

**N° 8132**

**CHAMBRE DES DEPUTES**

Session ordinaire 2022-2023

---

## **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 et portant modification de la loi modifiée du 4 juillet 2014 portant réorganisation de l'ILNAS**

\* \* \*

*Document de dépôt*

*Dépôt: le 3.1.2023*

\*

### **ARRETE GRAND-DUCAL DE DEPOT**

Nous HENRI, Grand-Duc de Luxembourg, Duc de Nassau,

Sur rapport de Notre Ministre de l'Économie et après délibération du Gouvernement en conseil;

Arrêtons:

*Article unique.* Notre Ministre de l'Économie est autorisé à déposer en Notre nom à la Chambre des Députés le 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 et portant modification de la loi modifiée du 4 juillet 2014 portant réorganisation de l'ILNAS.

Crans-Montana, le 23 décembre 2022

*Le Ministre de l'Économie,*

Franz FAYOT

HENRI

\*

I. Exposé des motifs	2
II. Texte du projet de loi	3
III. Commentaire des articles	9
IV. Fiche financière	12
V. Fiche d'impact	12
VI. Texte coordonné	15
VII. Règlement (UE) 2019/881	36

\*

## EXPOSE DES MOTIFS

L'importance de la cybersécurité a grandement évolué au cours de ces dernières années, passant d'un sujet d'experts à une menace ressentie par l'ensemble de la société civile.

Au Grand-Duché de Luxembourg, le secteur des Technologies de l'Information et de la Communication (TIC) fait partie intégrante de la politique de développement et de diversification. La pérennité des TIC est indispensable au développement du marché économique. En tant que technologie transversale, les TIC contribuent au bon fonctionnement d'autres secteurs, comme celui des transports, bancaire, de l'énergie, de l'éducation, de la recherche, etc.

Le législateur européen établit un nouveau mandat permanent pour l'ENISA (Agence de l'Union européenne pour la cybersécurité) et dote l'Union européenne d'un cadre pour la certification à l'échelle européenne des produits, services et processus liés aux TIC dans le but de garantir un niveau adéquat de cybersécurité des produits TIC, services TIC et processus TIC au sein des Etats membres, et ainsi dans le marché intérieur de l'Union européenne et afin d'éviter la fragmentation du marché intérieur des schémas de certification de cybersécurité souvent protectionnistes dans l'Union européenne.

Le présent projet de loi a pour objectif d'instituer les mesures d'application nationales 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), dénommé ci-après « règlement (UE) n° 2019/881 ».

En effet, ce projet de loi vise la mise en œuvre du règlement (UE) n° 2019/881 afin de légiférer au niveau national les questions nécessitant une intervention législative nationale, tel que la désignation de l'autorité nationale de certification de cybersécurité. Il a comme objectif d'exploiter les marges de manœuvres laissées au législateur national pour compléter et préciser certaines dispositions du règlement (UE) n° 2019/881 tel le rôle et les pouvoirs de l'autorité nationale de certification de cybersécurité en l'occurrence de l'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS) et du comité national de certification de cybersécurité ( ci-après le « comité » ). L'ILNAS est désigné « autorité nationale de certification de cybersécurité » et est chargé de réaliser les activités de supervision en matière de cybersécurité. Les activités d'accréditation et de certification étant incompatibles au sein d'une même entité, étant donné que l'OLAS, au sein de l'ILNAS, est l'organisme luxembourgeois d'accréditation et de surveillance, l'ILNAS ne peut pas exercer de tâche de certification. Sa fonction est donc strictement limitée à la tâche de supervision, raison pour laquelle la tâche de certification sera confiée à une autre entité nationale ou à un autre Etat membre de l'Union européenne. Les mesures nationales visées par les articles 58, 60, 61, 63, 64 et 65 du règlement (UE) n° 2019/881 s'appliquent à partir du 28 juin 2021.

\*

## TEXTE DU PROJET DE LOI

### CHAPITRE 1<sup>er</sup> – Autorités compétentes et représentation nationale.

#### Art. 1<sup>er</sup>. 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 (ci-après « autorité nationale ») au sens de l'article 58 du règlement (UE) n° 2019/881, responsable des tâches de supervision.

#### Art. 2. Groupe européen de certification de cybersécurité

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

#### 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 :

- a) aviser sur le programme de travail glissant de l'Union européenne pour la certification européenne de cybersécurité;
- b) prendre position sur la politique de certification de cybersécurité de l'Union européenne ;
- c) prendre position sur les schémas européens de certification de cybersécurité ;
- d) prendre position sur la maintenance et le réexamen des schémas européens de certification de cybersécurité existants ;
- e) informer les parties prenantes concernées du processus consultatif prévu à l'article 56 paragraphe 3 point c) du règlement (UE) n° 2019/881 ;
- f) échanger des informations sur les évolutions dans le domaine de la cybersécurité.

### CHAPITRE 2 – Obligations.

#### Section 1<sup>re</sup> – Obligations générales d'information.

#### Art. 4. Accès aux informations

Lorsque les produits, services et processus 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

(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 toute information, document, personne, équipement et local dont elle a besoin pour pouvoir assurer sa tâche de supervision.

(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 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.

#### Section 2 – Obligations au secret professionnel.

#### Art. 6. Secret professionnel

(1) Toute personne chargée ou ayant été chargée de procéder à des audits par l'autorité nationale auprès des fabricants ou fournisseurs de produits TIC, services TIC et processus TIC est tenue au secret professionnel et passible des peines prévues à l'article 10, paragraphe 6 de la présente loi.

(2) L'obligation au secret cesse lorsque la révélation d'un renseignement est autorisée ou imposée par ou en vertu d'une disposition législative, même antérieure à la présente loi.

(3) L'obligation au secret professionnel n'existe pas à l'égard de l'autorité nationale et de l'organisme national d'accréditation agissant dans le cadre de ses missions et compétences légales.

### Section 3 – Les organismes d'évaluation de la conformité.

#### **Art. 7. Obligations des organismes d'évaluation de la conformité**

(1) L'organisme d'évaluation de la conformité qui souhaite certifier des produits TIC, des services TIC et processus TIC, dans le cadre d'un schéma européen de certification de cybersécurité, doit être accrédité au sens de l'article 60 du règlement (UE) n° 2019/881 et répondre aux exigences définies dans l'Annexe du règlement (UE) n° 2019/881.

(2) L'organisme d'évaluation de la conformité accrédité au sens de l'article 60 du règlement (UE) n° 2019/881, en informe dans un délai de soixante-douze heures l'autorité nationale.

(3) L'organisme d'évaluation de la conformité doit se soumettre au contrôle, par l'autorité nationale, des exigences spécifiques ou supplémentaires qui peuvent être définies dans les schémas européens de certification de cybersécurité, en application de l'article 54, paragraphe 1, point f) du règlement (UE) n° 2019/881, aux fins de notification et de supervision.

(4) L'autorité nationale 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.

### **CHAPITRE 3 – L'autorité nationale.**

#### **Art. 8. Rôle de l'autorité nationale**

(1) L'autorité nationale notifie, conformément à l'article 61 du règlement (UE) n° 2019/881, à la Commission européenne tout organisme d'évaluation de la conformité accrédité, et le cas échéant, autorisé au sens de l'article 58, paragraphe 7, point 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.

L'autorité nationale 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 défini dans l'article 61 du règlement (UE) n° 2019/881 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, 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 constate que les activités d'un organisme d'évaluation de la conformité qui émet des certificats de cybersécurité européens au niveau d'assurance dit « élémentaire » et « substantiel », tels que définis dans l'article 52 du règlement (UE) n° 2019/881, n'est pas conforme aux exigences du règlement (UE) n° 2019/881, des actes d'exécution pris en son exécution, des schémas européens de certification de cybersécurité correspondants et à la présente loi, elle invite l'organisme d'évaluation de la conformité à se conformer à ces exigences, dans les délais qu'elle détermine. Si, passé ce délai, l'organisme d'évaluation de la conformité ne s'est pas conformé à ces exigences, l'autorité nationale peut appliquer des sanctions administratives prévues à l'article 9 de la présente loi, respectivement dénonce les infractions par rapport à l'article 10 de la présente loi.

(3) Si l'autorité nationale constate que les activités d'un organisme d'évaluation de la conformité, tel que défini dans l'article 56 paragraphe 6 a) ou b) du règlement (UE) n° 2019/881, qui émet des certificats de cybersécurité européens au niveau d'assurance dit « élevé », tels que définis dans l'article 52 du règlement (UE) n° 2019/881, ne sont pas conformes aux exigences du règlement (UE) n° 2019/881, des actes d'exécution pris en son exécution, des schémas européens de certification de

cybersécurité correspondants et à la présente loi, elle invite l'organisme d'évaluation de la conformité à se conformer à ces exigences, dans les délais qu'elle détermine. Si, passé ce délai, l'organisme d'évaluation de la conformité ne s'est pas conformé à ces exigences, l'autorité nationale peut décider des sanctions administratives prévues à l'article 9 de la présente loi, respectivement dénonce les infractions par rapport à l'article 10 de la présente loi.

(4) Si l'autorité nationale constate que les activités d'un titulaire de certificats ou d'un émetteur d'une déclaration de conformité ne sont pas conformes aux exigences du règlement (UE) n° 2019/881, des actes d'exécution pris en son exécution, des schémas européens de certification de cybersécurité correspondants et à la présente loi, elle invite le titulaire de certificats respectivement l'émetteur d'une déclaration de conformité à se conformer, dans les délais qu'elle détermine. Si, passé ce délai, le titulaire de certificats ou l'émetteur d'une déclaration de conformité ne s'est pas conformé à ces exigences, l'autorité nationale peut leur appliquer des sanctions administratives prévues à l'article 9 de la présente loi, respectivement dénonce les infractions par rapport à l'article 10 de la présente loi.

(5) En cas de constatation d'une violation grave par un titulaire de certificats, d'un émetteur d'une déclaration de conformité ou d'un organisme d'évaluation de la conformité des exigences fixées dans le règlement (UE) n° 2019/881, des actes d'exécution pris en son exécution, des schémas européens de certification de cybersécurité, à la législation européenne applicable et à la présente loi, l'autorité nationale peut en informer à telles fins que de droit les ministères compétents. Les rapports établis à l'attention de l'autorité nationale peuvent être communiqués à ces autorités, dans la mesure où le titulaire de certificats et l'émetteur de déclarations de conformité en a reçu communication par l'autorité nationale.

(6) L'autorité nationale peut procéder à tout moment, aussi sur demande dûment justifiée de personnes intéressées, 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 peut avoir recours à des experts externes pour effectuer ces vérifications. Les frais d'experts sont couverts par 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.

(7) L'autorité nationale peut collaborer avec d'autres autorités compétentes dans un autre Etat membre pour exécuter ses tâches de supervision. Si l'autorité nationale rencontre des difficultés dans l'exercice de ses pouvoirs de contrôle, elle peut requérir l'assistance de la Police grand-ducale en vertu des dispositions contenues aux articles 27 et ss dans la loi du 18 juillet 2018 sur la Police Grand-Ducale.

(8) L'autorité nationale 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 9. Sanctions administratives**

(1) Le chef de l'administration 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 :

- a) l'article 53, paragraphe 1<sup>er</sup>, du règlement (UE) n° 2019/881 en produisant des déclarations de conformité d'un niveau autre que « élémentaire » ;
- b) l'article 54, paragraphe 1<sup>er</sup>, point e<sup>o</sup>, du règlement (UE) n° 2019/881, en publiant des déclarations de conformité alors que ce n'est pas prévu dans le schéma européen de certification ;
- c) les dispositions du schéma européen de certification de cybersécurité concernant l'utilisation des labels et des marques conformément à l'article 54, paragraphe 1<sup>er</sup>, point i<sup>o</sup>, du règlement (UE) n° 2019/881 ;
- d) l'article 53, paragraphe 2, du règlement (UE) n° 2019/881 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<sup>er</sup>, point j<sup>o</sup>, du règlement (UE) n° 2019/881 ;

- e) 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<sup>er</sup>, point l<sup>o</sup>, du règlement (UE) n° 2019/881 ;
- f) 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<sup>er</sup>, point m<sup>o</sup>, et 56, paragraphe 8, du règlement (UE) n° 2019/881 ;
- g) 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<sup>er</sup>, point p<sup>o</sup>, du règlement (UE) n° 2019/881 ;
- h) l'article 53, paragraphe 3 du règlement (UE) n° 2019/881, et les dispositions du schéma européen de certification de cybersécurité de l'article 54, paragraphe 1<sup>er</sup>, point q<sup>o</sup>, du règlement (UE) n° 2019/881, concernant la disponibilité de la déclaration de conformité;
- i) l'article 55 du règlement (UE) n° 2019/881, en ne mettant les informations supplémentaires spécifiées dans le schéma européen de certification de cybersécurité pas à disposition du public, respectivement en ne les mettant pas à jour ;
- j) l'article 58, paragraphe 8, point a<sup>o</sup>, du règlement (UE) n° 2019/881 en ne mettant pas à disposition de l'ILNAS toute information dont elle a besoin pour l'exécution de ses tâches ;
- k) l'article 58, paragraphe 8, point b<sup>o</sup>, du règlement (UE) n° 2019/881, en entravant les enquêtes de l'ILNAS.

(2) Le chef de l'administration de l'ILNAS peut infliger une amende administrative de 250 euros à 25.000 euros aux titulaires de certificats de cybersécurité européens qui enfreignent :

- a) les articles 55, paragraphe 1<sup>er</sup>, points a<sup>o</sup>, b<sup>o</sup>, c<sup>o</sup>, ou d<sup>o</sup>, ou 55, paragraphe 2, du règlement (UE) n° 2019/881, en ne mettant les informations supplémentaires spécifiées dans le schéma européen de certification de cybersécurité pas à disposition du public, respectivement en ne les mettant pas à jour ;
- b) les articles 52, paragraphe 2, et 54, paragraphe 1<sup>er</sup>, point d<sup>o</sup>, du règlement (UE) n° 2019/881, en publiant des informations par rapport à leur certification sans spécifier le niveau d'assurance ;
- c) les dispositions du schéma européen de certification de cybersécurité concernant l'utilisation des labels et des marques conformément à l'article 54, paragraphe 1<sup>er</sup>, point i<sup>o</sup>, du règlement (UE) n° 2019/881 ;
- d) les dispositions du schéma européen de certification de cybersécurité concernant son champ d'application relatives à l'article 54, paragraphe 1<sup>er</sup>, point a<sup>o</sup>, du règlement (UE) n° 2019/881, en ne mettant pas ces informations à disposition du public.

(3) Le chef de l'administration de l'ILNAS peut infliger une amende administrative de 250 euros à 25 000 euros aux titulaires de certificats de cybersécurité européens qui, au niveau d'assurance dit « élémentaire », 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<sup>er</sup>, point m<sup>o</sup>, et 56, paragraphe 8, du règlement (UE) n° 2019/881.

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

- a) 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<sup>er</sup>, point p<sup>o</sup>, du règlement (UE) n°2019/881 ;
- b) les disposition du schéma européen de certification de cybersécurité concernant la période de disponibilité de la documentation technique ou de toutes les autres informations pertinentes qui doivent être mises à disposition par le fabricant ou le fournisseur de produits TIC, services TIC ou processus TIC, conformément aux articles 53, paragraphe 3, et 54, paragraphe 1<sup>er</sup>, point q<sup>o</sup>, du règlement (UE) n° 2019/881;

- c) les dispositions du schéma européen de certification de cybersécurité concernant la durée maximale de validité des certificats conformément à l'article 54, paragraphe 1<sup>er</sup>, point r<sup>o</sup>, du règlement (UE) n° 2019/881 ;
- d) l'article 56, paragraphe 7, du règlement (UE) n° 2019/881, en ne mettant pas à disposition de l'ILNAS respectivement de l'organisme d'évaluation de la conformité les informations nécessaires à une certification ;
- e) l'article 56, paragraphe 8, du règlement (UE) n° 2019/881, en n'informant pas l'ILNAS respectivement 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 ;
- f) l'article 58, paragraphe 8, point a<sup>o</sup>, du règlement (UE) n° 2019/881, en ne mettant pas à disposition de l'ILNAS toute information dont elle a besoin pour l'exécution de ses tâches ;
- g) l'article 58, paragraphe 8, point b<sup>o</sup>, du règlement (UE) n° 2019/881, en entravant les enquêtes de l'ILNAS.

(5) Le chef de l'administration 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:

- a) l'article 52, paragraphe 5 du règlement (UE) n° 2019/881 en n'appliquant pas les activités d'évaluation appropriées lors d'une certification ;
- b) l'article 56, paragraphe 4, du règlement (UE) n° 2019/881 en ne respectant pas, lors de leur certification, les critères figurant dans les schémas de certification tel que définis dans les articles 54, paragraphe 1<sup>er</sup>, point a<sup>o</sup>, paragraphe 1<sup>er</sup>, point d<sup>o</sup>, paragraphe 1<sup>er</sup>, point f<sup>o</sup>, paragraphe 1<sup>er</sup>, point g<sup>o</sup>, paragraphe 1<sup>er</sup>, point j<sup>o</sup>, paragraphe 1<sup>er</sup>, point k<sup>o</sup>, paragraphe 1<sup>er</sup>, point l<sup>o</sup>, paragraphe 1<sup>er</sup>, point n<sup>o</sup> ;
- c) l'article 58, paragraphe 8, point a<sup>o</sup>, du règlement (UE) n° 2019/881 en ne mettant pas à disposition de l'ILNAS toute information dont elle a besoin pour l'exécution de ses tâches ;
- d) l'article 58, paragraphe 8, point b<sup>o</sup>, du règlement (UE) n° 2019/881 en entravant les enquêtes de l'ILNAS ;
- e) l'article 63, paragraphes 1<sup>er</sup> ou 2, du règlement (UE) n° 2019/881, en n'acceptant pas respectivement ne traitant pas les réclamations en rapport avec un certificat de cybersécurité européen délivré par lui-même ;
- f) l'annexe du règlement (UE) n° 2019/881, en ne respectant pas les exigences auxquelles doivent satisfaire les organismes d'évaluation de la conformité telles que spécifiées ;
- g) l'article 54, paragraphe 1<sup>er</sup>, point i<sup>o</sup>, du règlement (UE) n° 2019/881 et les dispositions du schéma européen de certification de cybersécurité en délivrant des certificats non conformes ;
- h) l'article 56, paragraphe 5, du règlement (UE) n° 2019/881 respectivement l'article 56, paragraphe 6, en octroyant, renouvelant ou en retirant des certificats du schéma européen de certification de cybersécurité sans avoir le mandat, respectivement sans disposer de l'accréditation requise.

(6) 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.

(7) 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 pénales**

(1) Sont punis d'une amende de 251 euros jusqu'à 25 000 euros et d'une peine d'emprisonnement de huit jours à 6 mois ou d'une de ces peines seulement les titulaires de certificats de cybersécurité européen, au niveau d'assurance dit 'substantiel', qui enfreignent :

- a) 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<sup>er</sup>, point m<sup>o</sup>, et 56, paragraphe 8, du règlement (UE) n° 2019/881 ;
- b) l'article 58, paragraphe 8, point a<sup>o</sup>, du règlement (UE) n° 2019/881, en ne mettant pas à disposition de l'ILNAS toute information dont elle a besoin pour l'exécution de ses tâches ;

c) l'article 58, paragraphe 8, point b°, du règlement (UE) n° 2019/881, en entravant les enquêtes de l'ILNAS.

(2) Sont punis d'une amende de 251 euros jusqu'à 500 000 euros et d'une peine d'emprisonnement de huit jours à 5 ans ou d'une de ces peines seulement, les titulaires de certificats de cybersécurité européens, au niveau d'assurance dit 'élevé', qui enfreignent :

- a) 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<sup>er</sup>, point p°, du règlement (UE) n° 2019/881 ;
- b) 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 doivent être 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<sup>er</sup>, point q°, du règlement (UE) n° 2019/881;
- c) 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<sup>er</sup>, point m°, et 56, paragraphe 8, du règlement (UE) n° 2019/881 ;
- d) les dispositions du schéma européen de certification de cybersécurité concernant la durée maximale de validité des certificats conformément à l'article 54, paragraphe 1<sup>er</sup>, point r°, du règlement (UE) n° 2019/881 ;
- e) l'article 56, paragraphe 7, du règlement (UE) n° 2019/881, en ne mettant pas à disposition de l'ILNAS respectivement de l'organisme d'évaluation de la conformité les informations nécessaires à une certification ;
- f) l'article 56, paragraphe 8, du règlement (UE) n° 2019/881, en n'informant pas l'ILNAS respectivement 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 ;
- g) l'article 58, paragraphe 8, point a°, du règlement (UE) n° 2019/881, en ne mettant pas à disposition de l'ILNAS toute information dont elle a besoin pour l'exécution de ses tâches.
- h) l'article 58, paragraphe 8, point b°, du règlement (UE) n° 2019/881, en entravant les enquêtes de l'ILNAS.

(3) Sont punis d'une amende de 251 euros jusqu'à 25 000 euros et d'une peine d'emprisonnement de huit jours à 6 mois ou d'une de ces peines seulement aux organismes d'évaluation de la conformité européens qui certifient au niveau d'assurance dit 'substantiel' ou 'élevé', et qui enfreignent l'article 63, paragraphes 1<sup>er</sup> et 2, du règlement (UE) n° 2019/881, en n'acceptant pas respectivement ne traitant pas les réclamations en rapport avec un certificat de cybersécurité européen délivré par lui-même.

(4) Sont punis d'une amende de 251 euros jusqu'à 250 000 euros et d'une peine d'emprisonnement de huit jours à 2 ans ou d'une de ces peines seulement les organismes d'évaluation de la conformité européens qui certifient au niveau d'assurance 'substantiel', et enfreignent :

- a) l'article 52, paragraphe 6, du règlement (UE) n° 2019/881 en n'appliquant pas les activités d'évaluation appropriées lors d'une certification ;
- b) l'article 56, paragraphe 4, du règlement (UE) n° 2019/881 en ne respectant pas, lors de leur certification, les critères figurant dans les schémas de certification tel que définis dans les articles 54, paragraphe 1<sup>er</sup>, point a°, paragraphe 1<sup>er</sup>, point d°, paragraphe 1<sup>er</sup>, point f°, paragraphe 1<sup>er</sup>, point g°, paragraphe 1<sup>er</sup>, point j°, paragraphe 1<sup>er</sup>, point k°, paragraphe 1<sup>er</sup>, point l°, paragraphe 1<sup>er</sup>, point n° ;
- c) l'article 60, paragraphe 1, du règlement (UE) n° 2019/881 en octroyant, renouvelant ou en retirant des certificats du schéma européen de certification de cybersécurité sans avoir été accrédité ;
- d) l'article 58, paragraphe 8, point a°, du règlement (UE) n° 2019/881 en ne mettant pas à disposition de l'ILNAS toute information dont elle a besoin pour l'exécution de ses tâches ;
- e) l'article 58, paragraphe 8, point b°, du règlement (UE) n° 2019/881 en entravant les enquêtes de l'ILNAS;
- f) l'annexe du règlement (UE) n° 2019/881, en ne respectant pas les exigences auxquelles doivent satisfaire les organismes d'évaluation de la conformité telles que spécifiées;

g) l'article 54, paragraphe 1<sup>er</sup>, point i°, du règlement (UE) n° 2019/881 et les dispositions du schéma européen de certification de cybersécurité en délivrant des certificats non conformes.

(5) Sont punis d'une amende de 251 euros jusqu'à 500 000 euros et d'une peine d'emprisonnement de huit jours à 5 ans ou d'une de ces peines seulement tous organismes d'évaluation de la conformité qui certifient au niveau d'assurance dit 'élevé' et qui enfreignent :

- a) l'article 52, paragraphe 7, du règlement (UE) n° 2019/881 en n'appliquant pas les activités d'évaluation appropriées lors d'une certification ;
- b) l'article 56, paragraphe 5, du règlement (UE) n° 2019/881 respectivement l'article 56, paragraphe 6, en octroyant, renouvelant ou en retirant des certificats du schéma européen de certification de cybersécurité sans avoir le mandat;
- c) l'article 58, paragraphe 8, point a°, du règlement (UE) n° 2019/881 en ne mettant pas à disposition de l'ILNAS toute information dont elle a besoin pour l'exécution de ses tâches ;
- d) l'article 58, paragraphe 8, point b°, du règlement (UE) n° 2019/881 en entravant les enquêtes de l'ILNAS ;
- e) l'annexe du règlement (UE) n° 2019/881, en ne respectant pas les exigences auxquelles doivent satisfaire les organismes d'évaluation de la conformité telles que spécifiées;
- f) l'article 54, paragraphe 1<sup>er</sup>, point i°, du règlement (UE) n°2019/881 et les dispositions du schéma européen de certification de cybersécurité en délivrant des certificats non conformes.

(6) Est puni d'une amende de 251 euros à 500 000 euros et d'une peine d'emprisonnement de huit jours à cinq ans ou d'une de ces peines seulement toute personne qui ne s'est pas conformée au secret professionnel prévu par l'article 6, paragraphe 1<sup>er</sup>.

#### **CHAPITRE 5 – Dispositions modificatives.**

##### **Art 11. 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, au point 5°, de la même loi, le point final est remplacé par un point-virgule et à la fin du point 5°, un nouveau point 6° au libellé suivant est inséré :

« 6° à assumer les tâches d'autorité nationale de certification de cybersécurité 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 ».

\*

### **COMMENTAIRE DES ARTICLES**

#### CHAPITRE 1<sup>er</sup> – Autorités compétentes et représentation nationale

##### *Ad article 1<sup>er</sup> – Autorité nationale de certification de cybersécurité*

L'article 1<sup>er</sup> du projet de loi désigne l'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et des services (ci-après « l'ILNAS ») en tant qu'autorité nationale de certification de cybersécurité 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) [ci-après, le « règlement n° 2019/881 »].

Etant l'autorité nationale de certification de cybersécurité, l'ILNAS assure les tâches de supervision des organismes d'évaluation de la conformité, des émetteurs de déclarations de conformité de l'Union européenne et des titulaires de certificats de cybersécurité européens visés par le règlement n° 2019/881.

*Ad article 2 – Groupe européen de certification de cybersécurité*

L'article 2 précise que l'ILNAS est membre du groupe européen de certification de cybersécurité au sens de l'article 62 du règlement (UE) n° 2019/881 (ci-après « le GECC »). L'ILNAS représente le Grand-Duché du Luxembourg au sein de l'Union européenne et participe à toutes les activités liées à ses missions.

*Ad article 3 – Comité national de certification de cybersécurité*

Cet article prévoit la création d'un comité national de certification de cybersécurité qui est placé sous l'autorité du Ministère de l'Economie.

La certification européenne de cybersécurité est un moyen efficace pour renforcer la confiance dans le domaine de la cybersécurité. L'échange d'informations entre les acteurs étatiques principaux qui sont le ministère de l'Économie et le ministère d'État est important pour d'une part garantir que les certificats répondent aux besoins de notre pays et d'autre part que tout événement susceptible d'avoir un impact négatif sur l'économie nationale respectivement les infrastructures critiques soit échangé entre les parties concernées.

La composition et l'organisation sont déterminées par règlement grand-ducal.

## CHAPITRE 2 – Obligations

Section 1<sup>re</sup> – Obligations générales d'information*Ad article 4 – Accès aux informations*

La certification de cybersécurité européenne a pour but de renforcer la confiance de toutes les parties prenantes dans les produits services et processus certifiés. Pour ne pas nuire à cet effet positif pour l'économie, il est nécessaire que les titulaires de certificats de cybersécurité européens et les émetteurs de déclarations de conformité de l'Union européenne affichent clairement les prix ainsi que les conditions de vente pour leurs produits, services et processus.

*Ad article 5 – Echanges avec l'autorité nationale*

Le paragraphe 1 énonce la nécessité pour les titulaires de certificats de cybersécurité européens, les émetteurs de déclarations de conformité de l'Union européenne et les organismes de déclarations de conformité de donner aux autorités compétentes un accès à toute information nécessaire pour démontrer et vérifier la conformité de leurs produits TIC, services TIC et processus TIC aux exigences du règlement (UE) n° 2019/881 et par rapport aux exigences énoncées dans les schémas de certification et le règlement. La vérification de cette conformité est le garant de la confiance introduite par la certification de cybersécurité européenne.

Le paragraphe 2 énonce la nécessité pour 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 d'informer l'ILNAS de toute vulnérabilité ou irrégularité détectée ultérieurement qui est susceptible d'avoir une incidence sur le respect des exigences du règlement (UE) n° 2019/881, des schémas européens de certification de cybersécurité, à la législation européenne applicable et à la présente loi, pour tous les des produits TIC, services TIC et processus TIC couverts par un certificat de cybersécurité européen ou une déclaration de conformité de l'Union européenne. Il importe de détecter ces vulnérabilités et irrégularités, qui auront un impact sur toutes les parties prenantes, notamment les citoyens et entreprises, et de permettre à l'ILNAS d'effectuer ses missions de surveillance et de contrôle qui pourra vérifier la remédiation aux vulnérabilités ou irrégularités pour rapidement réduire le risque global en matière de cybersécurité et, par-là, de renforcer la cybersécurité.

## Section 2 – Obligations du secret professionnel

*Ad article 6 – Secret professionnel*

Tous les acteurs doivent se tenir au secret professionnel pour protéger leurs activités et tous les utilisateurs de certificats de cybersécurité européen et de déclarations de conformité de l'Union européenne.

L'article 10 punit spécifiquement le non-respect du secret professionnel par des sanctions pénales en veillant au caractère effectif, proportionné et dissuasif des sanctions applicables.

### Section 3 – Les organismes d'évaluation de la conformité

#### *Ad article 7 – Obligations des organismes d'évaluation de la conformité*

En vertu de l'article 60 du règlement (UE) n° 2019/881, les organismes d'évaluation de la conformité accrédités doivent en informer l'ILNAS, se soumettre à leur contrôle et le tenir informé des certificats délivrés.

### CHAPITRE 3 – L'autorité nationale

#### *Ad article 8 – Rôle de l'autorité nationale*

Comme autorité nationale de certification de cybersécurité et membre du groupe européen de certification de cybersécurité, l'ILNAS dispose des pouvoirs d'investigation et d'enquête prévus dans le règlement (UE) n° 2019/881, dans les règlements pris en son exécution et dans les schémas européens de certification de cybersécurité. Pour assurer la conformité de toutes ces exigences, renforcer la confiance et partant améliorer leur résilience générale face aux cyberattaques, l'ILNAS devra avoir les pouvoirs et les moyens nécessaires pour investiguer des non-conformités potentielles et éviter les impacts de matérialisation de risques éventuels, causant des perturbations aux personnes physiques ou morales ou au bon fonctionnement de l'économie nationale. Afin d'assurer ce rôle, l'ILNAS peut inviter les titulaires de certificats de cybersécurité européens niveau « élémentaire », « substantiel » et « élevé », les organismes d'évaluation de la conformité de certificats de cybersécurité européen au niveau de l'octroi, du renouvellement et du retrait de la certification et les émetteurs de déclarations de conformité de l'Union européenne à se conformer aux exigences du règlement (UE) n° 2019/881, des actes d'exécution pris en son exécution et à la présente loi, dans les délais qu'il détermine. Passé ce délai, l'ILNAS peut appliquer des sanctions administratives à cette non-conformité en vertu de l'article 9.

Dans le cadre de sa mission de supervision l'ILNAS peut, en vertu des articles 27 et suivants de la loi du 18 juillet sur la Police grand-ducale, se voir obligé d'avoir recours à la Police grand-ducale. Il pourrait s'avérer judicieux de pouvoir demander l'assistance de la Police grand-ducale en vue d'avoir par exemple accès aux locaux ou d'avoir une assistance d'ordre sécuritaire se traduisant par la protection physique des agents ILNAS.

En cas de constatation d'une violation grave l'ILNAS peut en informer à telles fins que de droit les Ministères compétents parce qu'il est jugé nécessaire de communiquer ces informations aux autorités compétentes pour des questions de sécurité nationale ou autre.

L'ILNAS peut publier pour informer le public, dans l'intérêt public, 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

Les sanctions administratives et pénales sont le fruit d'une longue réflexion. Elles reflètent d'une part, en vertu de l'article 65 du règlement (UE) n° 2019/881, la nécessité de fixer des sanctions effectives, proportionnées et dissuasives, et d'autre part elles s'appliquent aux différents niveaux d'assurance et nuancent les sanctions conférées. La combinaison de ces critères a permis d'adapter les sanctions des émetteurs de déclarations de conformité de l'Union européenne, des titulaires de certificats de cybersécurité européens, des organismes d'évaluation de la conformité européens et toute personne visée par l'article 6 de la présente loi en fonction de la gravité des faits et de la répercussion économique sur l'écosystème du pays et de ses citoyens.

#### *Ad article 9 – Sanctions administratives*

L'ILNAS peut recourir à des amendes administratives allant de 250 euros à 25 000 euros dans le cadre du contrôle et de la surveillance des émetteurs de déclarations de conformité de l'Union européenne, des titulaires de certificats de cybersécurité européens et des organismes d'évaluation de la conformité européens qui enfreignent les droits et devoirs prévus par le droit national ou le règlement (UE) n° 2019/881 et notamment des niveaux d'assurance dits 'élémentaire' et 'substantiel'.

#### *Ad article 10 – Sanctions pénales*

Les paragraphes 1 et 2 de cet article punissent, conformément au règlement (UE) n° 2019/881, les titulaires de certificats de cybersécurité européens des manquements de niveaux d'assurance dits 'substantiel' et 'élevé'.

Les paragraphes 3, 4 et 5 de cet article punissent, conformément au règlement (UE) n° 2019/881, les organismes d'évaluation de la conformité européens qui commettent des manquements de niveaux d'assurance 'substantiel' et 'élevé'.

Le paragraphe 6 sanctionne toute personne qui ne s'est pas conformée au secret professionnel prévu par l'article 7, paragraphe 1.

#### Chapitre 5 – Dispositions modificatives

##### *Ad article 11*

Le point 1 tient lieu d'une réorganisation interne au sein de l'ILNAS.

Le point 2 se réfère à la désignation de l'article 1<sup>er</sup> et en ce sens modifie l'article 4 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 actuellement en cours de révision dans le dossier parlementaire N° 7767 et l'avis du Conseil d'Etat N° 60.531.

Le présent projet de loi n'interfère pas avec les travaux en cours.

\*

### FICHE FINANCIERE

(art. 79 de la loi du 8 juin 1999 sur le Budget,  
la Comptabilité et la Trésorerie de l'Etat)

Le projet de loi ne comporte pas de dispositions dont l'application est susceptible de grever le budget de l'Etat.

\*

### FICHE D'EVALUATION D'IMPACT

<b>Intitulé du projet:</b>	<b>Projet de loi du jj/mm/aaaa 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) [ci-après, le « règlement (UE) n° 2019/881 »].</b>
<b>Ministère initiateur:</b>	<b>Ministère de l'Économie</b>
<b>Auteur:</b>	<b>Annick Hartung</b>
<b>Tél .:</b>	<b>+352 247-84320</b>
<b>Courriel:</b>	<b>Annick.Hartung@eco.etat.lu</b>
<b>Objectif(s) du projet:</b>	<b>Mise en œuvre d'un règlement communautaire</b>
<b>Autre(s) Ministère(s)/Organisme(s)/Commune(s)impliqué(e)(s):</b>	<b>le Ministère d'Etat, le Ministère des Finances, le Ministère de la Justice et l'ILNAS</b>
<b>Date:</b>	<b>décembre 2022</b>

#### Mieux légiférer

1. Partie(s) prenante(s) (organismes divers, citoyens, ...) consultée(s): Oui:  Non:   
 Si oui, laquelle/lesquelles: ...ILNAS, Ministère de la Justice...  
 Remarques/Observations: ...

2. Destinataires du projet:
- Entreprises/Professions libérales: Oui:  Non:
  - Citoyens: Oui:  Non:
  - Administrations: Oui:  Non:
3. Le principe « Think small first » est-il respecté? Oui:  Non:  N.a.:   
(c.à.d. des exemptions ou dérogations sont-elles prévues suivant la taille de l'entreprise et/ou son secteur d'activité?)  
Remarques/Observations: ...
4. Le projet est-il lisible et compréhensible pour le destinataire? Oui:  Non:   
Existe-t-il un texte coordonné ou un guide pratique, mis à jour et publié d'une façon régulière? Oui:  Non:   
Remarques/Observations: ...
5. Le projet a-t-il saisi l'opportunité pour supprimer ou simplifier des régimes d'autorisation et de déclaration existants, ou pour améliorer la qualité des procédures? Oui:  Non:   
Remarques/Observations: ...
6. Le projet contient-il une charge administrative pour le(s) destinataire(s)? (un coût imposé pour satisfaire à une obligation d'information émanant du projet?) Oui:  Non:   
Si oui, quel est le coût administratif approximatif total? (nombre de destinataires x coût administratif par destinataire) ...
7. a) Le projet prend-il recours à un échange de données inter-administratif (national ou international) plutôt que de demander l'information au destinataire? Oui:  Non:   
Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il? ...
- b) Le projet en question contient-il des dispositions spécifiques concernant la protection des personnes à l'égard du traitement des données à caractère personnel? Oui:  Non:   
Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il? ...
8. Le projet prévoit-il:
- une autorisation tacite en cas de non réponse de l'administration? Oui:  Non:  N.a.:
  - des délais de réponse à respecter par l'administration? Oui:  Non:  N.a.:
  - le principe que l'administration ne pourra demander des informations supplémentaires qu'une seule fois? Oui:  Non:  N.a.:
9. Y a-t-il une possibilité de regroupement de formalités et/ou de procédures (p. ex. prévues le cas échéant par un autre texte)? Oui:  Non:   
Si oui, laquelle: ...
10. En cas de transposition de directives communautaires, le principe « la directive, rien que la directive » est-il respecté? Oui:  Non:  N.a.:   
Si non, pourquoi? ...

11. Le projet contribue-t-il en général à une:
- a) simplification administrative, et/ou à une Oui:  Non:
- b) amélioration de la qualité réglementaire ? Oui:  Non:
- Remarques/Observations: ...
12. Des heures d'ouverture de guichet, favorables et adaptées aux besoins du/des destinataire(s), seront-elles introduites? Oui:  Non:  N.a.:
13. Y a-t-il une nécessité d'adapter un système informatique auprès de l'Etat (e-Government ou application back-office)? Oui:  Non:
- Si oui, quel est le délai pour disposer du nouveau système ?
14. Y a-t-il un besoin en formation du personnel de l'administration concernée? Oui:  Non:  N.a.:
- Si oui, lequel? ...
- Remarques/Observations: ...

### Egalité des chances

15. Le projet est-il:
- principalement centré sur l'égalité des femmes et des hommes? Oui:  Non:
- positif en matière d'égalité des femmes et des hommes? Oui:  Non:
- Si oui, expliquez de quelle manière: ...
- neutre en matière d'égalité des femmes et des hommes? Oui:  Non:
- Si oui, expliquez pourquoi: Tous les documents sont concernés indifféremment du genre
- négatif en matière d'égalité des femmes et des hommes? Oui:  Non:
- Si oui, expliquez de quelle manière: ...
16. Y a-t-il un impact financier différent sur les femmes et les hommes ? Oui:  Non:  N.a.:
- Si oui, expliquez de quelle manière: ...

### Directive « services »

17. Le projet introduit-il une exigence relative à la liberté d'établissement soumise à évaluation<sup>1</sup> ? Oui:  Non:  N.a.:
18. Le projet introduit-il une exigence relative à la libre prestation de services transfrontaliers<sup>2</sup> ? Oui:  Non:  N.a.:

\*

<sup>1</sup> Article 15, paragraphe 2 de la directive « services » (cf. Note explicative, p. 10-11)

<sup>2</sup> Article 16, paragraphe 1, troisième alinéa et paragraphe 3, première phrase de la directive « services » (cf. Note explicative, p. 10-11)

**TEXTE COORDONNE****LOI ILNAS****LOI DU 4 JUILLET 2014  
portant réorganisation de l'ILNAS**

(Mém. A – 135 du 28 juillet 2014, p. 2144, doc. parl. 6315)

modifiée par:

Loi du 25 mars 2015;

(Mém. A – 51 du 31 mars 2015, p. 1130, doc. parl. 6459)

Loi du 23 décembre 2016;

(Mém. A – 268 du 27 décembre 2016, p. 4751, doc. parl. 6981)

Loi du 23 décembre 2016;

(Mém. A – 268 du 27 décembre 2016, p. 4771, doc. parl. 6902)

Loi du 17 février 2017;

(Mém. A – 223 du 1<sup>er</sup> mars 2017, doc. parl. 7043)

Loi du 5 mai 2017;

(Mém. A – 484 du 12 mai 2017, doc. parl. 7039)

Loi du 14 décembre 2021;

(Mém. A – 871 du 15 décembre 2021, doc. parl. 7730)

Loi du 23 décembre 2022;

(Mém. A – du jj décembre 2022, doc. parl. 7767)

**Projet de loi****(gras/souligné)****CHAPITRE Ier – Dispositions générales.****Art. 1er. Définitions.**

Aux fins de la présente loi, l'on entend par:

*(Loi du 23 décembre 2022)*

- 1° *accréditation*: l'accréditation telle que définie à l'article 2, point 10°, du règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n°339/93 du Conseil, ci-après « règlement (CE) n° 765/2008 »;
- 2° *audit*: un processus systématique, indépendant et documenté, permettant d'obtenir des enregistrements, des énoncés de faits ou d'autres informations pertinentes, et de les évaluer de manière objective pour déterminer dans quelle mesure les exigences spécifiées sont respectées;
- 3° *bonnes pratiques de laboratoire*: un système de garantie de qualité portant sur le mode d'organisation des études de sécurité non cliniques ayant trait à la santé et à l'environnement et sur les conditions dans lesquelles ces études sont planifiées, réalisées, contrôlées, enregistrées, archivées et diffusées;

*(Loi du 23 décembre 2022)*

- 4° *confiance numérique*: climat de confiance dans l'environnement numérique, établi par la compétence de garantir la qualité et la sécurité d'un service numérique;
- 5° *distributeur*: toute personne physique ou morale faisant partie de la chaîne d'approvisionnement, autre que le fabricant ou l'importateur, qui met un produit à disposition sur le marché;
- 6° *document normatif*: un document qui donne des règles, des lignes directrices ou des caractéristiques pour des activités ou leurs résultats.

L'expression «document normatif» est un terme générique qui recouvre les documents tels que les normes, les spécifications techniques, les codes de bonne pratique et les règlements.

On considère comme «document» tout support d'information avec l'information qu'il porte.

Les termes relatifs aux différents types de documents normatifs sont définis comme comprenant le document et son contenu considérés comme un tout;

- 7° *étalon* : la réalisation de la définition d'une grandeur donnée, avec une valeur déterminée et une incertitude de mesure associée, utilisée comme référence;
- 8° *étalon national* : un étalon reconnu par une autorité nationale pour servir, dans un état ou une économie, comme base à l'attribution de valeurs à d'autres étalons de grandeurs de même nature;
- 9° *évaluation de la conformité* : un processus évaluant s'il est démontré que des exigences spécifiées relatives à un produit, processus, service, système, personne ou organisme ont été respectées;

(Loi du 23 décembre 2022)

- 10° *fabricant* : le fabricant tel que défini à l'article 3, point 8°, du règlement (UE) n° 2019/1020 du Parlement européen et du Conseil du 20 juin 2019 sur la surveillance du marché et la conformité des produits, et modifiant la directive 2004/42/CE et les règlements (CE) n° 765/2008 et (UE) n° 305/2011, ci-après « règlement (UE) n° 2019/1020 »;
- 11° *instruments de mesure* : un dispositif utilisé pour faire des mesurages, seul ou associé à un ou plusieurs dispositifs annexes;
- 12° *importateur* : toute personne physique ou morale établie dans l'Union européenne qui met un produit provenant d'un pays tiers sur le marché intérieur de l'Union européenne;
- 13° *infrastructure métrologique* : les acteurs de la métrologie;
- 14° *mandataire* : toute personne physique ou morale établie dans l'Union européenne ayant reçu mandat écrit d'un fabricant pour agir en son nom aux fins de l'accomplissement de tâches déterminées qui sont liées aux obligations incombant à ce dernier en vertu de la législation de l'Union européenne applicable;
- 15° *métrologie légale* : la partie de la métrologie se rapportant aux activités qui résultent d'exigences réglementaires et qui s'appliquent aux mesurages, aux unités de mesure, aux instruments de mesure et aux méthodes de mesure et sont effectuées par des organismes d'évaluation de la conformité compétents;
- 16° *mise à disposition sur le marché* : toute fourniture d'un produit destiné à être distribué, consommé ou utilisé sur le marché unique européen dans le cadre d'une activité commerciale, à titre onéreux ou gratuit;
- 17° *mise sur le marché* : la première mise à disposition d'un produit sur le marché unique européen;
- 18° *normalisation* : une activité propre à établir, face à des problèmes réels ou potentiels, des dispositions destinées à un usage commun et répété, visant à l'obtention du degré optimal d'ordre dans un contexte donné;
- 19° *norme* : un document établi par consensus et approuvé par un organisme luxembourgeois, européen ou international reconnu à activité normative, qui fournit, pour des usages communs et répétés, des règles, des lignes directrices ou des caractéristiques, pour des activités ou leurs résultats, garantissant un niveau d'ordre optimal dans un contexte donné;

(Loi du 23 décembre 2022)

- 20° *norme harmonisée* : une norme telle que définie à l'article 2, point 1°, lettre c), 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;

(Loi du 23 décembre 2022)

- 21° *opérateur économique* : l'opérateur tel que défini à l'article 3, point 13°, du règlement (UE) n° 2019/1020;

- 22° *organisme national d'accréditation* : un organisme dans un Etat membre chargé de l'accréditation, qui tire son autorité de cet Etat;
- 23° *organisme d'évaluation de la conformité* : un organisme qui effectue des opérations d'évaluation de la conformité sous forme d'étalonnages, d'essais, de certification, d'inspection, d'analyses ou de contrôles;
- 24° *organisme de normalisation* : un organisme à activités normatives reconnu au niveau national, régional ou international, dont l'une des principales fonctions est la préparation, l'approbation et l'adoption de normes qui sont mises à la disposition du public;

(Loi du 23 décembre 2022)

- 25° *organisme notifié* : un organisme d'évaluation de la conformité désigné et notifié auprès de la Commission européenne par l'autorité notifiante pour effectuer des tâches d'évaluation de la conformité prévues par la législation nationale transposant les dispositions législatives visant l'harmonisation au niveau de l'Union européenne de la mise sur le marché de produits;

(Loi du 23 décembre 2022)

- 26° *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 ;

(Loi du 23 décembre 2022)

- 26bis° *prestataire de services de dématérialisation ou de conservation*: un prestataire de services de dématérialisation ou de conservation au sens de l'article 2, lettre h), de la loi du 25 juillet 2015 relative à l'archivage électronique;

- 27° *produits en préemballages* : des produits préemballés en quantités variables et produits en préemballages à quantités nominales fixes;

(Loi du 23 décembre 2022)

- 27bis° *produit présentant un risque grave*: un produit tel que défini à l'article 3, point 20°, du règlement (UE) n° 2019/1020;

- 28° *programme de normalisation* : le plan de travail d'un organisme à activités normatives dressant la liste des questions faisant ou devant faire l'objet de travaux de normalisation;

- 29° *rappel* : toute mesure visant à obtenir le retour d'un produit qui a déjà été mis à la disposition de l'utilisateur final;

- 30° (Loi du 23 décembre 2022 - supprimé) ...;

- 31° *retrait* : toute mesure visant à empêcher la mise à disposition sur le marché d'un produit de la chaîne d'approvisionnement ou de retirer un produit de la chaîne d'approvisionnement;

(Loi du 23 décembre 2022)

- 32° *surveillance du marché* : la surveillance telle que définie à l'article 3, point 3°, du règlement (UE) n° 2019/1020 ;

- 33° *système international d'unités* : le système d'unités, fondé sur le système international de grandeurs, comptant les noms et symboles des unités, une série de préfixes avec leurs noms et symboles, ainsi que des règles pour leur emploi.

## CHAPITRE II – L'ILNAS et ses missions.

### Section 1<sup>re</sup> – L'ILNAS.

#### Art. 2. Organisation.

(1) Il est créé une administration appelée « Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services », désignée par son acronyme « ILNAS ».

L'ILNAS est placé sous l'autorité du membre du Gouvernement ayant l'Economie dans ses attributions, ci-après dénommé « le ministre ».

Le directeur est responsable de la gestion de l'ILNAS. Il en est le chef hiérarchique.

(2) L'ILNAS est composé de six départements, à savoir:

- 1° l'Organisme luxembourgeois de normalisation,
- 2° le ~~département de la confiance numérique~~ **Organisme luxembourgeois de la confiance numérique**,
- 3° l'Office luxembourgeois d'accréditation et de surveillance, désigné ci-après par l'acronyme « OLAS »,
- 4° le département de la surveillance du marché,
- 5° le Bureau luxembourgeois de métrologie, et
- 6° le département du budget et de l'administration.

Le directeur arrête les détails d'organisation et les modalités de fonctionnement des départements.

(3) Dans l'exercice des attributions lui conférées en vertu des articles 3 à 11, l'ILNAS jouit de l'indépendance scientifique.

## Section 2 – Attributions de l'Organisme luxembourgeois de normalisation.

### Art. 3. Normalisation.

(1) L'Organisme luxembourgeois de normalisation est l'organisme national de normalisation, dont les attributions consistent:

- 1° à exécuter la stratégie normative et les politiques en matière de normalisation définies par le ministre;
- 2° à harmoniser les règles sur lesquelles la normalisation doit être basée;
- 3° à recenser auprès des acteurs socio-économiques luxembourgeois les besoins en normes et autres documents normatifs nouveaux et à préparer le programme de normalisation en concordance avec la politique de normalisation déterminée par le ministre;
- 4° à coordonner au niveau national l'élaboration et l'adoption d'avant-projets de normes et autres documents normatifs inscrits au programme de normalisation, par les « *(Loi du 23 décembre 2022 – supprimé) ...* » parties intéressées « *(Loi du 23 décembre 2022)* inscrites au comité technique de normalisation national respectif »;

*(Loi du 23 décembre 2022)*

- 4bis° à créer et à dissoudre des comités techniques, sous-comités et groupes de travail de normalisation nationaux;
- 4ter° à faire appel aux acteurs socio-économiques luxembourgeois pour désigner des délégués possédant l'expérience et les compétences nécessaires pour participer aux comités techniques, sous-comités et groupes de travail de l'Organisme luxembourgeois de normalisation et des organismes de normalisation européens et internationaux, et de gérer le registre national des délégués en normalisation faisant partie des différents comités techniques, sous-comités et groupes de travail ;
- 5° à adopter « *(Loi du 23 décembre 2022 – supprimé) ...* » des normes et autres documents normatifs nationaux élaborés de manière consensuelle entre les parties intéressées « *(Loi du 23 décembre 2022)* inscrites au comité technique de normalisation national respectif » et à faire publier leurs références au Mémorial;
- 6° « *(Loi du 23 décembre 2022 – supprimé) ...* »;
- 7° à publier au Mémorial les références des normes et autres documents normatifs nationaux transposant des normes et autres documents normatifs élaborés et adoptés par les organismes de normalisation européens et internationaux;
- 8° à annuler des normes et autres documents normatifs nationaux « *(Loi du 23 décembre 2022 – supprimé) ...* » et à publier une notice renseignant sur cette annulation au Mémorial;
- 9° à centraliser et à garantir la mise à disposition au public de normes et autres documents normatifs, dont les modalités et barèmes de prix sont fixés par le ministre sur proposition de l'Organisme luxembourgeois de normalisation en fonction des obligations en matière de droits de reproduction envers les organismes de normalisation « *(Loi du 23 décembre 2022)* nationaux, » européens et internationaux;

- 10° « (Loi du 23 décembre 2022 – supprimé) ... »;
- 11° « (Loi du 23 décembre 2022 – supprimé) ... »;
- 12° à organiser et à coordonner la promotion de la normalisation et la formation « (Loi du 23 décembre 2022 – supprimé) ... » à la normalisation;
- 13° à communiquer son programme de travail aux organismes européens de normalisation et aux autres organismes nationaux de normalisation ainsi qu'à la Commission européenne;
- 14° à notifier à la Commission européenne tout projet de réglementation technique ou de règle relative aux services de la société de l'information avant que ceux-ci ne soient adoptés en droit national.

(2) Les normes et autres documents normatifs validés, adoptés et approuvés par l'Organisme luxembourgeois de normalisation sont d'application volontaire.

(3) Un règlement grand-ducal détermine les modalités d'inscription au programme de normalisation, les modalités d'élaboration et d'adoption d'avant-projets de normes et autres documents normatifs, les modalités d'approbation des normes et autres documents normatifs, la procédure d'enquête publique afférente, les critères d'inscription au registre national des délégués en normalisation, ainsi que le mode de fonctionnement des comités techniques, sous-comités et groupes de travail.

### Section 3 – Attributions du ~~département de la confiance numérique~~ Organisme luxembourgeois de la confiance numérique.

« (Loi du 23 décembre 2022)

#### **Art. 4. Confiance numérique**

(1) Les attributions du ~~département de la confiance numérique~~ **Organisme luxembourgeois de la confiance numérique** consistent:

- 1° à promouvoir les instruments susceptibles de garantir la compétence des prestataires de services de dématérialisation ou de conservation, ainsi que des prestataires de services de confiance en relation avec la qualité et la sécurité des services prestés;
- 2° à définir des lignes directrices à destination des prestataires de services de confiance et des prestataires de services de dématérialisation ou de conservation nécessaires ou utiles à l'accomplissement de la mission de contrôle visée au paragraphe 1<sup>er</sup>, points 4° et 5°;
- 3° à établir, à tenir à jour, et à publier sur le site internet de l'ILNAS, la liste de confiance nationale conformément à l'article 22 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, ci-après « règlement (UE) n° 910/2014 » ;
- 4° à faire fonction d'organe de contrôle national au sens de l'article 17 du règlement (UE) n° 910/2014 et à assumer les tâches de contrôle des prestataires de services de confiance établis au Grand-Duché de Luxembourg conformément à la loi modifiée du 14 août 2000 relative au commerce électronique ;
- 5° à assumer les tâches de contrôle des prestataires de services de dématérialisation ou de conservation établis au Grand-Duché de Luxembourg conformément à la loi du 25 juillet 2015 relative à l'archivage électronique ;
- 6° à **assumer les tâches d'autorité nationale de certification de cybersécurité 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** .

(2) 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, seront facturés respectivement aux prestataires de services de confiance et aux prestataires de services de dématérialisation ou de conservation. Le barème tarifaire, approuvé par le ministre, est publié sur le site électronique installé à cet effet par l'ILNAS. »

## Section 4 – Attributions de l'OLAS.

**Art. 5. Accréditation des organismes d'évaluation de la conformité.**

(1) L'OLAS est l'organisme national d'accréditation des organismes d'évaluation de la conformité dont les attributions consistent:

- 1° à accréditer les organismes d'évaluation de la conformité sur base de la législation nationale et européenne « *(Loi du 23 décembre 2022)* ainsi que des normes techniques nationales, européennes et internationales » ;
- 2° « *(Loi du 23 décembre 2022 – supprimé)* ... »;
- 3° à créer et à gérer un registre des organismes d'évaluation de la conformité accrédités « *(Loi du 23 décembre 2022)* par l'OLAS et publié » sur le site électronique installé à cet effet par l'ILNAS.

(2) Après vérification du respect par l'organisme d'évaluation de la conformité des exigences fixées au point 1° du paragraphe 1<sup>er</sup> sur base du rapport d'audit, l'OLAS décide de l'accréditation après avoir demandé l'avis du comité d'accréditation, dont la composition et l'organisation sont déterminées par règlement grand-ducal. L'OLAS peut avoir recours à des experts « *(Loi du 23 décembre 2022 – supprimé)* ... » pour vérifier le respect de ces exigences.

L'OLAS peut inviter les autorités compétentes concernées par le domaine audité à participer aux audits d'accréditation en tant qu'observateur.

L'accréditation est valable pour cinq ans, sauf disposition contraire arrêtée dans la décision d'accréditation. Elle est soumise à une surveillance périodique et peut être renouvelée, à la demande de l'organisme accrédité, pour de nouveaux termes consécutifs de 5 ans.

« *(Loi du 23 décembre 2022)* En cas de non-respect par l'organisme d'évaluation de la conformité des conditions de son accréditation, définies au paragraphe 1<sup>er</sup>, point 1°, l'OLAS peut procéder à la suspension temporaire de l'accréditation ou d'une partie de celle-ci ou au retrait définitif de tout ou partie de l'accréditation. »

(3) Un règlement grand-ducal détermine le système d'accréditation des organismes d'évaluation de la conformité.

(4) Toute accréditation d'un organisme d'évaluation de la conformité est soumise au paiement d'un droit de dossier annuel déterminé par règlement grand-ducal et qui ne peut pas dépasser 3.000 euros.

(5) Les membres et le secrétaire du comité d'accréditation ont droit à des jetons de présence dont le montant est fixé par règlement grand-ducal.

« *(Loi du 23 décembre 2022)* (6) Les frais relatifs à la préparation de l'audit, les frais d'audit proprement dits, ainsi que les frais relatifs à la rédaction des rapports d'audits, facturés à l'OLAS par les auditeurs, seront refacturés à l'organisme d'évaluation de la conformité accrédité ou au candidat à l'accréditation. Le barème tarifaire, approuvé par le ministre, est publié sur le site électronique installé à cet effet par l'ILNAS. »

(7) L'OLAS informe sans délai les autorités compétentes concernées par le domaine audité lorsqu'il identifie, dans le cadre de ses activités d'accréditation, un risque auprès d'un organisme d'évaluation de la conformité qui met en danger la santé et la sécurité des personnes, la santé et le bien-être des animaux ou l'environnement.

**Art. 6. Bonnes pratiques de laboratoire.**

(1) « *(Loi du 23 décembre 2022 – supprimé)* ... ».

(2) L'OLAS organise les audits des bonnes pratiques de laboratoire « *(Loi du 23 décembre 2022 – supprimé)* sur demande d'une autorité de vérification ».

**Art. 7. « (Loi du 23 décembre 2022) Notification des organismes d'évaluation de la conformité ».**

(1) L'OLAS est l'autorité chargée de la notification à la Commission européenne et aux autres Etats membres de l'Union européenne d'organismes d'évaluation de la conformité accrédités dans des domaines légaux qui prévoient cette notification.

(2) Tout organisme d'évaluation de la conformité qui demande à être notifié doit être établi au Grand-Duché de Luxembourg, posséder la personnalité juridique et être accrédité dans la matière légale dans le cadre de laquelle la notification est demandée.

« (Loi du 23 décembre 2022 – supprimé) ... ».

Les ministres ou les représentants des administrations concernés par la matière dont relève la notification sont invités à assister en qualité d'observateurs aux audits d'accréditation.

Tout changement susceptible d'affecter les conditions « (Loi du 23 décembre 2022) d'accréditation, » de qualification professionnelle, d'intégrité, d'impartialité, d'indépendance ou de confidentialité oblige le ou les dirigeants de l'organisme notifié d'en informer l'OLAS dans la semaine suivant ce changement et d'indiquer comment le respect des conditions de la notification est assuré à titre provisoire. Dans les trois mois qui suivent « (Loi du 23 décembre 2022) ce changement », l'organisme est tenu de se mettre en conformité avec les exigences de sa notification.

En cas de non-respect par l'organisme notifié des conditions de sa notification, l'OLAS peut procéder au retrait « (Loi du 23 décembre 2022 – supprimé) ... » de la notification « (Loi du 23 décembre 2022 – supprimé) ... ».

« (Loi du 23 décembre 2022) En cas de suspension de l'accréditation d'un organisme notifié, l'OLAS peut maintenir sa notification. Si la compétence technique de l'organisme est remise en question, il ne peut plus émettre de nouveaux certificats jusqu'au rétablissement de son accréditation pour les tâches d'évaluation de la conformité concernées.

En cas de retrait d'une accréditation, la notification est retirée. »

(3) Avant de lancer la procédure « (Loi du 23 décembre 2022) notifiante », toute candidature doit être approuvée par le ministre, qui prend sa décision après avoir demandé l'avis des ministres concernés par la matière dont relève la notification.

(4) Un règlement grand-ducal détermine les obligations qui incombent aux organismes notifiés en matière de participation aux activités de normalisation et de groupes de coordination, de recours à une filiale ou à un sous-traitant pour certaines tâches d'évaluation de la conformité, d'obligation d'information de l'autorité de notification et de modification de son statut d'organisme notifié.

« (Loi du 17 février 2017) **Art. 7bis.** « (Loi du 23 décembre 2022) **Mode de fonctionnement de l'OLAS.**»

L'OLAS « (Loi du 23 décembre 2022) , dans l'exercice de ses missions d'accréditation et de notification des organismes d'évaluation de la conformité » :

- 1° est établi de manière à éviter tout conflit d'intérêts avec les organismes d'évaluation de la conformité;
- 2° est organisé et fonctionne de façon à garantir l'objectivité et l'impartialité de ses activités;
- 3° est organisé de telle sorte que chaque décision concernant la notification « (Loi du 23 décembre 2022) ou l'accréditation » d'un organisme d'évaluation de la conformité est prise par des personnes compétentes différentes de celles qui ont réalisé l'évaluation;
- 4° ne propose ni ne fournit aucune des activités réalisées par les organismes d'évaluation de la conformité, ni aucun service de conseil sur une base commerciale ou concurrentielle;
- 5° garantit la confidentialité des informations qu'il obtient;
- 6° dispose d'un personnel compétent en nombre suffisant pour la bonne exécution de ses tâches;
- 7° communique à la Commission européenne, sur demande, toutes les informations relatives au fondement de la notification ou au maintien de la compétence de l'organisme d'évaluation de la conformité concerné. »

## Section 5 – Attributions du département de la surveillance du marché.

**Art. 8. Surveillance du marché.**

(1) Le département de la surveillance du marché établit de façon périodique un programme général de surveillance du marché qui regroupe les programmes sectoriels de surveillance du marché élaborés par les membres du Gouvernement et les administrations compétents pour la surveillance du marché de produits couverts par le règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93, tel que modifié par la suite.

Le programme général est publié sur le site électronique installé à cet effet par l'ILNAS.

(2) Le département de la surveillance du marché coordonne la mise en place du programme général visé à l'alinéa précédent.

(3) Dans les conditions du paragraphe 1<sup>er</sup>, le département de la surveillance du marché procède périodiquement à l'évaluation du fonctionnement des activités de surveillance du marché.

(4) Le département de la surveillance du marché assure la surveillance du marché dans le cadre de la législation applicable relative:

- 1° aux appareils à gaz;
- 2° aux appareils et systèmes de protection destinés à être utilisés en atmosphères explosibles;
- 3° à la mise sur le marché des articles pyrotechniques;
- 4° aux ascenseurs;
- 5° à la compatibilité électromagnétique;
- 6° aux équipements de protection individuelle;
- 7° aux équipements sous pression;
- 8° aux équipements sous pression transportables;
- 9° aux équipements hertziens et aux équipements terminaux de télécommunications;
- 10° à l'étiquetage de pneumatiques en relation avec l'efficacité en carburant et d'autres paramètres essentiels;
- 11° aux exigences en matière d'écoconception applicables aux produits liés à l'énergie;
- 12° à la mise sur le marché et au contrôle des explosifs à usage civil;
- 13° à la dénomination des fibres textiles et à l'étiquetage et aux marquages correspondants des produits textiles au regard de leur composition en fibres;
- 14° aux générateurs d'aérosols;
- 15° à l'indication de la consommation des appareils domestiques en énergie et en autres ressources par voie d'étiquetage et d'informations uniformes relatives aux produits;
- 16° aux installations à câbles transportant des personnes;
- 17° aux instruments de mesure;
- 18° aux instruments de pesage à fonctionnement non automatique;
- 19° à la sécurité des jouets;
- 20° aux machines;
- 21° au matériel électrique destiné à être employé dans certaines limites de tension;
- 22° aux produits de construction;
- 23° aux produits en préemballages en ce qui concerne les aspects métrologiques;
- 24° aux récipients à pression simple; et
- 25° à la sécurité générale des produits;
- 26° (*Loi du 23 décembre 2016*) « aux bateaux de plaisance »;
- 27° (*Loi du 23 décembre 2016*) « aux équipements marins »;
- 28° (*Loi du 17 février 2017*) « aux véhicules agricoles et forestiers »;

- 29° aux véhicules à deux ou trois roues et des quadricycles;
- 30° aux véhicules à moteur et leurs remorques, ainsi que les systèmes composants et entités techniques distincts destinés à ces véhicules »;

« (Loi du 23 décembre 2022)

- 31° aux moteurs à combustion interne destinés aux engins mobiles non routiers ;
- 32° à l'étiquetage des matériaux utilisés dans les principaux éléments des articles chaussants ;
- 33° aux systèmes d'aéronefs sans équipage à bord et aux exploitants. »

« (4bis) L'ILNAS assure la mission d'autorité compétente dans les matières visées au paragraphe 4 conformément au règlement (UE) n° 2019/515 du Parlement européen et du Conseil du 19 mars 2019 relatif à la reconnaissance mutuelle des biens commercialisés légalement dans un autre État membre et abrogeant le règlement (CE) n° 764/2008 et au règlement (UE) n° 2019/1020.

(4ter) Le département de la surveillance du marché réalise des essais dans le cadre de la législation énoncée au paragraphe 4. »

(5) « (Loi du 23 décembre 2022) Lorsqu'une institution de la sécurité sociale a connaissance d'un accident ayant entraîné » des dommages corporels « (Loi du 23 décembre 2022) dus » à un produit concerné par les dispositions légales visées aux paragraphes 1<sup>er</sup> et 4, « (Loi du 23 décembre 2022) elle en informe le département de la surveillance du marché ».

(6) Le département de la surveillance du marché gère, au niveau national, le système d'alerte rapide de l'Union européenne ainsi que le système général d'aide à l'information conformément aux règlements du Parlement européen et du Conseil fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits.

« (Loi du 23 décembre 2022) (7) La surveillance du marché réalisée par l'ILNAS s'exerce à l'égard des opérateurs économiques. »

#### Section 6 – Attributions du Bureau luxembourgeois de métrologie.

##### **Art. 9. Métrologie.**

« (Loi du 23 décembre 2022) (1) Les missions du Bureau luxembourgeois de métrologie consistent:

- 1° à proposer au ministre les organismes en charge de la mise en œuvre de la politique nationale de métrologie, et particulièrement ceux chargés d'établir, de conserver, d'entretenir, d'améliorer et de reproduire les étalons nationaux en fonction des besoins du pays et d'assurer leur traçabilité au système international d'unités;
- 2° à organiser « (Loi du 23 décembre 2022) et à maintenir l'infrastructure nationale de métrologie et », à coordonner et à superviser les activités des organismes désignés « (Loi du 23 décembre 2022 – supprimé) ... » ;
- 3° à déterminer « (Loi du 23 décembre 2022 – supprimé) ... » les besoins en étalons « (Loi du 23 décembre 2022 – supprimé) ... » ;
- 4° à définir le système d'étalons nationaux;
- 5° à « (Loi du 23 décembre 2022) mettre en œuvre » et à veiller à une application correcte et uniforme « (Loi du 23 décembre 2022) des unités » du système international d'unités et des autres unités légales;
- 6° à faciliter la reconnaissance internationale des organismes et des systèmes nationaux de métrologie;
- 7° à organiser la promotion et la formation volontaire à la métrologie « (Loi du 23 décembre 2022) ; »
- 8° à exécuter la législation en matière de métrologie légale se rapportant aux mesurages, aux unités de mesure, aux instruments de mesure, aux méthodes de mesurage et aux produits préemballés et plus précisément:
  - à organiser et à exécuter les contrôles métrologiques et vérifications en rapport avec les instruments de mesure;

- à organiser et à réaliser la surveillance métrologique des instruments de mesure en usage dans les secteurs réglementés ainsi que de leur utilisation et des méthodes de mesurage appliquées;
  - à organiser et à exécuter le contrôle, en ce qui concerne les aspects métrologiques, des produits en préemballages et des quantités indiquées dans des débits de marchandises;
  - « *(Loi du 23 décembre 2022 – supprimé) ...* » ;
- « *(Loi du 23 décembre 2022)*
- 9° à exécuter des opérations d'étalonnage dont les tarifs sont fixés dans le barème tarifaire, approuvé par le ministre, et publié sur le site électronique installé à cet effet par l'ILNAS ;
  - 10° à assurer la mise en place, la conservation, le développement et le transfert d'étalons nationaux ;
  - 11° à exécuter et à coordonner la stratégie nationale en matière de métrologie, validée par le ministre. »

#### Section 7 – Autres missions de l'ILNAS.

##### **Art. 10. Etudes et recherche.**

(1) L'ILNAS est chargé de réaliser des recherches scientifiques dans le domaine de la normalisation, de la confiance numérique et de la métrologie et d'en publier les résultats.

Sous réserve de l'approbation du ministre « *(Loi du 23 décembre 2022 supprimé) ...* », l'ILNAS est autorisé à entreprendre, dans le domaine qui le concerne, des activités de R&D « *(Loi du 23 décembre 2022 – supprimé) ...* ».

(2) L'ILNAS est autorisé à publier des études ou des travaux de recherche contribuant au développement de la normalisation, de la confiance numérique et de la métrologie.

(3) Dans le cadre de ses attributions l'ILNAS peut collaborer, sur décision du ministre, avec des centres de recherche économique et sociale au Luxembourg et à l'étranger. Il peut les charger de travaux de recherches et d'études.

##### **Art. 11. Autres missions de l'ILNAS.**

« *(Loi du 23 décembre 2022) (1)* » Le ministre peut charger l'ILNAS de toute autre mission susceptible de contribuer à la réalisation des attributions reprises aux articles 3 à 9.

« *(Loi du 23 décembre) (2)* L'ILNAS assure la désignation, le contrôle et l'évaluation des organismes d'évaluation technique conformément au règlement (UE) n° 305/2011 du Parlement européen et du Conseil du 9 mars 2011 établissant des conditions harmonisées de commercialisation pour les produits de construction et abrogeant la directive 89/106/CEE du Conseil.

(3) L'ILNAS assure les missions de bureau de liaison unique conformément à l'article 10 du règlement (UE) n° 2019/1020.

(4) L'ILNAS assure la mission de point de contact produit conformément à l'article 9 du règlement (UE) n° 2019/515 du Parlement européen et du Conseil du 19 mars 2019 relatif à la reconnaissance mutuelle des biens commercialisés légalement dans un autre État membre et abrogeant le règlement (CE) n° 764/2008, ci-après « règlement (UE) n° 2019/515 ». »

#### **CHAPITRE III. – Assistance par des « *(Loi du 23 décembre 2022) organismes agréés* ».**

##### **Art. 12. Assistance et délégation.**

(1) Le ministre peut agréer des organismes de droit public ou privé en vue de participer aux missions prévues au paragraphe 2. Les organismes agréés exercent leur mission sous la direction et la surveillance de l'ILNAS.

En vue de son agrément, l'organisme doit présenter les garanties nécessaires de qualification professionnelle, d'intégrité, d'impartialité, d'indépendance et de confidentialité qui s'apprécient sur base d'une accréditation appropriée délivrée par l'OLAS conformément à l'article 5, paragraphe 1<sup>er</sup>, sous 1° ou sur base d'une accréditation reconnue équivalente par l'OLAS dans le cadre des accords de

reconnaissance mutuelle européens ou internationaux. L'organisme doit également garantir la disponibilité des ressources humaines et des infrastructures et équipements requis en vue de l'exécution de la mission pour laquelle il sollicite un agrément.

Tout changement susceptible d'affecter les conditions de qualification professionnelle, d'intégrité, d'impartialité, d'indépendance ou de confidentialité oblige le ou les dirigeants de l'organisme agréé d'en informer l'ILNAS dans les huit jours suivant ce changement et d'indiquer comment le respect des conditions de l'agrément est assuré à titre provisoire. Dans les trois mois qui suivent, l'organisme est tenu de se mettre en conformité avec les exigences de son agrément.

En cas de non-respect par l'organisme agréé des conditions de son agrément, le ministre peut, après avoir entendu l'ILNAS, procéder au retrait temporaire ou définitif de l'agrément.

(2) Dans le cadre de la surveillance du marché et de la métrologie légale, le ministre peut charger des organismes agréés de droit public ou privé d'études, de contrôles, de vérifications ainsi que d'autres missions de surveillance destinées à contribuer à la réalisation des missions qui sont confiées à l'ILNAS en vertu des articles 8 et 9.

L'attribution des tâches en question aux organismes agréés se fait par voie conventionnelle.

Les tâches visées portent sur:

- 1° la recherche de produits non conformes, la vérification des marquages sur les produits ou leurs emballages et le contrôle à l'œil nu des critères de conformité facilement perceptibles sans altération, destruction ou démontage du produit dans les parties librement accessibles au public d'un établissement de vente dans le cadre de l'article 8, paragraphe 4;
- 2° les contrôles métrologiques et les vérifications en rapport avec les instruments de mesure;
- 3° la surveillance métrologique des instruments de mesure en usage dans les secteurs réglementés ainsi que de leur utilisation et des méthodes de mesurage appliquées;
- 4° le contrôle des aspects métrologiques des produits en préemballages et des quantités indiquées dans les débits de marchandises.

(3) Un règlement grand-ducal précise:

- 1° les modalités d'établissement des rapports et, le cas échéant, les marques d'identification, d'acceptation, de refus et de scellement ainsi que les modalités d'octroi et d'utilisation de celles-ci;
- 2° les relations avec l'ILNAS ainsi que les modalités opérationnelles et financières pour chaque domaine d'intervention.

#### CHAPITRE IV – Pouvoirs d'investigation.

##### **Art. 13. Mesures administratives « (Loi du 23 décembre 2022) et modalités de contrôle » dans le cadre de la surveillance du marché.**

(1) L'ILNAS et « (Loi du 23 décembre 2022) les agents de » l'Administration des douanes et accises « (Loi du 23 décembre 2022 – supprimé) ... » sont chargés des contrôles de conformité des produits prévus par les législations visées à l'article 8, paragraphe 4.

(2) En vue des contrôles visés au paragraphe 1<sup>er</sup>, « (Loi du 23 décembre 2022) l'ILNAS peut »:

- 1° ordonner que les personnes susceptibles d'être exposées au risque découlant d'un produit soient averties de ce risque en temps utile et sous une forme appropriée, y compris par la publication de ces avertissements;
- 2° interdire temporairement, pendant la période nécessaire aux différents contrôles, « (Loi du 23 décembre 2022 – supprimé) ... » de proposer de fournir ou d'exposer un produit ou un lot de produits lorsqu'il existe des indices précis et convergents concernant leur non-conformité aux dispositions légales visées au paragraphe 1<sup>er</sup>;
- 3° interdire ou restreindre la mise à disposition sur le marché d'un produit ou d'un lot de produits qui n'est pas conforme aux dispositions légales visées au paragraphe 1<sup>er</sup> « (Loi du 23 décembre 2022 – supprimé) ... » ;
- 4° ordonner, coordonner ou, le cas échéant, organiser avec les opérateurs économiques, le rappel, le retrait ou la modification d'un produit présentant un risque grave, y compris un risque grave dont

les effets ne sont pas immédiats, du marché ou auprès des consommateurs et sa destruction dans les conditions adéquates « (Loi du 23 décembre 2022) , ou le rendre inutilisable » ;

5° interdire d'exposer un produit en vente de façon qui induit ou risque d'induire en erreur sur ses caractéristiques réelles ;

« (Loi du 23 décembre 2022)

6° prélever ou faire prélever, contre paiement de leur prix, aux fins d'examen ou d'analyse, des produits comportant ou étant susceptibles de comporter une non-conformité aux dispositions légales visées à l'article 8, paragraphe 4. »

« (Loi du 23 décembre 2022 – supprimé) ... »

« (Loi du 23 décembre 2022) (2bis) Les décisions intervenues en exécution du paragraphe 2 sont adressées selon le cas :

1° au fabricant ou à son mandataire;

2° à l'importateur;

3° dans les limites de leurs activités respectives, aux distributeurs ou notamment au responsable de la première distribution sur le marché national;

4° à toute autre personne, lorsque ceci s'avère nécessaire, en vue de la collaboration aux actions engagées pour éviter des risques découlant d'un produit. »

(3) Les décisions intervenues dans les conditions du paragraphe 2, points 3° à 5°, sont susceptibles d'un recours en réformation à introduire devant le tribunal administratif dans un délai de trois mois à compter de leur notification.

« (Loi du 23 décembre 2022)

(4) Les personnes visées au paragraphe 1<sup>er</sup> ne sont pas tenues de signaler leur présence lors de vérifications effectuées dans les parties librement accessibles au public d'un établissement de vente lors :

1° de la recherche de produits non conformes;

2° de la vérification des marquages sur les produits ou leurs emballages, sans pour autant les déemballer;

3° du contrôle à l'œil nu de critères de conformité facilement perceptibles sans altération, destruction ou démontage du produit.

(5) Les opérateurs économiques ainsi que leurs préposés, les propriétaires ou détenteurs des installations, appareils, dispositifs, locaux, terrains, produits, matières ou substances, ainsi que toute personne responsable de travaux ou d'une activité généralement quelconque, susceptibles de tomber sous les dispositions de la présente loi ou de ses règlements d'exécution, sont tenus, à la réquisition des fonctionnaires ou agents chargés du contrôle, de ne pas entraver les opérations auxquelles ceux-ci procèdent en vertu de la présente loi.

(6) En cas de constatation d'un manquement aux dispositions de la législation applicable, les frais de surveillance du marché, tels que, l'achat, le transport, le stockage, l'essai et la destruction, sont supportés par la personne physique ou morale qui a déclaré le produit pour la mise en libre pratique en vertu du Chapitre VII du règlement (UE) n° 2019/1020 ou de la présente loi.

(7) En cas d'un rappel d'un produit présentant un risque grave, les frais engagés par l'ILNAS et liés à la communication au public concernant ce rappel sont refacturés par l'ILNAS à la personne physique ou morale qui a déclaré le produit pour la mise en libre pratique en vertu du Chapitre VII du règlement (UE) n° 2019/1020 ou de la présente loi. »

**Art. 14. Personnes compétentes en matière d'investigation** « (Loi du 23 décembre 2022) , agissant en tant qu'officier de police judiciaire, » dans le cadre de la surveillance du marché « (Loi du 23 décembre 2022) , de la métrologie légale et de la confiance numérique ».

(1) « (Loi du 23 décembre 2022) Sans préjudice de l'article 10 du Code de procédure pénale, les infractions à la présente loi et à ses règlements d'exécution ainsi qu'à la loi modifiée du 17 mai 1882

sur les poids et mesures et ses règlements d'exécution sont constatées par les agents de l'Administration des douanes et accises du groupe de traitement D1, à partir du grade 5 de brigadier principal et des fonctionnaires ou employés de l'Etat de l'ILNAS des groupes de traitement ou d'indemnité A1 et A2 et du groupe de traitement ou d'indemnité B1, à partir du niveau supérieur. »

Les fonctionnaires « (Loi du 23 décembre 2022) et employés de l'État » visés à l'alinéa 1<sup>er</sup> doivent avoir suivi une formation professionnelle spéciale portant sur la recherche et la constatation des infractions ainsi que sur les dispositions pénales de la présente loi. Le programme et la durée de la formation ainsi que les modalités de contrôle des connaissances sont arrêtés par règlement grand-ducal.

Dans l'exercice de leurs fonctions les personnes visées à l'alinéa 1<sup>er</sup> ont la qualité d'officiers de police judiciaire. Ils constatent les infractions par des procès-verbaux faisant foi jusqu'à preuve du contraire. Leur compétence s'étend à tout le territoire du Grand-Duché de Luxembourg.

Avant d'entrer en fonction ils prêtent, devant le tribunal d'arrondissement de leur domicile, siégeant en matière civile, le serment suivant : « Je jure de remplir mes fonctions avec intégrité, exactitude et impartialité. ».

L'article 458 du Code pénal leur est applicable.

(2) « (Loi du 23 décembre 2022 – abrogé) ... »

**Art. 15. Modalités de contrôle « (Loi du 23 décembre 2022) des agents agissant en tant qu'officier de police judiciaire ».**

(1) Les « (Loi du 23 décembre 2022) officiers et agents de police judiciaire » grand-ducale visés à l'article 10 du Code « (Loi du 23 décembre 2022) de procédure pénale » et les personnes visées à l'article 14, paragraphe 1<sup>er</sup> 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.

Toutefois, et sans préjudice de l'article 33 du Code « (Loi du 23 décembre 2022) de procédure pénale », s'il existe des indices graves faisant présumer que l'origine de l'infraction se trouve dans les locaux destinés à l'habitation, il peut être procédé à une visite domiciliaire entre six heures et demie et vingt heures par « (Loi du 23 décembre 2022) un officier » de police judiciaire, « (Loi du 23 décembre 2022 – supprimé) ... » de la Police grand-ducale « (Loi du 23 décembre 2022 – supprimé) ... » agissant en vertu d'un mandat du juge d'instruction.

(2) Dans les mêmes conditions, « (Loi du 23 décembre 2022) officiers et agents de police judiciaire » de la Police grand-ducale visés à l'article 10 du Code « (Loi du 23 décembre 2022) de procédure pénale » et les personnes visées à l'article 14, paragraphe 1<sup>er</sup> sont autorisés à:

1<sup>o</sup> « (Loi du 23 décembre 2022) organiser, pour tout produit relevant du champ d'application de la présente loi, même après sa mise sur le marché ou sa mise à disposition sur le marché, les vérifications de sa conformité aux dispositions légales et réglementaires relatives aux produits visés à l'article 8, paragraphe 4; »

« (Loi du 23 décembre 2022)

1bis<sup>o</sup> demander aux opérateurs économiques, ainsi qu'aux personnes visées à l'article 13, paragraphe 1<sup>er</sup>, toute documentation et toute information, quel qu'en soit le support, en prendre copie et recueillir sur place les renseignements et justifications qu'ils jugent nécessaires pour constater une infraction éventuelle aux dispositions législatives et réglementaires relatives aux produits visés à l'article 8, paragraphe 4;

1ter<sup>o</sup> appliquer, s'ils en sont requis par les personnes visées à l'article 13, paragraphe 1<sup>er</sup>, les décisions administratives prises en vertu de l'article 13, paragraphe 2; »

2<sup>o</sup> demander communication de tous livres, registres et fichiers relatifs à une installation, activité ou produit « (Loi du 23 décembre 2022) entrant dans le champ d'application » de la présente loi, en vue d'en vérifier la conformité, à les copier ou à établir des extraits;

3<sup>o</sup> prélever ou à faire prélever, aux fins d'examen ou d'analyse, des échantillons de produits, matières ou substances fabriqués, utilisés, manipulés, stockés, déposés ou extraits, comportant

- ou étant susceptibles de comporter une non-conformité aux dispositions légales « (*Loi du 23 décembre 2022*) et réglementaires relatives aux produits visés à l'article 8, paragraphe 4 » ;
- 4° saisir et, au besoin, à mettre sous séquestre les appareils, dispositifs, produits, matières ou substances qui sont de nature à comporter une non-conformité aux dispositions légales « (*Loi du 23 décembre 2022*) et réglementaires relatives aux produits visés à l'article 8, paragraphe 4 ».

Les échantillons prélevés conformément au point 3° font l'objet d'une remise ou de l'apposition d'un procès-verbal constatant les prélèvements effectués. Un échantillon, cacheté et scellé, est remis à l'opérateur économique concerné, à moins que celui-ci ne soit pas présent ou y renonce expressément ou que des raisons techniques ne s'y opposent.

(3) « (*Loi du 23 décembre 2022 – supprimé*) ... ».

Lorsque le résultat des contrôles « (*Loi du 23 décembre 2022*) », effectués par les officiers et agents de police judiciaire de la Police grand-ducale visés à l'article 10 du Code de procédure pénale et les personnes visées à l'article 14, paragraphe 1<sup>er</sup>, » donne lieu à au moins une remarque, ils dressent un procès-verbal relatif aux vérifications et contrôles opérés. Une copie de ce procès-verbal est remise à l'opérateur économique concerné par les installations, locaux, terrains, documents, appareils, dispositifs, produits, matières ou substances contrôlés ou à son représentant ou en cas d'absence de celui-ci au responsable du local, de l'installation ou du site ou à celui qui le remplace.

« (*Loi du 23 décembre 2022*) (3bis) Les agents de l'ILNAS visés à l'article 14, paragraphe 1<sup>er</sup>, nonobstant les pouvoirs qui leur sont conférés au paragraphe 2, peuvent prendre toutes les décisions énumérées à l'article 13, paragraphe 2. »

(4) « (*Loi du 23 décembre 2022 – supprimé*) ... »

(5) « (*Loi du 23 décembre 2022 – supprimé*) ... »

(6) « (*Loi du 23 décembre 2022 – supprimé*) ... »

#### **Art. 16. Coopération internationale.**

Dans la mesure nécessaire à l'accomplissement de ses missions légales, l'ILNAS coopère avec les instances, institutions et agences internationales et européennes ainsi qu'avec les autorités compétentes des autres Etats membres de l'Union européenne et de pays tiers ayant signé avec le Grand-Duché de Luxembourg une convention de coopération dans une ou plusieurs des matières visées par la présente loi et procède à l'échange des informations et documentations utiles aux recherches requises effectuées de sa propre initiative ou initiées par une instance, institution ou agence internationale ou européenne ou une autorité étrangère compétente.

### **CHAPITRE V – Sanctions.**

#### Section 1<sup>re</sup> – Dispositions administratives.

**Art. 17. Amendes administratives dans le cadre de la surveillance du marché.**

(1) « (*Loi du 23 décembre 2022*) L'ILNAS peut » infliger une amende de 250 euros à « (*Loi du 23 décembre 2022*) 15 000 » euros à tout opérateur économique qui a mis sur le marché ou qui a mis à disposition sur le marché un produit ou un lot de produits « (*Loi du 23 décembre 2022*) couverts par les législations visées à l'article 8, paragraphe 4 » et:

- 1° dont les marquages ou les étiquettes ne sont pas conformes aux règles et conditions de présentation, d'apposition des marquages ou étiquettes prévues par l'article 30 et l'annexe II du règlement (CE) n° 765/2008;
- 2° « (*Loi du 23 décembre 2022*) dont la » déclaration « CE » de conformité prévue par les articles 4 et 5 et l'annexe III de la décision n° 768/2008/CE du Parlement européen et du Conseil du 9 juillet 2008 relative à un cadre commun pour la commercialisation des produits et abrogeant la décision 93/465/CEE du Conseil, « (*Loi du 23 décembre 2022*) n'a soit pas été établie, soit établie de manière

incorrecte ou incomplète, ou qui n'est pas dûment accompagné d'une déclaration « CE » de conformité bien que requise par la loi ; »

« (Loi du 23 décembre 2022)

3° dont les avertissements, les instructions et autres informations ou marquages obligatoires prévus par les législations visées à l'article 8, paragraphe 4, sont défectueux, incomplets ou incorrects. »

(2) « (Loi du 23 décembre 2022) L'ILNAS peut » infliger une amende de 250 euros à 15.000 euros à tout opérateur économique qui:

1° refuse de fournir les documents et informations ou autres renseignements demandés dans le cadre de la surveillance du marché;

2° fait obstacle à l'exercice de la surveillance du marché ;

« (Loi du 23 décembre 2022)

3° viole l'article 4, paragraphes 1<sup>er</sup>, 3 et 4, et l'article 5 du règlement (UE) n° 2019/1020. »

(3) Les amendes sont payables dans les trente jours de la notification de la décision écrite, nonobstant l'exercice d'une voie de recours.

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 partir de la notification.

« (Loi du 23 décembre 2022)

#### **Art. 17bis. Amendes administratives dans le cadre de la métrologie légale**

L'ILNAS peut infliger une amende de 250 euros à 15 000 euros à tout détenteur d'instruments qui:

1° utilise un instrument de pesage à fonctionnement non-automatique pour la détermination de la masse pour l'application d'une législation ou d'une réglementation ou pour des expertises judiciaires, dans la pratique médicale en ce qui concerne le pesage de patients pour des raisons de surveillance, de diagnostic et de traitements médicaux, pour la fabrication de médicaments, pour la détermination de la masse lors des analyses effectuées dans les laboratoires médicaux et pharmaceutiques, pour des transactions commerciales, pour le calcul d'un péage, d'un tarif, d'une taxe, d'une prime, d'une amende, d'une rémunération, d'une indemnité ou d'une redevance de type similaire ou bien qui est non-conforme ou non adapté aux conditions d'emploi, ou bien qui n'a pas fait l'objet de la vérification périodique, ou bien qui est refusé ou réparé sans avoir fait l'objet d'une vérification ultérieure, ou bien qui ne suffit pas aux règles d'installation et d'utilisation qui lui sont propres;

2° utilise un instrument de mesure ou un instrument de pesage à fonctionnement non-automatique d'une manière qui n'est pas conforme à la réglementation nationale applicable ;

3° utilise un instrument de mesure ou un instrument de pesage à fonctionnement non-automatique ne portant pas tous les marquages métrologiques;

4° détruit, enlève, falsifie ou modifie les poinçons officiels du Bureau luxembourgeois de métrologie;

5° détient dans les lieux de vente public un instrument de pesage non-automatique non-conforme à la loi modifiée du 17 mai 1882 sur les poids et mesures et à ses règlements d'exécution;

6° vend des préemballages qui ne remplissent pas les exigences de la loi modifiée du 17 mai 1882 sur les poids et mesures et ses règlements d'exécution;

7° procède à la vente de boissons dans des mesures de capacité non-conformes à la loi modifiée du 17 mai 1882 sur les poids et mesures et ses règlements d'exécution;

8° utilise une unité de mesure non-conforme à la loi modifiée du 17 mai 1882 sur les poids et mesures et ses règlements d'exécution;

9° refuse de fournir le matériel, les charges d'épreuve et, le cas échéant, le personnel nécessaire pour que le Bureau luxembourgeois de métrologie puisse faire les contrôles métrologiques prévues par la réglementation;

10° ne respecte pas les dispositions prévues pour la confection des préemballages.

**Art. 17ter. Amendes administratives dans le cadre de la confiance numérique**

L'ILNAS peut infliger une amende de 250 euros à 15 000 euros à tout prestataire de services de dématérialisation ou de conservation et à tout prestataire de services de confiance qui:

- 1° refuse de fournir les documents et informations ou autres renseignements demandés dans le cadre du contrôle de ce prestataire;
- 2° fait obstacle à l'exercice par l'ILNAS de son pouvoir de contrôle.

**Art. 17quater. Aspects procéduraux en relation avec les amendes administratives**

(1) Les amendes sont payables dans les trente jours de la notification de la décision écrite, nonobstant l'exercice d'une voie de recours.

(2) 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 partir de la notification de la décision administrative.

(3) Le recouvrement des amendes et de toutes autres créances est confié à l'Administration de l'enregistrement, des domaines et de la TVA. Il se fait comme en matière d'enregistrement. »

## Section 2 – Dispositions pénales.

**Art. 18. Dispositions pénales dans le cadre de l'accréditation des organismes d'évaluation de la conformité.**

Est punie d'une amende de 251 euros à 25.000 euros, d'une peine d'emprisonnement de 8 jours à 6 mois ou d'une de ces peines seulement:

- 1° toute personne qui se prévaut d'une accréditation sans être titulaire d'une accréditation en cours de validité;

« (Loi du 23 décembre 2022)

- 1bis° toute personne qui se prévaut d'une notification au sens de l'article 7, sans en être titulaire;»
- 2° toute personne qui a utilisé ou apposé la marque semi-figurative „OLAS“, telle qu'enregistrée à l'Office Benelux de la Propriété intellectuelle, sans être titulaire d'une accréditation en cours de validité;
- 3° toute personne qui a utilisé ou apposé la marque semi-figurative „OLAS“, telle qu'enregistrée à l'Office Benelux de la Propriété intellectuelle, sur des certificats ou rapports pour des activités autres que celles pour lesquelles il dispose d'une accréditation.

**Art. 19. Dispositions pénales dans le cadre de la surveillance du marché.**

(1) Est punie d'une amende de 251 euros à 500.000 euros et d'une peine d'emprisonnement de 8 jours à trois ans ou d'une de ces peines seulement, toute personne qui a mis sur le marché ou qui a mis à disposition sur le marché un produit, dont le contenu ou les caractéristiques ne sont pas conformes aux « (Loi du 23 décembre 2022) dispositions législatives et réglementaires relatives aux produits visés à l'article 8, paragraphe 4 ».

(2) Est punie des mêmes peines, le maximum de l'amende prévue étant porté à 1.000.000 euros, toute personne qui ne s'est pas conformée aux décisions prises en application de l'article 13, paragraphe 2.

(3) Les tribunaux peuvent prononcer la confiscation et la destruction des biens ayant servi à l'infraction ainsi que la confiscation des bénéfices illicites.

**CHAPITRE VI – Cadre de l'administration.****Art. 20. Emplois et fonctions.**

« (Loi du 25 mars 2015) (1) Le cadre du personnel comprend un directeur et des fonctionnaires des différentes catégories de traitement telles que prévues par la loi du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat.»

(2) Le directeur doit satisfaire aux conditions de nomination à la carrière supérieure de l'Etat.

(3) Le cadre prévu au paragraphe 1<sup>er</sup> peut être complété par des stagiaires, des employés de l'Etat ainsi que des salariés de l'Etat selon les besoins de service et dans les limites des crédits budgétaires disponibles.

**Art. 21. Conditions et modalités d'admission au stage.**

Sans préjudice des conditions générales d'admission au service de l'Etat, les conditions particulières de formation, d'admission au stage, de nomination et de promotion du personnel des cadres dans l'administration sont déterminées par règlement grand-ducal qui peut également déterminer les attributions particulières de ces fonctionnaires.

**Art. 22. Nominations des fonctionnaires.**

Sont nommés par le Grand-Duc les fonctionnaires dont les fonctions sont supérieures à celles du grade 8. Le ministre nomme aux autres fonctions.

**CHAPITRE VII – Dispositions modificatives et abrogatoires.**

**Art. 23.** Modification de la loi modifiée du 17 mai 1882 sur les poids et mesures.

La loi modifiée du 17 mai 1882 sur les poids et mesures est modifiée comme suit:

1° L'article 9 est modifié comme suit:

- Au paragraphe 1 le bout de phrase « Le ministre ayant l'Economie dans ses attributions, ci-après désigné le ministre » est remplacé par le bout de phrase suivant: „Le directeur de l'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services, ci-après désigné le directeur ».
- Au paragraphe 2 le bout de phrase « service de métrologie » est remplacé par les mots « Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services » et le mot « ministre » est remplacé par le mot « directeur ».

2° A l'article 10, le paragraphe 5 est remplacé par le texte suivant: « En cas de constatation d'un manquement aux dispositions de la législation applicable, les frais de contrôle qui ont été à la base de cette constatation de non-conformité sont mis à charge des prévenus. ».

**Art. 24. Modification de la loi modifiée du 31 juillet 2006 relative à la sécurité générale des produits.**

La loi modifiée du 31 juillet 2006 relative à la sécurité générale des produits est modifiée comme suit:

1° A l'article 4 au paragraphe 3 les mots « ministre ayant la protection des consommateurs dans ses attributions, désigné ci-après par « le ministre » » sont remplacés par « le directeur de l'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services, désigné ci-après par « le directeur » ».

2° A l'article 5 au paragraphe 1 et au paragraphe 3 point 5 le mot « ministre » est remplacé par le mot « directeur ».

3° A l'article 5 le texte du paragraphe 2 est supprimé et est remplacé par le texte suivant:

« Les personnes compétentes en matière d'investigation sont celles prévues à l'article 14 paragraphe 1 de la loi du 4 juillet 2014 portant réorganisation de l'ILNAS.

L'investigation est réalisée conformément à l'article 14 paragraphe 2 de la loi précitée du 4 juillet 2014. »

4° A l'article 5 le texte du paragraphe 3 est supprimé et est remplacé par le texte suivant :

« La recherche et la constatation des infractions a lieu conformément à l'article 15 de la loi précitée du 4 juillet 2014. »

5° Le texte de l'article 6 est supprimé et remplacé par le texte suivant :

« (1) Les mesures administratives sont celles prévues à l'article 13 paragraphe 2 de la loi précitée du 4 juillet 2014.

- Les amendes administratives sont celles prévues à l'article 17 de la loi précitée du 4 juillet 2014. »
- 6° A l'article 7 le mot „ministre“ est remplacé par le mot « directeur » et les mots « les services du ministre » sont remplacés par « l'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services ».
- 7° Le texte de l'article 8 est supprimé et remplacé par le texte suivant : « Les dispositions pénales sont celles prévues à l'article 19 de la loi précitée du 4 juillet 2014. »
- 8° L'article 9 est supprimé.

**Art. 25. Modifications de la loi modifiée du 19 décembre 2008 établissant un cadre pour la fixation d'exigences en matière d'écoconception applicables aux produits consommateurs d'énergie.**

- 1° A l'article 3, paragraphe 2 la partie de phrase « 10 et 14 à 19 de la loi du 20 mai 2008 relative à la création d'un Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services » est remplacé par la partie de phrase « 8 et 13 à 15 de la loi du 4 juillet 2014 portant réorganisation de l'ILNAS ».
- 2° Le texte de l'article 14 est supprimé et remplacé par le texte suivant : « Les dispositions pénales sont celles prévues à l'article 19 de la loi du 4 juillet 2014 portant réorganisation de l'ILNAS.».
- 3° Le texte de l'article 14bis est supprimé et remplacé par le texte suivant : « Les amendes administratives sont celles prévues à l'article 17 de la loi précitée du 4 juillet 2014. ».

**Art. 26. Modification de la loi du 25 mars 2009 relative à la compatibilité électromagnétique.**

La loi du 25 mars 2009 relative à la compatibilité électromagnétique est modifiée comme suit:

- 1° A l'article 10, paragraphe 1<sup>er</sup> la partie de phrase « 9 de la loi du 20 mai 2008 relative à la création d'un Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services » est remplacé par la partie de phrase « 7 de la loi du 4 juillet 2014 portant réorganisation de l'ILNAS ».
- 2° A l'article 10 point 4 le mot « ministre » est remplacé par le mot « directeur de l'Institut ».
- 3° A l'article 12 le bout de phrase « 14, 15 et 16 de la loi du 20 mai 2008 relative à la création d'un Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services » est remplacé par le bout de phrase « 14 et 15 de la loi du 4 juillet 2014 portant réorganisation de l'ILNAS ».
- 4° A l'article 13 le bout de phrase « 17 de la loi du 20 mai 2008 relative à la création d'un Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services“ » est remplacé par le bout de phrase « 13 de la loi du 4 juillet 2014 portant réorganisation de l'ILNAS ».
- 5° Le texte de l'article 14 est remplacé par le texte suivant:  
« Les sanctions pénales sont celles prévues à l'article 18 de la loi du 4 juillet 2014 portant réorganisation de l'ILNAS. »
- 6° L'article 15 est remplacé par le nouvel article 15 suivant:

« **Art. 15.** Les amendes administratives.

Les amendes administratives sont celles prévues à l'article 17 de la loi du 4 juillet 2014 portant réorganisation de l'ILNAS. »

**Art. 27. Modification de la loi modifiée du 27 mai 2010 relative aux machines.**

La loi modifiée du 27 mai 2010 relative aux machines est modifiée comme suit:

- 1° A l'article 4, paragraphe 1<sup>er</sup> la partie de phrase « 14 à 17 de la loi modifiée du 20 mai 2008 relative à la création d'un Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services » est remplacée par la partie de phrase « 13 à 15 de la loi du 4 juillet 2014 portant réorganisation de l'ILNAS ».
- 2° A l'article 4, paragraphe 2 les mots « les articles 14 à 17 de la loi précitée du 20 mai 2008. » sont remplacés par les mots « les articles 13 à 15 de la loi précitée du 4 juillet 2014 ».

- 3° A l'article 8, paragraphe 1<sup>er</sup> le bout de phrase « le ministre ayant le travail dans ses attributions, dénommé ci-après « le ministre » » est remplacé par les mots « l'ILNAS ».
- 4° A l'article 8, paragraphe 1<sup>er</sup> la phrase « Il informe en pareil cas l'ILNAS, de la démarche entamée. » est supprimée.
- 5° A l'article 8, paragraphe 2 les mots « le ministre » sont remplacés par les mots « le directeur de l'ILNAS ».
- 6° A l'article 9 les mots « le ministre » sont remplacés par les mots « le directeur de l'ILNAS ».
- 7° A l'article 9 la phrase « Il informe en pareil cas l'ILNAS, de la démarche entamée. » est supprimée.
- 8° A l'article 10, paragraphe 1<sup>er</sup> la partie de phrase « le ministre respectivement l'ITM, chacun dans le domaine de ses compétences respectives, prennent » est remplacée par les mots « l'ILNAS, prend ». Au même article les mots « 17 de la loi du 20 mai 2008 » sont remplacés par les mots « 13 de la loi précitée du 4 juillet 2014 ».
- 9° A l'article 10, paragraphe 2 les mots « Le ministre » sont supprimés et remplacés par les mots « L'ILNAS ».
- 10° A l'article 10, paragraphe 3 les mots « le ministre » sont supprimés et remplacés par les mots « L'ILNAS ».
- 11° A l'article 10, paragraphe 4 le mot « ITM » est remplacé par le mot « ILNAS ». Au même paragraphe après le bout de phrase « et en informe le » les mots « et en informe le ministre » sont supprimés et le bout de phrase « Le ministre peut interdire par arrêté ministériel, » est supprimé et remplacé par les mots « Le directeur de l'ILNAS peut interdire ». La phrase « Cet arrêté est publié au Mémorial » est supprimée. Dans la dernière phrase du même paragraphe le mot « ministre » est remplacé par les mots « directeur de l'ILNAS ».
- 12° A l'article 13, paragraphe 1<sup>er</sup> les mots « Après avoir demandé l'avis de l'Inspection du travail et des mines, le ministre ayant dans ses attributions l'économie notifie, conformément aux dispositions du paragraphe 2 de l'article 11 de la loi précitée du 20 mai 2008 » sont remplacés par les mots « l'Office Luxembourgeois d'Accréditation et de Surveillance de l'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services notifie, conformément aux dispositions de l'article 7, paragraphes 2 à 5 de la loi précitée du 4 juillet 2014 ».
- 13° A l'article 13, paragraphe 2 les mots « sur base de l'article 9 de la loi précitée du 20 mai 2008 » sont remplacés par les mots « sur base de l'article 7, paragraphes 2 à 5 de la loi précitée du 4 juillet 2014 ».
- 14° A l'article 13, paragraphe 5, alinéas 1, 2 et 3 le mot « ITM » est remplacé par le mot « ILNAS ».
- 15° A l'article 13, paragraphe 5, alinéa 3 le bout de phrase « en informe le ministre. Le ministre » est supprimé.
- 16° A l'article 13 le paragraphe 6 est supprimé.
- 17° A l'article 13, paragraphe 7 le bout de phrase « le ministre demande au ministre ayant l'économie dans ses attributions de retirer » est remplacé par le bout de phrase « l'Office Luxembourgeois d'Accréditation et de Surveillance de l'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services retire ».
- 18° A l'article 13, paragraphe 7 les mots « l'article 9 de la loi précitée du 20 mai 2008 » sont remplacés par les mots « l'article 7 de la loi précitée du 4 juillet 2014 ».
- 19° A l'article 13, paragraphe 7, dernière phrase, le bout de phrase « Le ministre ayant l'économie dans ses attributions » est remplacé par le bout de phrase « L'Office Luxembourgeois d'Accréditation et de Surveillance ».
- 20° A l'article 18 la partie de phrase « Sans préjudice des attributions de l'ILNAS, l'ITM est compétente » est remplacée par la partie de phrase « L'ILNAS est compétent ».
- 21° A l'article 20 au paragraphe 5 après les mots « fonctionnaires enquêteurs » sont ajoutés les mots « de l'ITM » et après le mot « ministre » sont ajoutés les mots « ayant le Travail dans ses attributions ». Au même paragraphe le bout de phrase « quant à la mise sur le marché de machines sont aussi chargés de rechercher et de constater les infractions » est supprimé.
- 22° A l'article 21, paragraphe 3 après les mots « fonctionnaires enquêteurs » sont ajoutés les mots « de l'ITM » et après le mot « ministre » sont ajoutés les mots « ayant le Travail dans ses attributions ».

Au même paragraphe le bout de phrase « quant à la mise sur le marché de machines sont aussi chargés de rechercher et de constater les infractions » sont supprimés.

- 23° Dans le titre de la section 5 le mot « ITM » est remplacé par le mot « ILNAS ».
- 24° Dans l'article 22 les mots « du ministre, l'ITM » sont remplacés par les mots « de l'ILNAS, l'ILNAS ».
- 25° A l'article 23, paragraphe 1<sup>er</sup> la date „20 mai 2008“ est remplacée par la date „4 juillet 2014“.
- 26° A l'article 23, paragraphe 2 la date „20 mai 2008“ est remplacée par la date „4 juillet 2014“.
- 27° Le texte de l'article 24 est remplacé par le texte suivant :
- « Les sanctions pénales sont celles prévues à l'article 18 de la loi du 4 juillet 2014 portant réorganisation de l'ILNAS.
- Les amendes administratives sont celles prévues à l'article 17 de la loi du 4 juillet 2014 portant réorganisation de l'ILNAS. »
- 28° L'article 25 est abrogé sans préjudice des dispositions de l'article 31, paragraphe 3 de la loi du 4 juillet 2014 portant réorganisation de l'ILNAS.

**Art. 28. Modification de la loi modifiée du 15 décembre 2010 relative à la sécurité des jouets.**

La loi du 15 décembre 2010 relative à la sécurité des jouets est modifiée comme suit:

- 1° A l'article 3 la définition de « Institut » est modifiée comme suit : La date « 20 mai 2008 » est remplacée par la date « 4 juillet 2014 ».
- 2° A l'article 3 la définition « loi du 20 mai 2008 » est supprimée et remplacée par la définition « loi du 4 juillet 2014 : loi du 4 juillet 2014 portant réorganisation de l'ILNAS ».
- 3° Le texte de l'article 21 est remplacé par le texte suivant: « Conformément à l'article 7, paragraphes 2 à 4 de la loi du 4 juillet 2014 portant réorganisation de l'ILNAS, l'ILNAS notifie à la Commission européenne et aux autres Etats membres, les organismes autorisés à effectuer des tâches d'évaluation de la conformité par un tiers, au titre de l'article 19 de la présente loi. »
- 4° L'article 22 est supprimé.
- 5° A l'article 28, paragraphe 1<sup>er</sup> les mots « le ministre » sont remplacés par les mots « L'Institut ». Au même paragraphe les mots « 9 de la loi du 20 mai 2008 » sont remplacés par les mots « 7 de la loi du 4 juillet 2014 portant réorganisation de l'ILNAS ».
- 6° A l'article 28, paragraphe 2 le bout de phrase « , au nom du ministre, » est supprimé.
- 7° A l'article 29, paragraphe 1 le bout de phrase « le ministre sur proposition de » est supprimé.
- 8° A l'article 30 les mots « le ministre sur avis de » sont supprimés.
- 9° A l'article 37 le bout de phrase « 17 de la loi du 20 mai 2008 » est remplacé par le bout de phrase « 13 de la loi du 4 juillet 2014 ».

**Art. 29. Modification de la loi du 21 décembre 2012 concernant les équipements sous pression transportables.**

La loi du 21 décembre 2012 concernant les équipements sous pression transportables est modifiée comme suit:

- 1° A l'article 21, paragraphe 1<sup>er</sup>, 1<sup>er</sup> alinéa, les mots « loi modifiée du 20 mai 2008 relative à la création d'un Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services » sont remplacés par les mots « loi du 4 juillet 2014 portant réorganisation de l'ILNAS ».
- 2° A l'article 21, paragraphe 1<sup>er</sup>, 3<sup>ème</sup> alinéa les mots « loi modifiée du 20 mai 2008 relative à la création d'un Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services » sont remplacés par les mots « loi du 4 juillet 2014 portant réorganisation de l'ILNAS ».

**Art. 30.** Abrogation de la loi modifiée du 20 mai 2008 relative à la création d'un Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services.

La loi modifiée du 20 mai 2008 relative à la création d'un Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services est abrogée.

## CHAPITRE VIII – Dispositions transitoires.

### Art. 31. Dispositions relatives au personnel.

(1) Pour chaque carrière, il est établi un tableau d'avancement unique regroupant tous les fonctionnaires de cette carrière. Les nominations des fonctionnaires aux grades supérieurs de leur carrière se font par application des lois et règlements déterminant les conditions et modalités d'avancement des fonctionnaires de l'Etat. Toutefois, les fonctionnaires transférés vers l'ILNAS au 1er juin 2008 peuvent bénéficier d'une promotion à un grade supérieur de leur carrière par dérogation à ces lois et règlements, s'il est établi qu'ils auraient bénéficié dans leur administration d'origine de la même promotion s'ils avaient continué à faire partie de cette administration.

Cette disposition produira ses effets jusqu'au 31 mai 2018.

(2) Les fonctionnaires de la carrière de l'expéditionnaire technique engagés le 1er février 1991 auprès du Service de l'énergie de l'Etat, pourront être désignés par le Ministre pour les missions définies à l'article 14.

(3) L'ILNAS est autorisé à procéder à l'engagement de huit fonctionnaires de la carrière moyenne de l'ingénieur technicien en plus du contingent déjà légalement autorisé, déduction faite du nombre de fonctionnaires que l'Inspection du travail et des mines a engagés à la date de l'entrée en vigueur de la présente loi sur base de l'article 25 abrogé de la loi modifiée du 27 mai 2010 relative aux machines. Les fonctionnaires en question de l'Inspection du travail et des mines sont transférés à l'ILNAS.

(4) Les stagiaires des carrières de l'attaché de direction et de l'ingénieur engagés à la date de l'entrée en vigueur de la présente loi sur base de l'article 25 abrogé de la loi modifiée du 27 mai 2010 relative aux machines sont transférés à l'ILNAS.

Les stagiaires en question sont admissibles à l'examen de formation spéciale et à l'examen de fin de stage de l'année 2014 de l'Inspection du travail et des mines.

## CHAPITRE IX – Dispositions finales.

### Art. 32. Références à la présente loi.

Dans toute disposition légale et réglementaire future, la référence à la présente loi pourra se faire sous une forme abrégée en utilisant les termes de „loi du 4 juillet 2014 portant réorganisation de l'ILNAS“.

\*

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

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

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

vu la proposition de la Commission européenne,

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

vu l'avis du Comité économique et social européen <sup>(1)</sup>,

vu l'avis du Comité des régions <sup>(2)</sup>,

statuant conformément à la procédure législative ordinaire <sup>(3)</sup>,

considérant ce qui suit:

- (1) Les réseaux et systèmes d'information et les réseaux et services de communications électroniques remplissent une fonction essentielle dans la société et sont devenus le nerf de la croissance économique. Les technologies de l'information et des communications (TIC) sont le fondement des systèmes complexes qui rendent possibles les activités sociales quotidiennes, permettent à nos économies de fonctionner dans des secteurs clés comme la santé, l'énergie, la finance et les transports, et soutiennent, en particulier, le fonctionnement du marché intérieur.
- (2) L'utilisation des réseaux et des systèmes d'information par les citoyens, les organisations et les entreprises s'est généralisée dans l'Union tout entière. La numérisation et la connectivité deviennent des caractéristiques essentielles d'un nombre toujours croissant de produits et de services et avec l'avènement de l'internet des objets (IdO), un nombre extrêmement élevé de dispositifs numériques connectés devrait être mis en service dans toute l'Union au cours de la prochaine décennie. Alors qu'un nombre croissant de dispositifs sont connectés à l'internet, leur conception n'intègre pas suffisamment la sécurité et la résilience, de sorte que la cybersécurité est insuffisante. Dans ce contexte, le recours limité à la certification conduit les utilisateurs — qu'ils soient des particuliers, des organisations ou des entreprises — à ne pas disposer de suffisamment d'informations sur les caractéristiques en matière de cybersécurité des produits TIC, services TIC et processus TIC, ce qui nuit à la confiance dans les solutions numériques. Les réseaux et systèmes d'information sont à même de nous assister dans tous les aspects de notre vie et constituent le moteur de la croissance économique de l'Union. Ils constituent le pilier de la réalisation du marché unique numérique.
- (3) Une numérisation et une connectivité accrues augmentent les risques liés à la cybersécurité, ce qui rend l'ensemble de la société plus vulnérable aux cybermenaces et exacerbe les dangers auxquels sont confrontés les individus, notamment les personnes vulnérables telles que les enfants. Afin d'atténuer ces risques, il convient de prendre toutes les mesures nécessaires pour améliorer la cybersécurité dans l'Union afin que les réseaux et systèmes d'information, les réseaux de communication, les produits, services et appareils numériques utilisés par les citoyens, les organisations et les entreprises — depuis les petites et moyennes entreprises (PME), telles qu'elles sont définies dans la recommandation 2003/361/CE de la Commission <sup>(4)</sup>, jusqu'aux opérateurs d'infrastructures critiques — soient mieux protégés contre les cybermenaces.

<sup>(1)</sup> JO C 227 du 28.6.2018, p. 86.

<sup>(2)</sup> JO C 176 du 23.5.2018, p. 29.

<sup>(3)</sup> Position du Parlement européen du 12 mars 2019 (non encore parue au Journal officiel) et décision du Conseil du 9 avril 2019.

<sup>(4)</sup> Recommandation de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises (JO L 124 du 20.5.2003, p. 36).

- (4) En mettant les informations utiles à la disposition du public, l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA), instituée par le règlement (UE) n° 526/2013 du Parlement européen et du Conseil <sup>(5)</sup>, contribue au développement du secteur de la cybersécurité dans l'Union, en particulier les PME et les start-ups. L'ENISA devrait s'efforcer d'établir une coopération plus étroite avec les universités et les entités de recherche afin de contribuer à réduire la dépendance à l'égard des produits et services de cybersécurité provenant de l'extérieur de l'Union et de renforcer les chaînes d'approvisionnement à l'intérieur de l'Union.
- (5) Les cyberattaques sont en augmentation, et une économie et une société connectées qui sont plus vulnérables aux cybermenaces et aux cyberattaques ont besoin de dispositifs de défense renforcés. Cependant, alors que les cyberattaques sont souvent de nature transfrontière, les compétences des autorités chargées de la cybersécurité et des autorités chargées de l'application de la loi ainsi que les réponses politiques qu'elles y apportent sont surtout nationales. Des incidents majeurs pourraient perturber la fourniture de services essentiels dans l'ensemble de l'Union. Cela nécessite de mettre en place des réponses efficaces et coordonnées et une gestion de la crise à l'échelon de l'Union, sur la base de politiques spécifiques et d'instruments élargis aux fins de la solidarité européenne et de l'assistance mutuelle. En outre, il est important pour les décideurs, les entreprises du secteur et les utilisateurs que la situation en matière de cybersécurité et de résilience dans l'Union soit régulièrement évaluée, sur la base de données de l'Union fiables et d'une anticipation systématique des évolutions, défis et menaces futurs au niveau de l'Union et à l'échelle mondiale.
- (6) Compte tenu de l'augmentation des enjeux auxquels l'Union est confrontée dans le domaine de la cybersécurité, il est nécessaire de disposer d'un ensemble complet de mesures qui s'appuieraient sur les actions déjà menées par l'Union et favoriseraient des objectifs complémentaires. Ces objectifs comprennent la poursuite du renforcement des capacités et de l'état de préparation des États membres et des entreprises, ainsi qu'une amélioration de la coopération, du partage d'informations et de la coordination entre les États membres et les institutions, organes et organismes de l'Union. En outre, étant donné que les cybermenaces ignorent les frontières, il est nécessaire d'augmenter, au niveau de l'Union, les capacités susceptibles de compléter l'action des États membres, notamment dans les cas d'incidents et de crises transfrontières majeurs, tout en prenant en compte l'importance de préserver et de renforcer les capacités nationales de réaction en cas de cybermenaces de tous types.
- (7) Des efforts supplémentaires sont également nécessaires pour sensibiliser davantage les citoyens, les organisations et les entreprises aux questions de cybersécurité. En outre, étant donné que les incidents nuisent à la confiance dans les fournisseurs de services numériques et dans le marché unique numérique lui-même, en particulier chez les consommateurs, cette confiance devrait être encore renforcée par la communication, en toute transparence, d'informations sur le niveau de sécurité qui caractérise les produits TIC, services TIC et processus TIC, qui précisent que la certification de cybersécurité, aussi élevée soit-elle, ne peut garantir qu'un produit TIC, service TIC ou processus TIC soit complètement sécurisé. Un renforcement de la confiance peut être facilité par une certification mise en œuvre à l'échelle de l'Union prévoyant des exigences et des critères d'évaluation communs en matière de cybersécurité dans l'ensemble des marchés nationaux et des secteurs.
- (8) La cybersécurité n'est pas qu'une question liée à la technologie, mais une question pour laquelle le comportement humain est tout aussi important. C'est pourquoi il convient d'encourager vivement les citoyens, les organisations et les entreprises à adopter une «hygiène informatique», à savoir des mesures simples, de routine qui, lorsqu'ils les mettent en œuvre et les effectuent régulièrement, réduisent au minimum leur exposition aux risques liés aux cybermenaces.
- (9) En vue de renforcer les structures de cybersécurité de l'Union, il est important de préserver et de développer les capacités de réaction globale des États membres en cas de cybermenaces, y compris en cas d'incidents transfrontières.
- (10) Les entreprises et les consommateurs individuels devraient disposer d'informations précises sur le niveau d'assurance auquel la sécurité de leurs produits TIC, services TIC et processus TIC a été certifiée. Dans le même temps, aucun produit TIC ou service TIC n'est totalement sécurisé sur le plan de la cybersécurité, et des règles fondamentales d'hygiène informatique doivent être promues et privilégiées. Compte tenu de la disponibilité croissante de dispositifs IdO, le secteur privé peut prendre une série de mesures volontaires dans l'optique de renforcer la sécurité des produits TIC, services TIC et processus TIC.
- (11) Souvent, les produits et systèmes TIC modernes intègrent une ou plusieurs technologies et composants tiers et reposent sur ceux-ci, par exemple des modules logiciels, des bibliothèques ou des interfaces de programmation d'applications. Ce rapport dit de «dépendance» pourrait présenter des risques supplémentaires liés à la cybersécurité car les vulnérabilités des composants tiers pourraient aussi affecter la sécurité des produits TIC, services TIC et processus TIC. Dans bon nombre de cas, recenser et documenter ces dépendances permet aux utilisateurs finaux des produits TIC, services TIC et processus TIC d'optimiser leurs activités de gestion des risques liés à la cybersécurité en améliorant, par exemple, les procédures qu'ils mettent en œuvre pour gérer les vulnérabilités liées à la cybersécurité et y remédier.

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

- (12) Les organisations, les fabricants ou les fournisseurs impliqués dans la conception et le développement de produits TIC, services TIC ou processus TIC devraient être encouragés à mettre en œuvre, aux stades les plus précoces de la conception et du développement, des mesures permettant de protéger au mieux la sécurité de ces produits, services et processus, de manière que la survenue de cyberattaques soit présumée et que leur incidence soit anticipée et minimisée («sécurité dès le stade de la conception»). La sécurité devrait être prise en charge tout au long du cycle de vie du produit TIC, service TIC ou processus TIC par les processus de conception et de développement qui évoluent constamment pour réduire le risque de préjudice causé par une utilisation malveillante.
- (13) Les entreprises, les organisations et le secteur public devraient configurer les produits TIC, services TIC ou processus TIC qu'ils conçoivent de manière à assurer un niveau de sécurité plus élevé, ce qui permettrait au premier utilisateur de recevoir une configuration par défaut avec les paramètres les plus sûrs possibles (ci-après dénommée «sécurité par défaut»), réduisant ainsi la charge qui pèse sur les utilisateurs de devoir configurer un produit TIC, service TIC ou processus TIC de manière adéquate. Pour fonctionner, la sécurité par défaut ne devrait pas nécessiter une configuration approfondie, ou une compréhension des détails techniques spécifique, ou encore un comportement non intuitif de la part de l'utilisateur, et devrait fonctionner facilement et de façon fiable lorsqu'elle est mise en œuvre. Si, au cas par cas, une analyse des risques et de la facilité d'utilisation aboutit à la conclusion qu'une configuration par défaut n'est pas réalisable, les utilisateurs devraient être incités à choisir le paramétrage le plus sécurisé.
- (14) Le règlement (CE) n° 460/2004 du Parlement européen et du Conseil <sup>(6)</sup> a institué l'ENISA aux fins de contribuer à la réalisation des objectifs visant à assurer un niveau élevé et efficace de sécurité des réseaux et de l'information au sein de l'Union et à favoriser l'émergence d'une culture de la sécurité des réseaux et de l'information dans l'intérêt des citoyens, des consommateurs, des entreprises et des administrations publiques. Le règlement (CE) n° 1007/2008 du Parlement européen et du Conseil <sup>(7)</sup> a prorogé le mandat de l'ENISA jusqu'en mars 2012. Le règlement (UE) n° 580/2011 du Parlement européen et du Conseil <sup>(8)</sup> a prorogé le mandat de l'ENISA une nouvelle fois jusqu'au 13 septembre 2013. Le règlement (UE) n° 526/2013 a prorogé le mandat de l'ENISA jusqu'au 19 juin 2020.
- (15) L'Union a déjà pris d'importantes mesures pour garantir la cybersécurité et renforcer la confiance dans les technologies numériques. En 2013, la stratégie de cybersécurité de l'Union européenne a été adoptée afin d'orienter la politique que l'Union entendait mener en réaction aux cybermenaces et aux risques liés à la cybersécurité. Dans le but de mieux protéger les citoyens en ligne, l'Union a adopté en 2016 son premier acte juridique dans le domaine de la cybersécurité sous la forme de la directive (UE) 2016/1148 du Parlement européen et du Conseil <sup>(9)</sup>. La directive (UE) 2016/1148 a instauré des exigences concernant les capacités nationales dans le domaine de la cybersécurité, a établi les premiers mécanismes destinés à améliorer la coopération stratégique et opérationnelle entre les États membres, et a introduit des obligations concernant les mesures de sécurité et la notification des incidents dans différents secteurs qui revêtent une importance vitale pour l'économie et la société tels que l'énergie, les transports, la fourniture et la distribution d'eau potable, les banques, les infrastructures des marchés financiers, les soins de santé, les infrastructures numériques ainsi que les fournisseurs de services numériques fondamentaux (moteurs de recherche, services d'informatique en nuage et places de marché en ligne).

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

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

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

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

<sup>(9)</sup> Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (JO L 194 du 19.7.2016, p. 1).

<sup>(10)</sup> Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

<sup>(11)</sup> Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37).

<sup>(12)</sup> Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen (JO L 321 du 17.12.2018, p. 36).

- (16) Depuis l'adoption de la stratégie de cybersécurité de l'Union européenne en 2013 et la dernière révision du mandat de l'ENISA, le cadre d'action général a considérablement évolué en raison d'un environnement mondial devenu plus incertain et moins sécurisé. Dans ce contexte, et compte tenu de l'évolution positive du rôle que l'ENISA joue en tant que point de référence par ses conseils et ses compétences, et en tant que facilitatrice de coopération et de renforcement des capacités, ainsi que dans le cadre de la nouvelle politique de cybersécurité de l'Union, il est nécessaire de réviser le mandat de l'ENISA pour définir son rôle dans le nouvel écosystème de la cybersécurité et faire en sorte qu'elle contribue efficacement à la réponse apportée par l'Union aux défis en matière de cybersécurité qui résultent de la transformation radicale de la situation en ce qui concerne les cybermenaces, à l'égard desquels le mandat actuel de l'ENISA est insuffisant ainsi qu'il est apparu lors de l'évaluation de l'ENISA.
- (17) L'ENISA instituée par le présent règlement devrait succéder à l'ENISA instituée par le règlement (UE) n° 526/2013. L'ENISA devrait remplir les tâches qui lui sont confiées par le présent règlement et par les autres actes juridiques de l'Union dans le domaine de la cybersécurité, notamment en fournissant des conseils et en apportant des compétences, ainsi qu'en jouant le rôle de centre d'information et de connaissance de l'Union. Elle devrait promouvoir l'échange de bonnes pratiques entre les États membres et les parties prenantes du secteur privé, proposer des actions politiques à la Commission et aux États membres, agir en tant que point de référence pour les initiatives politiques sectorielles au niveau de l'Union en ce qui concerne les questions de cybersécurité, et favoriser la coopération opérationnelle à la fois entre les États membres et entre ceux-ci et les institutions, organes et organismes de l'Union.
- (18) Dans le cadre de la décision 2004/97/CE, Euratom prise d'un commun accord entre les représentants des États membres réunis au niveau des chefs d'État ou de gouvernement <sup>(13)</sup>, les représentants des États membres ont décidé que l'ENISA aurait son siège dans une ville en Grèce qui serait désignée par le gouvernement grec. L'État membre d'accueil de l'ENISA devrait offrir les meilleures conditions possibles pour un fonctionnement harmonieux et efficace de l'ENISA. Il est impératif, pour l'exécution correcte et efficace de ses tâches, pour le recrutement et la fidélisation du personnel et pour une plus grande efficacité des activités de mise en réseau, que l'ENISA soit établie dans un lieu approprié, offrant, entre autres, des liaisons de transport et des aménagements appropriés pour les conjoints et enfants accompagnant les membres du personnel de l'ENISA. Les dispositions nécessaires devraient être arrêtées dans un accord conclu entre l'ENISA et l'État membre d'accueil, après approbation du conseil d'administration de l'ENISA.
- (19) Compte tenu de l'aggravation des risques et des défis liés à la cybersécurité auxquels l'Union est confrontée, il faudrait augmenter les ressources financières et humaines allouées à l'ENISA pour tenir compte du renforcement de son rôle et de ses tâches, ainsi que de sa position critique parmi les organisations qui défendent l'écosystème numérique de l'Union, pour lui permettre d'exécuter efficacement les tâches qui lui sont confiées en vertu du présent règlement.
- (20) L'ENISA devrait acquérir et maintenir un niveau élevé de compétence et servir de point de référence qui instaure la confiance dans le marché intérieur du fait de son indépendance, de la qualité des conseils qu'elle fournit et des informations qu'elle diffuse, de la transparence de ses procédures, de la transparence de ses modes de fonctionnement et de sa diligence à exécuter ses tâches. L'ENISA devrait soutenir activement les efforts déployés au niveau national et devrait contribuer de manière anticipée aux efforts consentis par l'Union, tout en s'acquittant de ses missions en totale coopération avec les institutions, organes et organismes de l'Union et avec les États membres, en évitant les doubles emplois et en favorisant les synergies. De plus, l'ENISA devrait s'appuyer sur les informations fournies par le secteur privé et les autres parties prenantes concernées et travailler en coopération avec ceux-ci. Un ensemble de tâches devrait déterminer la manière dont l'ENISA doit atteindre ses objectifs tout en lui laissant une certaine souplesse de fonctionnement.
- (21) Pour être en mesure d'apporter un soutien adéquat à la coopération opérationnelle entre les États membres, l'ENISA devrait renforcer davantage ses capacités et aptitudes techniques et humaines. Elle devrait accroître son savoir-faire et ses capacités. Sur une base volontaire, l'ENISA et les États membres pourraient élaborer des programmes visant à détacher des experts nationaux auprès de l'ENISA, en créant des groupes d'experts et des programmes d'échanges de personnel.
- (22) L'ENISA devrait assister la Commission au moyen de conseils, d'avis et d'analyses sur toutes les questions de l'Union liées à l'élaboration, l'actualisation et la révision des politiques et de la législation dans le domaine de la cybersécurité et de ses aspects sectoriels spécifiques, afin d'améliorer la pertinence des politiques et de la législation de l'Union ayant une dimension liée à la cybersécurité et de permettre la mise en œuvre cohérente de ces politiques et législations au niveau national. L'ENISA devrait agir comme point de référence, par ses conseils et ses compétences, pour les initiatives politiques et législatives sectorielles spécifiques au niveau de l'Union lorsque des questions liées à la cybersécurité sont en jeu. L'ENISA devrait tenir le Parlement européen régulièrement informé de ses activités.

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

- (23) Le noyau public de l'internet ouvert, à savoir ses principaux protocoles et ses principales infrastructures, qui constituent un bien public mondial, joue un rôle essentiel dans la fonction de l'internet en général et soutient son fonctionnement normal. L'ENISA devrait soutenir la sécurité du noyau public de l'internet ouvert et la stabilité de son fonctionnement, y compris, sans s'y limiter, ses protocoles clés (notamment DNS, BGP et IPv6), le fonctionnement du système des noms de domaines (tel que le fonctionnement de tous les domaines de premier niveau) et le fonctionnement de la zone racine.
- (24) La principale tâche de l'ENISA consiste à promouvoir la mise en œuvre cohérente du cadre juridique applicable, et notamment la mise en œuvre effective de la directive (UE) 2016/1148 ainsi que des autres instruments juridiques pertinents comportant des aspects liés à la cybersécurité, ce qui est essentiel pour renforcer la cyber-résilience. Compte tenu de l'évolution rapide de la situation en ce qui concerne les cybermenaces, il est clair que les États membres doivent s'appuyer sur une approche plus globale, transsectorielle, du développement de la cyber-résilience.
- (25) L'ENISA devrait assister les États membres et les institutions, organes et organismes de l'Union dans leurs efforts pour mettre en place et développer les capacités et la préparation requises aux fins de prévenir et de détecter les cybermenaces et incidents et d'y réagir, et en ce qui concerne la sécurité des réseaux et des systèmes d'information. L'ENISA devrait notamment soutenir le développement et l'amélioration des centres de réponse aux incidents de sécurité informatique (CSIRT) nationaux et de l'Union prévus par la directive (UE) 2016/1148, afin qu'ils atteignent un niveau de maturité commun élevé dans l'ensemble de l'Union. Les activités entreprises par l'ENISA concernant les capacités opérationnelles des États membres devraient soutenir activement les mesures prises par les États membres pour respecter les obligations qui leur incombent au titre de la directive (UE) 2016/1148 et ne devraient donc pas s'y substituer.
- (26) L'ENISA devrait également contribuer à l'élaboration et à la mise à jour des stratégies en matière de sécurité des réseaux et systèmes d'information au niveau de l'Union et, sur demande, au niveau des États membres, notamment en matière de cybersécurité, et devrait promouvoir la diffusion de telles stratégies et suivre les progrès de leur mise en œuvre. L'ENISA devrait en outre contribuer à couvrir les besoins en matière de formations et de matériel pédagogique, y compris les besoins des organismes publics et, le cas échéant, dans une large mesure, «former les formateurs» en s'appuyant sur le cadre de compétences numériques pour les citoyens, en vue d'aider les États membres ainsi que les institutions, organes et organismes de l'Union à mettre en place leurs propres capacités de formation.
- (27) L'ENISA devrait soutenir les États membres dans le domaine de la sensibilisation et de l'éducation à la cybersécurité en favorisant une coordination plus étroite et l'échange de bonnes pratiques entre les États membres. Un tel soutien pourrait consister à développer un réseau de points de contact nationaux en matière d'éducation ainsi qu'une plateforme de formation à la cybersécurité. Le réseau de points de contact nationaux en matière d'éducation pourrait fonctionner au sein du réseau des agents de liaison nationaux et être un point de départ pour une future coordination au sein des États membres.
- (28) L'ENISA devrait aider le groupe de coopération créé par la directive (UE) 2016/1148 à exécuter ses tâches, notamment en le faisant bénéficier de ses conseils et de ses compétences, et en facilitant l'échange de bonnes pratiques en matière de risques et d'incidents, entre autres en ce qui concerne l'identification des opérateurs de services essentiels par les États membres, ainsi que les dépendances transfrontalières.
- (29) Afin de stimuler la coopération entre le secteur public et le secteur privé et au sein de ce dernier, notamment pour soutenir la protection des infrastructures critiques, l'ENISA devrait soutenir le partage d'informations au sein des secteurs et entre ceux-ci, en particulier les secteurs énumérés à l'annexe II de la directive (UE) 2016/1148, en proposant des bonnes pratiques et des orientations sur les outils disponibles et sur les procédures, ainsi qu'en proposant des orientations sur la manière de traiter les questions de réglementation liées au partage d'informations, par exemple en facilitant la mise en place de centres de partage et d'analyse d'informations sectoriels.
- (30) Comme l'incidence négative potentielle des vulnérabilités des produits TIC, services TIC et processus TIC croît constamment, il importe de détecter ces vulnérabilités et d'y remédier pour réduire le risque global en matière de cybersécurité. Il est prouvé que la coopération entre les organisations, les fabricants de produits TIC vulnérables ou les fournisseurs de services et processus TIC vulnérables ainsi que les acteurs du secteur de la recherche en matière de cybersécurité et les autorités qui détectent les vulnérabilités permet d'améliorer sensiblement le taux de détection et le rythme de l'élimination des vulnérabilités dans les produits TIC, services TIC et processus TIC. La divulgation coordonnée des vulnérabilités consiste en un processus structuré de coopération dans lequel les vulnérabilités sont signalées au propriétaire du système d'information, ce qui donne à l'organisation la possibilité de diagnostiquer la vulnérabilité et d'y remédier avant que des informations détaillées à ce sujet soient divulguées à des tiers ou au public. Ce processus prévoit en outre une coordination entre la partie qui a procédé à la détection et l'organisation en ce qui concerne la publication de ces vulnérabilités. Les politiques coordonnées de divulgation des vulnérabilités pourraient jouer un rôle important dans le cadre des efforts que les États membres déploient pour renforcer la cybersécurité.

- (31) L'ENISA devrait agréger et analyser les rapports nationaux partagés volontairement et qui émanent des CSIRT et de l'équipe d'intervention en cas d'urgence informatique pour les institutions, organes et organismes de l'Union interinstitutionnelle instituée en vertu de l'accord entre le Parlement européen, le Conseil européen, le Conseil de l'Union européenne, la Commission européenne, la Cour de justice de l'Union européenne, la Banque centrale européenne, la Cour des comptes européenne, le Service européen pour l'action extérieure, le Comité économique et social européen, le Comité européen des régions et la Banque européenne d'investissement relatif à l'organisation et au fonctionnement d'une équipe d'intervention en cas d'urgence informatique pour les institutions, organes et organismes de l'Union (CERT-UE) <sup>(14)</sup> afin de contribuer à établir des procédures, un langage et une terminologie communs pour l'échange d'informations. Dans ce contexte, l'ENISA devrait impliquer le secteur privé, dans le cadre de la directive (UE) 2016/1148, laquelle fixe les bases de l'échange volontaire d'informations techniques à l'échelon opérationnel au sein du réseau des centres de réponse aux incidents de sécurité informatique (ci-après dénommé «réseau des CSIRT») institué par ladite directive.
- (32) L'ENISA devrait contribuer à l'élaboration de réponses au niveau de l'Union en cas d'incidents et de crises trans-frontières majeurs liés à la cybersécurité. Cette tâche devrait être effectuée conformément au mandat de l'ENISA en application du présent règlement, ainsi qu'à une approche devant faire l'objet d'un accord des États membres dans le cadre de la recommandation (UE) 2017/1584 de la Commission <sup>(15)</sup> et des conclusions du Conseil du 26 juin 2018 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs de l'Union. Cette tâche pourrait comprendre la collecte d'informations pertinentes et un rôle de facilitateur entre le réseau des CSIRT et la communauté technique, ainsi qu'entre les décideurs chargés de la gestion des crises. En outre, l'ENISA devrait soutenir la coopération opérationnelle entre les États membres si un ou plusieurs États membres le demandent, pour le traitement des incidents sur le plan technique, en facilitant les échanges de solutions techniques pertinents entre les États membres et en contribuant à l'élaboration des communications au public. L'ENISA devrait soutenir la coopération opérationnelle en testant les modalités de cette coopération grâce à des exercices réguliers de cybersécurité.
- (33) Pour soutenir la coopération opérationnelle, l'ENISA devrait recourir aux compétences techniques et opérationnelles disponibles de la CERT-UE grâce à une coopération structurée. Une telle coopération structurée pourrait s'appuyer sur les compétences de l'ENISA. Le cas échéant, des accords dédiés entre les deux entités devraient être conclus afin de définir les modalités pratiques de la mise en œuvre de cette coopération et d'éviter la duplication des activités.
- (34) En exécutant sa tâche consistant à soutenir la coopération opérationnelle au sein du réseau des CSIRT, l'ENISA devrait être en mesure de fournir un appui aux États membres, à leur demande, par exemple en fournissant des conseils sur la manière d'améliorer leurs capacités de prévention et de détection des incidents et de réaction aux incidents, en facilitant la gestion technique des incidents ayant un impact significatif ou substantiel, ou en assurant l'analyse des cybermenaces et des incidents. L'ENISA devrait faciliter la gestion technique des incidents ayant un impact significatif ou substantiel, en particulier en soutenant le partage volontaire de solutions techniques entre États membres ou en produisant des informations techniques combinées, telles que des solutions techniques partagées volontairement par les États membres. La recommandation (UE) 2017/1584 recommande aux États membres de coopérer de bonne foi et de partager sans retard indu, entre eux et avec l'ENISA, les informations relatives aux incidents et crises de cybersécurité majeurs. Ces informations devraient apporter une aide supplémentaire à l'ENISA dans l'exécution de sa tâche de soutien à la coopération opérationnelle.
- (35) Dans le cadre de la coopération régulière sur le plan technique menée pour étayer l'appréciation de la situation au niveau de l'Union, l'ENISA devrait préparer à intervalles réguliers, en coopération étroite avec les États membres, un rapport approfondi de situation technique en matière de cybersécurité sur les incidents et cybermenaces dans l'Union, sur la base d'informations du domaine public, de sa propre analyse et de rapports que lui communiquent les CSIRT des États membres ou les points de contact nationaux uniques en matière de sécurité des réseaux et des systèmes d'information (ci-après dénommés «points de contact uniques») prévus par la directive (UE) 2016/1148, sur une base volontaire dans les deux cas, le Centre européen de lutte contre la cybercriminalité (EC3) au sein d'Europol, la CERT-UE et, le cas échéant, le Centre de l'Union européenne pour l'analyse du renseignement (INTCEN UE) au sein du Service européen pour l'action extérieure. Ce rapport devrait être mis à la disposition du Conseil, de la Commission, du haut représentant de l'Union pour les affaires étrangères et la politique de sécurité et du réseau des CSIRT.
- (36) Le soutien apporté par l'ENISA aux enquêtes techniques ex post sur les incidents ayant un impact significatif ou substantiel, effectuées à la demande des États membres concernés, devrait être axé sur la prévention des incidents futurs. Les États membres concernés devraient fournir les informations et l'assistance nécessaires pour permettre à l'ENISA de soutenir efficacement l'enquête technique ex post.

<sup>(14)</sup> JO C 12 du 13.1.2018, p. 1.

<sup>(15)</sup> Recommandation (UE) 2017/1584 de la Commission du 13 septembre 2017 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs (JO L 239 du 19.9.2017, p. 36).

- (37) Les États membres peuvent inviter les entreprises concernées par l'incident à coopérer en fournissant les renseignements et l'assistance nécessaires à l'ENISA, sans préjudice de leur droit de protéger les informations commercialement sensibles et les informations pertinentes du point de vue de la sécurité publique.
- (38) Pour mieux comprendre les défis dans le domaine de la cybersécurité, et en vue de fournir aux États membres et aux institutions, organes et organismes de l'Union des conseils stratégiques à long terme, l'ENISA devrait analyser les risques actuels et émergents liés à la cybersécurité. À cet effet, l'ENISA devrait, en coopération avec les États membres et, le cas échéant, avec des organismes de statistique et d'autres organismes, recueillir des informations pertinentes du domaine public ou partagées volontairement sur les technologies émergentes, les soumettre à des analyses et fournir des évaluations thématiques spécifiques sur les effets sociétaux, juridiques, économiques et réglementaires à attendre des innovations technologiques sur la sécurité des réseaux et de l'information, notamment sur la cybersécurité. L'ENISA devrait en outre aider les États membres et les institutions, organes et organismes de l'Union à recenser les risques émergents liés à la cybersécurité et à prévenir les incidents, en procédant à l'analyse des cybermenaces, des vulnérabilités et des incidents.
- (39) Afin de renforcer la résilience de l'Union, l'ENISA devrait développer des compétences dans le domaine de la cybersécurité des infrastructures, en soutenant en particulier les secteurs énumérés à l'annexe II de la directive (UE) 2016/1148 et ceux utilisés par les fournisseurs des services numériques énumérés à l'annexe III de ladite directive, en fournissant des conseils et des lignes directrices et en échangeant de bonnes pratiques. En vue de faciliter l'accès à des informations mieux structurées sur les risques liés à la cybersécurité et les solutions possibles, l'ENISA devrait mettre sur pied et gérer le «pôle d'information» de l'Union, un portail servant de guichet unique fournissant au public des informations sur la cybersécurité en provenance des institutions, organes et organismes de l'Union et nationaux. Faciliter l'accès à des informations mieux structurées sur les risques liés à la cybersécurité et les solutions possibles pourrait aussi aider les États membres à consolider leurs capacités, à harmoniser leurs pratiques et, partant, à améliorer leur résilience générale face aux cyberattaques.
- (40) L'ENISA devrait contribuer à sensibiliser le public aux risques liés à la cybersécurité, y compris en organisant une campagne de sensibilisation à l'échelle de l'Union en favorisant l'éducation, et à fournir, à l'intention des citoyens, des organisations et des entreprises des orientations sur les bonnes pratiques à adopter par les utilisateurs individuels. L'ENISA devrait également contribuer à promouvoir les meilleures pratiques et solutions, y compris en matière d'hygiène informatique et d'habileté numérique au niveau des citoyens, des organisations et des entreprises en collectant et en analysant des informations du domaine public sur les incidents significatifs, et en rédigeant et en publiant des rapports et des orientations à l'intention des citoyens, des organisations et des entreprises en vue d'améliorer leur niveau global de préparation et de résilience. L'ENISA devrait également s'efforcer de fournir aux consommateurs des informations pertinentes concernant les schémas de certification en vigueur, par exemple en fournissant des lignes directrices et des recommandations. L'ENISA devrait en outre organiser, conformément au plan d'action en matière d'éducation numérique établi par la communication de la Commission du 17 janvier 2018 et en coopération avec les États membres et les institutions, organes et organismes de l'Union, des campagnes d'information régulières et des campagnes publiques d'éducation s'adressant aux utilisateurs finaux, en vue de promouvoir une navigation en ligne plus sûre pour les particuliers et l'habileté numérique, de sensibiliser aux cybermenaces potentielles, y compris les activités criminelles en ligne telles que le hameçonnage, les réseaux zombies, les fraudes financières et bancaires, la falsification de données, et de favoriser la fourniture de conseils de base en matière d'authentification multifacteurs, de mises à jour de sécurité, de chiffrement, d'anonymisation et de protection des données.
- (41) L'ENISA devrait jouer un rôle central dans l'accélération de la sensibilisation des utilisateurs finaux à la sécurité des appareils et à la sécurité de l'utilisation des services, et devrait promouvoir les concepts de sécurité dès la conception et de protection de la vie privée dès la conception au niveau de l'Union. En poursuivant cet objectif, l'ENISA devrait utiliser les meilleures pratiques et les compétences disponibles, en particulier les meilleures pratiques et les compétences développées par le monde universitaire et par les chercheurs en sécurité informatique.
- (42) Afin de soutenir les entreprises actives dans le secteur de la cybersécurité, ainsi que les utilisateurs qui recourent aux solutions de cybersécurité, l'ENISA devrait mettre sur pied et gérer un «observatoire du marché» en procédant à des analyses régulières et en diffusant des informations sur les principales tendances observées sur le marché de la cybersécurité, tant du côté de la demande que du côté de l'offre.
- (43) L'ENISA devrait contribuer aux efforts que l'Union déploie en vue de coopérer avec les organisations internationales ainsi qu'au sein des cadres internationaux de coopération concernés dans le domaine de la cybersécurité. En particulier, l'ENISA devrait contribuer, s'il y a lieu, à une coopération avec des organisations telles que l'OCDE, l'OSCE et l'OTAN. Une telle coopération pourrait comprendre des exercices conjoints dans le domaine de la cybersécurité ainsi qu'une coordination conjointe de la réponse à apporter aux incidents. Ces activités doivent se dérouler dans le plein respect des principes d'inclusion, de réciprocité et d'autonomie décisionnelle de l'Union, sans préjudice du caractère particulier de la politique de sécurité et de défense de tout État membre.

- (44) Afin de réaliser pleinement ses objectifs, l'ENISA devrait se concerter avec les autorités de contrôle de l'Union compétentes et avec d'autres autorités compétentes de l'Union ainsi qu'avec les institutions, organes et organismes de l'Union, notamment la CERT-UE, l'EC3, l'Agence européenne de défense (AED), l'Agence du système global de navigation par satellite (GNSS — *Global Navigation Satellite Systems*) européen (ci-après dénommée «Agence du GNSS européen»), l'Organe des régulateurs européens des communications électroniques (ORECE), l'Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA), la Banque centrale européenne (BCE), l'Autorité bancaire européenne (ABE), le comité européen de la protection des données, l'Agence de coopération des régulateurs de l'énergie (ACER), l'Agence de l'Union européenne pour la sécurité aérienne (AESA) et toute autre agence de l'Union jouant un rôle dans le domaine de la cybersécurité. L'ENISA devrait aussi se concerter avec les autorités chargées de la protection des données en vue de procéder à des échanges de savoir-faire et de bonnes pratiques et devrait leur fournir des conseils sur les questions liées à la cybersécurité qui sont susceptibles d'avoir une incidence sur leurs travaux. Les représentants des autorités chargées de l'application de la loi et des autorités chargées de la protection des données au niveau national et à l'échelon de l'Union devraient pouvoir être représentés au sein du groupe consultatif de l'ENISA. Dans ses relations avec les autorités chargées de l'application de la loi concernant les questions de sécurité des réseaux et de l'information susceptibles d'avoir une incidence sur leurs travaux, l'ENISA devrait respecter les canaux d'information existants et les réseaux établis.
- (45) Des partenariats pourraient être noués avec des établissements universitaires menant des initiatives de recherche dans les domaines en question, et il convient que les organisations de consommateurs et autres disposent de canaux adéquats pour leurs contributions, lesquelles devraient être prises en compte.
- (46) L'ENISA, dans son rôle de secrétariat du réseau des CSIRT, devrait soutenir les CSIRT des États membres et la CERT-UE dans le cadre de la coopération opérationnelle en rapport avec les tâches pertinentes du réseau des CSIRT, telles qu'elles sont visées dans la directive (EU) 2016/1148. En outre, l'ENISA devrait promouvoir et soutenir la coopération entre les CSIRT concernés en cas d'incidents, d'attaques ou de perturbations sur les réseaux ou infrastructures dont les CSIRT assurent la gestion ou la protection et impliquant, ou susceptibles d'impliquer, au moins deux CSIRT, tout en tenant dûment compte des procédures opératoires standard du réseau des CSIRT.
- (47) Afin que l'Union soit mieux préparée pour réagir aux incidents, l'ENISA devrait organiser régulièrement des exercices de cybersécurité au niveau de l'Union et aider les États membres et les institutions, organes et organismes de l'Union à organiser de tels exercices s'ils en font la demande. Il convient d'organiser tous les deux ans des exercices globaux à grande échelle incluant des éléments techniques, opérationnels ou stratégiques. En outre, l'ENISA devrait pouvoir organiser régulièrement des exercices moins globaux avec le même objectif, à savoir celui de faire en sorte que l'Union soit mieux préparée pour répondre à des incidents.
- (48) L'ENISA devrait continuer à développer et maintenir ses compétences en matière de certification de cybersécurité en vue de soutenir la politique de l'Union dans ce domaine. L'ENISA devrait s'appuyer sur les meilleures pratiques existantes et promouvoir l'adoption de la certification de cybersécurité dans l'Union, notamment en contribuant à l'établissement et au maintien d'un cadre de certification de cybersécurité au niveau de l'Union (ci-après dénommé «cadre européen de certification de cybersécurité»), en vue d'accroître la transparence de l'assurance en matière de cybersécurité des produits TIC, services TIC et processus TIC et, partant, de renforcer la confiance dans le marché intérieur numérique ainsi que sa compétitivité.
- (49) Des politiques de cybersécurité efficaces devraient reposer sur des méthodes d'évaluation des risques bien élaborées, dans le secteur public comme dans le secteur privé. Les méthodes d'évaluation des risques sont utilisées à différents niveaux, et il n'existe pas de pratiques communes en ce qui concerne leur application efficace. La promotion et le développement des meilleures pratiques en matière d'évaluation des risques et de solutions interopérables de gestion des risques dans les organisations des secteurs public et privé relèveront le niveau de cybersécurité dans l'Union. À cette fin, l'ENISA devrait favoriser la coopération entre parties prenantes au niveau de l'Union et contribuer à leurs efforts concernant l'établissement et l'adoption de normes européennes et internationales en matière de gestion des risques et de sécurité mesurable des produits, systèmes, réseaux et services électroniques, lesquels, conjointement avec les logiciels, constituent les réseaux et systèmes d'information.
- (50) L'ENISA devrait encourager les États membres, les fabricants ou les fournisseurs de produits TIC, services TIC ou processus TIC à renforcer leurs normes de sécurité générales afin que tous les utilisateurs d'internet puissent prendre les mesures nécessaires pour garantir leur propre cybersécurité et devraient inciter à le faire. En particulier, les fabricants et les fournisseurs de produits TIC, services TIC ou processus TIC devraient fournir les mises à jour nécessaires et devraient rappeler, retirer ou recycler les produits TIC, services TIC ou processus TIC qui ne satisfont pas aux normes de cybersécurité, tandis que les importateurs et les distributeurs devraient veiller à ce que les produits TIC, services TIC et processus TIC qu'ils mettent sur le marché de l'Union respectent les exigences applicables et ne présentent pas de risque pour les consommateurs de l'Union.

- (51) En coopération avec les autorités compétentes, l'ENISA devrait pouvoir diffuser des informations sur le niveau de cybersécurité des produits TIC, services TIC et processus TIC offerts sur le marché intérieur, et devrait émettre des alertes visant des fabricants ou fournisseurs de produits TIC, services TIC ou processus TIC et les contraignant à améliorer la sécurité de leurs produits TIC, services TIC et processus TIC, y compris la cybersécurité.
- (52) L'ENISA devrait prendre pleinement en compte les activités en cours en matière de recherche, de développement et d'évaluation technologique, et plus particulièrement les activités menées dans le cadre des différentes initiatives de recherche de l'Union, pour fournir des conseils aux institutions, organes et organismes de l'Union et, le cas échéant, aux États membres, s'ils en font la demande, sur les besoins et les priorités en matière de recherche dans le domaine de la cybersécurité. Pour recenser les besoins et les priorités en matière de recherche, l'ENISA devrait également consulter les groupes d'utilisateurs concernés. Plus spécifiquement, une coopération pourrait être établie avec le Conseil européen de la recherche, l'Institut européen d'innovation et de technologie et l'Institut d'études de sécurité de l'Union européenne.
- (53) L'ENISA devrait consulter régulièrement les organismes de normalisation, en particulier les organismes européens de normalisation, lors de l'élaboration des schémas européens de certification de cybersécurité.
- (54) Les cybermenaces constituent un problème mondial. Il est nécessaire de renforcer la coopération internationale pour améliorer les normes de cybersécurité, y compris en ce qui concerne la nécessité de définir des normes de comportement communes, d'adopter des codes de conduite, de recourir à des normes internationales, et de partager des informations, d'encourager une collaboration internationale plus rapide en réponse aux problèmes de sécurité des réseaux et de l'information et de favoriser une approche globale commune de ces problèmes. À cette fin, l'ENISA devrait aider l'Union à poursuivre son engagement et sa coopération avec les pays tiers et les organisations internationales en mettant les compétences et l'analyse nécessaires au service des institutions, organes et organismes de l'Union concernés, le cas échéant.
- (55) L'ENISA devrait être en mesure de répondre aux demandes de conseil et d'assistance ad hoc qui sont formulées par les États membres et les institutions, organes et organismes de l'Union sur des questions qui relèvent du mandat de l'ENISA.
- (56) Il est raisonnable et recommandé de mettre en œuvre certains principes relatifs à la gouvernance de l'ENISA afin de se conformer à la déclaration commune et à l'approche commune convenues par le groupe de travail interinstitutionnel sur les agences décentralisées de l'Union en juillet 2012, dont l'objectif est de rationaliser les activités des agences décentralisées et d'améliorer leur efficacité. Il convient par ailleurs de tenir compte, s'il y a lieu, des recommandations figurant dans la déclaration commune et de l'approche commune dans les programmes de travail de l'ENISA, les évaluations de l'ENISA ainsi que les pratiques de l'ENISA en matière d'établissement de rapports et ses pratiques administratives.
- (57) Le conseil d'administration, composé de représentants des États membres et de la Commission, devrait fixer l'orientation générale des activités de l'ENISA et veiller à ce qu'elle exécute ses tâches conformément au présent règlement. Le conseil d'administration devrait être doté des pouvoirs nécessaires pour établir le budget, vérifier l'exécution du budget, adopter des règles financières appropriées, instaurer des procédures de travail transparentes pour la prise de décisions par l'ENISA, adopter le document unique de programmation de l'ENISA, adopter son propre règlement intérieur, nommer le directeur exécutif et statuer sur la prorogation et la cessation du mandat du directeur exécutif.
- (58) Pour assurer le fonctionnement correct et efficace de l'ENISA, la Commission et les États membres devraient veiller à ce que les personnes nommées au conseil d'administration soient dotées de compétences professionnelles et d'une expérience appropriées. La Commission et les États membres devraient également s'efforcer de limiter le roulement de leurs représentants respectifs au sein du conseil d'administration, afin de garantir la continuité des travaux de ce dernier.
- (59) Le bon fonctionnement de l'ENISA exige que le directeur exécutif de celle-ci soit nommé sur la base de son mérite et de ses aptitudes attestées dans le domaine de l'administration et de la gestion, ainsi que de ses compétences et de son expérience pertinentes en matière de cybersécurité. Il convient que le directeur exécutif exerce ses fonctions en toute indépendance. Le directeur exécutif devrait élaborer une proposition de programme de travail annuel pour l'ENISA, après consultation préalable de la Commission, et prendre toutes les mesures nécessaires pour garantir la bonne mise en œuvre de ce programme de travail. Le directeur exécutif devrait préparer un rapport annuel à soumettre au conseil d'administration, portant sur la mise en œuvre du programme de travail annuel de l'ENISA, établir un projet d'état prévisionnel des recettes et des dépenses de l'ENISA et exécuter le budget. Le directeur exécutif devrait, en outre, avoir la possibilité de créer des groupes de travail ad hoc pour traiter de questions spécifiques, en particulier de questions de nature scientifique, technique, juridique ou socio-économique. La création d'un groupe de travail ad hoc est notamment jugée nécessaire pour la préparation d'un schéma européen de

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

- (60) Le conseil exécutif devrait contribuer au fonctionnement efficace du conseil d'administration. Dans le cadre de ses travaux préparatoires liés aux décisions du conseil d'administration, le conseil exécutif devrait examiner de manière approfondie les informations pertinentes, étudier les options disponibles et proposer des conseils et des solutions afin de préparer les décisions du conseil d'administration.
- (61) L'ENISA devrait disposer, à titre d'organe consultatif, d'un groupe consultatif de l'ENISA pour assurer un dialogue régulier avec le secteur privé, les organisations de consommateurs et d'autres parties prenantes concernées. Le groupe consultatif de l'ENISA, institué par le conseil d'administration sur proposition du directeur exécutif, devrait s'attacher à examiner des questions pertinentes pour les parties prenantes et devrait les porter à l'attention de l'ENISA. Le groupe consultatif de l'ENISA devrait être consulté en particulier au sujet du projet de programme de travail annuel de l'ENISA. La composition du groupe consultatif de l'ENISA et les tâches assignées à ce groupe devraient assurer une représentation suffisante des parties prenantes dans les travaux de l'ENISA.
- (62) Le groupe des parties prenantes pour la certification de cybersécurité devrait être institué pour aider l'ENISA et la Commission à faciliter la consultation des parties prenantes concernées. Le groupe des parties prenantes pour la certification de cybersécurité devrait être composé de membres représentant le secteur dans des proportions équilibrées, du côté tant de la demande que de l'offre de produits TIC et services TIC, y compris, en particulier, les PME, les fournisseurs de services numériques, les organismes européens et internationaux de normalisation, les organismes d'accréditation nationaux, les autorités de contrôle de la protection des données, les organismes d'évaluation de la conformité en application du règlement (CE) n° 765/2008 du Parlement européen et du Conseil <sup>(16)</sup>, et les universités ainsi que les organisations de consommateurs.
- (63) L'ENISA devrait disposer de règles en matière de prévention et de gestion des conflits d'intérêts. L'ENISA devrait aussi appliquer les dispositions pertinentes du droit de l'Union en ce qui concerne l'accès du public aux documents prévu par le règlement (CE) n° 1049/2001 du Parlement européen et du Conseil <sup>(17)</sup>. Le traitement des données à caractère personnel devrait être régi par le règlement (UE) 2018/1725 du Parlement européen et du Conseil <sup>(18)</sup>. L'ENISA devrait respecter les dispositions applicables aux institutions, organes et organismes de l'Union et la législation nationale concernant le traitement des informations, notamment les informations non classifiées sensibles et les informations classifiées de l'Union européenne (ICUE).
- (64) Pour garantir l'autonomie et l'indépendance complètes de l'ENISA et lui permettre d'exécuter des tâches supplémentaires, y compris des tâches urgentes imprévues, il convient de la doter d'un budget suffisant et autonome dont l'essentiel des recettes devrait provenir d'une contribution de l'Union et de contributions des pays tiers participant aux travaux de l'ENISA. Doter l'ENISA d'un budget adéquat est primordial pour garantir qu'elle dispose d'une capacité suffisante pour exécuter l'ensemble de ses tâches toujours plus nombreuses et atteindre ses objectifs. La majeure partie des effectifs de l'ENISA devrait se consacrer directement à la mise en œuvre opérationnelle du mandat de l'ENISA. L'État membre d'accueil et tout autre État membre devrait être autorisé à apporter des contributions volontaires au budget de l'ENISA. La procédure budgétaire de l'Union devrait rester applicable en ce qui concerne toute subvention imputable sur le budget général de l'Union. En outre, la Cour des comptes devrait contrôler les comptes de l'ENISA afin de garantir la transparence et la responsabilité.
- (65) La certification de cybersécurité joue un rôle important dans l'amélioration de la sécurité des produits TIC, services TIC et processus TIC et le renforcement de la confiance qui leur est accordée. Le marché unique numérique, et en particulier l'économie des données et l'IdO, ne peuvent prospérer que si le grand public est convaincu que ces produits, services et processus offrent un certain niveau de cybersécurité. Les voitures connectées et automatisées, les dispositifs médicaux électroniques, les systèmes de contrôle-commande industriels et les réseaux intelligents ne sont que quelques exemples de secteurs dans lesquels la certification est déjà largement utilisée ou est susceptible de l'être dans un avenir proche. Les secteurs régis par la directive (UE) 2016/1148 sont également des secteurs où la certification de cybersécurité joue un rôle critique.

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

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

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

- (66) Dans la communication de 2016 intitulée «Renforcer le système européen de cyber-résilience et promouvoir la compétitivité et l'innovation dans le secteur européen de la cybersécurité», la Commission a souligné le besoin de produits et de solutions de très bonne qualité, abordables et interopérables en matière de cybersécurité. L'offre de produits TIC, services TIC et processus TIC au sein du marché unique reste très fragmentée sur le plan géographique. Cela est dû au fait que le secteur de la cybersécurité en Europe s'est développé principalement en fonction de la demande des gouvernements nationaux. En outre, le manque de solutions interopérables (normes techniques), de pratiques et de dispositifs de certification à l'échelle de l'Union constitue l'une des autres lacunes affectant le marché unique dans le domaine de la cybersécurité. Il en résulte que les entreprises européennes ont des difficultés à être concurrentielles au niveau national, à l'échelon de l'Union et au niveau mondial. Cela restreint également le choix des technologies viables et utilisables en matière de cybersécurité qui s'offre aux particuliers et aux entreprises. De la même façon, dans la communication de 2017 sur la révision à mi-parcours de la mise en œuvre de la stratégie pour le marché unique numérique — Un marché unique numérique connecté pour tous, la Commission a insisté sur le besoin de produits et systèmes connectés qui soient sûrs, et a indiqué que la création d'un cadre européen de la sécurité des TIC fixant des règles sur les modalités d'organisation de la certification de sécurité des TIC dans l'Union pourrait à la fois préserver la confiance dans l'internet et permettre de lutter contre la fragmentation actuelle du marché intérieur.
- (67) Actuellement, la certification de cybersécurité des produits TIC, services TIC et processus TIC n'est utilisée que de façon limitée. Lorsqu'elle existe, elle intervient essentiellement au niveau des États membres ou dans le cadre de schémas pilotés par les entreprises du secteur. Dans ce contexte, un certificat délivré par une autorité nationale de certification de cybersécurité n'est pas, en principe, reconnu dans d'autres États membres. Il arrive donc que les entreprises doivent certifier leurs produits TIC, services TIC et processus TIC dans les différents États membres où elles exercent leurs activités, par exemple pour participer à des procédures nationales de passage de marchés, ce qui implique des coûts supplémentaires. En outre, alors que de nouveaux schémas voient le jour, il ne semble pas exister d'approche cohérente et globale des questions de cybersécurité transversales, par exemple dans le domaine de l'IoD. Les schémas existants présentent des lacunes importantes et des différences en termes de couverture des produits, de niveaux d'assurance, de critères de fond et d'utilisation effective, ce qui entrave les mécanismes de reconnaissance mutuelle au sein de l'Union.
- (68) Des efforts ont été réalisés pour garantir une reconnaissance mutuelle des certificats dans l'Union. Cependant, ils n'ont que partiellement abouti. L'exemple le plus marquant à cet égard est l'accord de reconnaissance mutuelle (ARM) du groupe des hauts fonctionnaires pour la sécurité des systèmes d'information (SOG-IS). Même s'il est le modèle le plus remarquable en ce qui concerne la coopération et la reconnaissance mutuelle dans le domaine de la certification de sécurité, le SOG-IS ne réunit que certains États membres. De ce fait, l'ARM du SOG-IS n'a eu qu'une efficacité limitée dans la perspective du marché intérieur.
- (69) Dès lors, il est nécessaire d'adopter une approche commune et d'établir un cadre européen de certification de cybersécurité établissant les principales exigences horizontales pour les schémas européens de certification de cybersécurité à développer, et permettant la reconnaissance et l'utilisation dans tous les États membres des certificats de cybersécurité européens et des déclarations de conformité de l'Union européenne pour les produits TIC, services TIC ou processus TIC. Ce faisant, il est essentiel de s'appuyer sur des schémas nationaux et internationaux existants, ainsi que sur des systèmes de reconnaissance mutuelle, en particulier le SOG-IS, et de créer les conditions d'une transition en douceur des schémas existants relevant de ces systèmes vers les schémas relevant du nouveau cadre européen de certification de cybersécurité. Le cadre européen de certification de cybersécurité devrait poursuivre un double objectif. Tout d'abord, il devrait contribuer à renforcer la confiance dans les produits TIC, services TIC et processus TIC qui ont été certifiés au titre des schémas européens de certification de cybersécurité. Ensuite, il devrait aider à éviter la multiplication de schémas de certification de cybersécurité nationales contradictoires ou faisant double emploi, réduisant ainsi les coûts à la charge des entreprises exerçant leurs activités sur le marché unique numérique. Les schémas européens de certification de cybersécurité devraient être non discriminatoires et fondés sur des normes européennes ou internationales, sauf si ces normes sont inefficaces ou inapprises pour remplir les objectifs légitimes de l'Union à cet égard.
- (70) Le cadre européen de certification de cybersécurité devrait être établi de manière homogène dans tous les États membres afin d'éviter la pratique du «shopping de certifications» en raison des différents niveaux d'exigence dans les différents États membres.
- (71) Les schémas européens de certification de cybersécurité devraient reposer sur les éléments déjà existants au niveau international et national et, au besoin, sur les spécifications techniques des forums et consortiums, en tirant les leçons des points forts actuels et en évaluant et en corrigeant les points faibles.
- (72) Des solutions de cybersécurité flexibles sont nécessaires pour que les entreprises du secteur gardent une longueur d'avance sur les cybermenaces; dès lors, tout schéma de certification devrait être conçu de manière à éviter le risque d'obsolescence rapide.

- (73) La Commission devrait être habilitée à adopter des schémas européens de certification de cybersécurité concernant des groupes spécifiques de produits TIC, services TIC et processus TIC. Ces schémas devraient être mis en œuvre et contrôlés par des autorités nationales de certification de cybersécurité, et les certificats délivrés au titre de ces schémas devraient être valables et reconnus sur tout le territoire de l'Union. Les schémas de certification gérés par les entreprises du secteur ou d'autres organismes privés devraient être exclus du champ d'application du présent règlement. Toutefois, les organismes qui gèrent de tels schémas devraient pouvoir proposer que la Commission les prenne pour base en vue de les approuver en tant que schéma européen de certification de cybersécurité.
- (74) Les dispositions du présent règlement devraient être sans préjudice du droit de l'Union qui prévoit des règles spécifiques concernant la certification des produits TIC, services TIC et processus TIC. En particulier, le règlement (UE) 2016/679 fixe des dispositions en vue de la mise en place de mécanismes de certification ainsi que de labels et de marques en matière de protection des données aux fins de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent ledit règlement. Ces mécanismes de certification et ces labels et marques en matière de protection des données devraient permettre aux personnes concernées d'évaluer rapidement le niveau de protection des données offert par les produits TIC, services TIC et processus TIC en question. Le présent règlement est sans préjudice de la certification des opérations de traitement des données au titre du règlement (UE) 2016/679, y compris lorsque ces opérations sont intégrées dans des produits TIC, services TIC et processus TIC.
- (75) Les schémas européens de certification de cybersécurité devraient avoir pour finalité de garantir que les produits TIC, services TIC et processus TIC certifiés selon de tels schémas respectent les exigences définies qui visent à protéger la disponibilité, l'authenticité, l'intégrité et la confidentialité de données stockées, transmises ou traitées, ou des fonctions connexes de ces produits, services et processus tout au long de leur cycle de vie, ou des services qu'ils offrent ou qui sont accessibles par leur intermédiaire. Il n'est pas possible d'exposer en détail les exigences de cybersécurité se rapportant à tous les produits TIC, services TIC et processus TIC dans le présent règlement. Les produits TIC, services TIC et processus TIC et les besoins de cybersécurité relatifs à ces produits, services et processus sont si divers qu'il est très difficile d'élaborer des exigences de cybersécurité générales qui soient valables en toutes circonstances. Il est donc nécessaire d'adopter, aux fins de la certification, une notion large et générale de la cybersécurité, laquelle devrait être complétée par une série d'objectifs spécifiques en matière de cybersécurité à prendre en compte lors de la conception de schémas européens de certification de cybersécurité. Les modalités selon lesquelles ces objectifs doivent être atteints pour des produits TIC, services TIC et processus TIC spécifiques devraient ensuite être précisées en détail au niveau de chaque schéma de certification adopté par la Commission, par exemple en faisant référence à des normes ou à des spécifications techniques s'il n'existe aucune norme appropriée.
- (76) Les spécifications techniques à utiliser dans les schémas européens de certification de cybersécurité devraient respecter les exigences énoncées à l'annexe II du règlement (UE) n° 1025/2012 du Parlement européen et du Conseil <sup>(19)</sup>. Il pourrait toutefois être jugé nécessaire de s'écarter quelque peu de ces exigences dans des cas dûment justifiés, lorsque ces spécifications techniques doivent être utilisées dans un schéma européen de certification de cybersécurité renvoyant à un niveau d'assurance dit «élevé». Les motifs de ces écarts devraient être rendus publics.
- (77) L'évaluation de la conformité est une procédure consistant à évaluer s'il est satisfait aux exigences relatives à un produit TIC, service TIC ou processus TIC qui ont été définies. Cette procédure est réalisée par un tiers indépendant, autre que le fabricant ou le fournisseur des produits TIC, services TIC ou processus TIC qui font l'objet de l'évaluation. Un certificat de cybersécurité européen devrait être délivré à l'issue d'une procédure d'évaluation d'un produit TIC, service TIC ou processus TIC réussie. Il convient de considérer le certificat de cybersécurité européen comme une confirmation que l'évaluation a été dûment réalisée. En fonction du niveau d'assurance, le schéma européen de certification de cybersécurité devrait indiquer si le certificat de cybersécurité européen doit être délivré par un organisme privé ou public. L'évaluation de la conformité et la certification ne peuvent en soi garantir que les produits TIC, services TIC et processus TIC certifiés sont sécurisés du point de vue de la cybersécurité. Il s'agit plutôt de procédures et de méthodologies techniques visant à attester que des produits TIC, services TIC et processus TIC ont été soumis à des essais et qu'ils respectent certaines exigences de cybersécurité établies par ailleurs, par exemple dans des normes techniques.
- (78) Le choix, par les utilisateurs de certificats de cybersécurité européens, de la certification appropriée et des exigences de sécurité correspondantes devrait se fonder sur une analyse des risques associés à l'utilisation des produits TIC, services TIC ou processus TIC. En conséquence, le niveau d'assurance devrait correspondre au niveau de risque associé à l'utilisation prévue d'un produit TIC, service TIC ou processus TIC.

<sup>(19)</sup> Règlement (UE) n° 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision n° 1673/2006/CE du Parlement européen et du Conseil (JO L 316 du 14.11.2012, p. 12).

- (79) Les schémas européens de certification de cybersécurité pourraient prévoir une évaluation de la conformité devant être effectuée sous la seule responsabilité du fabricant ou du fournisseur de produits TIC, services TIC ou processus TIC (ci-après dénommée «autoévaluation de la conformité»). En pareils cas, il devrait suffire que le fabricant ou le fournisseur de produits TIC, services TIC ou processus TIC effectue lui-même tous les contrôles pour garantir que les produits TIC, services TIC ou processus TIC sont conformes au schéma européen de certification de cybersécurité. L'autoévaluation de la conformité devrait être considérée comme appropriée pour les produits TIC et services TIC de faible complexité ou pour les processus TIC qui présentent un risque faible pour le public, tels que des mécanismes de conception et de production simples. En outre, l'autoévaluation de la conformité ne devrait être autorisée pour les produits TIC, services TIC ou processus TIC que lorsqu'ils correspondent à un niveau d'assurance dit «élémentaire».
- (80) Les schémas européens de certification de cybersécurité pourraient permettre à la fois les autoévaluations de la conformité et les certifications de produits TIC, services TIC ou processus TIC. Dans ce cas, le schéma devrait prévoir des moyens clairs et compréhensibles pour les consommateurs ou les autres utilisateurs de distinguer entre les produits TIC, services TIC ou processus TIC à l'égard desquels le fabricant ou le fournisseur des produits TIC, services TIC ou processus TIC est responsable de l'évaluation, et les produits TIC, services TIC et processus TIC qui sont certifiés par un tiers.
- (81) Le fabricant ou le fournisseur de produits TIC, services TIC ou processus TIC qui effectue une autoévaluation de la conformité devrait pouvoir délivrer et signer la déclaration de conformité de l'Union européenne dans le cadre de la procédure d'évaluation de la conformité. Une déclaration de conformité de l'Union européenne est un document qui indique qu'un produit TIC, service TIC ou processus TIC spécifique respecte les exigences du schéma européen de certification de cybersécurité. En délivrant et en signant la déclaration de conformité de l'Union européenne, le fabricant ou le fournisseur de produits TIC, services TIC ou processus TIC assume la responsabilité du respect par le produit TIC, service TIC ou processus TIC des exigences légales du schéma européen de certification de cybersécurité. Une copie de la déclaration de conformité de l'Union européenne devrait être soumise à l'autorité nationale de certification de cybersécurité et à l'ENISA.
- (82) Le fabricant ou le fournisseur de produits TIC, services TIC ou processus TIC devrait mettre à la disposition de l'autorité nationale de certification de cybersécurité compétente, pour une durée fixée dans le schéma européen de certification de cybersécurité concerné, la déclaration de conformité de l'Union européenne, la documentation technique et toutes les autres informations pertinentes relatives à la conformité des produits TIC, services TIC ou processus TIC avec un schéma européen de certification de cybersécurité. La documentation technique devrait préciser les exigences applicables au titre du schéma et devrait couvrir la conception, la fabrication et le fonctionnement du produit TIC, service TIC ou processus TIC dans la mesure nécessaire à l'autoévaluation de la conformité. La documentation technique devrait être compilée de façon à permettre d'évaluer si un produit TIC ou un service TIC respecte les exigences applicables au titre de ce schéma.
- (83) La gouvernance du cadre européen de certification de cybersécurité prend en compte la participation des États membres ainsi qu'une participation appropriée des parties prenantes, et définit le rôle de la Commission pendant la planification et la proposition, la demande, l'élaboration, l'adoption ainsi que l'évaluation des schémas européens de certification de cybersécurité.
- (84) La Commission devrait préparer, avec le soutien du groupe européen de certification de cybersécurité (GECC) et du groupe des parties prenantes pour la certification de cybersécurité et à la suite d'une large consultation ouverte, un programme de travail glissant de l'Union pour les schémas européens de certification de cybersécurité et devrait le publier sous la forme d'un instrument non contraignant. Le programme de travail glissant de l'Union devrait consister en un document stratégique permettant aux entreprises du secteur, aux autorités nationales et aux organismes de normalisation, en particulier, de se préparer à l'avance dans la perspective des futurs schémas européens de certification de cybersécurité. Le programme de travail glissant de l'Union devrait comporter un aperçu pluriannuel des demandes de schémas candidats que la Commission compte adresser à l'ENISA pour préparation, sur la base de motifs spécifiques. La Commission devrait tenir compte du programme de travail glissant de l'Union lors de la préparation de son plan glissant pour la normalisation des TIC et des demandes de normalisation adressées à des organismes européens de normalisation. Compte tenu de la rapidité de l'introduction et de l'adoption des nouvelles technologies, de l'apparition de risques liés à la cybersécurité auparavant inconnus et de l'évolution de la législation et des marchés, la Commission ou le GECC devrait être habilité(e) à demander à l'ENISA de préparer des schémas candidats qui n'ont pas été prévus dans le programme de travail glissant de l'Union. En pareils cas, la Commission et le GECC devraient en outre évaluer le bien-fondé d'une telle demande en tenant compte des finalités et objectifs généraux du présent règlement et de la nécessité d'assurer la continuité en ce qui concerne la planification et l'utilisation des ressources par l'ENISA.

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

- (85) L'ENISA devrait maintenir un site internet fournissant des informations sur les schémas européens de certification de cybersécurité et leur donnant une visibilité, qui devrait, entre autres, comprendre les demandes de préparation d'un schéma candidat ainsi que les retours d'information reçus lors du processus de consultation réalisé par l'ENISA au cours de la phase préparatoire. Le site internet devrait en outre fournir des informations sur les certificats de cybersécurité européens et les déclarations de conformité de l'Union européenne délivrés en application du présent règlement, notamment des informations concernant le retrait et l'expiration de tels certificats de cybersécurité européens et déclarations de conformité de l'Union européenne. Le site internet devrait en outre indiquer les schémas nationaux de certification de cybersécurité qui ont été remplacés par un schéma européen de certification de cybersécurité.
- (86) Le niveau d'assurance d'un schéma européen de certification constitue le fondement permettant de garantir qu'un produit TIC, service TIC ou processus TIC satisfait aux exigences de sécurité d'un schéma européen de certification de cybersécurité spécifique. Pour assurer la cohérence du cadre européen de certification de cybersécurité, un schéma européen de certification de cybersécurité devrait pouvoir préciser les niveaux d'assurance pour les certificats de cybersécurité européens et les déclarations de conformité de l'Union européenne délivrés dans le cadre de ce schéma. Chaque certificat de cybersécurité européen pourrait renvoyer à l'un des niveaux d'assurance, à savoir «élémentaire», «substantiel» ou «élevé», tandis que la déclaration de conformité de l'Union européenne pourrait ne renvoyer qu'au niveau d'assurance dit «élémentaire». Les niveaux d'assurance prévoieraient la rigueur et l'ampleur correspondantes de l'évaluation du produit TIC, du service TIC ou du processus TIC et seraient déterminés par référence aux spécifications techniques, normes et procédures qui y sont liées, y compris les contrôles techniques, dont l'objectif est de limiter les incidents ou de les prévenir. Chaque niveau d'assurance devrait être cohérent dans les différents domaines sectoriels dans lesquels la certification s'applique.
- (87) Un schéma européen de certification de cybersécurité pourrait préciser plusieurs niveaux d'évaluation, en fonction de la rigueur et de l'ampleur de la méthode d'évaluation utilisée. Les niveaux d'évaluation devraient correspondre à l'un des niveaux d'assurance et être associés à une combinaison appropriée de composantes d'assurance. Pour tous les niveaux d'assurance, le produit TIC, service TIC ou processus TIC devrait contenir un certain nombre de fonctions sécurisées, telles qu'elles sont définies par le schéma, pouvant comprendre: une configuration sécurisée prête à l'emploi, un code signé, une mise à jour sécurisée, ainsi que la limitation de l'exploitation de failles et des protections complètes («full stack») ou du tas de la mémoire. Ces fonctions devraient faire l'objet d'un développement et d'une maintenance fondés sur des approches de développement mettant l'accent sur la sécurité et des outils associés, afin de garantir que des mécanismes efficaces au niveau tant du logiciel que du matériel sont incorporés de manière fiable.
- (88) Pour le niveau d'assurance dit «élémentaire», l'évaluation devrait au moins porter sur les composantes d'assurance suivantes: l'évaluation devrait comprendre au moins un examen, par l'organisme d'évaluation de la conformité, de la documentation technique accompagnant le produit TIC, service TIC ou processus TIC. Lorsque la certification inclut des processus TIC, le processus de conception, de développement et de maintenance d'un produit TIC ou service TIC devrait également être soumis à l'examen technique. Lorsqu'un schéma européen de certification de cybersécurité prévoit une autoévaluation de la conformité, il devrait suffire que le fabricant ou le fournisseur de produits TIC, services TIC ou processus TIC ait effectué une autoévaluation de la conformité du produit TIC, service TIC ou processus TIC avec le schéma de certification.
- (89) Pour le niveau d'assurance dit «substantiel», l'évaluation devrait au moins porter sur, outre les exigences liées au niveau d'assurance dit «élémentaire», la vérification de la conformité des fonctionnalités de sécurité du produit TIC, service TIC ou processus TIC avec sa documentation technique.

- (90) Pour le niveau d'assurance dit «élevé», l'évaluation devrait au moins porter sur, outre les exigences liées au niveau d'assurance dit «substantiel», un test d'efficacité évaluant la résistance des fonctionnalités de sécurité du produit TIC, service TIC ou processus TIC face à des cyberattaques élaborées lancées par des personnes aux aptitudes solides et aux ressources importantes.
- (91) Le recours à la certification de cybersécurité européenne et aux déclarations de conformité de l'Union européenne devrait rester volontaire, sauf disposition contraire du droit de l'Union ou du droit d'un État membre adoptée conformément au droit de l'Union. En l'absence d'harmonisation du droit de l'Union, les États membres peuvent adopter des réglementations techniques nationales prévoyant une certification obligatoire dans le cadre du schéma européen de certification de cybersécurité conformément à la directive (UE) 2015/1535 du Parlement européen et du Conseil<sup>(20)</sup>. Les États membres ont aussi recours à la certification européenne de cybersécurité dans le cadre d'un marché public et de la directive 2014/24/UE du Parlement européen et du Conseil<sup>(21)</sup>.
- (92) Dans certains domaines, il pourrait s'avérer nécessaire, à l'avenir, d'imposer certaines exigences spécifiques en matière de cybersécurité et de rendre la certification y afférente obligatoire pour certains produits TIC, services TIC ou processus TIC, afin d'améliorer le niveau de la cybersécurité dans l'Union. À intervalles réguliers, la Commission devrait assurer un suivi de l'incidence des schémas européens de certification de cybersécurité adoptés sur la disponibilité dans le marché intérieur de produits TIC, services TIC et processus TIC sécurisés et devrait régulièrement évaluer le niveau d'utilisation des schémas de certification par les fabricants ou les fournisseurs de produits TIC, services TIC ou processus TIC dans l'Union. Il convient d'évaluer l'efficacité des schémas européens de certification de cybersécurité et la question de savoir si certains schémas devraient être rendus obligatoires à la lumière de la législation de l'Union relative à la cybersécurité, en particulier la directive (UE) 2016/1148, en tenant compte de la sécurité du réseau et des systèmes d'information utilisés par les opérateurs de services essentiels.
- (93) Les certificats de cybersécurité européens et les déclarations de conformité de l'Union européenne devraient aider les utilisateurs finaux à faire des choix éclairés. Dès lors, les produits TIC, services TIC et processus TIC qui ont été certifiés ou pour lesquels une déclaration de conformité de l'Union européenne a été émise, devraient être accompagnés d'informations structurées, adaptées au niveau technique attendu de l'utilisateur final auquel ils sont destinés. Toutes ces informations devraient être disponibles en ligne et, le cas échéant, sous une forme physique. L'utilisateur final devrait avoir accès à des informations concernant le numéro de référence du schéma de certification, le niveau d'assurance, la description des risques liés à la cybersécurité qui sont associés au produit TIC, service TIC ou processus TIC, et l'autorité ou l'organisme de délivrance, ou devrait être en mesure d'obtenir une copie du certificat de cybersécurité européen. En outre, l'utilisateur final devrait recevoir des informations sur la politique d'assistance en matière de cybersécurité du fabricant ou du fournisseur de produits TIC, services TIC ou processus TIC (à savoir combien de temps l'utilisateur final peut escompter recevoir des mises à jour ou des correctifs en matière de cybersécurité). Le cas échéant, des orientations en ce qui concerne les mesures que l'utilisateur final peut prendre ou les paramétrages qu'il peut effectuer pour maintenir ou accroître la cybersécurité du produit TIC ou service TIC et des informations de contact d'un point de contact unique auquel s'adresser ou auprès duquel recevoir une aide en cas de cyberattaque (outre le signalement automatique) devraient être fournis. Ces informations devraient être actualisées régulièrement et être mises à disposition sur un site internet fournissant des informations sur les schémas européens de certification de cybersécurité.
- (94) En vue d'atteindre les objectifs du présent règlement et d'éviter la fragmentation du marché intérieur, les procédures ou schémas nationaux de certification de cybersécurité applicables aux produits TIC, services TIC ou processus TIC couverts par un schéma européen de certification de cybersécurité devraient cesser de produire leurs effets à compter d'une date fixée par la Commission par voie d'actes d'exécution. De plus, les États membres devraient s'abstenir d'instaurer de nouveaux schémas nationaux de certification de cybersécurité applicables aux produits TIC, services TIC ou processus TIC déjà couverts par un schéma européen de certification de cybersécurité existant. Toutefois, il convient de ne pas empêcher les États membres d'adopter ou de maintenir des schémas nationaux de certification de cybersécurité à des fins de sécurité nationale. Les États membres devraient informer la Commission et le GECC de leur intention éventuelle d'élaborer de nouveaux schémas nationaux de certification de cybersécurité. La Commission et le GECC devraient évaluer l'incidence des nouveaux schémas nationaux de certification de cybersécurité sur le bon fonctionnement du marché intérieur, à la lumière de tout intérêt stratégique qu'il y aurait à demander, en leur lieu et place, un schéma européen de certification de cybersécurité.
- (95) Les schémas européens de certification de cybersécurité ont vocation à contribuer à harmoniser les pratiques de cybersécurité au sein de l'Union. Ils doivent contribuer à augmenter le niveau de cybersécurité dans l'Union. La conception des schémas européens de certification de cybersécurité devrait également prendre en compte et permettre la mise au point d'innovations dans le domaine de la cybersécurité.

<sup>(20)</sup> Directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information (JO L 241 du 17.9.2015, p. 1).

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

- (96) Les schémas européens de certification de cybersécurité devraient tenir compte des méthodes actuelles de développement des logiciels et du matériel et, en particulier, de l'incidence sur des certificats de cybersécurité européens individuels de mises à jour fréquentes des logiciels ou des micrologiciels. Les schémas européens de certification de cybersécurité devraient préciser les conditions dans lesquelles une mise à jour peut nécessiter qu'un produit TIC, service TIC ou processus TIC doive être de nouveau certifié ou que le champ d'application d'un certificat de cybersécurité européen particulier doive être réduit, compte tenu des éventuels effets négatifs de la mise à jour sur le respect des exigences de ce certificat en matière de sécurité.
- (97) Une fois qu'un schéma européen de certification de cybersécurité a été adopté, les fabricants ou les fournisseurs de produits TIC, services TIC ou processus TIC devraient être en mesure de soumettre des demandes de certification de leurs produits TIC ou services TIC à l'organisme d'évaluation de la conformité de leur choix établi où que ce soit dans l'Union. Les organismes d'évaluation de la conformité devraient être accrédités par un organisme d'accréditation national s'ils satisfont à certaines exigences définies telles qu'elles sont énoncées dans le présent règlement. L'accréditation devrait être accordée pour une durée maximale de cinq ans et devrait pouvoir être renouvelée dans les mêmes conditions, pourvu que l'organisme d'évaluation de la conformité satisfasse encore aux exigences. L'accréditation devrait être limitée, suspendue ou révoquée par des organismes d'accréditation nationaux lorsque les conditions de l'accréditation ne sont pas ou ne sont plus remplies ou lorsque l'organisme d'évaluation de la conformité viole le présent règlement.
- (98) Les références faites dans la législation nationale à des normes nationales qui ont cessé de produire leurs effets en raison de l'entrée en vigueur d'un schéma européen de certification de cybersécurité peuvent être une source de confusion. Dès lors, les États membres devraient tenir compte, dans leur législation nationale, de l'adoption d'un schéma européen de certification de cybersécurité.
- (99) Pour parvenir à l'équivalence des normes dans toute l'Union, faciliter la reconnaissance mutuelle et favoriser l'acceptation globale des certificats de cybersécurité européens et des déclarations de conformité de l'Union européenne, il est nécessaire de mettre en place un système d'examen par les pairs entre les autorités nationales de certification de cybersécurité. L'examen par les pairs devrait couvrir les procédures de contrôle de la conformité des produits TIC, services TIC et processus TIC avec les certificats de cybersécurité européens, de surveillance du respect des obligations des fabricants ou des fournisseurs de produits TIC, services TIC ou processus TIC qui procèdent à une autoévaluation de la conformité, et de surveillance des organismes d'évaluation de la conformité ainsi que de l'adéquation des compétences du personnel des organismes qui délivrent les certificats pour les niveaux d'assurance dits «élevés». La Commission devrait pouvoir, par voie d'actes d'exécution, établir au moins un plan quinquennal pour les examens par les pairs, et fixer les critères et les méthodes de fonctionnement du système d'examen par les pairs.
- (100) Sans préjudice du système général d'examen par les pairs à mettre en place entre toutes les autorités nationales de certification de cybersécurité au sein du cadre européen de certification de cybersécurité, certains schémas européens de certification de cybersécurité peuvent comporter un mécanisme d'évaluation par les pairs pour les organismes délivrant des certificats de cybersécurité européens pour des produits TIC, services TIC et processus TIC avec un niveau d'assurance dit «élevé» en application de ces schémas. Le GECC devrait soutenir la mise en œuvre de ces mécanismes d'évaluation par les pairs. Les évaluations par les pairs devraient en particulier évaluer si les organismes concernés s'acquittent de leurs tâches de façon harmonisée, et peuvent comporter des mécanismes de recours. Les résultats des évaluations par les pairs devraient être rendus publics. Les organismes concernés peuvent adopter des mesures appropriées pour adapter leurs pratiques et leurs compétences en conséquence.
- (101) Les États membres devraient désigner une ou plusieurs autorités nationales de certification de cybersécurité afin de contrôler le respect des obligations découlant du présent règlement. Une autorité nationale de certification de cybersécurité peut être une autorité existante ou une nouvelle autorité. Un État membre devrait également pouvoir désigner, après en être convenu avec un autre État membre, une ou plusieurs autorités nationales de certification de cybersécurité sur le territoire de cet autre État membre.
- (102) Les autorités nationales de certification de cybersécurité devraient en particulier contrôler et faire respecter les obligations qui incombent aux fabricants ou fournisseurs de produits TIC, services TIC ou processus TIC établis sur leur territoire respectif en ce qui concerne la déclaration de conformité de l'Union européenne, assister les organismes nationaux d'accréditation dans le contrôle et la supervision des activités des organismes d'évaluation de la conformité en leur offrant leurs compétences et en leur fournissant des informations utiles, autoriser les organismes d'évaluation de la conformité à exécuter leurs tâches lorsque ces organismes satisfont aux exigences supplémentaires fixées dans un schéma européen de certification de cybersécurité, et suivre les évolutions pertinentes dans le domaine de la certification de cybersécurité. Les autorités nationales de certification de cybersécurité devraient également traiter les réclamations introduites par des personnes physiques ou morales en rapport avec les

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

- (103) Afin d'assurer une application cohérente du cadre européen de certification de cybersécurité, un GECC qui est composé de représentants des autorités nationales de certification de cybersécurité ou d'autres autorités nationales compétentes devrait être mis en place. Les tâches principales du GECC devraient consister à conseiller et assister la Commission dans ses efforts pour assurer une mise en œuvre et une application cohérentes du cadre européen de certification de cybersécurité, à assister l'ENISA et à coopérer étroitement avec elle dans la préparation des schémas de certification de cybersécurité candidats, à demander à l'ENISA, dans des cas dûment justifiés, de préparer un schéma candidat, à adopter des avis adressés à l'ENISA sur les schémas candidats et à adopter des avis à l'intention de la Commission concernant la maintenance et le réexamen de schémas européens de certification de cybersécurité existants. Le GECC devrait faciliter l'échange de bonnes pratiques et de compétences entre les diverses autorités nationales de certification de cybersécurité qui sont responsables de l'accréditation des organismes d'évaluation de la conformité et de la délivrance des certificats de cybersécurité européens.
- (104) Dans une optique de sensibilisation et pour faciliter l'acceptation de futurs schémas européens de certification de cybersécurité, la Commission peut publier des lignes directrices générales ou sectorielles dans le domaine de la cybersécurité, par exemple sur les bonnes pratiques ou les comportements responsables en matière de cybersécurité, en soulignant les effets positifs de l'utilisation de produits TIC, services TIC et processus TIC certifiés.
- (105) Pour faciliter encore davantage les échanges, et compte tenu du fait que les chaînes d'approvisionnement TIC sont mondiales, des accords de reconnaissance mutuelle concernant les certificats de cybersécurité européens peuvent être conclus par l'Union conformément à l'article 218 du traité sur le fonctionnement de l'Union européenne. La Commission, tenant compte de l'avis de l'ENISA et du GECC, peut recommander l'ouverture de négociations à cette fin. Chaque schéma européen de certification de cybersécurité devrait prévoir des conditions spécifiques pour de tels accords de reconnaissance mutuelle avec des pays tiers.
- (106) Afin d'assurer des conditions uniformes d'exécution du présent règlement, il convient de conférer des compétences d'exécution à la Commission. Ces compétences devraient être exercées en conformité avec le règlement (UE) n° 182/2011 du Parlement européen et du Conseil <sup>(22)</sup>.
- (107) Il convient d'avoir recours à la procédure d'examen pour l'adoption d'actes d'exécution concernant les schémas européens de certification de cybersécurité applicables à des produits TIC, services TIC ou processus TIC, pour l'adoption d'actes d'exécution concernant les modalités d'exécution des enquêtes menées par l'ENISA, pour l'adoption d'actes d'exécution concernant un plan pour l'examen par les pairs des autorités nationales de certification de cybersécurité et pour l'adoption d'actes d'exécution concernant les circonstances, les formats et les procédures de notification à la Commission des organismes d'évaluation de la conformité accrédités par les autorités nationales de certification de cybersécurité.
- (108) Les activités de l'ENISA devraient faire l'objet d'évaluations régulières et indépendantes. Ces évaluations devraient porter sur les objectifs, les méthodes de travail et la pertinence des tâches de l'ENISA, en particulier les tâches qui ont trait à la coopération opérationnelle au niveau de l'Union. Ces évaluations devraient également porter sur l'impact, l'efficacité et l'efficience du cadre européen de certification de cybersécurité. En cas de réexamen, la Commission devrait évaluer comment le rôle de l'ENISA en tant que point de référence pour les conseils et les compétences peut être renforcé, et devrait également évaluer le rôle que l'ENISA pourrait jouer pour soutenir l'évaluation des produits TIC, services TIC et processus TIC de pays tiers qui ne respectent pas les règles de l'Union, lorsque ces produits, services et processus entrent dans l'Union.

<sup>(22)</sup> Règlement (UE) n° 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

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

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

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

## TITRE I

### DISPOSITIONS GÉNÉRALES

#### *Article premier*

#### **Objet et champ d'application**

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

- a) les objectifs, les tâches et les questions organisationnelles concernant l'ENISA (l'Agence de l'Union européenne pour la cybersécurité); et
- b) un cadre pour la mise en place de schémas européens de certification de cybersécurité dans le but de garantir un niveau adéquat de cybersécurité des produits TIC, services TIC et processus TIC dans l'Union, ainsi que dans le but d'éviter la fragmentation du marché intérieur pour ce qui est des schémas de certification dans l'Union.

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

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

#### *Article 2*

#### **Définitions**

Aux fins du présent règlement, on entend par:

- 1) «cybersécurité», les actions nécessaires pour protéger les réseaux et les systèmes d'information, les utilisateurs de ces systèmes et les autres personnes exposées aux cybermenaces;
- 2) «réseau et système d'information», un réseau et système d'information au sens de l'article 4, point 1), de la directive (UE) 2016/1148;
- 3) «stratégie nationale en matière de sécurité des réseaux et des systèmes d'information», une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information au sens de l'article 4, point 3), de la directive (UE) 2016/1148;
- 4) «opérateur de services essentiels», un opérateur de services essentiels au sens de l'article 4, point 4), de la directive (UE) 2016/1148;
- 5) «fournisseur de service numérique», un fournisseur de service numérique au sens de l'article 4, point 6), de la directive (UE) 2016/1148;
- 6) «incident», un incident au sens de l'article 4, point 7), de la directive (UE) 2016/1148;
- 7) «gestion d'incident», la gestion d'incident au sens de l'article 4, point 8), de la directive (UE) 2016/1148;

- 8) «cybermenace», toute circonstance, tout événement ou toute action potentiels susceptibles de nuire ou de porter autrement atteinte aux réseaux et systèmes d'information, aux utilisateurs de tels systèmes et à d'autres personnes, ou encore de provoquer des interruptions de ces réseaux et systèmes;
- 9) «schéma européen de certification de cybersécurité», un ensemble complet de règles, d'exigences techniques, de normes et de procédures qui sont établies à l'échelon de l'Union et qui s'appliquent à la certification ou à l'évaluation de la conformité de produits TIC, services TIC ou processus TIC spécifiques;
- 10) «schéma national de certification de cybersécurité», un ensemble complet de règles, d'exigences techniques, de normes et de procédures élaborées et adoptées par une autorité publique nationale et qui s'appliquent à la certification ou à l'évaluation de la conformité des produits TIC, services TIC et processus TIC relevant de ce schéma spécifique;
- 11) «certificat de cybersécurité européen», un document délivré par un organisme compétent attestant qu'un produit TIC, service TIC ou processus TIC donné a été évalué en ce qui concerne sa conformité aux exigences de sécurité spécifiques fixées dans un schéma européen de certification de cybersécurité;
- 12) «produit TIC», un élément ou un groupe d'éléments appartenant à un réseau ou à un schéma d'information;
- 13) «service TIC», un service consistant intégralement ou principalement à transmettre, stocker, récupérer ou traiter des informations au moyen de réseaux et de systèmes d'information;
- 14) «processus TIC», un ensemble d'activités exécutées pour concevoir, développer ou fournir un produit TIC ou service TIC ou en assurer la maintenance;
- 15) «accréditation», l'accréditation au sens de l'article 2, point 10), du règlement (CE) n° 765/2008;
- 16) «organisme national d'accréditation», un organisme national d'accréditation au sens de l'article 2, point 11), du règlement (CE) n° 765/2008;
- 17) «évaluation de la conformité», une évaluation de la conformité au sens de l'article 2, point 12), du règlement (CE) n° 765/2008;
- 18) «organisme d'évaluation de la conformité», un organisme d'évaluation de la conformité au sens de l'article 2, point 13), du règlement (CE) n° 765/2008;
- 19) «norme», une norme au sens de l'article 2, point 1), du règlement (UE) n° 1025/2012;
- 20) «spécification technique», un document qui établit les exigences techniques auxquelles un produit TIC, service TIC ou processus TIC doit répondre ou des procédures d'évaluation de la conformité afférentes à un produit TIC, service TIC ou processus TIC;
- 21) «niveau d'assurance», le fondement permettant de garantir qu'un produit TIC, service TIC ou processus TIC satisfait aux exigences de sécurité d'un schéma européen de certification de cybersécurité spécifique, indique le niveau auquel un produit TIC, service TIC ou processus TIC a été évalué mais, en tant que tel, ne mesure pas la sécurité du produit TIC, service TIC ou processus TIC concerné;
- 22) «autoévaluation de la conformité», une action effectuée par un fabricant ou un fournisseur de produits TIC, services TIC ou processus TIC, qui évalue si ces produits TIC, services TIC ou processus TIC satisfont aux exigences fixées dans un schéma européen de certification de cybersécurité spécifique.

## TITRE II

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

## CHAPITRE I

**Mandat et objectifs***Article 3***Mandat**

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

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

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

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

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

*Article 4***Objectifs**

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

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

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

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

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

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

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

## CHAPITRE II

*Tâches**Article 5***Élaboration et mise en œuvre de la politique et du droit de l'Union**

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

- 1) en apportant son concours et en fournissant des conseils concernant l'élaboration et la révision de la politique et du droit de l'Union dans le domaine de la cybersécurité, et concernant les initiatives politiques et législatives sectorielles mettant en jeu des questions liées à la cybersécurité, notamment en fournissant des avis et des analyses indépendants, ainsi qu'en effectuant des travaux préparatoires;
- 2) en aidant les États membres à mettre en œuvre la politique et le droit de l'Union en matière de cybersécurité de manière cohérente, notamment en ce qui concerne la directive (UE) 2016/1148, y compris en délivrant des avis et des lignes directrices, et en fournissant des conseils et des meilleures pratiques sur des thèmes tels que la gestion des risques, le signalement des incidents et le partage d'informations, ainsi qu'en facilitant l'échange de meilleures pratiques entre les autorités compétentes à cet égard;
- 3) en aidant les États membres et les institutions, organes et organismes de l'Union à élaborer et à promouvoir des politiques en matière de cybersécurité visant à soutenir la disponibilité ou l'intégrité générales du noyau public de l'internet ouvert;
- 4) en contribuant, par ses compétences et son concours, aux travaux du groupe de coopération institué en application de l'article 11 de la directive (UE) 2016/1148;
- 5) en soutenant:
  - a) l'élaboration et la mise en œuvre de la politique de l'Union dans le domaine de l'identification électronique et des services de confiance, en particulier en fournissant des conseils et en délivrant des lignes directrices techniques, ainsi qu'en facilitant l'échange de meilleures pratiques entre les autorités compétentes;
  - b) la promotion d'une amélioration du niveau de sécurité des communications électroniques, y compris en fournissant des conseils et des compétences, ainsi qu'en facilitant l'échange de meilleures pratiques entre les autorités compétentes;
  - c) les États membres dans la mise en œuvre d'aspects spécifiques en matière de cybersécurité des politiques et du droit de l'Union concernant la protection des données et la vie privée, y compris en fournissant des avis au comité européen de la protection des données à sa demande;
- 6) en soutenant le réexamen périodique des activités liées aux politiques de l'Union, par la préparation d'un rapport annuel sur l'état d'avancement de la mise en œuvre du cadre juridique applicable en ce qui concerne:
  - a) les informations sur les notifications d'incidents des États membres transmises par les points de contact uniques au groupe de coopération conformément à l'article 10, paragraphe 3, de la directive (UE) 2016/1148;
  - b) les résumés des notifications d'atteinte à la sécurité ou de perte d'intégrité reçues des prestataires de services de confiance et transmises à l'ENISA par les organes de contrôle, conformément à l'article 19, paragraphe 3, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil <sup>(23)</sup>;
  - c) les notifications d'incidents de sécurité transmises par les fournisseurs de réseaux de communications publics ou de services de communications électroniques accessibles au public, fournies à l'ENISA par les autorités compétentes, conformément à l'article 40 de la directive (UE) 2018/1972.

<sup>(23)</sup> Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (JO L 257 du 28.8.2014, p. 73).

*Article 6***Renforcement des capacités**

1. L'ENISA assiste:
  - a) les États membres dans leurs efforts pour améliorer la prévention, la détection et l'analyse des cybermenaces et incidents, ainsi que la capacité d'y réagir, en leur fournissant des connaissances et des compétences;
  - b) les États membres et les institutions, organes et organismes de l'Union pour établir et mettre en œuvre, sur une base volontaire, des politiques en matière de divulgation des vulnérabilités;
  - c) les institutions, organes et organismes de l'Union dans leurs efforts pour améliorer la prévention, la détection et l'analyse des cybermenaces et incidents, et pour améliorer leur capacité à y réagir, notamment en apportant un soutien adapté à la CERT-UE;
  - d) les États membres dans la mise en place de CSIRT nationaux, lorsqu'ils le demandent conformément à l'article 9, paragraphe 5, de la directive (UE) 2016/1148;
  - e) les États membres dans l'élaboration de stratégies nationales en matière de sécurité des réseaux et des systèmes d'information, lorsqu'ils le demandent conformément à l'article 7, paragraphe 2, de la directive (UE) 2016/1148, et favorise la diffusion de ces stratégies et prend note de l'avancement de leur mise en œuvre dans toute l'Union afin de promouvoir les meilleures pratiques;
  - f) les institutions de l'Union dans l'élaboration et la révision des stratégies de l'Union en matière de cybersécurité, la promotion de leur diffusion et le suivi de l'avancement de leur mise en œuvre;
  - g) les CSIRT nationaux et de l'Union dans le relèvement du niveau de leurs capacités, y compris en favorisant le dialogue et les échanges d'informations, pour faire en sorte que chaque CSIRT, eu égard à l'état de l'art, possède un socle commun de capacités minimales et fonctionne selon les meilleures pratiques;
  - h) les États membres en organisant régulièrement les exercices de cybersécurité au niveau de l'Union visés à l'article 7, paragraphe 5, au moins tous les deux ans, et en formulant des recommandations en vue d'actions sur la base de l'évaluation de ces exercices et des enseignements qui en ont été tirés;
  - i) les organismes publics concernés en proposant des formations sur la cybersécurité, le cas échéant en coopération avec des parties prenantes;
  - j) le groupe de coopération pour ce qui est de l'échange de meilleures pratiques, notamment en ce qui concerne l'identification, par les États membres, des opérateurs de services essentiels, conformément à l'article 11, paragraphe 3, point l), de la directive (UE) 2016/1148, y compris au regard des dépendances transfrontières, en matière de risques et d'incidents.
2. L'ENISA soutient le partage d'informations au sein des secteurs et entre ceux-ci, en particulier dans les secteurs énumérés à l'annexe II de la directive (UE) 2016/1148, en fournissant des meilleures pratiques et des orientations sur les outils disponibles, les procédures, ainsi que la manière de traiter les questions de réglementation liées au partage d'informations.

*Article 7***Coopération opérationnelle au niveau de l'Union**

1. L'ENISA apporte son soutien à la coopération opérationnelle entre les États membres, les institutions, organes et organismes de l'Union, et entre les parties prenantes.
2. L'ENISA coopère sur le plan opérationnel et crée des synergies avec les institutions, organes et organismes de l'Union, y compris la CERT-UE, avec les services traitant de la cybercriminalité et avec les autorités de contrôle responsables de la protection de la vie privée et des données à caractère personnel, en vue de traiter des questions d'intérêt commun, y compris:
  - a) en échangeant savoir-faire et meilleures pratiques;
  - b) en fournissant des conseils et des lignes directrices sur des questions pertinentes liées à la cybersécurité;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

#### Article 8

##### **Marché, certification de cybersécurité et normalisation**

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

- a) en surveillant, en permanence, les évolutions dans les domaines connexes de la normalisation et en recommandant des spécifications techniques d'utilisation appropriées dans le développement des schémas européens de certification de cybersécurité en application de l'article 54, paragraphe 1, point c), dans les cas où il n'existe aucune norme;
- b) en préparant des schémas européens de certification de cybersécurité candidats (ci-après dénommés «schémas candidats») pour des produits TIC, services TIC et processus TIC, conformément à l'article 49;
- c) en évaluant les schémas européens de certification de cybersécurité, conformément à l'article 49, paragraphe 8;
- d) en participant aux examens par les pairs, conformément à l'article 59, paragraphe 4;
- e) en aidant la Commission à assurer le secrétariat du GECC, conformément à l'article 62, paragraphe 5.

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

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

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

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

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

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

#### Article 9

##### **Connaissance et information**

L'ENISA:

- a) analyse les technologies émergentes et fournit des évaluations thématiques sur les incidences escomptées des innovations technologiques en matière de cybersécurité, du point de vue sociétal, juridique, économique et réglementaire;
- b) produit des analyses stratégiques à long terme des cybermenaces et des incidents afin d'identifier les tendances émergentes et de contribuer à prévenir les incidents;

- c) en coopération avec des experts des autorités des États membres et les parties prenantes concernées, fournit des avis, des orientations et des meilleures pratiques en matière de sécurité des réseaux et des systèmes d'information, en particulier pour la sécurité des infrastructures sur lesquelles s'appuient les secteurs énumérés à l'annexe II de la directive (UE) 2016/1148 et de celles utilisées par les fournisseurs des services numériques énumérés à l'annexe III de ladite directive;
- d) par l'intermédiaire d'un portail spécialisé, regroupe, organise et met à la disposition du public des informations sur la cybersécurité, fournies par les institutions, organes et organismes de l'Union et des informations sur la cybersécurité fournies, sur une base volontaire, par les États membres et les parties prenantes des secteurs public et privé;
- e) collecte et analyse des informations du domaine public sur les incidents importants, et rédige des rapports en vue de fournir des orientations aux citoyens, organisations et entreprises dans toute l'Union.

#### *Article 10*

#### **Sensibilisation et éducation**

L'ENISA:

- a) sensibilise le public aux risques liés à la cybersécurité et fournit, à l'intention des citoyens, des organisations et des entreprises, des orientations sur les bonnes pratiques à adopter par les utilisateurs individuels, y compris en matière d'hygiène informatique et d'habileté numérique;
- b) en coopération avec les États membres, ainsi que les institutions, organes et organismes de l'Union et les entreprises du secteur, organise à intervalles réguliers des campagnes d'information afin de renforcer la cybersécurité et d'en accroître la visibilité dans l'Union, et encourage un large débat public;
- c) aide les États membres dans leurs efforts visant à mieux faire connaître la cybersécurité et à promouvoir l'éducation à la cybersécurité;
- d) encourage une coordination plus étroite et l'échange de meilleures pratiques entre les États membres en matière de sensibilisation et d'éducation à la cybersécurité.

#### *Article 11*

#### **Recherche et innovation**

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

- a) conseille les institutions, organes et organismes de l'Union et les États membres sur les besoins et les priorités en matière de recherche dans le domaine de la cybersécurité, afin que des réponses efficaces puissent être apportées aux risques et aux cybermenaces actuels et émergents, y compris en ce qui concerne les technologies de l'information et de la communication nouvelles et émergentes, et afin que les technologies de prévention des risques soient utilisées de manière efficace;
- b) participe, lorsque la Commission lui a conféré les pouvoirs correspondants, à la phase de mise en œuvre des programmes de financement de la recherche et de l'innovation, ou est bénéficiaire de ces programmes;
- c) contribue au programme stratégique de recherche et d'innovation au niveau de l'Union dans le domaine de la cybersécurité.

#### *Article 12*

#### **Coopération internationale**

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

- a) le cas échéant, en s'impliquant en tant qu'observateur dans l'organisation d'exercices internationaux, ainsi qu'en analysant les résultats de ces exercices et en en rendant compte au conseil d'administration;
- b) à la demande de la Commission, en facilitant l'échange de meilleures pratiques;

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

### CHAPITRE III

#### **Organisation de l'ENISA**

##### Article 13

#### **Structure de l'ENISA**

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

- a) un conseil d'administration;
- b) un conseil exécutif;
- c) un directeur exécutif;
- d) un groupe consultatif de l'ENISA;
- e) un réseau des agents de liaison nationaux.

##### Section 1

#### **Conseil d'administration**

##### Article 14

#### **Composition du conseil d'administration**

1. Le conseil d'administration est composé d'un membre nommé par chaque État membre, et de deux membres nommés par la Commission. Tous les membres disposent du droit de vote.
2. Chaque membre du conseil d'administration dispose d'un suppléant. Ce suppléant représente le membre en son absence.
3. Les membres du conseil d'administration et leurs suppléants sont nommés sur la base de leurs connaissances dans le domaine de la cybersécurité, compte tenu de leurs aptitudes managériales, administratives et budgétaires pertinentes. La Commission et les États membres s'efforcent de limiter le roulement de leurs représentants au sein du conseil d'administration, afin de garantir la continuité des travaux du conseil d'administration. La Commission et les États membres visent à atteindre une représentation hommes-femmes équilibrée au sein du conseil d'administration.
4. La durée du mandat des membres du conseil d'administration et de leurs suppléants est de quatre ans. Ce mandat est renouvelable.

##### Article 15

#### **Fonctions du conseil d'administration**

1. Le conseil d'administration:
  - a) fixe l'orientation générale du fonctionnement de l'ENISA et veille à ce que l'ENISA fonctionne conformément aux règles et principes fixés dans le présent règlement; il assure aussi la cohérence des travaux de l'ENISA avec les activités menées par les États membres ainsi qu'au niveau de l'Union;
  - b) adopte le projet de document unique de programmation de l'ENISA visé à l'article 24, avant de le soumettre pour avis à la Commission;

- c) adopte le document unique de programmation de l'ENISA, en tenant compte de l'avis de la Commission;
- d) supervise la mise en œuvre de la programmation annuelle et pluriannuelle contenue dans le document unique de programmation;
- e) adopte le budget annuel de l'ENISA et exerce d'autres fonctions en ce qui concerne le budget de l'ENISA conformément au chapitre IV;
- f) évalue et adopte le rapport annuel consolidé sur les activités de l'ENISA, y compris les comptes et une description de la manière dont l'ENISA a atteint ses indicateurs de performance, et transmet, au plus tard le 1<sup>er</sup> juillet de l'année suivante, le rapport annuel et l'évaluation de ce rapport au Parlement européen, au Conseil, à la Commission et à la Cour des comptes; elle publie le rapport annuel;
- g) adopte les règles financières applicables à l'ENISA, conformément à l'article 32;
- h) adopte une stratégie antifraude qui est proportionnée aux risques de fraude compte tenu de l'analyse coûts-bénéfices des mesures à mettre en œuvre;
- i) adopte des règles en matière de prévention et de gestion des conflits d'intérêts concernant ses membres;
- j) assure le suivi approprié des conclusions et des recommandations découlant des enquêtes de l'Office européen de lutte antifraude (OLAF) et des divers rapports d'audit et évaluations internes et externes;
- k) adopte son règlement intérieur, y compris les règles relatives aux décisions provisoires sur la délégation de tâches spécifiques, en vertu de l'article 19, paragraphe 7;
- l) exerce, à l'égard du personnel de l'ENISA, les compétences qui sont dévolues par le statut des fonctionnaires de l'Union européenne (ci-après dénommé «statut des fonctionnaires») et le régime applicable aux autres agents de l'Union européenne (ci-après dénommé «régime applicable aux autres agents»), fixés par le règlement (CEE, Euratom, CECA) n° 259/68 du Conseil <sup>(24)</sup>, à l'autorité investie du pouvoir de nomination et à l'autorité habilitée à conclure les contrats d'engagement (ci-après dénommées «compétences de l'autorité investie du pouvoir de nomination») conformément au paragraphe 2 du présent article;
- m) arrête les règles d'exécution du statut des fonctionnaires et du régime applicable aux autres agents conformément à la procédure prévue à l'article 110 du statut des fonctionnaires;
- n) nomme le directeur exécutif et, le cas échéant, proroge son mandat ou le démet de ses fonctions conformément à l'article 36;
- o) nomme un comptable, qui peut être le comptable de la Commission et qui est totalement indépendant dans l'exercice de ses fonctions;
- p) prend toutes les décisions relatives à la mise en place des structures internes de l'ENISA et, le cas échéant, à leur modification, en tenant compte des besoins liés à l'activité de l'ENISA et en respectant le principe d'une gestion budgétaire saine;
- q) autorise la conclusion d'arrangements de travail conformément à l'article 7;
- r) autorise l'élaboration ou la conclusion d'arrangements de travail conformément à l'article 42.

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

<sup>(24)</sup> JO L 56 du 4.3.1968, p. 1.

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

#### Article 16

##### **Présidence du conseil d'administration**

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

#### Article 17

##### **Réunions du conseil d'administration**

1. Les réunions du conseil d'administration sont convoquées par son président.
2. Le conseil d'administration tient une réunion ordinaire au moins deux fois par an. Il tient aussi des réunions extraordinaires à l'initiative de son président, à la demande de la Commission ou à la demande d'au moins un tiers de ses membres.
3. Le directeur exécutif participe aux réunions du conseil d'administration mais ne dispose pas du droit de vote.
4. Sur invitation du président, des membres du groupe consultatif de l'ENISA peuvent participer aux réunions du conseil d'administration, mais ne disposent pas du droit de vote.
5. Les membres du conseil d'administration et leurs suppléants peuvent, dans le respect du règlement intérieur du conseil d'administration, être assistés au cours des réunions du conseil d'administration par des conseillers ou des experts.
6. L'ENISA assure le secrétariat du conseil d'administration.

#### Article 18

##### **Règles de vote du conseil d'administration**

1. Les décisions du conseil d'administration sont prises à la majorité de ses membres.
2. Une majorité des deux tiers des membres du conseil d'administration est nécessaire pour adopter le document unique de programmation et le budget annuel, et pour nommer le directeur exécutif, proroger son mandat ou le révoquer.
3. Chaque membre dispose d'une voix. En l'absence d'un membre, son suppléant peut exercer le droit de vote du membre.
4. Le président du conseil d'administration prend part au vote.
5. Le directeur exécutif ne prend pas part au vote.
6. Le règlement intérieur du conseil d'administration fixe les modalités détaillées du vote, notamment les conditions dans lesquelles un membre peut agir au nom d'un autre membre.

## Section 2

**Conseil exécutif**

## Article 19

**Conseil exécutif**

1. Le conseil d'administration est assisté d'un conseil exécutif.
2. Le conseil exécutif:
  - a) prépare les décisions qui doivent être adoptées par le conseil d'administration;
  - b) assure, avec le conseil d'administration, le suivi approprié des conclusions et des recommandations découlant des enquêtes de l'OLAF ainsi que des divers rapports d'audit et des évaluations internes ou externes;
  - c) sans préjudice des tâches du directeur exécutif énoncées à l'article 20, assiste et conseille le directeur exécutif dans la mise en œuvre des décisions du conseil d'administration relatives à des questions administratives et budgétaires, conformément à l'article 20.
3. Le conseil exécutif est composé de cinq membres. Les membres du conseil exécutif sont nommés parmi les membres du conseil d'administration. Un des membres est le président du conseil d'administration, qui peut également présider le conseil exécutif, et un autre membre est un des représentants de la Commission. Les nominations des membres du conseil exécutif visent à assurer une représentation hommes-femmes équilibrée au sein du conseil exécutif. Le directeur exécutif participe aux réunions du conseil exécutif, mais ne dispose pas du droit de vote.
4. La durée du mandat des membres du conseil exécutif est de quatre ans. Ce mandat est renouvelable.
5. Le conseil exécutif se réunit au moins une fois par trimestre. Le président du conseil exécutif convoque des réunions supplémentaires à la demande de ses membres.
6. Le conseil d'administration établit le règlement intérieur du conseil exécutif.
7. Lorsque l'urgence le requiert, le conseil exécutif peut prendre certaines décisions provisoires au nom du conseil d'administration, en particulier sur des questions de gestion administrative, comme la suspension de la délégation des compétences dévolues à l'autorité investie du pouvoir de nomination, et sur des questions budgétaires. De telles décisions provisoires sont notifiées sans retard indu. Le conseil d'administration décide ensuite s'il approuve ou s'il rejette la décision provisoire trois mois au plus tard après la prise de décision. Le conseil exécutif ne prend pas de décisions au nom du conseil d'administration qui doivent être approuvées par une majorité des deux tiers des membres du conseil d'administration.

## Section 3

**Directeur exécutif**

## Article 20

**Tâches du directeur exécutif**

1. L'ENISA est gérée par son directeur exécutif, qui est indépendant dans l'exécution de ses tâches. Le directeur exécutif rend compte de ses activités au conseil d'administration.
2. Le directeur exécutif fait rapport au Parlement européen sur l'exécution de ses tâches, lorsqu'il y est invité. Le Conseil peut inviter le directeur exécutif à lui faire rapport sur l'exécution de ses tâches.
3. Le directeur exécutif est chargé:
  - a) d'assurer l'administration courante de l'ENISA;

- b) de mettre en œuvre les décisions adoptées par le conseil d'administration;
- c) de préparer le projet de document unique de programmation et de le soumettre au conseil d'administration pour approbation, avant qu'il ne soit soumis à la Commission;
- d) de mettre en œuvre le document unique de programmation et d'en faire rapport au conseil d'administration;
- e) de préparer le rapport annuel consolidé sur les activités de l'ENISA, y compris la mise en œuvre du programme de travail annuel de l'ENISA, et de le présenter au conseil d'administration pour évaluation et adoption;
- f) de préparer un plan d'action faisant suite aux conclusions des évaluations rétrospectives et de faire rapport tous les deux ans à la Commission sur les progrès accomplis;
- g) de préparer un plan d'action donnant suite aux conclusions des rapports d'audit internes ou externes, ainsi qu'aux enquêtes de l'OLAF, et de présenter des rapports semestriels à la Commission et des rapports réguliers au conseil d'administration sur les progrès accomplis;
- h) de préparer le projet de règles financières applicables à l'ENISA visé à l'article 32;
- i) de préparer le projet d'état prévisionnel des recettes et dépenses de l'ENISA et d'exécuter son budget;
- j) de protéger les intérêts financiers de l'Union par l'application de mesures préventives contre la fraude, la corruption et d'autres activités illégales, par des contrôles efficaces et, si des irrégularités sont constatées, par le recouvrement des montants indûment payés et, le cas échéant, par des sanctions administratives et financières effectives, proportionnées et dissuasives;
- k) de préparer une stratégie antifraude pour l'ENISA et de la présenter au conseil d'administration pour approbation;
- l) d'établir et de maintenir le contact avec le secteur des entreprises et les organisations de consommateurs afin d'assurer un dialogue régulier avec les parties prenantes concernées;
- m) d'avoir un échange de vues et d'informations régulier avec les institutions, organes et organismes de l'Union sur leurs activités en matière de cybersécurité, pour assurer la cohérence dans l'élaboration et dans la mise en œuvre de la politique de l'Union;
- n) d'exécuter les autres tâches qui sont assignées au directeur exécutif par le présent règlement.

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

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

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

## Section 4

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

## Article 21

**Groupe consultatif de l'ENISA**

1. Le conseil d'administration crée de manière transparente, sur proposition du directeur exécutif, le groupe consultatif de l'ENISA composé d'experts reconnus représentant les parties prenantes concernées, telles que les entreprises du secteur des TIC, les fournisseurs de réseaux ou de services de communications électroniques accessibles au public, les PME, les opérateurs de services essentiels, les organisations de consommateurs, les experts universitaires en matière de cybersécurité, les représentants des autorités compétentes qui ont fait l'objet d'une notification conformément à la directive (UE) 2018/1972, les organisations européennes de normalisation ainsi que les autorités chargées de l'application de la loi et les autorités de contrôle de la protection des données. Le conseil d'administration s'efforce d'assurer un équilibre approprié entre les hommes et les femmes et un équilibre géographique, ainsi qu'un équilibre entre les différents groupes de parties prenantes.
2. Les procédures applicables au groupe consultatif de l'ENISA, notamment en ce qui concerne sa composition, la proposition du directeur exécutif visée au paragraphe 1, le nombre de membres et leur nomination, ainsi que le fonctionnement du groupe consultatif de l'ENISA sont précisées dans les règles internes de fonctionnement de l'ENISA et sont rendues publiques.
3. Le groupe consultatif de l'ENISA est présidé par le directeur exécutif ou par toute personne qu'il désigne à cet effet au cas par cas.
4. La durée du mandat des membres du groupe consultatif de l'ENISA est de deux ans et demi. Les membres du conseil d'administration ne peuvent pas être membres du groupe consultatif de l'ENISA. Des experts de la Commission et des États membres sont autorisés à assister aux réunions et à prendre part aux travaux du groupe consultatif de l'ENISA. Des représentants d'autres organismes jugés intéressants par le directeur exécutif, qui ne sont pas membres du groupe consultatif de l'ENISA, peuvent être invités à assister aux réunions du groupe consultatif de l'ENISA et à prendre part à ses travaux.
5. Le groupe consultatif de l'ENISA conseille l'ENISA en ce qui concerne l'exécution des tâches de celle-ci, excepté l'application des dispositions du titre III du présent règlement. Il conseille en particulier le directeur exécutif pour ce qui est de l'élaboration d'une proposition de programme de travail annuel pour l'ENISA et de la communication à assurer avec les parties prenantes concernées sur les questions liées au programme de travail annuel.
6. Le groupe consultatif de l'ENISA informe régulièrement le conseil d'administration de ses activités.

## Article 22

**Groupe des parties prenantes pour la certification de cybersécurité**

1. Il est établi un groupe des parties prenantes pour la certification de cybersécurité.
2. Le groupe des parties prenantes pour la certification de cybersécurité se compose de membres sélectionnés parmi des experts reconnus représentant les parties prenantes concernées. La Commission, à la suite d'un appel transparent et ouvert, sélectionne, sur la base d'une proposition de l'ENISA, les membres du groupe des parties prenantes pour la certification de cybersécurité en assurant un équilibre entre les différents groupes de parties prenantes ainsi qu'un équilibre approprié entre les hommes et les femmes et un équilibre géographique.
3. Le groupe des parties prenantes pour la certification de cybersécurité est chargé:
  - a) de conseiller la Commission sur des questions stratégiques relatives au cadre européen de certification de cybersécurité;
  - b) sur demande, de conseiller l'ENISA sur des questions générales et stratégiques concernant les tâches de l'ENISA relatives au marché, à la certification de cybersécurité et à la normalisation;
  - c) d'aider la Commission à préparer le programme de travail glissant de l'Union visé à l'article 47;

- d) de rendre un avis sur le programme de travail glissant de l'Union conformément à l'article 47, paragraphe 4; et
- e) en cas d'urgence, de donner un avis à la Commission et au GECC sur la nécessité de disposer de schémas de certification supplémentaires qui ne sont pas compris dans le programme de travail glissant de l'Union, comme indiqué aux articles 47 et 48.
4. Le groupe des parties prenantes pour la certification de cybersécurité est coprésidé par les représentants de la Commission et de l'ENISA, et son secrétariat est assuré par l'ENISA.

#### Article 23

##### **Réseau des agents de liaison nationaux**

1. Le conseil d'administration crée, sur proposition du directeur exécutif, un réseau des agents de liaison nationaux composé de représentants de tous les États membres (les agents de liaison nationaux). Chaque État membre nomme un représentant au sein du réseau des agents de liaison nationaux. Les réunions du réseau des agents de liaison nationaux peuvent se tenir dans différentes configurations d'experts.
2. Le réseau des agents de liaison nationaux facilite en particulier l'échange d'informations entre l'ENISA et les États membres et aide l'ENISA à faire connaître ses activités et à diffuser les résultats de ses travaux et ses recommandations auprès des parties prenantes concernées dans l'ensemble de l'Union.
3. Les agents de liaison nationaux servent de point de contact au niveau national pour faciliter la coopération entre l'ENISA et les experts nationaux dans le cadre de la mise en œuvre du programme de travail annuel de l'ENISA.
4. Si les agents de liaison nationaux coopèrent étroitement avec les représentants du conseil d'administration de leurs États membres respectifs, le réseau des agents de liaison nationaux en lui-même ne doit pas dupliquer le travail du conseil d'administration ou d'autres instances de l'Union.
5. Les fonctions et les procédures du réseau des agents de liaison nationaux sont précisées dans les règles internes de fonctionnement de l'ENISA et sont rendues publiques.

#### Section 5

##### **Fonctionnement**

#### Article 24

##### **Document unique de programmation**

1. L'ENISA opère conformément à un document unique de programmation qui décrit sa programmation annuelle et pluriannuelle, et qui contient l'ensemble de ses activités planifiées.
2. Le directeur exécutif établit chaque année un projet de document unique de programmation contenant sa programmation annuelle et pluriannuelle, ainsi que la planification des ressources financières et humaines correspondantes, conformément à l'article 32 du règlement délégué (UE) n° 1271/2013 de la Commission<sup>(25)</sup>, et tenant compte des lignes directrices fixées par la Commission.
3. Le conseil d'administration adopte, au plus tard le 30 novembre de chaque année, le document unique de programmation visé au paragraphe 1 et le transmet au Parlement européen, au Conseil et à la Commission au plus tard le 31 janvier de l'année suivante, ainsi que toute version de ce document actualisée ultérieurement.
4. Le document unique de programmation devient définitif après l'adoption définitive du budget général de l'Union et il est adapté en tant que de besoin.

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

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

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

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

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

#### *Article 25*

##### **Déclaration d'intérêts**

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

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

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

#### *Article 26*

##### **Transparence**

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

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

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

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

#### *Article 27*

##### **Confidentialité**

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

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

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

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

#### Article 28

##### Accès aux documents

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

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

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

#### CHAPITRE IV

##### Établissement et structure du budget de l'ENISA

#### Article 29

##### Établissement du budget de l'ENISA

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

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

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

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

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

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

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

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

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

#### Article 30

##### Structure du budget de l'ENISA

1. Sans préjudice d'autres ressources, les recettes de l'ENISA sont constituées:
  - a) d'une contribution provenant du budget général de l'Union;
  - b) de recettes allouées à des postes de dépense spécifiques conformément à ses règles financières visées à l'article 32;
  - c) d'un financement de l'Union sous la forme de conventions de délégation ou de subventions ad hoc, conformément à ses règles financières visées à l'article 32 et aux dispositions des instruments pertinents appuyant les politiques de l'Union;
  - d) de contributions de pays tiers participant aux travaux de l'ENISA conformément à l'article 42;
  - e) de toute contribution volontaire des États membres en espèces ou en nature.

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

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

#### Article 31

##### Exécution du budget de l'ENISA

1. Le directeur exécutif est responsable de l'exécution du budget de l'ENISA.
2. L'auditeur interne de la Commission exerce à l'égard de l'ENISA les mêmes pouvoirs que ceux qui lui sont attribués à l'égard des services de la Commission.
3. Le comptable de l'ENISA transmet les comptes provisoires pour l'exercice (exercice N) au comptable de la Commission et à la Cour des comptes au plus tard le 1<sup>er</sup> mars de l'exercice suivant (exercice N + 1).
4. À la réception des observations formulées par la Cour des comptes sur les comptes provisoires de l'ENISA en vertu de l'article 246 du règlement (UE, Euratom) 2018/1046 du Parlement européen et du Conseil <sup>(28)</sup>, le comptable de l'ENISA établit les comptes définitifs de l'ENISA sous sa propre responsabilité et les soumet au conseil d'administration pour avis.
5. Le conseil d'administration rend un avis sur les comptes définitifs de l'ENISA.
6. Au plus tard le 31 mars de l'année N + 1, le directeur exécutif transmet le rapport sur la gestion budgétaire et financière au Parlement européen, au Conseil, à la Commission et à la Cour des comptes.
7. Au plus tard le 1<sup>er</sup> juillet de l'année N + 1, le comptable de l'ENISA transmet les comptes définitifs de l'ENISA, accompagnés de l'avis du conseil d'administration, au Parlement européen, au Conseil, au comptable de la Commission et à la Cour des comptes.

<sup>(28)</sup> Règlement (UE, Euratom) 2018/1046 du Parlement européen et du Conseil du 18 juillet 2018 relatif aux règles financières applicables au budget général de l'Union, modifiant les règlements (UE) n° 1296/2013, (UE) n° 1301/2013, (UE) n° 1303/2013, (UE) n° 1304/2013, (UE) n° 1309/2013, (UE) n° 1316/2013, (UE) n° 223/2014, (UE) n° 283/2014 et la décision n° 541/2014/UE, et abrogeant le règlement (UE, Euratom) n° 966/2012 (JO L 193 du 30.7.2018, p. 1).

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

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

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

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

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

#### Article 32

##### Règles financières

Les règles financières applicables à l'ENISA sont arrêtées par le conseil d'administration, après consultation de la Commission. Elles ne peuvent s'écarter du règlement délégué (UE) n° 1271/2013 que si le fonctionnement de l'ENISA le nécessite spécifiquement et moyennant l'accord préalable de la Commission.

#### Article 33

##### Lutte contre la fraude

1. Afin de faciliter la lutte contre la fraude, la corruption et d'autres activités illégales au titre du règlement (UE, Euratom) n° 883/2013 du Parlement européen et du Conseil <sup>(29)</sup>, l'ENISA adhère, au plus tard le 28 décembre 2019, à l'accord interinstitutionnel du 25 mai 1999 entre le Parlement européen, le Conseil de l'Union européenne et la Commission des Communautés européennes relatif aux enquêtes internes effectuées par l'Office européen de lutte antifraude (OLAF) <sup>(30)</sup>. L'ENISA adopte les dispositions appropriées applicables à tout le personnel de l'ENISA, en utilisant le modèle figurant à l'annexe dudit accord.

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

3. L'OLAF peut effectuer des enquêtes, y compris des contrôles et vérifications sur place, conformément aux dispositions et procédures prévues par le règlement (UE, Euratom) n° 883/2013 et le règlement (Euratom, CE) n° 2185/96 du Conseil <sup>(31)</sup>, en vue d'établir l'existence éventuelle d'une fraude, d'un acte de corruption ou de toute autre activité illégale portant atteinte aux intérêts financiers de l'Union, en lien avec une subvention ou un contrat financés par l'ENISA.

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

<sup>(29)</sup> Règlement (UE, Euratom) n° 883/2013 du Parlement européen et du Conseil du 11 septembre 2013 relatif aux enquêtes effectuées par l'Office européen de lutte antifraude (OLAF) et abrogeant le règlement (CE) n° 1073/1999 du Parlement européen et du Conseil et le règlement (Euratom) n° 1074/1999 du Conseil (JO L 248 du 18.9.2013, p. 1).

<sup>(30)</sup> JO L 136 du 31.5.1999, p. 15.

<sup>(31)</sup> Règlement (Euratom, CE) n° 2185/96 du Conseil du 11 novembre 1996 relatif aux contrôles et vérifications sur place effectués par la Commission pour la protection des intérêts financiers des Communautés européennes contre les fraudes et autres irrégularités (JO L 292 du 15.11.1996, p. 2).

## CHAPITRE V

**Personnel**

## Article 34

**Dispositions générales**

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

## Article 35

**Privilèges et immunités**

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

## Article 36

**Directeur exécutif**

1. Le directeur exécutif est engagé en tant qu'agent temporaire de l'ENISA conformément à l'article 2, point a), du régime applicable aux autres agents.
2. Le directeur exécutif est nommé par le conseil d'administration sur la base d'une liste de candidats proposés par la Commission, à la suite d'une procédure de sélection ouverte et transparente.
3. Aux fins de la conclusion du contrat de travail du directeur exécutif, l'ENISA est représentée par le président du conseil d'administration.
4. Avant d'être nommé, le candidat retenu par le conseil d'administration est invité à faire une déclaration devant la commission concernée du Parlement européen et à répondre aux questions des députés.
5. Le mandat du directeur exécutif est de cinq ans. Au terme de cette période, la Commission procède à une évaluation du travail accompli par le directeur exécutif et des tâches et défis futurs de l'ENISA.
6. Le conseil d'administration statue sur la nomination, la prorogation du mandat et la révocation du directeur exécutif conformément à l'article 18, paragraphe 2.
7. Le conseil d'administration, sur proposition de la Commission tenant compte de l'évaluation visée au paragraphe 5, peut proroger une fois le mandat du directeur exécutif pour une durée de cinq ans.
8. Le conseil d'administration informe le Parlement européen de son intention de proroger le mandat du directeur exécutif. Dans les trois mois précédant cette prorogation, le directeur exécutif fait, s'il y est invité, une déclaration devant la commission concernée du Parlement européen et répond aux questions des députés.
9. Un directeur exécutif dont le mandat a été prorogé ne peut pas participer à une nouvelle procédure de sélection pour le même poste.
10. Le directeur exécutif ne peut être démis de ses fonctions que sur décision du conseil d'administration, statuant sur proposition de la Commission.

## Article 37

**Experts nationaux détachés et personnel autre**

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

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

#### CHAPITRE VI

### **Dispositions générales concernant l'ENISA**

#### Article 38

#### **Statut juridique de l'ENISA**

1. L'ENISA est un organisme de l'Union et elle est dotée de la personnalité juridique.
2. Dans chaque État membre, l'ENISA jouit de la capacité juridique la plus étendue accordée aux personnes morales en droit national. Elle peut notamment acquérir ou aliéner des biens mobiliers et immobiliers et ester en justice.
3. L'ENISA est représentée par le directeur exécutif.

#### Article 39

#### **Responsabilité de l'ENISA**

1. La responsabilité contractuelle de l'ENISA est régie par le droit applicable au contrat en question.
2. La Cour de justice de l'Union européenne est compétente pour statuer en vertu de toute clause compromissoire contenue dans un contrat conclu par l'ENISA.
3. En cas de responsabilité non contractuelle, l'ENISA répare tout dommage causé par ses services ou par son personnel dans l'exercice de leurs fonctions, conformément aux principes généraux communs aux législations des États membres.
4. La Cour de justice de l'Union européenne est compétente pour traiter de tout litige relatif à la réparation d'un dommage visé au paragraphe 3.
5. La responsabilité personnelle du personnel de l'ENISA envers l'ENISA est régie par les dispositions pertinentes applicables au personnel de l'ENISA.

#### Article 40

#### **Régime linguistique**

1. Le règlement n° 1 du Conseil <sup>(32)</sup> s'applique à l'ENISA. Les États membres et les autres organismes désignés par les États membres peuvent s'adresser à l'ENISA et recevoir une réponse dans la langue officielle des institutions de l'Union qu'ils choisissent.
2. Les services de traduction nécessaires au fonctionnement de l'ENISA sont assurés par le Centre de traduction des organes de l'Union européenne.

#### Article 41

#### **Protection des données à caractère personnel**

1. Les opérations de traitement de données à caractère personnel effectuées par l'ENISA sont soumises au règlement (UE) 2018/1725.
2. Le conseil d'administration adopte les dispositions d'application visées à l'article 45, paragraphe 3, du règlement (UE) 2018/1725. Le conseil d'administration peut adopter des mesures supplémentaires nécessaires pour l'application du règlement (UE) 2018/1725 par l'ENISA.

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

*Article 42***Coopération avec des pays tiers et des organisations internationales**

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

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

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

*Article 43***Règles de sécurité en matière de protection des informations sensibles non classifiées et des informations classifiées**

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

*Article 44***Accord de siège et conditions de fonctionnement**

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

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

*Article 45***Contrôle administratif**

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

## TITRE III

**CADRE DE CERTIFICATION DE CYBERSÉCURITÉ***Article 46***Cadre européen de certification de cybersécurité**

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

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

#### Article 47

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

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

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

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

- a) la disponibilité et le développement de schémas nationaux de certification de cybersécurité couvrant toute catégorie spécifique de produits TIC, services TIC ou processus TIC et, en particulier, en ce qui concerne le risque de fragmentation;
- b) le droit ou la politique applicable de l'Union ou d'un État membre;
- c) la demande du marché;
- d) l'évolution de la situation en ce qui concerne les cybermenaces;
- e) une demande de préparation d'un schéma candidat spécifique par le GECC.

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

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

#### Article 48

##### **Demande de schéma européen de certification de cybersécurité**

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

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

#### Article 49

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

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

2. À la suite d'une demande formulée par le GECC en vertu de l'article 48, paragraphe 2, l'ENISA peut préparer un schéma candidat qui satisfait aux exigences énoncées aux articles 51, 52 et 54. Si l'ENISA rejette une telle demande, elle doit motiver son refus. Toute décision de rejeter une telle demande est prise par le conseil d'administration.
3. Lors de la préparation d'un schéma candidat, l'ENISA consulte toutes les parties prenantes concernées au moyen d'un processus de consultation formel, ouvert, transparent et inclusif.
4. Pour chaque schéma candidat, l'ENISA crée un groupe de travail ad hoc, conformément à l'article 20, paragraphe 4, afin qu'il lui fournisse des conseils et des compétences spécifiques.
5. L'ENISA coopère étroitement avec le GECC. Celui-ci fournit aide et expertise à l'ENISA dans le cadre de la préparation du schéma candidat et adopte un avis sur le schéma candidat.
6. L'ENISA tient le plus grand compte de l'avis du GECC avant de transmettre à la Commission le schéma candidat préparé conformément aux paragraphes 3, 4 et 5. L'avis du GECC n'est pas contraignant pour l'ENISA, et l'absence d'un tel avis n'empêche pas l'ENISA de transmettre le schéma candidat à la Commission.
7. La Commission, se fondant sur le schéma candidat préparé par l'ENISA, peut adopter des actes d'exécution prévoyant un schéma européen de certification de cybersécurité pour les produits TIC, services TIC et processus TIC qui satisfont aux exigences des articles 51, 52 et 54. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 66, paragraphe 2.
8. L'ENISA procède au moins tous les cinq ans à une évaluation de chacun des schémas européens de certification de cybersécurité adoptés, en tenant compte des informations reçues en retour des parties intéressées. Si nécessaire, la Commission ou le GECC peut demander à l'ENISA de lancer le processus d'élaboration d'un schéma candidat révisé, conformément à l'article 48 et au présent article.

#### *Article 50*

##### **Site internet sur les schémas européens de certification de cybersécurité**

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

#### *Article 51*

##### **Objectifs de sécurité des schémas européens de certification de cybersécurité**

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

- a) protéger les données stockées, transmises ou traitées de toute autre façon contre le stockage, le traitement, l'accès ou la diffusion accidentels ou non autorisés au cours de l'ensemble du cycle de vie du produit TIC, service TIC ou processus TIC;
- b) protéger les données stockées, transmises ou traitées de toute autre façon contre la destruction accidentelle ou non autorisée, la perte ou l'altération, ou l'absence de disponibilité, au cours de l'ensemble du cycle de vie du produit TIC, service TIC ou processus TIC;
- c) faire en sorte que les personnes autorisées, les programmes ou les machines ne puissent accéder qu'aux données, services ou fonctions concernés par leurs droits d'accès;
- d) identifier et documenter les dépendances et vulnérabilités connues;

- e) garder une trace des données, fonctions ou services qui ont été consultés, utilisés ou traités de toute autre façon, du moment où ils l'ont été et par qui;
- f) faire en sorte qu'il soit possible de vérifier quels données, services ou fonctions ont été consultés, utilisés ou traités de toute autre façon, à quel moment et par qui;
- g) vérifier que les produits TIC, services TIC et processus TIC ne contiennent pas de vulnérabilités connues;
- h) rétablir la disponibilité des données, services et fonctions ainsi que l'accès à ceux-ci dans les plus brefs délais en cas d'incident physique ou technique;
- i) faire en sorte que les produits TIC, services TIC et processus TIC soient sécurisés par défaut et dès la conception;
- j) faire en sorte que les produits TIC, services TIC et processus TIC soient dotés de logiciels et de matériel à jour et sans vulnérabilités connues du public, et de mécanismes permettant d'assurer les mises à jour en toute sécurité.

#### Article 52

##### **Niveaux d'assurance des schémas européens de certification de cybersécurité**

1. Un schéma européen de certification de cybersécurité peut préciser un ou plusieurs des niveaux d'assurance suivants pour les produits TIC, services TIC et processus TIC: «élémentaire», «substantiel» ou «élevé». Le niveau d'assurance correspond au niveau de risque associé à l'utilisation prévue du produit TIC, service TIC ou processus TIC, en termes de probabilité et de répercussions d'un incident.
2. Les certificats de cybersécurité européens et les déclarations de conformité de l'Union européenne mentionnent tout niveau d'assurance précisé dans le schéma européen de certification de cybersécurité dans le cadre duquel le certificat de cybersécurité européen ou la déclaration de conformité de l'Union européenne a été délivré(e).
3. Les exigences de sécurité correspondant à chaque niveau d'assurance sont fournies dans le schéma européen de certification de cybersécurité concerné, y compris les fonctionnalités de sécurité correspondantes ainsi que la rigueur et l'ampleur correspondantes de l'évaluation à laquelle le produit TIC, service TIC ou processus TIC doit être soumis.
4. Le certificat ou la déclaration de conformité de l'Union européenne fait référence aux spécifications techniques, aux normes et aux procédures connexes, y compris les contrôles techniques, l'objectif étant de réduire le risque d'incidents de cybersécurité ou de les prévenir.
5. Un certificat de cybersécurité européen ou une déclaration de conformité de l'Union européenne qui se réfère au niveau d'assurance dit «élémentaire» offre l'assurance que les produits TIC, services TIC et processus TIC pour lesquels ce certificat ou cette déclaration de conformité de l'Union européenne est délivré(e) satisfont aux exigences de sécurité correspondantes, y compris les fonctionnalités de sécurité, et qu'ils ont été évalués à un niveau qui vise à minimiser les risques élémentaires connus d'incidents et de cyberattaques. Les activités d'évaluation à entreprendre comprennent au moins un examen de la documentation technique. Lorsqu'un tel examen n'est pas approprié, des activités d'évaluation de substitution ayant un effet équivalent sont entreprises.
6. Un certificat de cybersécurité européen qui se réfère au niveau d'assurance dit «substantiel» offre l'assurance que les produits TIC, services TIC et processus TIC pour lesquels ce certificat est délivré satisfont aux exigences de sécurité correspondantes, y compris des fonctionnalités de sécurité, et qu'ils ont été évalués à un niveau qui vise à minimiser les risques liés à la cybersécurité connus, et le risque d'incidents et de cyberattaques émanant d'acteurs aux aptitudes et aux ressources limitées. Les activités d'évaluation à entreprendre comprennent au moins: un examen visant à démontrer l'absence de vulnérabilités connues du public et des vérifications tendant à démontrer que les produits TIC, services TIC ou processus TIC mettent correctement en œuvre les fonctionnalités de sécurité nécessaires. Lorsque de telles activités d'évaluation ne sont pas appropriées, des activités d'évaluation de substitution ayant un effet équivalent sont entreprises.

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

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

#### Article 53

##### **Autoévaluation de la conformité**

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

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

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

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

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

#### Article 54

##### **Éléments des schémas européens de certification de cybersécurité**

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

- a) l'objet et le champ d'application du schéma de certification, notamment le type ou les catégories de produits TIC, services TIC et processus TIC couverts;
- b) une description claire de la finalité du schéma et de la façon dont les normes, les méthodes d'évaluation et les niveaux d'assurance sélectionnés correspondent aux besoins des utilisateurs auxquels le schéma est destiné;
- c) des références aux normes internationales, européennes ou nationales appliquées dans le cadre de l'évaluation ou, lorsque de telles normes n'existent pas ou ne sont pas appropriées, à des spécifications techniques qui satisfont aux exigences énoncées à l'annexe II du règlement (UE) n° 1025/2012 ou, lorsque de telles spécifications ne sont pas disponibles, à des spécifications techniques ou d'autres exigences de cybersécurité définies dans le schéma européen de certification de cybersécurité;
- d) le cas échéant, un ou plusieurs niveaux d'assurance;

- e) une mention indiquant si l'autoévaluation de la conformité est autorisée dans le cadre du schéma;
- f) le cas échéant, des exigences spécifiques ou supplémentaires auxquelles sont soumis les organismes d'évaluation de la conformité aux fins de garantir qu'ils disposent des compétences techniques nécessaires pour évaluer les exigences de cybersécurité;
- g) les critères et méthodes d'évaluation spécifiques qui doivent être utilisés, notamment les types d'évaluation, afin de démontrer que les objectifs de sécurité visés à l'article 51 sont atteints;
- h) le cas échéant, les informations nécessaires à la certification qu'un demandeur doit fournir aux organismes d'évaluation de la conformité ou mettre à leur disposition d'une autre façon;
- i) lorsque le schéma prévoit des marques ou des labels, les conditions dans lesquelles ces marques ou labels peuvent être utilisés;
- j) les règles relatives au contrôle du respect par les produits TIC, services TIC et processus TIC des exigences liées aux certificats de cybersécurité européens ou aux déclarations de conformité de l'Union européenne, notamment les mécanismes permettant de démontrer le respect constant des exigences de cybersécurité qui ont été définies;
- k) le cas échéant, les conditions permettant de délivrer, de maintenir, de prolonger et de renouveler les certificats européen de cybersécurité, ainsi que les conditions auxquelles il est possible d'étendre ou de réduire leur champ d'application;
- l) les règles relatives aux conséquences pour les produits TIC, services TIC et processus TIC qui ont été certifiés ou pour lesquels une déclaration de conformité de l'Union européenne a été délivrée, mais qui ne respectent pas les exigences du schéma;
- m) les règles relatives aux modalités de signalement et de traitement des vulnérabilités de cybersécurité non détectées précédemment dans des produits TIC, services TIC et processus TIC;
- n) le cas échéant, les règles relatives à la conservation des archives par les organismes d'évaluation de la conformité;
- o) l'identification des schémas nationaux ou internationaux de certification de cybersécurité couvrant le même type ou les mêmes catégories de produits TIC, services TIC et processus TIC, d'exigences de sécurité, de critères et méthodes d'évaluation et de niveaux d'assurance;
- p) le contenu et le format des certificats de cybersécurité européens et des déclarations de conformité de l'Union européenne à délivrer;
- q) la période de disponibilité de la déclaration de conformité de l'Union européenne, de la documentation technique et de toutes les autres informations pertinentes qui doivent être mises à disposition par le fabricant ou le fournisseur de produits TIC, services TIC ou processus TIC;
- r) la durée maximale de validité des certificats de cybersécurité européens délivrés dans le cadre du schéma;
- s) la politique de divulgation concernant les certificats de cybersécurité européens délivrés, modifiés ou retirés dans le cadre du schéma;
- t) les conditions de reconnaissance mutuelle des schémas de certification avec les pays tiers;
- u) le cas échéant, les règles relatives à tout mécanisme d'évaluation par les pairs établi par le schéma pour les autorités ou organismes qui délivrent des certificats de cybersécurité européens pour le niveau d'assurance dit «élevé» en vertu de l'article 56, paragraphe 6. Un tel mécanisme est sans préjudice de l'examen par les pairs prévu à l'article 59;
- v) le format et les procédures que les fabricants ou les fournisseurs de produits TIC, services TIC ou processus TIC doivent appliquer pour fournir et mettre à jour les informations supplémentaires en matière de cybersécurité conformément à l'article 55.

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

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

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

#### Article 55

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

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

- a) des orientations et des recommandations pour aider les utilisateurs finaux à assurer, de façon sécurisée, la configuration, l'installation, le déploiement, le fonctionnement et la maintenance des produits TIC ou services TIC;
- b) la période pendant laquelle une assistance en matière de sécurité sera offerte aux utilisateurs finaux, en particulier en ce qui concerne la disponibilité de mises à jour liées à la cybersécurité;
- c) les informations de contact du fabricant ou du fournisseur et les méthodes acceptées pour recevoir des informations concernant des vulnérabilités de la part d'utilisateurs finaux et de chercheurs dans le domaine de la sécurité;
- d) une mention relative aux répertoires en ligne recensant les vulnérabilités publiquement divulguées liées au produit TIC, service TIC ou processus TIC ainsi que tout conseil pertinent en matière de cybersécurité.

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

#### Article 56

#### **Certification de cybersécurité**

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

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

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

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

Lorsqu'elle prépare l'évaluation, la Commission:

- a) tient compte de l'incidence des mesures, du point de vue des coûts, sur les fabricants ou fournisseurs de ces produits TIC, services TIC ou processus TIC et sur les utilisateurs, ainsi que des avantages sociétaux ou économiques résultant du renforcement escompté du niveau de sécurité des produits TIC, services TIC ou processus TIC ciblés;
- b) tient compte de l'existence et de la mise en œuvre du droit des États membres et des pays tiers concernés;
- c) engage un processus de consultation ouvert, transparent et inclusif avec toutes les parties prenantes concernées et les États membres;
- d) prend en considération les délais de mise en œuvre ainsi que les mesures et périodes transitoires, en ce qui concerne, en particulier, l'incidence éventuelle de la mesure sur les fabricants ou les fournisseurs de produits TIC, services TIC ou processus TIC, y compris les PME;
- e) propose la façon la plus rapide et la plus efficace de mettre en œuvre la transition des schémas de certification volontaires vers les schémas de certification obligatoires.

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

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

- a) une autorité nationale de certification de cybersécurité visée à l'article 58, paragraphe 1; ou
- b) un organisme public accrédité en tant qu'organisme d'évaluation de la conformité conformément à l'article 60, paragraphe 1.

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

- a) moyennant l'approbation préalable de l'autorité nationale de certification de cybersécurité pour chaque certificat de cybersécurité européen délivré par un organisme d'évaluation de la conformité; ou
- b) sur la base d'une délégation préalable de la tâche consistant à délivrer de tels certificats de cybersécurité européens à un organisme d'évaluation de la conformité par l'autorité nationale de certification de cybersécurité.

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

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

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

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

#### Article 57

##### **Schémas nationaux de certification de cybersécurité et certificats**

1. Sans préjudice du paragraphe 3 du présent article, les schémas nationaux de certification de cybersécurité et les procédures connexes pour les produits TIC, services TIC et processus TIC couverts par un schéma européen de certification de cybersécurité cessent de produire leurs effets à partir de la date fixée dans l'acte d'exécution adopté en application de l'article 49, paragraphe 7. Les schémas nationaux de certification de cybersécurité et les procédures connexes pour les produits TIC, services TIC et processus TIC qui ne sont pas couverts par un schéma européen de certification de cybersécurité continuent à exister.
2. Les États membres s'abstiennent d'instaurer de nouveaux schémas nationaux de certification de cybersécurité pour les produits TIC, services TIC et processus TIC qui sont déjà couverts par un schéma européen de certification de cybersécurité en vigueur.
3. Les certificats existants, qui ont été délivrés dans le cadre de schémas nationaux de certification de cybersécurité et qui sont couverts par un schéma européen de certification de cybersécurité, restent valables jusqu'à leur date d'expiration.
4. En vue d'éviter la fragmentation du marché intérieur, les États membres informent la Commission et le GECC de leur intention éventuelle d'élaborer de nouveaux schémas nationaux de certification de cybersécurité.

#### Article 58

##### **Autorités nationales de certification de cybersécurité**

1. Chaque État membre désigne une ou plusieurs autorités nationales de certification de cybersécurité sur son territoire ou, moyennant l'accord d'un autre État membre, désigne une ou plusieurs autorités nationales de certification de cybersécurité établies dans cet autre État membre comme responsables des tâches de supervision dans l'État membre qui procède à la désignation.
2. Chaque État membre informe la Commission de l'identité des autorités nationales de certification de cybersécurité désignées. Lorsqu'un État membre désigne plus d'une autorité, il communique en outre à la Commission des informations sur les tâches confiées à chacune de ces autorités.
3. Sans préjudice de l'article 56, paragraphe 5, point a), et de l'article 56, paragraphe 6, chaque autorité nationale de certification de cybersécurité est indépendante des entités qu'elle surveille en ce qui concerne son organisation, ses décisions de financement, sa structure juridique et son processus décisionnel.
4. Les États membres veillent à ce que les activités des autorités nationales de certification de cybersécurité liées à la délivrance de certificats de cybersécurité européens visées à l'article 56, paragraphe 5, point a), et à l'article 56, paragraphe 6, soient strictement distinctes de leurs activités de supervision visées au présent article, et à ce que ces activités soient exécutées indépendamment l'une de l'autre.
5. Les États membres veillent à ce que les autorités nationales de certification de cybersécurité disposent de ressources adéquates pour exercer leurs pouvoirs et exécuter leurs tâches de manière efficace et efficiente.
6. Afin d'assurer la mise en œuvre efficace du présent règlement, il convient que les autorités nationales de certification de cybersécurité participent de manière active, efficace, efficiente et sécurisée au GECC.
7. Les autorités nationales de certification de cybersécurité:
  - a) supervisent et font respecter les règles prévues dans les schémas européens de certification de cybersécurité, en application de l'article 54, paragraphe 1, point j), aux fins du contrôle du respect par les produits TIC, services TIC et processus TIC des exigences des certificats de cybersécurité européens délivrés sur leurs territoires respectifs, en coopération avec les autres autorités compétentes de surveillance du marché;

- b) contrôlent le respect des obligations qui incombent aux fabricants ou fournisseurs de produits TIC, services TIC ou processus TIC qui sont établis sur leurs territoires respectifs et qui procèdent à une autoévaluation de conformité et font respecter ces obligations, et contrôlent, en particulier, le respect des obligations de ces fabricants ou fournisseurs visées à l'article 53, paragraphes 2 et 3, et dans le schéma européen de certification de cybersécurité correspondant, et font respecter ces obligations;
  - c) sans préjudice de l'article 60, paragraphe 3, assistent et soutiennent activement les organismes nationaux d'accréditation dans le contrôle et la supervision des activités des organismes d'évaluation de la conformité aux fins du présent règlement;
  - d) contrôlent et supervisent les activités des organismes publics visées à l'article 56, paragraphe 5;
  - e) lorsqu'il y a lieu, autorisent les organismes d'évaluation de la conformité à effectuer leurs tâches conformément à l'article 60, paragraphe 3, et limitent, suspendent ou retirent les autorisations existantes lorsque les organismes d'évaluation de la conformité violent les exigences du présent règlement;
  - f) traitent les réclamations introduites par des personnes physiques ou morales en rapport avec les certificats de cybersécurité européens délivrés par des autorités nationales de certification de cybersécurité ou en rapport avec les certificats de cybersécurité européens délivrés par des organismes d'évaluation de la conformité conformément à l'article 56, paragraphe 6, ou en rapport avec les déclarations de conformité de l'Union européenne délivrées au titre de l'article 53, examinent l'objet de ces réclamations dans la mesure nécessaire et informent l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable;
  - g) communiquent à l'ENISA et au GECC un résumé annuel des activités entreprises en application des points b), c) et d) du présent paragraphe ou du paragraphe 8;
  - h) coopèrent avec les autres autorités nationales de certification de cybersécurité ou d'autres autorités publiques, notamment en partageant des informations sur l'éventuel non-respect par des produits TIC, services TIC et processus TIC des exigences du présent règlement ou des exigences de schémas de certification de cybersécurité spécifiques; et
  - i) suivent les évolutions pertinentes dans le domaine de la certification de cybersécurité.
8. Chaque autorité nationale de certification de cybersécurité dispose au moins des pouvoirs suivants:
- a) de demander aux organismes d'évaluation de la conformité, aux titulaires de certificats de cybersécurité européens et aux émetteurs de déclarations de conformité de l'Union européenne de lui communiquer toute information dont elle a besoin pour l'exécution de ses tâches;
  - b) d'effectuer des enquêtes, sous la forme d'audits, auprès des organismes d'évaluation de la conformité, des titulaires de certificats de cybersécurité européens et des émetteurs de déclarations de conformité de l'Union européenne afin de vérifier qu'ils respectent le présent titre;
  - c) de prendre les mesures appropriées, conformément au droit national, pour veiller à ce que les organismes d'évaluation de la conformité, les titulaires de certificats de cybersécurité européens et les émetteurs de déclarations de conformité de l'Union européenne respectent le présent règlement ou un schéma européen de certification de cybersécurité;
  - d) d'obtenir l'accès aux locaux des organismes d'évaluation de la conformité ou des titulaires de certificats de cybersécurité européens afin d'effectuer des enquêtes conformément au droit procédural de l'Union ou au droit procédural d'un État membre;
  - e) de retirer, conformément au droit national, les certificats de cybersécurité européens délivrés par les autorités nationales de certification de cybersécurité ou les certificats de cybersécurité européens délivrés par les organismes d'évaluation de la conformité conformément à l'article 56, paragraphe 6, lorsque de tels certificats ne respectent pas le présent règlement ou un schéma européen de certification de cybersécurité;
  - f) d'imposer des sanctions conformément au droit national, comme le prévoit l'article 65, et d'exiger la cessation immédiate des violations des obligations énoncées dans le présent règlement.

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

#### *Article 59*

##### **Examen par les pairs**

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

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

3. L'examen par les pairs évalue:

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

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

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

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

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

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

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

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

#### *Article 60*

##### **Organismes d'évaluation de la conformité**

1. Les organismes d'évaluation de la conformité sont accrédités par les organismes nationaux d'accréditation désignés conformément au règlement (CE) n° 765/2008. Cette accréditation n'est délivrée que lorsque l'organisme d'évaluation de la conformité satisfait aux exigences énoncées à l'annexe du présent règlement.

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

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

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

#### Article 61

##### Notification

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

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

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

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

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

#### Article 62

##### Groupe européen de certification de cybersécurité

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

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

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

4. Le GECC a pour mission:

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

- b) d'assister et de conseiller l'ENISA et de coopérer avec elle en ce qui concerne la préparation d'un schéma candidat en vertu de l'article 49;
  - c) d'adopter un avis sur les schémas candidats préparés par l'ENISA en vertu de l'article 49;
  - d) de demander à l'ENISA de préparer un schéma candidat en vertu de l'article 48, paragraphe 2;
  - e) d'adopter des avis adressés à la Commission concernant la maintenance et le réexamen de schémas européens de certification de cybersécurité existants;
  - f) d'examiner les évolutions pertinentes dans le domaine de la certification de cybersécurité et d'échanger des informations et de bonnes pratiques sur les schémas de certification de cybersécurité;
  - g) de faciliter la coopération entre les autorités nationales de certification de cybersécurité en vertu du présent titre par le renforcement des capacités et l'échange d'informations, notamment en établissant des méthodes permettant un échange d'informations efficace sur toutes les questions relatives à la certification de cybersécurité;
  - h) de fournir un soutien à la mise en œuvre des mécanismes d'évaluation par les pairs conformément aux règles fixées dans un schéma européen de certification de cybersécurité en vertu de l'article 54, paragraphe 1, point u);
  - i) de faciliter l'alignement des schémas européens de certification de cybersécurité sur les normes internationalement reconnues, y compris en examinant les schémas européens de certification de cybersécurité existants et, s'il y a lieu, en recommandant à l'ENISA de nouer le dialogue avec les organisations internationales de normalisation compétentes dans le but de remédier à des insuffisances ou à des lacunes affectant les normes internationalement reconnues en vigueur.
5. Avec l'aide de l'ENISA, la Commission préside le GECC et en assure le secrétariat, conformément à l'article 8, paragraphe 1, point e).

#### *Article 63*

##### **Droit d'introduire une réclamation**

1. Les personnes physiques et morales ont le droit d'introduire une réclamation auprès de l'émetteur d'un certificat de cybersécurité européen ou, lorsque la réclamation est en rapport avec un certificat de cybersécurité européen délivré par un organisme d'évaluation de la conformité agissant conformément à l'article 56, paragraphe 6, auprès de l'autorité nationale de certification de cybersécurité concernée.
2. L'autorité ou l'organisme auprès duquel la réclamation a été introduite informe l'auteur de la réclamation de l'état d'avancement de la procédure et de la décision prise, et l'informe de son droit à un recours juridictionnel effectif visé à l'article 64.

#### *Article 64*

##### **Droit à un recours juridictionnel effectif**

1. Nonobstant tout recours administratif ou tout autre recours non juridictionnel, les personnes physiques ou morales disposent d'un droit de recours juridictionnel effectif en ce qui concerne:
  - a) les décisions prises par l'autorité ou l'organisme visé à l'article 63, paragraphe 1, y compris, le cas échéant, en ce qui concerne la délivrance non justifiée, la non-délivrance ou la reconnaissance d'un certificat de cybersécurité européen détenu par ces personnes physiques ou morales;
  - b) l'absence de réaction à une réclamation introduite auprès de l'autorité ou de l'organisme visé à l'article 63, paragraphe 1.
2. Les recours formés en vertu du présent article sont portés devant les juridictions de l'État membre dans lequel se trouve l'autorité ou l'organisme à l'encontre duquel le recours juridictionnel a été formé.

*Article 65***Sanctions**

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

## TITRE IV

**DISPOSITIONS FINALES***Article 66***Comité**

1. La Commission est assistée par un comité. Ledit comité est un comité au sens du règlement (UE) n° 182/2011.
2. Lorsqu'il est fait référence au présent paragraphe, l'article 5, paragraphe 4, point b), du règlement (UE) n° 182/2011 s'applique.

*Article 67***Évaluation et révision**

1. Au plus tard le 28 juin 2024, et tous les cinq ans par la suite, la Commission évalue l'incidence, l'efficacité et l'efficience de l'ENISA et de ses méthodes de travail, ainsi que la nécessité éventuelle de modifier le mandat de l'ENISA et les conséquences financières d'une telle modification. L'évaluation tient compte de toute information communiquée en retour à l'ENISA en réaction à ses activités. Lorsque la Commission estime que le maintien du fonctionnement de l'ENISA n'est plus justifié au regard des objectifs, du mandat et des tâches qui lui ont été assignées, elle peut proposer que les dispositions du présent règlement relatives à l'ENISA soient modifiées.
2. L'évaluation porte également sur les effets, l'efficacité et l'efficience des dispositions du titre III du présent règlement au regard des objectifs consistant à garantir un niveau adéquat de cybersécurité des produits TIC, services TIC et processus TIC dans l'Union et à améliorer le fonctionnement du marché intérieur.
3. L'évaluation examine s'il est nécessaire de fixer des exigences essentielles en matière de cybersécurité comme condition d'accès au marché intérieur pour empêcher que des produits TIC, services TIC et processus TIC qui ne satisfont pas aux exigences de base en matière de cybersécurité entrent sur le marché de l'Union.
4. Au plus tard le 28 juin 2024, et tous les cinq ans par la suite, la Commission transmet le rapport d'évaluation, accompagné de ses conclusions, au Parlement européen, au Conseil et au conseil d'administration. Les conclusions de ce rapport sont rendues publiques.

*Article 68***Abrogation et succession**

1. Le règlement (UE) n° 526/2013 est abrogé avec effet au 27 juin 2019.
2. Les références au règlement (UE) n° 526/2013 et à l'ENISA telle qu'instituée par le présent règlement s'entendent comme faites au présent règlement et à l'ENISA telle qu'instituée par le présent règlement.
3. L'ENISA instituée par le présent règlement succède à l'ENISA instituée par le règlement (UE) n° 526/2013 en ce qui concerne tous les droits de propriété, accords, obligations légales, contrats de travail, engagements financiers et responsabilités. Toutes les décisions du conseil d'administration et du conseil exécutif adoptées conformément au règlement (UE) n° 526/2013 restent valables, pour autant qu'elles respectent le présent règlement.

4. L'ENISA est instituée pour une durée indéterminée à compter du 27 juin 2019.
5. Le directeur exécutif nommé en vertu de l'article 24, paragraphe 4, du règlement (UE) n° 526/2013 reste en fonction et exerce les fonctions du directeur exécutif visées à l'article 20 du présent règlement pour la durée restante de son mandat. Les autres conditions de son contrat demeurent inchangées.
6. Les membres du conseil d'administration et leurs suppléants nommés en application de l'article 6 du règlement (UE) n° 526/2013 restent en fonction et exercent les fonctions du conseil d'administration visées à l'article 15 du présent règlement pour la durée restante de leur mandat.

*Article 69*

**Entrée en vigueur**

1. Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.
2. Les articles 58, 60, 61, 63, 64 et 65 s'appliquent à partir du 28 juin 2021.

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

Fait à Strasbourg, le 17 avril 2019.

*Par le Parlement européen*

*Le président*

A. TAJANI

*Par le Conseil*

*Le président*

G. CIAMBA

---

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

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

1. Un organisme d'évaluation de la conformité est constitué en vertu du droit national et possède la personnalité juridique.
2. Un organisme d'évaluation de la conformité est un organisme tiers qui est indépendant de l'organisation ou des produits TIC, services TIC ou processus TIC qu'il évalue.
3. Un organisme appartenant à une association d'entreprises ou à une fédération professionnelle qui représente des entreprises participant à la conception, à la fabrication, à la fourniture, à l'assemblage, à l'utilisation ou à l'entretien des produits TIC, services TIC ou processus TIC qu'il évalue peut être considéré comme un organisme d'évaluation de la conformité à condition que son indépendance et que l'absence de tout conflit d'intérêts soient démontrées.
4. Les organismes d'évaluation de la conformité, leurs cadres supérieurs et les personnes chargées d'exécuter les tâches d'évaluation de la conformité ne peuvent être ni le concepteur, le fabricant, le fournisseur, l'installateur, l'acheteur, le propriétaire, l'utilisateur ou le responsable de l'entretien du produit TIC, service TIC ou processus TIC qui est évalué, ni le mandataire d'aucune de ces parties. Cette interdiction n'exclut pas l'utilisation des produits TIC évalués qui sont nécessaires au fonctionnement de l'organisme d'évaluation de la conformité ou l'utilisation de ces produits TIC à des fins personnelles.
5. Les organismes d'évaluation de la conformité, leurs cadres supérieurs et les personnes chargées d'exécuter les tâches d'évaluation de la conformité ne peuvent intervenir, ni directement ni comme mandataires, dans la conception, la fabrication ou la construction, la commercialisation, l'installation, l'utilisation ou l'entretien des produits TIC, services TIC ou processus TIC. Les organismes d'évaluation de la conformité, leurs cadres supérieurs et les personnes chargées d'exécuter les tâches d'évaluation de la conformité ne peuvent participer à aucune activité qui peut entrer en conflit avec l'indépendance de leur jugement ou leur intégrité en ce qui concerne leurs activités d'évaluation de la conformité. Cette interdiction s'applique, en particulier pour les services de conseil.
6. Si un organisme d'évaluation de la conformité appartient à une entité ou à une institution publique, ou est géré par une telle entité ou institution, l'indépendance de l'autorité nationale de certification de cybersécurité et de l'organisme d'évaluation de la conformité et l'absence de conflit d'intérêts entre ces deux instances sont garanties et documentées.
7. Les organismes d'évaluation de la conformité veillent à ce que les activités de leurs filiales et sous-traitants n'aient pas d'incidence sur la confidentialité, l'objectivité ou l'impartialité de leurs activités d'évaluation de la conformité.
8. Les organismes d'évaluation de la conformité et leur personnel accomplissent les activités d'évaluation de la conformité avec la plus haute intégrité professionnelle et la compétence technique requise dans le domaine spécifique et sont à l'abri de toute pression ou incitation susceptible d'influencer leur jugement ou les résultats de leurs travaux d'évaluation de la conformité, notamment des pressions ou incitations d'ordre financier, en particulier de la part de personnes ou de groupes de personnes intéressés par ces résultats.
9. Un organisme d'évaluation de la conformité est capable d'exécuter toutes les tâches d'évaluation de la conformité qui lui ont été assignées au titre du présent règlement, que ces tâches soient exécutées par l'organisme d'évaluation de la conformité lui-même ou en son nom et sous sa responsabilité. Toute sous-traitance ou consultation de personnel externe est documentée de manière appropriée, ne fait intervenir aucun intermédiaire et fait l'objet d'un accord écrit couvrant, entre autres, la confidentialité et les conflits d'intérêts. L'organisme d'évaluation de la conformité en question assume la responsabilité des tâches accomplies.
10. En toutes circonstances et pour chaque procédure d'évaluation de la conformité, ainsi que pour chaque type ou catégorie ou sous-catégorie de produits TIC, services TIC ou processus TIC, un organisme d'évaluation de la conformité dispose à suffisance:
  - a) du personnel requis ayant les connaissances techniques et l'expérience suffisante et appropriée pour exécuter les tâches d'évaluation de la conformité;
  - b) de descriptions des procédures à suivre pour effectuer l'évaluation de la conformité, afin de garantir la transparence et la reproductibilité de ces procédures. Il se dote de politiques et de procédures appropriées faisant la distinction entre les tâches qu'il exécute en tant qu'organisme notifié en vertu de l'article 61 et ses autres activités;

- c) de procédures pour accomplir ses activités qui tiennent dûment compte de la taille des entreprises, du secteur dans lequel elles exercent leurs activités, de leur structure, du degré de complexité de la technologie du produit TIC, service TIC ou processus TIC en question et de la nature, en masse ou en série, du processus de production.
11. Un organisme d'évaluation de la conformité se dote des moyens nécessaires à la bonne exécution des tâches techniques et administratives liées aux activités d'évaluation de la conformité et a accès à tous les équipements et installations nécessaires.
  12. Les personnes chargées d'effectuer des activités d'évaluation de la conformité possèdent:
    - a) une solide formation technique et professionnelle couvrant toutes les activités d'évaluation de la conformité;
    - b) une connaissance satisfaisante des exigences applicables aux évaluations de conformité auxquelles elles procèdent et l'autorité nécessaire pour effectuer ces évaluations;
    - c) une connaissance et une compréhension adéquates des exigences et des normes d'essai applicables;
    - d) l'aptitude à rédiger les attestations, procès-verbaux et rapports qui prouvent que des évaluations de conformité ont été effectuées.
  13. L'impartialité des organismes d'évaluation de la conformité, de leurs cadres supérieurs, des personnes chargées de l'exécution des activités d'évaluation de la conformité et de tout sous-traitant est garantie.
  14. La rémunération des cadres supérieurs et des personnes chargées de l'exécution des activités d'évaluation de la conformité ne dépend pas du nombre d'évaluations de la conformité effectuées ni de leurs résultats.
  15. Les organismes d'évaluation de la conformité souscrivent une assurance couvrant leur responsabilité civile, à moins que cette responsabilité ne soit assumée par l'État membre conformément à son droit national ou que l'évaluation de la conformité ne soit effectuée sous la responsabilité directe de l'État membre.
  16. L'organisme d'évaluation de la conformité et son personnel, ses comités, ses filiales, ses sous-traitants et tout organisme associé ainsi que le personnel des organes externes d'un organisme d'évaluation de la conformité assurent le respect de la confidentialité et sont liés par le secret professionnel pour toutes les informations obtenues dans l'exercice de leurs tâches d'évaluation de la conformité au titre du présent règlement ou de toute disposition de droit national donnant effet au présent règlement, sauf dans les cas où la communication d'informations est requise par le droit de l'Union ou de l'État membre auquel ces personnes sont soumises, et sauf à l'égard des autorités compétentes de l'État membre où il exerce ses activités. Les droits de propriété intellectuelle sont protégés. L'organisme d'évaluation de la conformité possède des procédures documentées concernant les exigences du présent point.
  17. À l'exception du point 16, les exigences de la présente annexe n'empêchent en rien les échanges d'informations techniques et d'orientations réglementaires entre un organisme d'évaluation de la conformité et une personne qui introduit une demande de certification ou envisage de le faire.
  18. Les organismes d'évaluation de la conformité agissent conformément à un ensemble conditions cohérentes, justes et raisonnables, en tenant compte des intérêts des PME pour ce qui est des redevances.
  19. Les organismes d'évaluation de la conformité respectent les exigences de la norme pertinente qui est harmonisée au titre du règlement (CE) n° 765/2008 en ce qui concerne l'accréditation des organismes d'évaluation de la conformité qui effectuent la certification de produits TIC, services TIC ou processus TIC.
  20. Les organismes d'évaluation de la conformité veillent à ce que les laboratoires d'essai auxquels il est fait appel à des fins d'évaluation de la conformité respectent les exigences de la norme pertinente qui est harmonisée au titre du règlement (CE) n° 765/2008 en ce qui concerne l'accréditation de laboratoires qui réalisent des essais.
-

**PROJET DE REGLEMENT GRAND-DUCAL  
portant création d'un comité « national de  
certification de cybersécurité »**

I.	Exposé des motifs	91
II.	Texte du projet de règlement grand-ducal	91
III.	Commentaire des articles	92
IV.	Fiche financière	93
V.	Fiche d'impact	94

\*

**EXPOSE DES MOTIFS**

L'importance de la cybersécurité a motivé le législateur européen de doter l'Union européenne d'un cadre juridique pour la certification des produits, services et processus liés aux TIC dans le but de garantir un niveau adéquat et harmonisé de cybersécurité dans le marché unique digital.

Le législateur luxembourgeois s'empresse par 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 (ci-après le projet de loi) de mettre la législation luxembourgeoise en conformité avec ledit règlement (UE) n° 2019/881.

Le projet de loi prévoit dans son article 3 un comité national de certification de cybersécurité « créé auprès du Ministre ayant l'Economie dans ses attributions et dont la composition et l'organisation sont déterminées par règlement grand-ducal ».

Le présent projet de règlement grand-ducal a dès lors pour objectif de déterminer la composition et l'organisation du comité national de certification de cybersécurité.

\*

**TEXTE DU PROJET DE REGLEMENT GRAND-DUCAL**

Nous HENRI, Grand-Duc de Luxembourg, Duc de Nassau,

Vu la 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 ;

Vu les avis ... ;

Notre Conseil d'État entendu ;

Sur le rapport de Notre Ministre de l'Économie et après délibération du Gouvernement en conseil ;

Arrêtons :

**Art. 1<sup>er</sup>.** (1) Il est institué un comité national de certification de cybersécurité, dénommé ci-après le « comité ».

(2) Le comité exerce ses missions dans le respect des compétences et obligations légales des ministères, administrations et établissements publics concernés.

**Art. 2.** (1) Le comité se compose des membres suivants :

a. un membre effectif et un membre suppléant désignés par le ministre ayant l'Economie dans ses attributions ;

- b. un membre effectif et un membre suppléant désignés par le ministre ayant le Haut-Commissariat à la Protection Nationale(HCPN) dans ses attributions;
- c. un membre effectif et un membre suppléant désignés par le ministre ayant l'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et des services (ILNAS) dans ses attributions.

Les membres peuvent se faire accompagner aux réunions du comité par un ou, le cas échéant, par plusieurs experts.

VII. Le comité peut inviter, en cas de besoin, des représentants d'autres ministères, administrations ou établissements publics ou des experts du secteur privé ou d'organismes européens ou internationaux, à participer à certains points de l'ordre du jour d'une réunion du comité.

**Art. 3.** (1) Le comité est présidé par un membre désigné par le ministre ayant l'Economie dans ses attributions.

(2) Le comité se réunit au moins tous les 6 mois ou, en cas de besoin, sur proposition de son président ou d'au moins deux membres.

(3) Le président convoque les réunions et la convocation mentionne l'ordre du jour. Les membres du comité peuvent proposer au président des sujets à mettre à l'ordre du jour.

(4) Le secrétariat du comité est assuré par un agent du ministère de l'Economie.

(5) Le comité peut mettre en place des groupes de travail sur des sujets spécifiques.

(6) Le comité peut solliciter des avis d'experts externes aux fins de l'accomplissement de ses missions.

**Art. 4.** (1) Hormis les exceptions prévues par le droit national ou le droit de l'Union européenne, les membres du comité, les personnes contribuant aux travaux du secrétariat ainsi que toute autre personne ayant participé aux réunions du comité ou à des groupes de travail créés par le comité et les personnes ayant exercé par le passé les fonctions précitées sont tenus de garder le secret des informations dont ils ont eu connaissance dans ou à l'occasion de l'exercice de leur fonction.

(2) Le comité peut se doter d'un règlement d'ordre intérieur qui est soumis pour approbation au Conseil de Gouvernement.

**Art. 5.** Notre Ministre ayant l'Économie dans ses attributions est chargé de l'exécution du présent règlement qui sera publié au Journal officiel du Grand-Duché de Luxembourg.

\*

## COMMENTAIRE DES ARTICLES

### *Ad article 1<sup>er</sup>*

Pour tenir compte de la situation particulière du Luxembourg, il est proposé de mettre en place un comité national 'Groupe européen de certification de cybersécurité' composé des autorités compétentes en matière de cybersécurité au Luxembourg et pouvant coordonner des mesures au sein de l'État, du secteur privé et des infrastructures critiques.

Le comité permet une bonne coordination des autorités représentées au comité dans leurs domaines de compétence respectifs. Il ne porte pas atteinte aux compétences propres de ces autorités, ni à leur indépendance.

### *Ad article 2*

L'article 2 régit la composition du comité.

Sont représentées au comité les autorités impliquées dans la réglementation et la surveillance en matière de cybersécurité et dont les mesures ont une influence importante sur l'écosystème luxembourgeois.

Le Ministère de l'Economie est responsable de la réglementation en la matière, l'ILNAS est désigné par le projet de loi et le HCPN règle l'organisation de la protection des infrastructures critiques qui comprend l'ensemble des activités visant à prévenir, à atténuer ou à neutraliser le risque d'une réduction ou d'une discontinuité de la disponibilité de fournitures ou de services indispensables à la sauvegarde des intérêts vitaux ou des besoins essentiels de tout ou partie du pays ou de la population.

Ces représentants peuvent inviter toute personne à participer à certains points de l'ordre du jour et à faire connaissance aux comité des connaissances spécifiques respectivement d'un point de vue autre que celui des membres de la composition du comité.

*Ad article 3*

L'article 3 régit le fonctionnement et le processus décisionnel du comité.

Comme l'article 3, paragraphe 1, de le projet de loi prévoit que le comité est créé auprès du Ministre ayant l'Economie dans ses attributions, le comité est présidé par un membre désigné par le ministre ayant l'Economie dans ses attributions et le secrétariat est logiquement aussi assuré par cette entité.

Le comité se réunit sur une base semestrielle ou en cas de besoin.

Le comité peut solliciter des avis d'experts sur une question en relation avec le domaine de la cybersécurité.

Le secrétariat du comité est assuré par un agent du Ministère de l'Economie. Le secrétariat est responsable de la préparation des réunions du comité. Le secrétariat du comité est appelé plus particulièrement à rédiger les projets d'avis ou de recommandation du comité et les procès-verbaux des réunions du comité. Il peut également rédiger des analyses en relation avec le champ de compétence du comité.

*Ad article 4*

Il paraît utile d'établir explicitement dans le présent règlement grand-ducal leur obligation au secret professionnel lorsqu'ils exercent une fonction au titre du présent règlement grand-ducal afin d'éviter toute insécurité juridique. Les autres personnes ayant participé aux réunions du comité sont également tenues au secret des délibérations.

\*

**FICHE FINANCIERE**

(art. 79 de la loi du 8 juin 1999 sur le Budget,  
la Comptabilité et la Trésorerie de l'Etat)

Le projet de règlement grand-ducal ne comporte pas de dispositions dont l'application est susceptible de grever le budget de l'Etat.

\*

## FICHE D'EVALUATION D'IMPACT

<b>Intitulé du projet:</b>	<b>Projet de règlement grand-ducal du XX portant sur la création d'un comité national de certification de cybersécurité (ci-après le « comité »)</b>
<b>Ministère initiateur:</b>	<b>Ministère de l'Économie</b>
<b>Auteur:</b>	<b>Annick Hartung</b>
<b>Tél .:</b>	<b>+352 247-84320</b>
<b>Courriel:</b>	<b>Annick.Hartung@eco.etat.lu</b>
<b>Objectif(s) du projet:</b>	<b>Mise en œuvre de l'article 2 de l'avant-projet de loi du xx 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)</b>
<b>Autre(s) Ministère(s)/Organisme(s)/Commune(s)impliqué(e)(s):</b>	<b>Ministère d'Etat, ILNAS</b>
<b>Date:</b>	<b>février</b>

## Mieux légiférer

- Partie(s) prenante(s) (organismes divers, citoyens, ...) consultée(s): Oui:  Non:   
Si oui, laquelle/lesquelles: ...ILNAS, Ministère de la Justice...  
Remarques/Observations: ...
- Destinataires du projet:
  - Entreprises/Professions libérales: Oui:  Non:
  - Citoyens: Oui:  Non:
  - Administrations: Oui:  Non:
- Le principe « Think small first » est-il respecté? Oui:  Non:  N.a.:   
(c.à.d. des exemptions ou dérogations sont-elles prévues suivant la taille de l'entreprise et/ou son secteur d'activité?)  
Remarques/Observations: ...
- Le projet est-il lisible et compréhensible pour le destinataire? Oui:  Non:   
Existe-t-il un texte coordonné ou un guide pratique, mis à jour et publié d'une façon régulière? Oui:  Non:   
Remarques/Observations: ...
- Le projet a-t-il saisi l'opportunité pour supprimer ou simplifier des régimes d'autorisation et de déclaration existants, ou pour améliorer la qualité des procédures? Oui:  Non:   
Remarques/Observations: ...
- Le projet contient-il une charge administrative pour le(s) destinataire(s)? (un coût imposé pour satisfaire à une obligation d'information émanant du projet?) Oui:  Non:   
Si oui, quel est le coût administratif approximatif total? (nombre de destinataires x coût administratif par destinataire) ...

7. a) Le projet prend-il recours à un échange de données inter-administratif (national ou international) plutôt que de demander l'information au destinataire? Oui:  Non:   
Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il?  
...
- b) Le projet en question contient-il des dispositions spécifiques concernant la protection des personnes à l'égard du traitement des données à caractère personnel? Oui:  Non:   
Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il?  
...
8. Le projet prévoit-il:
- une autorisation tacite en cas de non réponse de l'administration? Oui:  Non:  N.a.:
  - des délais de réponse à respecter par l'administration? Oui:  Non:  N.a.:
  - le principe que l'administration ne pourra demander des informations supplémentaires qu'une seule fois? Oui:  Non:  N.a.:
9. Y a-t-il une possibilité de regroupement de formalités et/ou de procédures (p. ex. prévues le cas échéant par un autre texte)? Oui:  Non:   
Si oui, laquelle: ...
10. En cas de transposition de directives communautaires, le principe « la directive, rien que la directive » est-il respecté? Oui:  Non:  N.a.:   
Si non, pourquoi? ...
11. Le projet contribue-t-il en général à une:
- a) simplification administrative, et/ou à une Oui:  Non:
  - b) amélioration de la qualité règlementaire? Oui:  Non:
- Remarques/Observations: ...
12. Des heures d'ouverture de guichet, favorables et adaptées aux besoins du/des destinataire(s), seront-elles introduites? Oui:  Non:  N.a.:
13. Y a-t-il une nécessité d'adapter un système informatique auprès de l'Etat (e-Government ou application back-office)? Oui:  Non:   
Si oui, quel est le délai pour disposer du nouveau système ?
14. Y a-t-il un besoin en formation du personnel de l'administration concernée? Oui:  Non:  N.a.:   
Si oui, lequel? ...  
Remarques/Observations: ...

#### **Fiche égalité des chances**

15. Le projet est-il:
- principalement centré sur l'égalité des femmes et des hommes? Oui:  Non:
  - positif en matière d'égalité des femmes et des hommes? Oui:  Non:   
Si oui, expliquez de quelle manière: ...
  - neutre en matière d'égalité des femmes et des hommes? Oui:  Non:   
Si oui, expliquez pourquoi: Tous les documents sont concernés indifféremment du genre...

– négatif en matière d'égalité des femmes et des hommes?

Oui:  Non:

Si oui, expliquez de quelle manière: ...

16. Y a-t-il un impact financier différent sur les femmes et les hommes ?

Oui:  Non:  N.a.:

Si oui, expliquez de quelle manière: ...

