



N°8132

PROJET DE LOI

portant sur certaines modalités d'application et les sanctions du règlement (UE) n° 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) et portant modification de la loi modifiée du 4 juillet 2014 portant réorganisation de l'ILNAS

*

Chapitre 1^{er} – Autorités compétentes et représentation nationale

Art. 1^{er}. Autorité nationale de certification de cybersécurité

L'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services, ci-après « ILNAS », est désigné comme Autorité nationale de certification de cybersécurité responsable des tâches de supervision au sens de l'article 58 du règlement (UE) n° 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, et responsable des tâches de certification pour les certificats européens de cybersécurité du niveau d'assurance dit « élevé » visés à l'article 56 du règlement (UE) n° 2019/881 précité.

Art. 2. Groupe européen de certification de cybersécurité

L'ILNAS, en tant qu'Autorité nationale de certification de cybersécurité, participe au Groupe européen de certification de cybersécurité au sens de l'article 62 du règlement (UE) n° 2019/881 précité.

Art. 3. Comité national de certification de cybersécurité

(1) Un Comité national de certification de cybersécurité, ci-après « comité », est créé auprès du ministre ayant l'Economie dans ses attributions, dont la composition et l'organisation sont déterminées par règlement grand-ducal.

(2) Le comité a les missions suivantes :

- 1° conseiller le ministre en ce qui concerne le programme de travail glissant de l'Union européenne pour la certification européenne de cybersécurité ;
- 2° prendre position sur la politique de certification de cybersécurité de l'Union européenne ;
- 3° prendre position sur les schémas européens de certification de cybersécurité ;
- 4° prendre position sur la maintenance et le réexamen des schémas européens de certification de cybersécurité existants ;
- 5° informer les parties prenantes concernées, les entreprises du secteur des TIC, les fournisseurs de réseaux ou de services de communications électroniques accessibles au public, les PME, les opérateurs de services essentiels, les organisations de consommateurs, les experts universitaires en matière de cybersécurité ainsi que les autorités chargées de l'application de la loi et les autorités de contrôle de la protection des données du processus consultatif prévu à l'article 56, paragraphe 3, alinéa 3, lettre c), du règlement (UE) n° 2019/881 précité ;
- 6° conseiller le ministre, par schéma de certification, en ce qui concerne l'application des objectifs et éléments définis par le règlement (UE) n° 2019/881 précité qui sont pris en compte pour délivrer, en application de l'article 56, paragraphe 6, lettre a), dudit règlement (UE) n° 2019/881, un certificat de cybersécurité au niveau d'assurance dit « élevé ».

Chapitre 2 – Obligations

Section 1^{re} – Obligations générales d'information

Art. 4. Accès aux informations

Lorsque les produits, services et processus des technologies de l'information et de la communication (TIC) des titulaires de certificats de cybersécurité européens et des émetteurs de déclarations de conformité de l'Union européenne font mention de prix et conditions de vente ou de réalisation de la prestation, ces derniers doivent être indiqués de manière précise et non équivoque. Il doit aussi être indiqué si toutes les taxes et frais additionnels sont compris dans le prix.

Art. 5. Echanges avec l'Autorité nationale de certification de cybersécurité

(1) Les titulaires de certificats de cybersécurité européens, les émetteurs de déclarations de conformité de l'Union européenne et les organismes d'évaluation de la conformité donnent accès à l'Autorité nationale de certification de cybersécurité à tout document, toute personne, tout équipement, tout local, toute installation, tout site et tout moyen de transport dont elle a besoin pour pouvoir assurer ses tâches.

(2) Les titulaires de certificats de cybersécurité européens, les émetteurs de déclarations de conformité de l'Union européenne et les organismes d'évaluation de la conformité informent l'Autorité nationale de certification de cybersécurité par écrit dans un délai de soixante-douze heures après avoir eu connaissance d'une vulnérabilité ou irrégularité qui est susceptible

d'avoir une incidence sur le respect des exigences de sécurité liées à la certification d'un produit, d'un service ou d'un processus selon le règlement (UE) n° 2019/881 précité.

(3) Les officiers et agents de police judiciaire visés à l'article 10 du Code de procédure pénale et les personnes visées à l'article 14, paragraphe 1^{er}, de la loi modifiée du 4 juillet 2014 portant réorganisation de l'ILNAS ont accès aux locaux, installations, sites et moyens de transport assujettis à la présente loi et aux règlements pris en son exécution. Ils peuvent pénétrer de jour et de nuit, lorsqu'il existe des indices graves faisant présumer une infraction à la présente loi et à ses règlements d'exécution, dans les locaux, installations, sites et moyens de transport visés ci-dessus. Ils signalent leur présence au chef du local, de l'installation ou du site ou à celui qui le remplace. Celui-ci a le droit de les accompagner lors de la visite.

Section 2 – Les organismes d'évaluation de la conformité

Art. 6. Obligations des organismes d'évaluation de la conformité

(1) L'organisme d'évaluation de la conformité accrédité au sens de l'article 60 du règlement (UE) n° 2019/881 précité informe, dans un délai de soixante-douze heures, l'Autorité nationale de certification de cybersécurité de son accréditation.

(2) L'Autorité nationale de certification de cybersécurité doit toujours être tenue informée, dans un délai de soixante-douze heures, des certificats délivrés par l'organisme d'évaluation de la conformité dans le cadre de l'article 60 du règlement (UE) n° 2019/881 précité.

Chapitre 3 – L'Autorité nationale de certification de cybersécurité

Art. 7. Rôle de l'Autorité nationale de certification de cybersécurité

(1) L'Autorité nationale de certification de cybersécurité notifie tout organisme d'évaluation de la conformité accrédité à la Commission européenne, conformément à l'article 61 du règlement (UE) n° 2019/881 précité, et le cas échéant, autorisé au sens de l'article 58, paragraphe 7, lettre e), qui certifie des produits TIC, des services TIC et processus TIC, dans le cadre d'un schéma européen de certification de cybersécurité aux niveaux d'assurances déterminés en vertu de l'article 52 du règlement (UE) n° 2019/881 précité.

L'Autorité nationale de certification de cybersécurité peut présenter à la Commission européenne une demande visant à retirer de la liste des organismes d'évaluation de la conformité, les organismes d'évaluation de la conformité qui ont fait l'objet d'une notification dans le cadre d'un schéma européen de certification de cybersécurité, tel que définie dans l'article 61 du règlement (UE) n° 2019/881 précité sur demande de l'organisme d'évaluation de la conformité ou si l'organisme d'évaluation de la conformité n'est pas conforme aux exigences du règlement (UE) n° 2019/881 précité, des actes d'exécution pris en son exécution, des schémas européens de certification de cybersécurité correspondants et à la présente loi.

(2) Si l'Autorité nationale de certification de cybersécurité constate qu'un émetteur de déclarations de conformité de l'Union Européenne, telles que visées à l'article 53 du règlement

(UE) n° 2019/881 précité, a un comportement visé à l'article 8 et sanctionné par ce même article, elle invite l'émetteur de déclarations de conformité de l'Union Européenne à y remédier, dans les délais qu'elle détermine. Si passé ce délai, l'émetteur de déclarations de conformité de l'Union Européenne n'y a pas remédié, l'autorité nationale de certification de cybersécurité peut appliquer les sanctions administratives afférentes prévues à l'article 8.

(3) Si l'Autorité nationale de certification de cybersécurité constate qu'un titulaire de certificat de cybersécurité au niveau d'assurance dit « élémentaire », tel que défini à l'article 52 du règlement (UE) n° 2019/881 précité, a un comportement visé à l'article 9 et sanctionné par ce même article, elle invite le titulaire de certificat de cybersécurité à y remédier, dans les délais qu'elle détermine. Passé ce délai, l'Autorité nationale de certification de cybersécurité peut appliquer les sanctions administratives afférentes prévues à l'article 9.

(4) Si l'Autorité nationale de certification de cybersécurité constate qu'un titulaire de certificat de cybersécurité au niveau d'assurance dit « substantiel », tel que défini à l'article 52 du règlement (UE) n° 2019/881 précité, a un comportement visé à l'article 10 et sanctionné par ce même article, elle invite le titulaire de certificat de cybersécurité à y remédier, dans les délais qu'elle détermine. Si, passé ce délai, le titulaire de certificat n'y a pas remédié, l'Autorité nationale de certification de cybersécurité peut appliquer les sanctions administratives afférentes prévues à l'article 10.

(5) Si l'Autorité nationale de certification de cybersécurité constate qu'un titulaire de certificat de cybersécurité au niveau d'assurance dit « élevé », tel que défini à l'article 52 du règlement (UE) n° 2019/881 précité, a un comportement visé à l'article 11 et sanctionné par ce même article, elle invite le titulaire de certificat de cybersécurité à y remédier, dans les délais qu'elle détermine. Si, passé ce délai, le titulaire de certificat n'y a pas remédié, l'Autorité nationale de certification de cybersécurité peut appliquer les sanctions administratives afférentes prévues à l'article 11.

(6) Si l'Autorité nationale de certification de cybersécurité constate qu'un organisme d'évaluation de la conformité qui émet des certificats de cybersécurité européens aux niveaux d'assurance tels que définis à l'article 52 du règlement (UE) n° 2019/881 précité, a un comportement visé à l'article 12 et sanctionné par ce même article, elle invite l'organisme d'évaluation de la conformité à y remédier, dans les délais qu'elle détermine. Si, passé ce délai, l'organisme d'évaluation de la conformité n'y a pas remédié, l'Autorité nationale de certification de cybersécurité peut appliquer les sanctions administratives afférentes prévues à l'article 12.

(7) L'Autorité nationale de certification de cybersécurité peut procéder à tout moment à des vérifications dans le contexte de l'octroi du maintien ou du retrait d'un certificat de cybersécurité européen ou d'une publication d'une déclaration de conformité de l'Union européenne. L'Autorité nationale de certification de cybersécurité peut avoir recours à des experts externes pour effectuer ces vérifications. Les frais d'experts sont refacturés aux titulaires de certificats de cybersécurité européens, aux émetteurs de déclarations de conformité de l'Union européenne et aux organismes d'évaluation de la conformité.

(8) Les frais relatifs à la préparation des contrôles, les frais des contrôles proprement dits, ainsi que les frais relatifs à la rédaction des rapports de contrôle, sont refacturés aux entités supervisées prévues à l'article 58, paragraphe 7, du règlement (UE) n° 2019/881 précité. Le barème tarifaire, approuvé par le ministre, est publié sur le site électronique installé à cet effet par l'ILNAS.

(9) L'Autorité nationale de certification de cybersécurité peut collaborer avec d'autres autorités compétentes dans un autre Etat membre pour exécuter ses tâches de supervision.

(10) L'Autorité nationale de certification de cybersécurité peut, dès lors que c'est dans l'intérêt public, publier soit au Journal officiel du Grand-Duché de Luxembourg, soit dans un ou plusieurs journaux luxembourgeois ou étrangers, un retrait d'un certificat de cybersécurité européen.

Chapitre 4 – Sanctions

Art. 8. Sanctions administratives à l'encontre d'émetteurs de déclarations de conformité de l'Union européenne

(1) Le directeur de l'ILNAS peut infliger une amende administrative de 250 euros à 25 000 euros aux émetteurs de déclarations de conformité de l'Union européenne qui enfreignent :

- 1° l'article 53, paragraphe 1^{er}, du règlement (UE) n° 2019/881 précité, en produisant des déclarations de conformité d'un niveau autre que « élémentaire » ;
- 2° l'article 54, paragraphe 1^{er}, lettre e), du règlement (UE) n° 2019/881 précité, en publiant des déclarations de conformité alors que ce n'est pas prévu dans le schéma européen de certification ;
- 3° les dispositions du schéma européen de certification de cybersécurité concernant l'utilisation des labels et des marques conformément à l'article 54, paragraphe 1^{er}, lettre i), du règlement (UE) n° 2019/881 précité ;
- 4° l'article 53, paragraphe 2, du règlement (UE) n° 2019/881 précité et les dispositions du schéma européen de certification de cybersécurité concernant les contrôles préalables à la publication des déclarations de conformité des exigences relatives à l'article 54, paragraphe 1^{er}, lettre j), du règlement (UE) n° 2019/881 précité ;
- 5° les dispositions du schéma européen de certification de cybersécurité concernant les conséquences résultant du contrôle des exigences et ne mettent pas à jour les déclarations de conformité conformément à l'article 54, paragraphe 1^{er}, lettre l), du règlement (UE) n° 2019/881 précité ;
- 6° les dispositions du schéma européen de certification de cybersécurité concernant le traitement des vulnérabilités de cybersécurité non détectées précédemment conformément aux articles 54, paragraphe 1^{er}, lettre m), et 56, paragraphe 8, du règlement (UE) n° 2019/881 précité ;
- 7° les dispositions du schéma européen de certification de cybersécurité concernant le format ou le contenu des déclarations de conformité conformément à l'article 54, paragraphe 1^{er}, lettre p), du règlement (UE) n° 2019/881 précité ;
- 8° l'article 53, paragraphe 3 du règlement (UE) n° 2019/881 précité et les dispositions du schéma européen de certification de cybersécurité de l'article 54, paragraphe 1^{er}, lettre q), du règlement (UE) n° 2019/881 précité, concernant la disponibilité de la déclaration de conformité ;
- 9° l'article 55 du règlement (UE) n° 2019/881 précité, en ne mettant les informations supplémentaires spécifiées dans le schéma européen de certification de cybersécurité pas à disposition du public ou en ne les mettant pas à jour.

(2) L'Administration de l'enregistrement, des domaines et de la TVA est chargée du recouvrement des amendes qui lui sont communiquées par le directeur de l'administration compétente. Le recouvrement est poursuivi comme en matière d'enregistrement.

(3) Les décisions d'infliger une amende administrative en vertu du présent article sont susceptibles d'un recours en réformation à introduire devant le tribunal administratif, dans le délai de trois mois à compter de la notification.

Art. 9. Sanctions administratives à l'encontre de titulaires de certificats de cybersécurité au niveau d'assurance dit « élémentaire »

(1) Le directeur de l'ILNAS peut infliger une amende administrative de 250 euros à 25 000 euros aux titulaires de certificats de cybersécurité européens au niveau d'assurance dit « élémentaire » qui enfreignent :

- 1° les articles 55, paragraphe 1^{er}, lettres a), b), c) ou d), ou 55, paragraphe 2, du règlement (UE) n° 2019/881 précité, en ne mettant les informations supplémentaires spécifiées dans le schéma européen de certification de cybersécurité pas à disposition du public ou en ne les mettant pas à jour ;
- 2° les articles 52, paragraphe 2, et 54, paragraphe 1^{er}, lettre d), du règlement (UE) n° 2019/881 précité, en publiant des informations par rapport à leur certification sans spécifier le niveau d'assurance ;
- 3° les dispositions du schéma européen de certification de cybersécurité concernant l'utilisation des labels et des marques conformément à l'article 54, paragraphe 1^{er}, lettre i), du règlement (UE) n° 2019/881 précité ;
- 4° les dispositions du schéma européen de certification de cybersécurité concernant son champ d'application relatives à l'article 54, paragraphe 1^{er}, lettre a), du règlement (UE) n° 2019/881 précité, en ne mettant pas ces informations à disposition du public ;
- 5° les dispositions du schéma européen de certification de cybersécurité concernant le traitement des vulnérabilités de cybersécurité non détectées précédemment conformément aux articles 54, paragraphe 1^{er}, lettre m), et 56, paragraphe 8, du règlement (UE) n° 2019/881 précité ;
- 6° les dispositions du schéma européen de certification de cybersécurité concernant le format ou le contenu des certificats de cybersécurité européens conformément à l'article 54, paragraphe 1^{er}, lettre p), du règlement (UE) n° 2019/881 précité ;
- 7° les dispositions du schéma européen de certification de cybersécurité concernant la période de disponibilité de la documentation technique ou de toutes les autres informations pertinentes qui sont mises à disposition par le fabricant ou le fournisseur de produits TIC, services TIC ou processus TIC, conformément aux articles 53, paragraphe 3, et 54, paragraphe 1^{er}, lettre q), du règlement (UE) n° 2019/881 précité ;
- 8° les dispositions du schéma européen de certification de cybersécurité concernant la durée maximale de validité des certificats conformément à l'article 54, paragraphe 1^{er}, lettre r), du règlement (UE) n° 2019/881 précité ;
- 9° l'article 56, paragraphe 7, du règlement (UE) n° 2019/881 précité, en ne mettant pas à disposition de l'ILNAS ou de l'organisme d'évaluation de la conformité les informations nécessaires à une certification ;
- 10° l'article 56, paragraphe 8, du règlement (UE) n° 2019/881 précité, en n'informant pas l'ILNAS ou l'organisme d'évaluation de la conformité de vulnérabilités ou d'irrégularités susceptibles d'avoir une incidence sur son respect des exigences liées à la certification.

- (2) L'Administration de l'enregistrement, des domaines et de la TVA est chargée du recouvrement des amendes qui lui sont communiquées par le directeur de l'administration compétente. Le recouvrement est poursuivi comme en matière d'enregistrement.
- (3) Les décisions d'infliger une amende administrative en vertu du présent article sont susceptibles d'un recours en réformation à introduire devant le tribunal administratif, dans le délai de trois mois à compter de la notification.

Art. 10. Sanctions administratives à l'encontre de titulaires de certificats de cybersécurité au niveau d'assurance dit « substantiel »

- (1) Le directeur de l'ILNAS peut infliger une amende administrative de 250 euros à 25 000 euros aux titulaires de certificats de cybersécurité européens au niveau d'assurance dit « substantiel » qui enfreignent :
 - 1° les articles 55, paragraphe 1^{er}, lettres a), b), c) ou d), ou 55, paragraphe 2, du règlement (UE) n° 2019/881 précité, en ne mettant les informations supplémentaires spécifiées dans le schéma européen de certification de cybersécurité pas à disposition du public ou en ne les mettant pas à jour ;
 - 2° les articles 52, paragraphe 2, et 54, paragraphe 1^{er}, lettre d), du règlement (UE) n° 2019/881 précité, en publiant des informations par rapport à leur certification sans spécifier le niveau d'assurance ;
 - 3° les dispositions du schéma européen de certification de cybersécurité concernant l'utilisation des labels et des marques conformément à l'article 54, paragraphe 1^{er}, lettre i), du règlement (UE) n° 2019/881 précité ;
 - 4° les dispositions du schéma européen de certification de cybersécurité concernant son champ d'application relatives à l'article 54, paragraphe 1^{er}, lettre a), du règlement (UE) n° 2019/881 précité, en ne mettant pas ces informations à disposition du public ;
 - 5° les dispositions du schéma européen de certification de cybersécurité concernant le format ou le contenu des certificats de cybersécurité européens conformément à l'article 54, paragraphe 1^{er}, lettre p), du règlement (UE) n° 2019/881 précité ;
 - 6° les dispositions du schéma européen de certification de cybersécurité concernant la période de disponibilité de la documentation technique ou de toutes les autres informations pertinentes qui sont mises à disposition par le fabricant ou le fournisseur de produits TIC, services TIC ou processus TIC, conformément aux articles 53, paragraphe 3, et 54, paragraphe 1^{er}, lettre q), du règlement (UE) n° 2019/881 précité ;
 - 7° les dispositions du schéma européen de certification de cybersécurité concernant la durée maximale de validité des certificats conformément à l'article 54, paragraphe 1^{er}, lettre r), du règlement (UE) n° 2019/881 précité ;
 - 8° l'article 56, paragraphe 7, du règlement (UE) n° 2019/881 précité, en ne mettant pas à disposition de l'ILNAS ou de l'organisme d'évaluation de la conformité les informations nécessaires à une certification ;
 - 9° l'article 56, paragraphe 8, du règlement (UE) n° 2019/881 précité, en n'informant pas l'ILNAS ou l'organisme d'évaluation de la conformité de vulnérabilités ou

d'irrégularités susceptibles d'avoir une incidence sur son respect des exigences liées à la certification.

- (2) Le directeur de l'ILNAS peut infliger une amende administrative de 251 euros jusqu'à 50 000 euros aux titulaires de certificats de cybersécurité européen, au niveau d'assurance dit « substantiel » qui enfreignent les dispositions du schéma européen de certification de cybersécurité concernant le traitement des vulnérabilités de cybersécurité non détectées précédemment conformément aux articles 54, paragraphe 1^{er}, lettre m), et 56, paragraphe 8, du règlement (UE) n° 2019/881 précité.
- (3) L'Administration de l'enregistrement, des domaines et de la TVA est chargée du recouvrement des amendes qui lui sont communiquées par le directeur de l'administration compétente. Le recouvrement est poursuivi comme en matière d'enregistrement.
- (4) Les décisions d'infliger une amende administrative en vertu du présent article sont susceptibles d'un recours en réformation à introduire devant le tribunal administratif, dans le délai de trois mois à compter de la notification.

Art. 11. Sanctions administratives à l'encontre de titulaires de certificats de cybersécurité au niveau d'assurance dit « élevé »

- (1) Le directeur de l'ILNAS peut infliger une amende administrative de 250 euros à 25 000 euros aux titulaires de certificats de cybersécurité européens au niveau d'assurance dit « élevé » qui enfreignent :
 - 1° les articles 55, paragraphe 1^{er}, lettres a), b), c) ou d), ou 55, paragraphe 2, du règlement (UE) n° 2019/881 précité, en ne mettant les informations supplémentaires spécifiées dans le schéma européen de certification de cybersécurité pas à disposition du public ou en ne les mettant pas à jour ;
 - 2° les articles 52, paragraphe 2, et 54, paragraphe 1^{er}, lettre d), du règlement (UE) n° 2019/881 précité, en publiant des informations par rapport à leur certification sans spécifier le niveau d'assurance ;
 - 3° les dispositions du schéma européen de certification de cybersécurité concernant l'utilisation des labels et des marques conformément à l'article 54, paragraphe 1^{er}, lettre i), du règlement (UE) n° 2019/881 précité ;
 - 4° les dispositions du schéma européen de certification de cybersécurité concernant son champ d'application relatives à l'article 54, paragraphe 1^{er}, lettre a), du règlement (UE) n° 2019/881 précité, en ne mettant pas ces informations à disposition du public.
- (2) Le directeur de l'ILNAS peut infliger une amende administrative de 251 euros jusqu'à 500 000 euros aux titulaires de certificats de cybersécurité européens, au niveau d'assurance dit « élevé », qui enfreignent :
 - 1° les dispositions du schéma européen de certification de cybersécurité concernant le format ou le contenu des certificats de cybersécurité européens conformément à l'article 54, paragraphe 1^{er}, lettre p), du règlement (UE) n° 2019/881 précité ;
 - 2° les dispositions du schéma européen de certification de cybersécurité concernant la période de disponibilité de la documentation technique ou de toutes les autres informations pertinentes qui sont mises à disposition par le fabricant ou le

fournisseur de produits TIC, services TIC ou processus TIC, conformément aux articles 53, paragraphe 3, et 54, paragraphe 1^{er}, lettre q), du règlement (UE) n° 2019/881 précité ;

- 3° les dispositions du schéma européen de certification de cybersécurité concernant le traitement des vulnérabilités de cybersécurité non détectées précédemment conformément aux articles 54, paragraphe 1^{er}, lettre m), et 56, paragraphe 8, du règlement (UE) n° 2019/881 précité ;
- 4° les dispositions du schéma européen de certification de cybersécurité concernant la durée maximale de validité des certificats conformément à l'article 54, paragraphe 1^{er}, lettre r), du règlement (UE) n° 2019/881 précité ;
- 5° l'article 56, paragraphe 7, du règlement (UE) n° 2019/881 précité, en ne mettant pas à disposition de l'ILNAS ou de l'organisme d'évaluation de la conformité les informations nécessaires à une certification ;
- 6° l'article 56, paragraphe 8, du règlement (UE) n° 2019/881 précité, en n'informant pas l'ILNAS ou l'organisme d'évaluation de la conformité de vulnérabilités ou d'irrégularités susceptibles d'avoir une incidence sur son respect des exigences liées à la certification.

(3) L'Administration de l'enregistrement, des domaines et de la TVA est chargée du recouvrement des amendes qui lui sont communiquées par le directeur de l'administration compétente. Le recouvrement est poursuivi comme en matière d'enregistrement.

(4) Les décisions d'infliger une amende administrative en vertu du présent article sont susceptibles d'un recours en réformation à introduire devant le tribunal administratif, dans le délai de trois mois à compter de la notification.

Art. 12. Sanctions administratives à l'encontre d'organismes d'évaluation de la conformité

(1) Le directeur de l'ILNAS peut infliger une amende administrative de 250 euros à 25 000 euros aux organismes d'évaluation de la conformité qui certifient au niveau d'assurance dit « élémentaire » et qui enfreignent :

- 1° l'article 52, paragraphe 5, du règlement (UE) n° 2019/881 précité, en n'appliquant pas les activités d'évaluation appropriées lors d'une certification ;
- 2° l'article 56, paragraphe 4, du règlement (UE) n° 2019/881 précité, en ne respectant pas, lors de leur certification, les critères figurant dans les schémas de certification tels que définis dans l'article 54, paragraphe 1^{er}, lettres a), d), f), g), j), k), l), n) ;
- 3° l'article 63, paragraphes 1^{er} ou 2, du règlement (UE) n° 2019/881 précité, en n'acceptant pas ou ne traitant pas les réclamations en rapport avec un certificat de cybersécurité européen délivré par lui-même ;
- 4° l'annexe du règlement (UE) n° 2019/881 précité, en ne respectant pas les exigences auxquelles doivent satisfaire les organismes d'évaluation de la conformité telles que spécifiées ;
- 5° l'article 54, paragraphe 1^{er}, lettre i), du règlement (UE) n° 2019/881 précité et les dispositions du schéma européen de certification de cybersécurité en délivrant des certificats non conformes ;

- 6° l'article 56, paragraphe 5, du règlement (UE) n° 2019/881 précité ou l'article 56, paragraphe 6, en octroyant, renouvelant ou en retirant des certificats du schéma européen de certification de cybersécurité sans avoir le mandat ou sans disposer de l'accréditation requise.
- (2) Le directeur de l'ILNAS peut infliger une amende administrative de 251 euros jusqu'à 50 000 euros aux organismes d'évaluation de la conformité qui certifient au niveau d'assurance dit « substantiel » ou « élevé » et qui enfreignent l'article 63, paragraphes 1^{er} et 2, du règlement (UE) n° 2019/881 précité, en n'acceptant pas ou ne traitant pas les réclamations en rapport avec un certificat de cybersécurité européen délivré par lui-même.
- (3) Le directeur de l'ILNAS peut infliger une amende administrative de 251 euros jusqu'à 250 000 euros aux organismes d'évaluation de la conformité qui certifient au niveau d'assurance « substantiel » et qui enfreignent :
- 1° l'article 52, paragraphe 6, du règlement (UE) n° 2019/881 précité, en n'appliquant pas les activités d'évaluation appropriées lors d'une certification ;
 - 2° l'article 56, paragraphe 4, du règlement (UE) n° 2019/881 précité, en ne respectant pas, lors de leur certification, les critères figurant dans les schémas de certification tels que définis dans l'article 54, paragraphe 1^{er}, lettres a), d), f), g), j), k), l), n) ;
 - 3° l'article 60, paragraphe 1^{er}, du règlement (UE) n° 2019/881 précité, en octroyant, renouvelant ou en retirant des certificats du schéma européen de certification de cybersécurité sans avoir été accrédité ;
 - 4° l'annexe du règlement (UE) n° 2019/881 précité, en ne respectant pas les exigences auxquelles doivent satisfaire les organismes d'évaluation de la conformité telles que spécifiées ;
 - 5° l'article 54, paragraphe 1^{er}, lettre i), du règlement (UE) n° 2019/881 précité et les dispositions du schéma européen de certification de cybersécurité en délivrant des certificats non conformes.
- (4) Le directeur de l'ILNAS peut infliger une amende administrative de 251 euros jusqu'à 500 000 euros aux organismes d'évaluation de la conformité qui certifient au niveau d'assurance dit « élevé » et qui enfreignent :
- 1° l'article 52, paragraphe 7, du règlement (UE) n° 2019/881 précité, en n'appliquant pas les activités d'évaluation appropriées lors d'une certification ;
 - 2° l'article 56, paragraphe 5, du règlement (UE) n° 2019/881 précité ou l'article 56, paragraphe 6, en octroyant, renouvelant ou en retirant des certificats du schéma européen de certification de cybersécurité sans avoir le mandat ;
 - 3° l'annexe du règlement (UE) n° 2019/881 précité, en ne respectant pas les exigences auxquelles doivent satisfaire les organismes d'évaluation de la conformité telles que spécifiées ;
 - 4° l'article 54, paragraphe 1^{er}, lettre i), du règlement (UE) n° 2019/881 précité et les dispositions du schéma européen de certification de cybersécurité en délivrant des certificats non conformes.
- (5) L'Administration de l'enregistrement, des domaines et de la TVA est chargée du recouvrement des amendes qui lui sont communiquées par le directeur de l'administration compétente. Le recouvrement est poursuivi comme en matière d'enregistrement.

- (6) Les décisions d'infliger une amende administrative en vertu du présent article sont susceptibles d'un recours en réformation à introduire devant le tribunal administratif, dans le délai de trois mois à compter de la notification.

Art. 13. Sanctions pénales

Sont punis d'une amende de 251 euros jusqu'à 500 000 euros et d'une peine d'emprisonnement de huit jours à cinq ans ou d'une de ces peines seulement les titulaires de certificats de cybersécurité européens et les émetteurs de déclarations de conformité de l'Union européenne qui enfreignent :

- 1° l'article 58, paragraphe 8, lettre a), du règlement (UE) n° 2019/881 précité, en ne mettant pas à disposition de l'ILNAS toute information dont il a besoin pour l'exécution de ses tâches ;
- 2° l'article 58, paragraphe 8, lettre b), du règlement (UE) n° 2019/881 précité, en entravant les enquêtes de l'ILNAS.

Chapitre 5 – Dispositions modificatives

Art. 14. Modification de la loi modifiée du 4 juillet 2014 portant réorganisation de l'ILNAS

La loi modifiée du 4 juillet 2014 portant réorganisation de l'ILNAS est modifiée comme suit :

- 1° Dans l'ensemble de la loi, les termes « département de la confiance numérique » sont remplacés par les termes « Organisme luxembourgeois de la confiance numérique ».
- 2° A l'article 4, paragraphe 1^{er}, point 5°, le point final est remplacé par un point-virgule et un point 6° nouveau est ajouté *in fine*, libellé comme suit :

« 6° à faire fonction d'Autorité nationale de certification de cybersécurité responsable des tâches de supervision au sens de l'article 58 du règlement (UE) n° 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) et responsable des tâches de certification au sens de l'article 56, paragraphe 6, du règlement (UE) n° 2019/881 précité. »

Projet de loi adopté par la Chambre des Députés
en sa séance publique du 10 décembre 2024

Le Secrétaire général,

Le Président,

s. Laurent Scheeck

s. Claude Wiseler