essentielles :

Mécanisme	*À fournir à l'autorité compétente*	*Entité essentielle*	*Entité importante*
Ex-ante	Mesures de sécurité mises en place	Oui	Non
Ex-post	Notification des incidents importants	Oui	Oui
Ex-post	Après l'incident important ou sur demande (voir explication ci-après)	Oui	Oui

Par conséquent, les entités « importantes » sont exemptées de la fourniture régulière de certains éléments, comme l'analyse des risques ou la description des mesures de sécurité en place, que les entités essentielles doivent fournir. Lors d'un incident important, il peut aussi s'avérer nécessaire pour les entités importantes de fournir des informations supplémentaires sur les mesures de sécurité mises en œuvre sur demande de l'ILR.

En cas de détection d'un incident important, l'entité concernée notifie sans retard injustifié, aux destinataires de leurs services les incidents importants susceptibles de nuire à la fourniture de ces services. L'entité signale, notamment toute information permettant à l'autorité compétente de déterminer si l'incident a un impact transfrontalier.[36] Dans ce contexte, par un souci de sécurité juridique, la Chambre des Métiers estime judicieux de définir plus clairement le terme « sans retard injustifié ».

Aux fins de la notification des incidents importants, les entités concernées doivent respecter, conformément à l'article 14, paragraphe 4 du projet de loi, les délais suivants :

- Une notification préliminaire (« Early warning ») doit être soumise à l'autorité compétente sans retard injustifié au plus tard 24 heures après avoir eu connaissance de l'incident important.
- Une notification d'incident (« Official incident notification ») qui met, le cas échéant à jour les informations et qui 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 doit être soumise dans les 72 heures après avoir eu connaissance de l'incident important.
- Après réception de la notification préliminaire et de la notification d'incident, l'autorité compétente ou le CSIRT peuvent demander à l'entité concernée de soumettre un rapport intermédiaire (Intermediate status report) sur les mises à jour pertinentes de la situation.
- Au plus tard un mois après la présentation de la notification d'incident important, un rapport final est soumis à l'autorité compétente, comprenant une description détaillée de l'incident, y compris sa gravité et son impact, le type de menace ou la cause profonde qui a probablement déclenché l'incident, les mesures d'atténuation appliquées en cours et le cas échéant, l'impact transfrontière de l'incident.

L'autorité compétente, en coopération avec le CSIRT, fournit une réponse à l'entité émettrice de la notification d'incident sans retard injustifiée et si possible dans les 24 heures suivant la réception de la notification préliminaire et à la demande de l'entité des orientations ou des conseils opérationnels sur la mise en œuvre d'éventuelles mesures d'atténuation.

2.2.5. *Utilisation de solutions d'authentification à plusieurs facteurs*

L'article 12, paragraphe 1er du projet de loi dispose que les entités concernées seront obligées de prendre les mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées

36 Selon le considérant 103 de la directive (UE) 2022/2555 l'obligation qui est faite aux entités d'informer les destinataires des cybermenaces importantes devrait être respectée par les entités dans toute la mesure du possible mais ne saurait les dispenser de l'obligation de prendre immédiatement, à leurs frais, les mesures appropriées pour prévenir ou remédier à toute menace pour la sécurité et pour rétablir le niveau normal de sécurité du service. La fourniture de telles informations aux destinataires du service au sujet des cybermenaces importantes devrait être gratuite et formulée dans un langage facile à comprendre.

pour gérer les risques qui menacent la sécurité de leurs réseaux et systèmes d'information que ces entités utilisent dans le cadre de leurs activités ou de la fourniture de leurs services.

L'article 12, paragraphe 2, points 8° et 10° du projet de loi exigent que les mesures de gestion des risques de cybersécurité se fondent sur une approche « tous risques » dans les domaines du chiffrement et d'authentification à plusieurs facteurs. L'ILR recommande aux entités de suivre les bonnes pratiques conformément aux normes européennes et internationales. La Chambre des Métiers estime cependant utile que l'autorité compétente publie une liste des mesures de sécurité à mettre en œuvre par les entités et des guides de bonnes pratiques pour chaque secteur précisant l'obligation d'utilisation de solutions d'authentification à plusieurs facteurs.

2.2.6. *Rôle des organes de direction et obligation de formation*

L'article 13 du projet de loi souligne le rôle actif des membres des organes de direction des entités en matière de cybersécurité :

- Les organes de direction des entités essentielles et importantes approuvent les mesures de gestion des risques prises en matière de cybersécurité.
- En outre, les organes de direction desdites entités sont obligés à superviser la mise en œuvre des mesures et pourront être tenus responsables en cas de violation de cette obligation.

Les membres des organes de direction des entités essentielles et importantes sont tenus à suivre régulièrement une formation et d'en offrir également 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.

Dans l'intérêt de la sécurité juridique, la Chambre des Métiers estime qu'il est indispensable, soit de préciser le contenu et la durée des formations nécessaires selon l'article 13 du projet de loi, soit de renvoyer à ce sujet vers un règlement grand-ducal à venir.

2.2.7. *Mesures de supervision et d'exécution des autorités compétentes*

Les articles 22 et 23 du projet de loi détaillent les mesures de supervision et d'exécution que les autorités compétentes prennent à l'égard des entités essentielles et importantes. Les entités essentielles sont soumises à un régime de supervision à part entière, ex ante et ex post, tandis que les entités importantes sont soumises à un régime de supervision léger uniquement ex post.

Les autorités compétentes ont le pouvoir de soumettre ces entités à :

- des inspections sur place et des contrôles à distance ;
- des audits de sécurité ;
- des scans de sécurité ;
- des demandes d'informations ;
- des demandes d'accès à des données et documents ;
- des demandes de preuves de mise en œuvre de politiques de cybersécurité ; et
- (uniquement pour les entités essentielles) des audits ad hoc, notamment lorsqu'ils sont justifiés en raison d'un incident important ou d'une violation du présent projet de loi par l'entité essentielle.

Lorsque les autorités compétentes exercent leurs pouvoirs d'exécution à l'égard des entités essentielles et importantes, elles possèdent les pouvoirs suivants :

- l'émission d'avertissements ;
- l'adoption d'instructions contraignantes ;
- l'ordonnance de mettre un terme à des comportements violant le projet de loi ;
- l'ordonnance de mises en conformité spécifiques ;
- l'ordonnance d'informer les personnes susceptibles d'être affectées par une cybermenace ;
- l'ordonnance de mettre en œuvre les recommandations ;
- l'ordonnance de rendre publics les aspects de violations du projet de loi ;
- l'imposition d'amendes administratives ; et

- (uniquement pour les entités essentielles) la désignation d'un responsable du contrôle du respect des articles 12 et 14 du projet de loi.

La Chambre des Métiers demande aux autorités compétentes d'adopter une approche collaborative et de conseiller les entreprises en la matière avant d'imposer des amendes administratives. Elle demande également au législateur et aux autorités compétentes de prévoir un délai de mise en conformité prolongé pour les entreprises entrant dans le champ d'application du projet de loi et qui ont de peu dépassé les seuils relatifs aux petites entreprises et qui sont ainsi devenues des entreprises moyennes au sens de l'annexe de la recommandation 2003/361/CE.[37] En effet, elles disposent de capacités limitées pendant leur phase de transition et doivent avant tout développer les compétences en la matière.

2.2.8. *Régime de sanctions*

Conformément à l'article 25 du projet de loi, l'autorité compétente peut frapper l'entité essentielle ou importante concernée en cas de violation des obligations prévus par les articles 11, paragraphe 4, 13, paragraphes 1 et 2, 15, 17 paragraphes 1er et 2, et 18, paragraphe 1er à 6 d'une ou de plusieurs sanctions suivantes :

- avertissement
- blâme
- 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

En cas de violation des articles 12 ou 14 du projet de loi par les entités essentielles, le montant maximal des amendes administratives s'élève à 10 millions d'euros ou 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.

En cas de violation des articles 12 ou 14 du projet de loi par les entités importantes, le montant maximal des amendes administratives s'élève à 7 millions d'euros ou 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.

Les autorités compétentes ont également le pouvoir d'assortir leur décision d'une astreinte pour contraindre une entité essentielle ou importante à mettre un terme à une violation du présent projet de loi. Le montant de l'astreinte par jour ne peut être supérieur à 250 euros, sans que le montant total imposé en raison du manquement constaté ne puisse dépasser 25 000 euros.

L'article 22, paragraphe 5 du projet de loi donne aux autorités compétentes le pouvoir de suspendre temporairement des certifications ou autorisations liées aux services fournis par l'entité essentielle, ou d'interdire temporairement à des responsables dirigeants de l'entité essentielle d'exercer leurs fonctions.

La Chambre des Métiers demande aux auteurs du projet de loi de prévoir obligatoirement une phase de mise en demeure qui laisse la possibilité à l'entité de remédier à d'éventuelles non-conformités constatées lors d'un contrôle et de prévoir un délai raisonnable avant un deuxième contrôle.

Elle demande par ailleurs d'établir des procédures standardisées et transparentes, p.ex. pour définir le déroulement des inspections sur place ou des contrôles à distance.

*

La Chambre des Métiers ne peut approuver le projet de loi lui soumis pour avis que sous la réserve expresse de la prise en considération de ses observations ci-avant formulées.

Luxembourg, le 10 décembre 2024

Pour la Chambre des Métiers

Le Directeur Général,
Tom WIRION

Le Président,
Tom OBERWEIS

37 Par exemple pour les entreprises qui ont juste dépassé les seuils d'un maximum de 20 %

Impression: CTIE – Division Imprimés et Fournitures de bureau