N° 7314[3]

CHAMBRE DES DEPUTES

Session ordinaire 2017-2018

P R O J E T D E L O I

portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne et modifiant

1° la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'Information de l'Etat et

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

* * *

SOMMAIRE:

*

DEPECHE DU MINISTRE AUX RELATIONS AVEC LE PARLEMENT AU PRESIDENT DE LA CHAMBRE DES DEPUTES

(2.10.2018)

Monsieur le Président,

À la demande du Premier Ministre, Ministre d'État, j'ai l'honneur de vous saisir d'amendements gouvernementaux relatifs au projet de loi sous rubrique.

À cet effet, je joins en annexe le texte des amendements avec un commentaire ainsi que deux versions coordonnées du projet de loi tenant compte desdits amendements.

Veuillez agréer, Monsieur le Président, l'assurance de ma haute considération.

Le Ministre aux Relations avec le Parlement,
Fernand ETGEN

*

TEXTE ET COMMENTAIRE DES AMENDEMENTS GOUVERNEMENTAUX

PROJET DE LOI

portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne et modifiant

1° la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat et

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

Amendement 1 –

Pour caractériser les énumérations, il est fait recours à des numéros suivis d'un exposant.

Motivation de l'amendement

Cet amendement tient compte des observations d'ordre légistique émises par le Conseil d'Etat.

Amendement 2 –

Lorsqu'un article se réfère au premier paragraphe ou alinéa, les lettres «er» sont insérées en exposant derrière le numéro.

Motivation de l'amendement

Cet amendement tient compte des observations d'ordre légistique émises par le Conseil d'Etat.

Amendement 3 –

Lorsqu'il est renvoyé à un paragraphe dans le corps du dispositif d'un article, les parenthèses entourant le chiffre faisant référence au paragraphe dont il s'agit sont omises.

Motivation de l'amendement

Cet amendement tient compte des observations d'ordre légistique émises par le Conseil d'Etat.

Amendement 4 –

Lorsqu'il est renvoyé à un point dans le corps du dispositif d'un article, il est fait abstraction du point ou de la parenthèse après le chiffre faisant référence au point dont il s'agit.

Motivation de l'amendement

Cet amendement tient compte des observations d'ordre légistique émises par le Conseil d'Etat.

Amendement 5 –

La formule « et/ou » est remplacée par « ou ».

Motivation de l'amendement

Cet amendement tient compte des observations d'ordre légistique émises par le Conseil d'Etat.

Amendement 6 –

Le terme « Union » est remplacé par « Union européenne ».

Motivation de l'amendement

Cet amendement tient compte des observations d'ordre légistique émises par le Conseil d'Etat.

Amendement 7 –

Lorsqu'il est renvoyé à une lettre faisant partie d'une subdivision, le terme « lettre » est utilisé avant la lettre référée, et non le terme « point ».

Motivation de l'amendement

Cet amendement tient compte des observations d'ordre légistique émises par le Conseil d'Etat.

Amendement 8 –

Lorsqu'une forme abrégée est introduite pour désigner un ensemble de termes, la dénomination complète est citée à sa première occurrence, suivie des termes «, ci-après « XXX » ».

Motivation de l'amendement

Cet amendement tient compte des observations d'ordre légistique émises par le Conseil d'Etat.

Amendement 9 –

Suite à l'insertion et à la suppression d'articles, de paragraphes et de points, les articles, paragraphes et points sont renumérotés. En outre, les références à ces articles, paragraphes et points sont adaptées en conséquence.

Motivation de l'amendement

Cet amendement vise à assurer la cohérence du projet de loi.

Amendement 10 –

L'intitulé du projet de loi est modifié comme suit :

« Projet de loi portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne et modifiant

1° la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat et

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

Motivation de l'amendement concernant l'intitulé du projet de loi

L'intitulé est modifié afin de tenir compte des observations d'ordre légistique du Conseil d'Etat. En effet, à part des amendements d'ordre légistique énoncés ci-avant, les actes à modifier sont à énoncer chronologiquement. En outre, l'intitulé n'est pas suivi d'un point final.

Amendement 11 –

L'ordre des articles 1er et 2 est inversé.

Motivation de l'amendement concernant les articles 1er et 2 du projet de loi

Afin de donner suite à l'avis du Conseil d'Etat dans lequel il est remarqué qu'en règle générale les dispositions relatives au champ d'application précèdent les dispositions qui énoncent des définitions, l'ordre des articles 1er et 2 est inversé et la numérotation des articles change en conséquence.

Amendement 12 –

L'article 1er, point 3 est modifié comme suit :

« 3.° « Opérateur de services essentiels » : une entité publique ou privée ~~ayant un établissement sur le territoire luxembourgeois~~ dont le type figure en annexe et qui répond aux critères énoncés à l'article 7~~6~~, paragraphe 2~~1~~er ; »

Motivation de l'amendement concernant l'article 1er, point 3 du projet de loi (article 2, point 3 du texte amendé)

Comme suggéré par le Conseil d'Etat, l'amendement sous revue supprime la partie de phrase « ayant un établissement sur le territoire luxembourgeois ». En limitant le champ d'application de la loi en

projet, ce bout de phrase ne devrait figurer dans un article consacré à de simples définitions. Ainsi, cette partie de phrase est supprimée au niveau des définitions et est insérée pour des raisons de cohérence et à l'instar de l'approche retenue pour les fournisseurs de service numérique (nouvel article 10, paragraphe 1er) en tant que disposition introductive au chapitre 3 consacré aux opérateurs de services essentiels (nouvel article 7, paragraphe 1er).

Amendement 13 –

A l'article 1er, les points 10 et 11 sont complétés comme suit :

« 10.° « Norme » : une norme au sens de l'article 2, point 1), du règlement (UE) n° 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision n° 1673/2006/CE du Parlement européen et du Conseil ;

11.° « Spécification » : une spécification technique au sens de l'article 2), point 4, du règlement (UE) n° 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision n° 1673/2006/CE du Parlement européen et du Conseil ; »

Motivation de l'amendement concernant l'article 1er, points 10 et 11 du projet de loi (article 2, points 10 et 11 du texte amendé)

Répondant à une observation du Conseil d'Etat, l'amendement consiste à reproduire l'intitulé complet des règlements européens cités.

Amendement 14 –

Les points 19 et 20 de l'article 1er sont supprimés et insérés dans un autre article.

« ~~19° « Autorité compétente concernée » : la Commission de surveillance du secteur financier (ci-après « la CSSF ») est l'autorité compétente en matière de sécurité des réseaux et des systèmes d'information couvrant les secteurs des banques et des infrastructures de marchés financiers tels que définis aux points 3. et 4. de l'annexe, ainsi que les services numériques fournis par une entité tombant sous la surveillance de la CSSF. L'Institut luxembourgeois de régulation (ci-après « l'ILR ») est l'autorité compétente en matière de sécurité des réseaux et des systèmes d'information couvrant les autres secteurs visés en annexe, ainsi que les services numériques fournis par une entité pour laquelle la CSSF n'est pas l'autorité compétente ;~~

~~20. « Point de contact national unique » : l'ILR constitue le point de contact national unique en matière de sécurité des réseaux et des systèmes d'information ;~~ »

Motivation de l'amendement concernant l'article 1er, points 19 et 20 du projet de loi

En conformité avec l'avis du Conseil d'Etat, la désignation des autorités compétentes, qui constitue une disposition à caractère normatif, est omise de l'article relatif aux définitions afin d'être insérée sous un article distinct au sein du chapitre 2 ayant trait aux autorités compétentes concernées (nouveaux articles 3 et 4).

Amendement 15 –

Les points 21 et 22 de l'article 1er sont modifiés comme suit :

« ~~21~~ 19.° « CERT Gouvernemental » : Centre de traitement des urgences informatiques, tel que défini à l'arrêté grand-ducal du ~~xx.xx.xx~~9 mai 2018 déterminant l'organisation et les attributions du Centre de traitement des urgences informatiques, dénommé « CERT Gouvernemental » ;

~~22~~ 20.° « CIRCL » : Computer Incident Response Center Luxembourg, opéré par le groupement d'intérêt économique~~G.I.E~~ Security Made in Lëtzebuerg ; »

Motivation de l'amendement concernant l'article 1er, points 21 et 22 du projet de loi (article 2, points 19 et 20 du texte amendé)

Suite à la suppression des points 19 et 20 initiaux en vue de leur insertion dans un article nouveau, la numérotation des points 21 et 22 initiaux doit être adaptée.

Au point 19 (nouvelle numérotation), la date de l'arrêté grand-ducal cité est rajoutée étant donné que l'arrêté grand-ducal en question a été publié entre la date du dépôt du texte initial et celle de la publication de l'avis du Conseil d'Etat.

Au point 20 (nouvelle numérotation), l'abréviation « G.I.E. » est remplacée par « groupement d'intérêt économique ».

Amendement 16 –

Le point final derrière l'article 1er, point 25 (nouvel article 2, point 23) est remplacé par un point-virgule.

Motivation de l'amendement concernant l'article 1er, point 25 du projet de loi (article 2, point 23 du texte amendé)

Puisque l'article relatif aux définitions sera complété par une nouvelle définition (voir amendement n° 17), il s'agit de remplacer le point final par un point-virgule.

Amendement 17 –

La définition du « point de contact national unique » est insérée à l'article 2.

« 24° « Point de contact national unique » : autorité qui exerce une fonction de liaison pour assurer une coopération transfrontalière entre les autorités des Etats membres, ainsi qu'avec les autorités concernées des autres Etats membres, le groupe de coopération et le réseau des CSIRT. »

Motivation de l'amendement concernant l'article 2, point 24 du projet de loi (article 5 du texte initial)

Comme suggéré par le Conseil d'Etat, la définition du «point de contact national unique », initialement prévue dans la partie normative (article 5 du projet de loi initial) est insérée au niveau de l'article 2 réservé aux définitions.

Amendement 18 –

L'article 3 est supprimé.

« ~~**Art. 3.** Dans la limite de leurs compétences et missions, les autorités compétentes concernées ont le pouvoir de prendre des règlements dans le cadre de l'exécution de la présente loi.~~ »

Motivation de l'amendement concernant l'article 3 du projet de loi

En réponse à l'opposition formelle émise par le Conseil d'Etat, l'article 3 conférant un pouvoir réglementaire général aux autorités compétentes est supprimé. Dans son avis du 10 juillet 2018, le Conseil d'Etat rappelle ses observations formulées dans son avis du 26 juin 2018 relatif au projet de loi portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, ci-après « projet de loi CNPD », en soulignant l'interprétation stricte qui doit être faite de l'article 108*bis* de la Constitution. En effet, à l'instar du projet de loi CNPD, le projet de loi sous rubrique accordait, dans sa version initiale, un pouvoir réglementaire général aux autorités compétentes, limité par une référence générale aux compétences et missions que le projet de loi leur attribue.

Cependant, un tel renvoi général n'est pas de nature à répondre au prescrit constitutionnel de l'article 108*bis* de la Constitution, tel qu'interprété par la Cour constitutionnelle. L'approche initialement suivie par les auteurs du projet de loi revient à investir les autorités compétentes d'un pouvoir d'exécution similaire au pouvoir d'exécution dit « spontané » dont dispose le Grand-Duc au titre de l'article 36 de la Constitution. Or, le pouvoir réglementaire d'un établissement public ne saurait avoir la portée du pouvoir réglementaire du Grand-Duc, mais ne peut s'exercer qu'au titre d'une base légale précise qui en détermine les limites. Dès lors, le Conseil d'Etat demande, sous peine d'opposition

formelle, que le texte du projet de loi soit complété avec les précisions nécessaires afin de limiter le pouvoir réglementaire des autorités compétentes concernées.

Il est par conséquent proposé de se rallier à la solution retenue au niveau du projet de loi CNPD (devenue par la suite la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données) et de supprimer l'article relatif au pouvoir réglementaire d'ordre général des autorités compétentes, tout en l'insérant aux articles pour l'exécution desquels un tel pouvoir est accordé aux autorités. Ce pouvoir réglementaire ne sera accordé aux autorité compétentes concernées que dans quelques domaines spécifiques et précisément délimités par l'article 7, paragraphe 4 (article 6, paragraphe 3 du texte initial), l'article 8, paragraphes 1er, 3 et 5 (article 7, paragraphes 1er, 3 et 5 du texte initial) et l'article 11, paragraphe 3 (article 10, paragraphe 3 du texte initial).

Amendement 19 –

L'article 3 est remplacé par le texte suivant :

« **Art. 3.** La Commission de surveillance du secteur financier, ci-après « la CSSF », est l'autorité compétente en matière de sécurité des réseaux et des systèmes d'information couvrant les secteurs des établissements de crédit et des infrastructures de marchés financiers tels que définis aux points 3 et 4 de l'annexe, ainsi que les services numériques fournis par une entité tombant sous la surveillance de la CSSF.

L'Institut luxembourgeois de régulation, ci-après « l'ILR », est l'autorité compétente en matière de sécurité des réseaux et des systèmes d'information couvrant les autres secteurs visés en annexe, ainsi que les services numériques fournis par une entité pour laquelle la CSSF n'est pas l'autorité compétente.

L'obligation au secret professionnel posée par l'article 16 de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier ne fait pas obstacle à l'échange d'informations entre autorités compétentes. »

Motivation de l'amendement concernant l'article 3 du projet de loi (article 1er, point 19 du texte initial)

Faisant suite aux recommandations du Conseil d'Etat et dans la lignée de l'amendement n° 14, la désignation de la CSSF et de l'ILR en tant qu'autorités compétentes concernées est omise de l'article relatif aux définitions (ancien article 1er, point 19) pour être rajoutée dans la partie normative du texte sous un nouvel article 3 qui remplace l'article 3 supprimé du texte initial.

En outre, la notion de « banque » a été remplacée par celle de « établissement de crédit », afin de refléter la nomenclature exacte du droit national et européen. Afin d'assurer une cohérence à travers le texte, le terme « banque » a également été remplacé dans le point 3. de l'annexe.

Enfin, l'article 3, alinéa 3 donne une autorisation expresse aux autorités compétentes d'échanger des informations et ce même si ces informations sont considérées confidentielles en vertu de l'article 16 de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier. En effet, cette disposition permet à la loi de déroger au principe général du secret. Un tel échange d'informations entre autorités compétentes pourrait être de mise lorsqu'un même opérateur de services essentiels est susceptible de tomber dans le champ de compétence des deux autorités compétentes.

Amendement 20 –

Il est inséré un nouvel article 4 libellé comme suit :

« **Art. 4.** L'ILR constitue le point de contact national unique en matière de sécurité des réseaux et des systèmes d'information. »

Motivation de l'amendement concernant l'article 4 du projet de loi (article 1er, point 20 du texte initial)

Faisant suite aux recommandations du Conseil d'Etat et dans la lignée de l'amendement n° 14, le nouvel article 4 consiste à insérer dans la partie normative du projet de loi un texte qui figurait initialement dans l'article relatif aux définitions (ancien article 1er, point 20).

Amendement 21 –

Le texte figurant sous l'article 4 (nouvel article 5) est modifié comme suit :

« **Art. ~~45.~~** Dans l'exercice de sa mission, l'ILR bénéficie d'une contribution financière à charge du budget de l'Etat, ~~à titre de participation aux~~afin de couvrir l'intégralité de ses frais de fonctionnement. »

Motivation de l'amendement concernant l'article 4 (article 5 du texte amendé)

Le nouvel article 5 a été amendé afin de clarifier que l'intégralité des frais à charge de l'ILR et en relation avec la mise en place de la présente loi seront couverts par une contribution financière étatique.

Amendement 22 –

L'article 5 du projet de loi est supprimé.

« ~~**Art. 5.** Le point de contact unique exerce une fonction de liaison pour assurer une coopération transfrontalière entre les autorités des Etats membres, ainsi qu'avec les autorités concernées des autres Etats membres, le groupe de coopération et le réseau des CSIRT~~. »

Motivation de l'amendement concernant l'ancien article 5 du projet de loi

Comme expliqué supra à l'amendement n° 16, la définition du « point de contact national unique » figure dorénavant à l'article relatif aux définitions (nouvel article 2, point 24).

L'article 5 du projet de loi initial est supprimé et les articles suivants sont partant renumérotés.

Amendement 23 –

Il est inséré un nouvel article 6 libellé comme suit :

« **Art. 6.** Dans la mesure nécessaire à l'accomplissement de leur mission en vertu de la présente loi, les autorités compétentes et le point de contact national unique consultent les services répressifs nationaux compétents et les autorités nationales chargées de la protection des données et coopèrent avec eux.

L'obligation au secret professionnel posée par l'article 16 de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier ne fait pas obstacle à cette coopération. »

Motivation de l'amendement concernant le nouvel article 6 du projet de loi

L'ajout de l'article 6 vise à répondre à une opposition formelle du Conseil d'Etat pour transposition incorrecte car incomplète de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, ci-après « direction NIS ». En effet, le Conseil d'Etat demande la transposition de l'article 8, paragraphe 6 de ladite directive relatif au pouvoir des autorités compétentes et du point de contact national unique de consulter les services répressifs nationaux et les autorités nationales chargées de la protection des données.

Afin de rendre cette coopération efficace, le secret auquel les agents de la CSSF sont tenus en vertu de l'article 16 de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier ne s'applique pas au cas d'espèce.

Amendement 24 –

Le texte figurant sous l'article 6 (nouvel article 7) est modifié comme suit :

« **Art. 6~~7~~.** (1) Tombent sous le champ d'application de la présente loi, les opérateurs de services essentiels ayant un établissement sur le territoire luxembourgeois.

(~~1~~2) L'identification des opérateurs de services essentiels par l'autorité compétente concernée se fait au moyen des critères d'identification suivants :

1~~.~~° une entité fournit un service qui est essentiel au maintien d'activités sociétales ~~et~~/ou économiques critiques ;

2~~.~~° la fourniture de ce service est tributaire des réseaux et des systèmes d'information ; et

3~~.~~° un incident ~~aurait~~ un effet disruptif important sur la fourniture dudit service.

L'autorité compétente concernée notifie la décision d'identification à l'opérateur de services essentiels.

« (~~2~~3) L'importance de l'effet disruptif visé au paragraphe 2~~1~~er, point 3~~.~~, est déterminée sur base de facteurs transsectoriels et sectoriels, dont ~~notamment~~ au moins :

1~~.~~° le nombre d'utilisateurs tributaires du service fourni par l'entité concernée ;

2~~.~~° la dépendance des autres secteurs visés en annexe à l'égard du service fourni par cette entité ;

3~~.~~° les conséquences que des incidents pourraient avoir, en termes de degré et de durée, sur les fonctions économiques ou sociétales ou sur la sûreté publique ;

4~~.~~° la part de marché de cette entité ;

5~~.~~° la portée géographique eu égard à la zone susceptible d'être touchée par un incident ;

6~~.~~° l'importance que revêt l'entité pour garantir un niveau de service suffisant, compte tenu de la disponibilité de solutions de rechange pour la fourniture de ce service.

(~~3~~4) La liste des services essentiels est fixée par l'autorité compétente concernée par voie de règlement.

(~~4~~5) Lorsqu'une entité fournit un service visé au paragraphe 2~~1~~er, point 1~~.~~, dans un autre Etat membre, l'autorité compétente concernée ~~se~~ consulte ~~avec~~ l'autorité compétente de l'autre Etat membre. La consultation intervient avant que l'identification ne fasse l'objet d'une décision. »

Motivation de l'amendement concernant l'article 6 (article 7 du texte amendé)

Dans son avis, le Conseil d'Etat recommande d'insérer la précision que seuls les opérateurs de services essentiels ayant un établissement sur le territoire luxembourgeois tombent dans le champ d'application de la présente loi dans la partie des dispositions législatives normatives.[1] Ainsi, ce nouveau paragraphe est inséré à l'article 6 (nouvel article 7).

Bien que le Conseil d'Etat ait suggéré d'insérer la nouvelle disposition à l'article 1er du texte, celle-ci figure en tant que disposition introductive au chapitre 3 relatif aux opérateurs de services essentiels. En ce faisant, les auteurs ont voulu créer un parallélisme avec le chapitre 4 relatif aux fournisseurs de service numérique qui débute avec des précisions quant à son champ d'application.

Ensuite, au paragraphe 2 (ancien paragraphe 1er), les amendements tiennent compte des observations d'ordre légistique émises par le Conseil d'Etat :

– les énumérations sont dorénavant caractérisées par des numéros suivis d'un exposant ;
– la formule « et/ou » est remplacée par « ou » et
– le recours au conditionnel est évité au point 3 en remplaçant « aurait » par « a ».

Au paragraphe 3 (ancien paragraphe 2), à part des modifications d'ordre légistique et de renumérotation, la formule « notamment » est remplacée par les termes « au moins », afin de refléter fidèlement la formulation utilisée dans la directive NIS.

Le nouveau paragraphe 4 est à lire en ligne avec l'amendement n° 17 qui propose de supprimer la disposition conférant un pouvoir réglementaire général aux autorités compétentes concernées et de compléter le projet de loi avec un nombre limité de cas dans lesquels les autorités compétentes disposent du pouvoir réglementaire. Ainsi, le paragraphe 4 précise que la liste des services essentiels est fixée par l'autorité compétente concernée par voie de règlement.

Les modifications apportées au paragraphe 5 (ancien paragraphe 4), donnent suite à l'observation d'ordre légistique du Conseil d'Etat, en remplaçant les termes « l'autorité compétente concernée se consulte avec l'autorité compétente de l'autre Etat membre » par « l'autorité compétente concernée consulte l'autorité compétente de l'autre Etat membre ».

Amendement 25 –

Le texte figurant sous l'article 7 (nouvel article 8) est modifié comme suit :

« **Art. ~~7~~8.** (1) Les opérateurs de services essentiels prennent les mesures techniques et organisationnelles nécessaires et proportionnées pour gérer les risques qui menacent la sécurité des réseaux

---

1 Voir aussi l'amendement n° 12.

et des systèmes d'information qu'ils utilisent dans le cadre de leurs activités. Ces mesures garantissent, pour les réseaux et les systèmes d'information, un niveau de sécurité adapté au risque existant, compte tenu de l'état des connaissances. Afin d'identifier les risques, les opérateurs de services essentiels utilisent un cadre d'analyse de risques approprié pouvant être précisé par l'autorité compétente concernée par voie de règlement.

(2) Les opérateurs de services essentiels prennent des mesures appropriées en vue de prévenir les incidents qui compromettent la sécurité des réseaux et des systèmes d'information utilisés pour la fourniture de ces services essentiels ou d'en limiter l'impact, en vue d'assurer la continuité de ces services.

(3) Les mesures prises sur base des paragraphes 1er et 2 sont notifiées à l'autorité compétente concernée. Les modalités de cette notification, ~~et notamment~~ le format et le délai, sont déterminées par l'autorité compétente concernée par voie de règlement.

(4) Les opérateurs de services essentiels notifient à l'autorité compétente concernée, sans retard injustifié, les incidents qui ont un impact significatif sur la continuité des services essentiels qu'ils fournissent. Ces notifications sont transmises au CERT Gouvernemental et au CIRCL en fonction de leurs compétences respectives. Les notifications contiennent des informations permettant à l'autorité compétente concernée de déterminer si l'incident a un impact au niveau transfrontalier. Cette notification n'accroît pas la responsabilité de la partie qui en est à l'origine.

(5) L'ampleur de l'impact d'un incident est déterminée en tenant compte, en particulier, des paramètres suivants :

1° le nombre d'utilisateurs touchés par la perturbation du service essentiel ;

2° la durée de l'incident ;

3° la portée géographique eu égard à la zone touchée par l'incident.

L'autorité compétente concernée peut préciser, par voie de règlement, les paramètres, les modalités et délais des notifications des incidents qui ont un impact significatif sur la continuité des services essentiels qu'ils fournissent.

(6) Sur la base des informations fournies dans la notification de l'opérateur de services essentiels, l'autorité compétente concernée signale aux autres Etats membres touchés si l'incident est susceptible d'avoir un impact significatif sur la continuité des services essentiels dans ces Etats membres. Sur demande de l'autorité compétente concernée, ce signalement est effectué par le point de contact national unique qui transmettra la notification aux points de contact nationaux des autres Etats membres touchés. Ce faisant, l'autorité compétente concernée doit~~, dans le respect du droit de l'Union ou de la législation nationale conforme au droit de l'Union,~~ préserver la sécurité et les intérêts commerciaux de l'opérateur de services essentiels ainsi que la confidentialité des informations communiquées dans sa notification.

Lorsque les circonstances le permettent, l'autorité compétente concernée fournit à l'opérateur de services essentiels qui est à l'origine de la notification des informations utiles au suivi de sa notification.

~~À la demande de l'autorité compétente concernée, le point de contact national transmet les notifications visées au premier alinéa aux points de contact nationaux des autres Etats membres touchés.~~

(7) Une fois par an, l'autorité compétente concernée transmet au point de contact national unique un rapport de synthèse sur les notifications reçues, y compris le nombre de notifications et la nature des incidents notifiés, ainsi que sur les mesures prises conformément aux paragraphes ~~(4)~~ et ~~(6)~~.

Tous les ans, le point de contact national unique transmet au groupe de coopération un rapport de synthèse sur les notifications reçues, y compris le nombre de notifications et la nature des incidents notifiés, ainsi que sur les mesures prises conformément aux paragraphes ~~(4)~~ et ~~(6)~~.

(8) Après avoir consulté l'opérateur de services essentiels qui est à l'origine de la notification, l'autorité compétente concernée peut informer le public d'incidents particuliers ou imposer à l'opérateur de services essentiels de le faire, lorsque la sensibilisation du public est nécessaire pour

prévenir un incident ou gérer un incident en cours, ou lorsque la divulgation de l'incident est dans l'intérêt public à d'autres égards. »

Motivation de l'amendement concernant l'article 7 du projet de loi (article 8 du texte amendé)

Dans son avis du 10 juillet 2018, le Conseil d'Etat relève que le paragraphe 1er de l'article 7 (nouvel article 8) manque de clarté en ce qu'il ne ressort pas du texte si l'autorité compétente concernée pourra déterminer un cadre d'analyse par voie règlementaire ou si l'autorité compétente devra adopter des décisions individuelles dans ce contexte. Le Conseil d'Etat s'oppose formellement au texte, vu l'insécurité juridique qui en découle. Il recommande de soit exprimer le pouvoir réglementaire clairement dans le libellé de la disposition sous revue afin de garantir le respect de l'article 108*bis* de la Constitution, soit d'insérer cette précision à l'endroit de l'article 3 du texte initial.

En réponse à cette opposition formelle et au vu des explications fournies sous l'amendement n° 17 relatif à la suppression de l'article 3 du texte initial, les auteurs des amendements ont décidé de supprimer le pouvoir réglementaire général des autorités compétentes consacré à l'article 3 et de préciser le pouvoir réglementaire des autorités compétentes concernées dans différents articles. Ainsi, ce pouvoir réglementaire est ajouté à l'article 8, paragraphes 1er, 3 et 5, alinéa 2.

Au paragraphe 3 de l'article 8, le terme « notamment » est écarté comme étant superfétatoire.

Au paragraphe 5, les termes « en particulier » sont rajoutés afin de répondre à une opposition formelle du Conseil d'Etat. En effet, la phrase introductive du paragraphe 5 a, par dérogation à l'article 14, paragraphe 4, de la directive NIS, omis les termes « en particulier », transformant ainsi la liste indicative de paramètres utilisés pour mesurer l'ampleur de l'impact d'un incident en une liste limitative.

Au paragraphe 6, alinéa 3 a été intégré dans l'alinéa 1er, afin de rendre la disposition plus lisible.

Le terme « national » est ajouté à deux reprises au paragraphe 7, afin de refléter les termes exacts utilisés dans les définitions (« point de contact national unique »).

En outre, les termes « dans le respect du droit de l'Union ou de la législation nationale conforme au droit de l'Union » sont supprimés, parce qu'ils sont superfétatoires. En effet, l'autorité compétente et la législation nationale doivent en tout état de cause se conformer au droit de l'Union européenne.

Amendement 26 –

L'article 8 (nouvel article 9) est modifié comme suit :

«**Art. 89.** (1) A la demande de l'autorité compétente concernée, les opérateurs de services essentiels lui fournissent :

1° les informations nécessaires pour évaluer la sécurité de leurs réseaux et systèmes d'information, y compris les documents relatifs à leurs politiques de sécurité ;

2° des éléments prouvant la mise en oeuvre effective des politiques de sécurité, tels que les résultats d'un audit de sécurité exécuté par l'autorité compétente concernée ou un auditeur qualifié et, dans ce dernier cas, qu'ils en mettent les résultats, y compris les éléments probants, à la disposition de l'autorité compétente concernée. L'autorité compétente concernée peut charger un auditeur externe de contrôler la mise en oeuvre effective de la politique de sécurité à charge de l'opérateur de services essentiels ;

3° toute information nécessaire à l'accomplissement de ses missions en vertu de la présente loi.

Les opérateurs de services essentiels fournissent ces informations en respectant les délais et le niveau de détail exigés par l'autorité compétente concernée.

Au moment de formuler une telle demande d'informations et de preuves, l'autorité compétente concernée mentionne la finalité de la demande et précise quelles sont les informations exigées.

(2) Après évaluation des informations ou des résultats des audits de sécurité visés au paragraphe 1er, l'autorité compétente concernée peut donner des instructions contraignantes aux opérateurs de services essentiels pour remédier aux défaillances identifiées.

(3) Pour traiter des incidents notifiés donnant lieu à des violations des données à caractère personnel, l'autorité compétente concernée coopère étroitement avec la Commission nationale pour la protection des données et lui transmet les informations en relation avec ~~cette~~ ces violations. »

Motivation de l'amendement concernant l'article 8 du projet de loi (article 9 du texte amendé)

Les modifications apportées à l'article 8 (nouvel article 9) répondent à des observations d'ordre légistique du Conseil d'Etat. Outre l'adaptation de l'énumération au paragraphe 1er, alinéa 1er, les termes « cette violation » sont mis au pluriel au paragraphe 3.

Amendement 27 –

Le texte de l'article 9 (nouvel article 10) est modifié comme suit :

« **Art. 910.** (1) Tombent ~~sous~~ dans le champ d'application de la présente loi, les fournisseurs de service numérique ayant leur établissement principal au Grand-Duché de Luxembourg. Un fournisseur de service numérique est réputé avoir son établissement principal au Grand-Duché de Luxembourg lorsque son siège social se trouve au Grand-Duché de Luxembourg. Le fournisseur de service numérique qui n'est pas établi dans l'Union européenne mais qui fournit un service numérique sur le territoire du Grand-Duché de Luxembourg et qui désigne un représentant au Grand-Duché de Luxembourg, relève de la compétence des autorités luxembourgeoises.

Le représentant peut être contacté par l'autorité compétente concernée à la place du fournisseur de service numérique concernant les obligations incombant audit fournisseur de service numérique en vertu de la présente loi.

La désignation d'un représentant par le fournisseur de service numérique est sans préjudice d'actions en justice qui pourraient être intentées contre le fournisseur de service numérique lui-même.

(2) Le chapitre 4 ne s'applique pas aux microentreprises et petites entreprises telles que définies dans ~~le règlement grand ducal du 16 mars 2005 portant adaptation de la définition des micro, petites et moyennes entreprises~~la recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises. »

Motivation de l'amendement concernant l'article 9 du projet de loi (article 10 du texte amendé)

Au paragraphe 1er de l'article 10, les termes « tombent sous le champ d'application » sont remplacés par « tombent dans le champ d'application ».

De plus, le paragraphe 2 ne fait plus référence au règlement grand-ducal du 16 mars 2005 portant adaptation de la définition des micro, petites et moyennes entreprises. En effet, contrairement aux références à des actes hiérarchiquement supérieurs ou de même nature, le renvoi à un acte situé à un niveau inférieur dans la hiérarchie des normes n'est pas admis. Ainsi, il est fait référence à la recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises.

Amendement 28 –

Le texte de l'article 10 (nouvel article 11) est modifié comme suit :

« **Art. ~~10~~11.** (1) Les fournisseurs de service numérique identifient les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'ils utilisent pour offrir, dans l'Union européenne, un service numérique et prennent les mesures techniques et organisationnelles nécessaires et proportionnées pour les gérer. Ces mesures garantissent, compte tenu de l'état des connaissances, un niveau de sécurité des réseaux et des systèmes d'information adapté au risque existant et prennent en considération les éléments suivants :

1~~.~~° la sécurité des systèmes et des installations ;

2~~.~~° la gestion des incidents ;

3~~.~~° la gestion de la continuité des activités ;

4~~.~~° le suivi, l'audit et le contrôle ;

5~~.~~° le respect des normes internationales.

La gestion des risques qui menacent la sécurité des réseaux et des systèmes d'information des fournisseurs de service numérique se fait conformément au règlement d'exécution (UE) 2018/151 de la Commission du 30 janvier 2018 portant modalités d'application de la directive (UE) 2016/1148 du Parlement européen et du Conseil précisant les éléments à prendre en considération par les fournisseurs de service numérique pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information ainsi que les paramètres permettant de déterminer si un incident a un impact significatif.

(2) Les fournisseurs de service numérique prennent des mesures pour éviter les incidents portant atteinte à la sécurité de leurs réseaux et systèmes d'information, et réduire au minimum l'impact de ces incidents sur les services numériques qui sont offerts dans l'Union européenne, de manière à garantir la continuité de ces services.

(3) Les fournisseurs de service numérique notifient à l'autorité compétente concernée, sans retard injustifié, tout incident ayant un impact significatif sur la fourniture d'un service numérique qu'ils offrent dans l'Union européenne. Les modalités de cette notification, le format et le délai, sont déterminés par l'autorité compétente concernée par voie de règlement. Ces notifications sont transmises au CERT Gouvernemental et au CIRCL en fonction de leurs compétences respectives. Les notifications contiennent des informations permettant à l'autorité compétente concernée d'évaluer l'ampleur de l'éventuel impact au niveau transfrontalier. Cette notification n'accroît pas la responsabilité de la partie qui en est à l'origine.

(4) L'importance de l'impact d'un incident est déterminée en tenant compte, en particulier, des paramètres suivants :

1° le nombre d'utilisateurs touchés par l'incident, en particulier ceux qui recourent au service pour la fourniture de leurs propres services ;

2° la durée de l'incident ;

3° la portée géographique eu égard à la zone touchée par l'incident ;

4° la gravité de la perturbation du fonctionnement du service ;

5° l'ampleur de l'impact sur les fonctions économiques et sociétales.

L'obligation de notifier un incident ne s'applique que lorsque le fournisseur de service numérique a accès aux informations nécessaires pour évaluer l'impact de l'incident eu égard aux paramètres visés au premier alinéa.

Les paramètres permettant de déterminer si un incident a un impact significatif sont précisés par le règlement d'exécution (UE) 2018/151 de la Commission du 30 janvier 2018 portant modalités d'application de la directive (UE) 2016/1148 du Parlement européen et du Conseil précisant les éléments à prendre en considération par les fournisseurs de service numérique pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information ainsi que les paramètres permettant de déterminer si un incident a un impact significatif.

(5) Lorsqu'un opérateur de services essentiels s'appuie sur un tiers fournisseur de service numérique pour la prestation d'un service essentiel au maintien de fonctions sociétales et économiques critiques, tout impact significatif sur la continuité des services essentiels en raison d'un incident touchant le fournisseur de service numérique est notifié par ledit opérateur.

(6) Lorsque l'incident visé au paragraphe 3 concerne deux Etats membres ou plus, l'autorité compétente concernée peut informer les autres Etats membres touchés. Ce faisant, l'autorité compétente concernée doit~~, dans le respect du droit de l'Union ou de la législation nationale conforme au droit de l'Union,~~ préserver la sécurité et les intérêts commerciaux du fournisseur de service numérique ainsi que la confidentialité des informations communiquées.

(7) Une fois par an, l'autorité compétente concernée transmet au point de contact national unique un rapport de synthèse sur les notifications reçues, y compris le nombre de notifications et la nature des incidents notifiés, ainsi que sur les mesures prises conformément aux paragraphes ~~(~~3~~)~~ et ~~(~~6~~)~~.

Tous les ans, le point de contact national unique transmet au groupe de coopération un rapport de synthèse sur les notifications reçues, y compris le nombre de notifications et la nature des incidents notifiés, ainsi que sur les mesures prises conformément aux paragraphes ~~(~~3~~)~~ et ~~(~~6~~)~~.

(8) Après avoir consulté le fournisseur de service numérique concerné, l'autorité compétente concernée, et les autorités ou les CSIRT des autres Etats membres concernés peuvent informer le public d'incidents particuliers ou imposer au fournisseur de service numérique de le faire, dans le cas où la sensibilisation du public est nécessaire pour prévenir un incident ou pour gérer un incident en cours, ou lorsque la divulgation de l'incident est dans l'intérêt public à d'autres égards. »

Motivation de l'amendement concernant l'article 10 du projet de loi (article 11 du texte amendé)

A part des modifications d'ordre légistique effectuées à travers l'article, le paragraphe 3 du nouvel article 11 précise que les modalités, le format et le délai des notifications à faire par les fournisseurs de service numérique seront précisés à l'aide d'un règlement de l'autorité compétente concernée. Comme expliqué *supra* sous l'amendement n° 17, cet ajout vise à préciser le pouvoir réglementaire des autorités compétentes.

Le rajout des termes « en particulier » au paragraphe 4 de l'article 10 (nouvel article 11) vise à répondre à une opposition formelle formulée par le Conseil d'Etat. Comme soulevé à l'occasion de l'article 7, paragraphe 5 (nouvel article 8, paragraphe 5), la Haute Corporation fait remarquer dans son avis du 10 juillet 2018 que les termes « en particulier » devraient être rajoutés dans le texte sous rubrique, afin de refléter l'esprit de la directive qui prévoit une liste exemplative de critères servant à mesurer l'importance de l'impact d'un incident.

Au paragraphe 6, les termes « dans le respect du droit de l'Union ou de la législation nationale conforme au droit de l'Union » sont supprimés à la demande du Conseil d'Etat, parce qu'ils sont superfétatoires.

Le terme « national » est ajouté à deux reprises au paragraphe 7, afin de refléter les termes exacts utilisés dans les définitions (« point de contact national unique »).

Amendement 29 –

L'article 11 (nouvel article 12) est modifié comme suit :

« **Art. ~~11~~12.** (1) L'autorité compétente concernée peut imposer aux fournisseurs de service numérique :

1~~.~~° de lui communiquer les informations nécessaires pour évaluer la sécurité de leurs réseaux et systèmes d'information, y compris les documents relatifs à leurs politiques de sécurité ;

2~~.~~° de corriger tout manquement aux obligations fixées à l'article 11~~10~~ ;

3~~.~~° de lui communiquer toute information nécessaire à l'accomplissement de ses missions en vertu de la présente loi.

(2) Si un fournisseur de service numérique a son établissement principal ou un représentant au Grand-Duché de Luxembourg alors que ses réseaux et systèmes d'information sont situés dans un ou plusieurs autres Etats membres, les autorités compétentes concernées luxembourgeoises et étrangère coopèrent étroitement et se prêtent mutuellement assistance dans la mesure nécessaire à l'application de la présente loi ~~l'autorité compétente concernée luxembourgeoise coopère avec l'autorité compétente de ces autres Etats membres~~.

L'obligation au secret professionnel posée par l'article 16 de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier ne fait pas obstacle à cette coopération. »

Motivation de l'amendement concernant l'article 11 du projet de loi (article 12 du texte amendé)

A part les modification d'ordre légistique effectuées au paragraphe 1er, le paragraphe 2, alinéa 1er tient compte de l'opposition formelle formulée par le Conseil d'Etat. En effet, alors que la directive NIS prévoit que « l'autorité compétente de l'État membre de l'établissement principal ou du représentant et les autorités compétentes de ces autres États membres coopèrent et se prêtent mutuellement assistance si nécessaire », la version initiale du texte envisageait que « l'autorité compétente concernée luxembourgeoise coopère avec l'autorité compétente de ces autres Etats membres », en omettant de préciser que les autorités compétentes se prêtent mutuellement assistance si nécessaire. Ainsi, le paragraphe 2 est modifié de sorte qu'aussi bien la coopération que l'assistance mutuelle entre autorités compétentes concernées soient visées.

Le paragraphe 2, alinéa 2 du nouvel article 11 autorise les autorités compétentes luxembourgeoises et étrangère de coopérer, sans que le secret auquel les personnes exerçant une fonction au sein de la CSSF sont tenues en vertu de l'article 16 de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier ne saurait s'y opposer.

Amendement 30 –

L'article 12 (nouvel article 13), paragraphe 2, alinéa 1er, est modifié comme suit :

« (2) Lorsqu'elle traite des notifications, l'autorité compétente concernée agit conformément à la procédure énoncée à l'article ~~8~~7. L'autorité compétente concernée peut traiter les notifications obligatoires en leur donnant la priorité par rapport aux notifications volontaires. Les notifications volontaires ne sont traitées que lorsque leur traitement ne fait pas peser de charge disproportionnée ou inutile sur l'autorités compétente concernée. »

Motivation de l'amendement concernant l'article 12 du projet de loi (article 13 du texte amendé)

Outre la référence à l'ancien article 7 qui a dû être adaptée suite à la renumérotation du projet de loi, le terme « autorité » est mis au singulier afin de redresser une erreur grammaticale.

Amendement 31 –

Le texte de l'article 13 (nouvel article 14) est modifié comme suit :

« **Art. ~~13~~14.** (1) Lorsque l'autorité compétente concernée constate une violation des obligations prévues par les articles ~~8~~7, ~~9~~8, 11~~10~~ et 12~~11~~ ou par des mesures prises en exécution de ~~cette~~ la présente loi, elle peut frapper l'opérateur de services essentiels ou le fournisseur de service numérique concerné d'une ou de plusieurs des sanctions suivantes :

1.° un avertissement ;

2.° un blâme ;

3.° une amende d'ordre, dont le montant est proportionné à la gravité du manquement, à la situation de l'intéressé, à l'ampleur du dommage et aux avantages qui en sont tirés sans pouvoir excéder 125 000 euros.

L'amende ne peut être prononcée que pour autant que les manquements visés ne fassent pas l'objet d'une sanction pénale.

~~Les sanctions sont effectives, proportionnées et dissuasives.~~

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

(3) Les décisions prises par l'autorité compétente concernée à l'issue de la procédure contradictoire sont motivées et notifiées à l'opérateur de services essentiels ou au fournisseur de service numérique concerné.

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

(5) La perception des amendes d'ordre prononcées par l'ILR est confiée à l'Administration de ~~l'Enregistrement~~ l'enregistrement et des ~~Domaines~~domaines. »

Motivation de l'amendement concernant l'article 13 du projet de loi (article 14 du texte amendé)

Au paragraphe 1er, alinéa 1er, les termes « de cette loi » sont remplacés par les termes « de la présente loi ».

De plus, au paragraphe 1er, alinéa 1er, point 3, les tranches de mille du montant d'argent sont dorénavant séparées par une espace insécable (« 125 000 »).

Le paragraphe 1er, alinéa 3, est supprimé en ce qu'il se limite à répéter le principe que « les sanctions sont effectives, proportionnées et dissuasives ». En ce faisant, les auteurs des amendements se rallient à l'avis du Conseil d'Etat qui considère que cette disposition est dépourvue de toute valeur normative dans le cadre de la loi de transposition proprement dite.

Finalement, au paragraphe 5, l'expression « Administration de l'enregistrement et des domaines » s'écrit avec des lettres « e » et « d » minuscules.

Amendement 32 –

L'article 14 (nouvel article 15) est modifié comme suit :

« **Art. 1415.** A l'article 2, ~~point~~ lettre y), de la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat, le point final est remplacé par un point-virgule et l'article 2 de la même loi est complété comme suit :

« z) l'exercice, dans le cadre de ces attributions, de la fonction d'Autorité d'agrément cryptographique, chargée de veiller à ce que les produits cryptographiques soient conformes aux politiques de sécurité respectives en matière cryptographique; d'évaluer et d'agréer les produits cryptographiques pour la protection des informations classifiées jusqu'à un certain niveau de classification dans leur environnement opérationnel; de conserver et de gérer les données techniques relatives aux produits cryptographiques. »

Motivation de l'amendement concernant l'article 14 du projet de loi (article 15 du texte amendé)

A l'alinéa 1er, le terme « point » est remplacé par celui de « lettre » et il est inséré l'article défini « la » entre les termes « de » et « loi ».

Amendement 33 –

Le texte de l'article 15 (nouvel article 16) est modifié comme suit :

« **Art. 16.** La loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale est modifiée comme suit :

1° A l'article 2, point 4, le point final est remplacé par un point-virgule et il est inséré à la suite du point 4 un nouveau point 5, libellé comme suit :

« 5. «stratégie nationale en matière de sécurité des réseaux et des systèmes d'information»: un cadre prévoyant des objectifs et priorités stratégiques en matière de sécurité des réseaux et des systèmes d'information au niveau national. » ;

2° A l'article 3, paragraphe 1er, lettre b), il est ajouté un nouveau point 4, libellé comme suit :

« 4. de coordonner et d'élaborer une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information; » ;

3° A l'article 8, paragraphe 1er, les termes « l'article 5 » sont remplacés par les termes « l'article 4 » ;

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

« Chapitre 4*bis* – La stratégie nationale en matière de sécurité des réseaux et des systèmes d'information

Art. 9*bis*. Le Haut-Commissariat à la Protection nationale élabore une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information, qui porte, en particulier, sur les points suivants:

a) les objectifs et les priorités de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information;

b) un cadre de gouvernance permettant d'atteindre les objectifs et les priorités de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information, prévoyant notamment les rôles et les responsabilités des organismes publics et des autres acteurs pertinents;

c) l'inventaire des mesures en matière de préparation, d'intervention et de récupération, y compris la coopération entre les secteurs public et privé;

d) un aperçu des programmes d'éducation, de sensibilisation et de formation en rapport avec la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information;

e) un aperçu des plans de recherche et de développement en rapport avec la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information;

f) un plan d'évaluation des risques permettant d'identifier les risques;

g) une liste des différents acteurs concernés par la mise en œuvre de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information. » »

Motivation de l'amendement concernant l'article 15 du projet de loi (article 16 du texte amendé)

L'article 16 est reformulé afin de tenir compte de l'avis du Conseil d'Etat qui fait remarquer que les modifications se rapportant à un même acte se font en les numérotant : 1°, 2°, 3°, 4°.

Amendement 34 –

L'article 16 (nouvel article 17) est modifié comme suit :

« **Art. ~~16~~17.** La présente loi entre en vigueur le premier jour du deuxième mois qui suit celui de sa publication au Journal officiel du Grand-Duché de Luxembourg.

~~Mandons et ordonnons que la présente loi soit insérée au Journal officiel du Grand Duché de Luxembourg pour être exécutée et observée par tous ceux que la chose concerne.~~ »

Motivation de l'amendement concernant l'article 16 du projet de loi (article 17 du texte amendé)

L'alinéa 1er est reformulé en utilisant la formulation proposée par le Conseil d'Etat.

L'alinéa 2 est supprimé, parce que la formule de promulgation est seulement ajoutée avant la soumission de l'acte en projet à la signature du Grand-Duc.

Amendement 35 –

Dans l'annexe, le terme « banques » est remplacé par la notion « établissements de crédit ».

Motivation de l'amendement concernant l'annexe du projet de loi

La notion « banques » a été remplacée par celle de « établissements de crédits » afin d'être en ligne avec la nomenclature nationale et européenne en la matière.

*

TABLEAU DE CONCORDANCE

Projet de loi	*Version initiale du projet de loi*	*Directive (UE) 2016/1148*
Article 1er, (1)	Article 2, (1)	Article 1er, (3)
Article 1er, (2)	Article 2, (2)	Article 1er, (7)
Article 2, 1°	Article 1er, 1.	Article 4, 1)
Article 2, 2°	Article 1er, 2.	Article 4, 2)
Article 2, 3°	Article 1er, 3.	Article 4, 4)
Article 2, 4°	Article 1er, 4.	Article 4, 5)
Article 2, 5°	Article 1er, 5.	Article 4, 6)
Article 2, 6°	Article 1er, 6.	Article 4, 7)
Article 2, 7°	Article 1er, 7.	Article 4, 8)
Article 2, 8°	Article 1er, 8.	Article 4, 9)
Article 2, 9°	Article 1er, 9.	Article 4, 10)
Article 2, 10°	Article 1er, 10.	Article 4, 11)
Article 2, 11°	Article 1er, 11.	Article 4, 12)
Article 2, 12°	Article 1er, 12.	Article 4, 13)
Article 2, 13°	Article 1er, 13.	Article 4, 14)
Article 2, 14°	Article 1er, 14.	Article 4, 15)
Article 2, 15°	Article 1er, 15.	Article 4, 16)
Article 2, 16°	Article 1er, 16.	Article 4, 17)
Article 2, 17°	Article 1er, 17.	Article 1er, 18)
Article 2, 18°	Article 1er, 18.	Article 1er, 19)

Projet de loi	*Version initiale du projet de loi*	*Directive (UE) 2016/1148*
Article 2, 19°	Article 1er, 21.	Nouveau
Article 2, 20°	Article 1er, 22.	Nouveau
Article 2, 21°	Article 1er, 23.	Nouveau
Article 2, 22°	Article 1er, 24.	Article 11, (1)
Article 2, 23°	Article 1er, 25.	Article 12, (1)
Article 2, 24°	Article 5	Article 8, (4)
Article 3, alinéa 1er	Article 1er, 19.	Article 8, (1)
Article 3, alinéa 2	Article 1er, 19.	Article 8, (1)
Article 3, alinéa 3	Nouveau	Nouveau
Article 4	Article 1er, 20.	Article 8, (3)
Article 5	Article 4	Nouveau
Article 6, alinéa 1er	Nouveau	Article 8, (6)
Article 6, alinéa 2	Nouveau	Nouveau
Article 7, (1)	Article 1er, 3.	Nouveau
Article 7, (2)	Article 6, (1)	Article 5, (2)
Article 7, (3)	Article 6, (2)	Article 6, (1) et (2)
Article 7, (4)	Article 6, (3)	Article 5, (3)
Article 7, (5)	Article 6, (4)	Article 5, (4)
Article 8, (1)	Article 7, (1)	Article 14, (1)
Article 8, (2)	Article 7, (2)	Article 14, (2)
Article 8, (3)	Article 7, (3)	Nouveau
Article 8, (4)	Article 7, (4)	Article 14, (3)
Article 8, (5), alinéa 1er	Article 7, (5), alinéa 1er	Article 14, (4)
Article 8, (5), alinéa 2	Article 7, (5), alinéa 2	Article 14, (7)
Article 8, (6), alinéa 1er	Article 7, (6), alinéa 1er	Article 14, (5), alinéa 1er et article 14, (5), alinéa 3
Article 8, (6), alinéa 2	Article 7, (6), alinéa 2	Article 14, (5), alinéa 2
Article 8, (7), alinéa 1er	Article 7, (7), alinéa 1er	Nouveau
Article 8, (7), alinéa 2	Article 7, (7), alinéa 2	Article 10, (3), alinéa 2
Article 8, (8)	Article 7, (8)	Article 14, (6)
Article 9, (1), alinéa 1er, 1°	Article 8, (1), alinéa 1er, 1.	Article 15, (2), alinéa 1er, a)
Article 9, (1) , alinéa 1er, 2°	Article 8, (1), alinéa 1er, 2.	Article 15, (2), alinéa 1er, b)
Article 9, (1), alinéa 1er, 3°	Article 8, (1), alinéa 1er, 3.	Nouveau
Article 9, (1), alinéa 2	Article 8, (1), alinéa 2	Nouveau
Article 9, (1), alinéa 3	Article 8, (1), alinéa 3	Article 15, (2), alinéa 2
Article 9, (2)	Article 8, (2)	Article 15, (3)
Article 9, (3)	Article 8, (3)	Article 15, (4)
Article 10, (1), alinéa 1er	Article 9, (1), alinéa 1er	Article 18, (1) et (2)
Article 10, (1), alinéa 2	Article 9, (1), alinéa 2	Article 4, 10)
Article 10, (1), alinéa 3	Article 9, (1), alinéa 3	Article 18, (3)
Article 10, (2)	Article 9, (2)	Article 16, (11)
Article 11, (1)	Article 10, (1)	Article 16, (1)

Projet de loi	*Version initiale du projet de loi*	*Directive (UE) 2016/1148*
Article 11, (2)	Article 10, (2)	Article 16, (2)
Article 11, (3)	Article 10, (3)	Article 16, (3)
Article 11, (4), alinéa 1er	Article 10, (4), alinéa 1er	Article 16, (4), alinéa 1
Article 11, (4), alinéa 2	Article 10, (4), alinéa 2	Article 16, (4), alinéa 2
Article 11, (4), alinéa 3	Article 10, (4), alinéa 3	Nouveau
Article 11, (5)	Article 10, (5)	Article 16, (5)
Article 11, (6)	Article 10, (6)	Article 16, (6)
Article 11, (7), alinéa 1er	Article 10, (7), alinéa 1er	Nouveau
Article 11, (7), alinéa 2	Article 10, (7), alinéa 2	Article 10, (3), alinéa 2
Article 11, (8)	Article 10, (8)	Article 16, (7)
Article 12, (1), 1°	Article 11, (1), 1.	Article 17, (2), a)
Article 12, (1), 2°	Article 11, (1), 2.	Article 17, (2), b)
Article 12, (1), 3°	Article 11, (1), 3.	Nouveau
Article 12, (2), alinéa 1er	Article 11, (2)	Article 17, (3)
Article 12, (2), alinéa 2	Nouveau	Nouveau
Article 13, (1)	Article 12, (1)	Article 20, (1)
Article 13, (2)	Article 12, (2)	Article 20, (2)
Article 14, (1)	Article 13, (1)	Article 21
Article 14, (2)	Article 13, (2)	Article 21
Article 14, (3)	Article 13, (3)	Article 21
Article 14, (4)	Article 13, (4)	Article 21
Article 14, (5)	Article 13, (5)	Article 21
Article 15	Article 14	Nouveau
Article 16, 1°	Article 15, (1)	Article 4, 3)
Article 16, 2 °	Article 15, (2)	Nouveau
Article 16, 3°	Article 15, (3)	Nouveau
Article 16, 4°	Article 15, (4)	Article 7, (1)
Article 17	Article 16	Nouveau
Annexe	Annexe	Annexe II

Directive (UE) 2016/1148	*Projet de loi*	*Version initiale du projet de loi*
Article 1er, (1)	-	-
Article 1er, (2)	-	-
Article 1er, (3)	Article 1er, (1)	Article 2, (1)
Article 1er, (4)	-	-
Article 1er, (5)	-	-
Article 1er, (6)	-	-
Article 1er, (7)	Article 1er, (2)	Article 2, (2)
Article 2, (1)	-	-
Article 2, (2)	-	-
Article 3	-	-
Article 4, 1)	Article 2, 1°	Article 1er, 1.
Article 4, 2)	Article 2, 2°	Article 1er, 2.
Article 4, 3)	Article 16, 1°	Article 15, (1)
Article 4, 4)	Article 2, 3°	Article 1er, 3.
Article 4, 5)	Article 2, 4°	Article 1er, 4.
Article 4, 6)	Article 2, 5°	Article 1er, 5.
Article 4, 7)	Article 2, 6°	Article 1er, 6.
Article 4, 8)	Article 2, 7°	Article 1er, 7.
Article 4, 9)	Article 2, 8°	Article 1er, 8.
Article 4, 10)	Article 2, 9° et article 10, (1), alinéa 2	Article 1er, 9. et article 9, (1), alinéa 2
Article 4, 11)	Article 2, 10°	Article 1er, 10.
Article 4, 12)	Article 2, 11°	Article 1er, 11.
Article 4, 13)	Article 2, 12 °	Article 1er, 12.
Article 4, 14)	Article 2, 13°	Article 1er, 13.
Article 4, 15)	Article 2, 14°	Article 1er, 14.
Article 4, 16)	Article 2, 15°	Article 1er, 15.
Article 4, 17)	Article 2, 16°	Article 1er, 16.
Article 4, 18)	Article 2, 17°	Article 1er, 17.
Article 4, 19)	Article 2, 18°	Article 1er, 18.
Article 5, (1)	-	-
Article 5, (2)	Article 7, (2)	Article 6, (1)
Article 5, (3)	Article 7, (4)	Article 6, (3)
Article 5, (4)	Article 7, (5)	Article 6, (4)
Article 5, (5)	-	-
Article 5, (6)	-	-
Article 5, (7)	-	-
Article 6, (1)	Article 7, (3)	Article 6, (2)
Article 6, (2)	Article 7, (3)	Article 6, (2)
Article 7, (1)	Article 16, 4°	Article 15, (4)
Article 7, (2)	-	-
Article 7, (3)	-	-

Directive (UE) 2016/1148	*Projet de loi*	*Version initiale du projet de loi*
Article 8, (1)	Article 3, alinéas 1er et 2	Article 1er, 19.
Article 8, (2)	-	-
Article 8, (3)	Article 4	Article 1, 20.
Article 8, (4)	Article 2, 24°	Article 5
Article 8, (5)	-	-
Article 8, (6)	Article 6, alinéa 1er	-
Article 8, (7)	-	-
Article 9, (1)	-	-
Article 9, (2)	-	-
Article 9, (3)	-	-
Article 9, (4)	-	-
Article 9, (5)	-	-
Article 10, (1)	-	-
Article 10, (2)	-	-
Article 10, (3), alinéa 1er	-	-
Article 10, (3), alinéa 2	Article 11, (7), alinéa 2	Article 10, (7), alinéa 2
Article 11, (1)	Article 2, 22°	Article 1er, 24.
Article 11, (2)	-	-
Article 11, (3)	-	-
Article 11, (4)	-	-
Article 11, (5)	-	-
Article 12, (1)	Article 2, 23°	Article 1er, 25.
Article 12, (2)	-	-
Article 12, (3)	-	-
Article 12, (4)	-	-
Article 12, (5)	-	-
Article 13	-	-
Article 14, (1)	Article 8, (1)	Article 7, (1)
Article 14, (2)	Article 8, (2)	Article 7, (2)
Article 14, (3)	Article 8, (4)	Article 7, (4)
Article 14, (4)	Article 8, (5), alinéa 1er	Article 7, (5), alinéa 1er
Article 14, (5), alinéa 1er	Article 8, (6), alinéa 1er	Article 7, (6), alinéa 1er
Article 14, (5), alinéa 2	Article 8, (6), alinéa 2	Article 7, (6), alinéa 2
Article 14, (5), alinéa 3	Article 8, (6), alinéa 1er	Article 7, (6), alinéa 3
Article 14, (6)	Article 8, (8)	Article 7, (8)
Article 14, (7)	Article 8, (5), alinéa 2	Article 7, (5), alinéa 2
Article 15, (1)	-	-
Article 15, (2)	Article 9, (1)	Article 8, (1)
Article 15, (3)	Article 9, (2)	Article 8, (2)
Article 15, (4)	Article 9, (3)	Article 8, (3)
Article 16, (1)	Article 11, (1)	Article 10, (1)
Article 16, (2)	Article 11, (2)	Article 10, (2)

Directive (UE) 2016/1148	*Projet de loi*	*Version initiale du projet de loi*
Article 16, (3)	Article 11, (3)	Article 10, (3)
Article 16, (4), alinéa 1er	Article 11, (4), alinéa 1er	Article 10, (4), alinéa 1er
Article 16, (4), alinéa 2	Article 11, (4), alinéa 2	Article 10, (4), alinéa 2
Article 16, (5)	Article 11, (5)	Article 10, (5)
Article 16, (6)	Article 11, (6)	Article 10, (6)
Article 16, (7)	Article 11, (8)	Article 10, (8)
Article 16, (8)	-	-
Article 16, (9)	-	-
Article 16, (10)	-	-
Article 16, (11)	Article 10, (2)	Article 9, (2)
Article 17, (1)	-	-
Article 17, (2)	Article 12, (1)	Article 11, (1)
Article 17, (3)	Article 12, (2), alinéa 1er	Article 11, (2)
Article 18, (1)	Article 10, (1), alinéa 1er	Article 9, (1), alinéa 1er
Article 18, (2)	Article 10, (1), alinéa 1er	Article 9, (1), alinéa 1er
Article 18, (3)	Article 10, (1), alinéa 3	Article 9, (1), alinéa 3
Article 19, (1)	-	-
Article 19, (2)	-	-
Article 20, (1)	Article 13, (1)	Article 12, (1)
Article 20, (2)	Article 13, (2)	Article 12, (2)
Article 21	Article 14, (1) – (5)	Article 13, (1) – (5)
Article 22, (1)	-	-
Article 22, (2)	-	-
Article 23, (1)	-	-
Article 23, (2)	-	-
Article 24, (1)	-	-
Article 24, (2)	-	-
Article 24, (3)	-	-
Article 25, (1)	-	-
Article 25, (2)	-	-
Article 26	-	-
Article 27	-	-
Annexe I	-	-
Annexe II	Annexe	Annexe
Annexe III	Intégré dans le texte de le projet de loi (article 2, 4°)	Intégré dans le texte de le projet de loi (article 1er, 4.)

*

TEXTE COORDONNE AVEC SUIVI DES MODIFICATIONS

PROJET DE LOI

portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne et modifiant

1°. la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat et.

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

~~**2. la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat.**~~

TEXTE DU PROJET DE LOI

Chapitre 1er – *Définitions et champ d'application*

Art. 1er. (1) Les exigences en matière de sécurité et de notification prévues par la présente loi ne s'appliquent pas aux entreprises soumises aux exigences énoncées aux articles 45 et 46 de la loi modifiée du 27 février 2011 sur les réseaux et les services de communications électroniques ni aux prestataires de services de confiance soumis aux exigences à l'article 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.

(2) Lorsqu'une loi ou un acte juridique sectoriel de l'Union européenne exige des opérateurs de services essentiels ou des fournisseurs de service numérique qu'ils assurent la sécurité de leurs réseaux et systèmes d'information ou qu'ils procèdent à la notification des incidents, à condition que les exigences en question aient un effet au moins équivalent à celui des obligations prévues par la présente loi, les dispositions de cette loi ou de cet acte juridique sectoriel de l'Union européenne s'appliquent.

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

1° « Réseau et système d'information » :

a) un réseau de communications électroniques au sens de l'article 2, paragraphe 24, de la loi modifiée du 27 février 2011 sur les réseaux et les services de communications électroniques ;

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

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

2° « Sécurité des réseaux et des systèmes d'information » : la capacité des réseaux et des systèmes d'information de résister, à un niveau de confiance donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles ;

3° « Opérateur de services essentiels » : une entité publique ou privée ~~ayant un établissement sur le territoire luxembourgeois~~ dont le type figure en annexe et qui répond aux critères énoncés à l'article 76, paragraphe 21er ;

4° « Service numérique » : un service au sens de l'article 1er, paragraphe 1er, ~~point~~ lettre b), de la loi du 8 novembre 2016 prévoyant une procédure d'information dans le domaine des réglemen-

tations techniques et des règles relatives aux services de la société de l'information du type « place de marché en ligne », « moteur de recherche en ligne » ou « service d'informatique en nuage » ;

5° « Fournisseur de service numérique » : une personne morale qui fournit un service numérique ;

6° « Incident » : tout événement ayant un impact négatif réel sur la sécurité des réseaux et des systèmes d'information;

7° « Gestion d'incident » : toutes les procédures utiles à la détection, à l'analyse et au confinement d'un incident et toutes les procédures utiles à l'intervention en cas d'incident ;

8° « Risque » : toute circonstance ou tout événement raisonnablement identifiable ayant un impact négatif potentiel sur la sécurité des réseaux et des systèmes d'information ;

9° « Représentant » : une personne physique ou morale établie dans l'Union européenne qui est expressément désignée pour agir pour le compte d'un fournisseur de service numérique non établi dans l'Union européenne ;

10° « Norme » : une norme au sens de l'article 2, point 1), du règlement (UE) n° 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision n° 1673/2006/CE du Parlement européen et du Conseil ;

11° « Spécification » : une spécification technique au sens de l'article 2, point 4), du règlement (UE) n° 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision n° 1673/2006/CE du Parlement européen et du Conseil ;

12° « Point d'échange internet », ci-après (« IXP) » : une structure de réseau qui permet l'interconnexion de plus de deux systèmes autonomes indépendants, essentiellement aux fins de faciliter l'échange de trafic internet ; un IXP n'assure l'interconnexion que pour des systèmes autonomes ; un IXP n'exige pas que le trafic internet passant entre une paire quelconque de systèmes autonomes participants transite par un système autonome tiers, pas plus qu'il ne modifie ou n'altère par ailleurs un tel trafic ;

13° « Système de noms de domaine », ci-après («DNS) » : un système hiérarchique et distribué d'affectation de noms dans un réseau qui résout les questions liées aux noms de domaines ;

14° « Fournisseur de services DNS » : une entité qui fournit des services DNS sur l'internet ;

15° « Registre de noms de domaine de haut niveau » : une entité qui administre et gère l'enregistrement de noms de domaine internet dans un domaine de haut niveau donné ;

16° « Place de marché en ligne » : un service numérique qui permet à des consommateurs et/ou à dès professionnels au sens de l'article L. 010-1, point 1) ou point 2) respectivement, du Code de la consommation de conclure des contrats de vente ou de service en ligne avec des professionnels soit sur le site internet de la place de marché en ligne, soit sur le site internet d'un professionnel qui utilise les services informatiques fournis par la place de marché en ligne ;

17° « Moteur de recherche en ligne » : un service numérique qui permet aux utilisateurs d'effectuer des recherches sur, en principe, tous les sites internet ou sur les sites internet dans une langue donnée, sur la base d'une requête lancée sur n'importe quel sujet sous la forme d'un mot clé, d'une phrase ou d'une autre entrée, et qui renvoie des liens à partir desquels il est possible de trouver des informations en rapport avec le contenu demandé ;

18° « Service informatique en nuage » : un service numérique qui permet l'accès à un ensemble modulable et variable de ressources informatiques pouvant être partagées ;

19. « Autorité compétente concernée » : la Commission de surveillance du secteur financier (ci-après « la CSSF ») est l'autorité compétente en matière de sécurité des réseaux et des systèmes d'information couvrant les secteurs des banques et des infrastructures de marchés financiers tels que définis aux points 3. et 4. de l'annexe, ainsi que les services numériques fournis par une entité tombant sous la surveillance de la CSSF. L'Institut luxembourgeois de régulation (ci-après

« l'ILR ») est l'autorité compétente en matière de sécurité des réseaux et des systèmes d'information couvrant les autres secteurs visés en annexe, ainsi que les services numériques fournis par une entité pour laquelle la CSSF n'est pas l'autorité compétente ;

20. « Point de contact national unique » : l'ILR constitue le point de contact national unique en matière de sécurité des réseaux et des systèmes d'information ;

2119.° «CERT Gouvernemental » : Centre de traitement des urgences informatiques, tel que défini à l'arrêté grand-ducal du xx.xx.xx9 mai 2018 déterminant l'organisation et les attributions du Centre de traitement des urgences informatiques, dénommé « CERT Gouvernemental » ;

2220.° « CIRCL » : Computer Incident Response Center Luxembourg, opéré par le groupement d'intérêt économiqueG.I.E. Security Made in Lëtzebuerg ;

2321.° « CSIRT » : centre de réponse aux incidents de sécurité informatiques ;

2422.° « Groupe de coopération » : groupe institué aux fins de soutenir et de faciliter la coopération stratégique et l'échange d'informations entre les Etats membres et de renforcer la confiance, et de parvenir à un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne ;

2523.° « Réseau des CSIRT » : groupe institué aux fins de contribuer au renforcement de la confiance entre les Etats membres et de promouvoir une coopération opérationnelle rapide et effective. ;

24° « Point de contact national unique » : autorité qui exerce une fonction de liaison pour assurer une coopération transfrontalière entre les autorités des Etats membres, ainsi qu'avec les autorités concernées des autres Etats membres, le groupe de coopération et le réseau des CSIRT.

Art. 2 (1) Les exigences en matière de sécurité et de notification prévues par la présente loi ne s'appliquent pas aux entreprises soumises aux exigences énoncées aux articles 45 et 46 de la loi modifiée du 27 février 2011 sur les réseaux et les services de communications électroniques ni aux prestataires de services de confiance soumis aux exigences à l'article 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.

(2) Lorsqu'une loi ou un acte juridique sectoriel de l'Union exige des opérateurs de services essentiels ou des fournisseurs de service numérique qu'ils assurent la sécurité de leurs réseaux et systèmes d'information ou qu'ils procèdent à la notification des incidents, à condition que les exigences en question aient un effet au moins équivalent à celui des obligations prévues par la présente loi, les dispositions de cette loi ou de cet acte juridique sectoriel de l'Union s'appliquent.

Chapitre 2 – *Autorités compétentes concernées et point de contact national unique*

Art. 3. Dans la limite de leurs compétences et missions, les autorités compétentes concernées ont le pouvoir de prendre des règlements dans le cadre de l'exécution de la présente loi.

Art. 3. La Commission de surveillance du secteur financier, (ci-après « la CSSF »), est l'autorité compétente en matière de sécurité des réseaux et des systèmes d'information couvrant les secteurs des banquesétablissements de crédits et des infrastructures de marchés financiers tels que définis aux points 3. et 4. de l'annexe, ainsi que les services numériques fournis par une entité tombant sous la surveillance de la CSSF.

L'Institut luxembourgeois de régulation, (ci-après « l'ILR »), est l'autorité compétente en matière de sécurité des réseaux et des systèmes d'information couvrant les autres secteurs visés en annexe, ainsi que les services numériques fournis par une entité pour laquelle la CSSF n'est pas l'autorité compétente.

L'obligation au secret professionnel posée par l'article 16 de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier ne fait pas obstacle à l'échange d'informations entre autorités compétentes.

Art. 4. L'ILR constitue le point de contact national unique en matière de sécurité des réseaux et des systèmes d'information.

Art. 45. Dans l'exercice de sa mission, l'ILR bénéficie d'une contribution financière à charge du budget de l'Etat, ~~à titre de participation aux~~afin de couvrir l'intégralité de ses frais de fonctionnement.

~~**Art. 5.** Le point de contact unique exerce une fonction de liaison pour assurer une coopération transfrontalière entre les autorités des Etats membres, ainsi qu'avec les autorités concernées des autres Etats membres, le groupe de coopération et le réseau des CSIRT.~~

Art. 6. Dans la mesure nécessaire à l'accomplissement de leur mission en vertu de la présente loi, les autorités compétentes et le point de contact national unique consultent les services répressifs nationaux compétents et les autorités nationales chargées de la protection des données et coopèrent avec eux.

L'obligation au secret professionnel posée par l'article 16 de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier ne fait pas obstacle à cette coopération.

Chapitre 3 – *Opérateurs de services essentiels*

Art. ~~6~~7. (1) Tombent sous le champ d'application de la présente loi, les opérateurs de services essentiels ayant un établissement sur le territoire luxembourgeois.

(~~1~~2) L'identification des opérateurs de services essentiels par l'autorité compétente concernée se fait au moyen des critères d'identification suivants :

1~~.~~° une entité fournit un service qui est essentiel au maintien d'activités sociétales ~~et/~~ou économiques critiques ;

2~~.~~° la fourniture de ce service est tributaire des réseaux et des systèmes d'information ; et

3~~.~~° un incident a~~urait~~ un effet disruptif important sur la fourniture dudit service.

L'autorité compétente concernée notifie la décision d'identification à l'opérateur de services essentiels.

(~~2~~3) L'importance de l'effet disruptif visé au paragraphe 2~~1~~er, point 3~~.~~, est déterminée sur base de facteurs transsectoriels et sectoriels, dont ~~notamment~~ au moins :

1~~.~~° le nombre d'utilisateurs tributaires du service fourni par l'entité concernée ;

2~~.~~° la dépendance des autres secteurs visés en annexe à l'égard du service fourni par cette entité ;

3~~.~~° les conséquences que des incidents pourraient avoir, en termes de degré et de durée, sur les fonctions économiques ou sociétales ou sur la sûreté publique ;

4~~.~~° la part de marché de cette entité ;

5~~.~~° la portée géographique eu égard à la zone susceptible d'être touchée par un incident ;

6~~.~~° l'importance que revêt l'entité pour garantir un niveau de service suffisant, compte tenu de la disponibilité de solutions de rechange pour la fourniture de ce service.

(~~3~~4) La liste des services essentiels est fixée par l'autorité compétente concernée par voie de règlement.

(~~4~~5) Lorsqu'une entité fournit un service visé au paragraphe 2~~1~~er, point 1~~.~~, dans un autre Etat membre, l'autorité compétente concernée ~~se~~ consulte ~~avec~~ l'autorité compétente de l'autre Etat membre. La consultation intervient avant que l'identification ne fasse l'objet d'une décision.

Art. ~~7~~8. (1) Les opérateurs de services essentiels prennent les mesures techniques et organisationnelles nécessaires et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'ils utilisent dans le cadre de leurs activités. Ces mesures garantissent, pour les réseaux et les systèmes d'information, un niveau de sécurité adapté au risque existant, compte tenu de l'état des connaissances. Afin d'identifier les risques, les opérateurs de services essentiels utilisent un cadre d'analyse de risques approprié pouvant être précisé par l'autorité compétente concernée par voie de règlement.

(2) Les opérateurs de services essentiels prennent des mesures appropriées en vue de prévenir les incidents qui compromettent la sécurité des réseaux et des systèmes d'information utilisés pour la fourniture de ces services essentiels ou d'en limiter l'impact, en vue d'assurer la continuité de ces services.

(3) Les mesures prises sur base des paragraphes 1er et 2 sont notifiées à l'autorité compétente concernée. Les modalités de cette notifications, ~~et notamment~~ le format et le délai, sont déterminées par l'autorité compétente concernée par voie de règlement.

(4) Les opérateurs de services essentiels notifient à l'autorité compétente concernée, sans retard injustifié, les incidents qui ont un impact significatif sur la continuité des services essentiels qu'ils fournissent. Ces notifications sont transmises au CERT Gouvernemental et au CIRCL en fonction de leurs compétences respectives. Les notifications contiennent des informations permettant à l'autorité compétente concernée de déterminer si l'incident a un impact au niveau transfrontalier. Cette notification n'accroît pas la responsabilité de la partie qui en est à l'origine.

(5) L'ampleur de l'impact d'un incident est déterminée en tenant compte, en particulier, des paramètres suivants :

1° le nombre d'utilisateurs touchés par la perturbation du service essentiel ;

2° la durée de l'incident ;

3° la portée géographique eu égard à la zone touchée par l'incident.

L'autorité compétente concernée peut préciser, par voie de règlement, les paramètres, les modalités et délais des notifications des incidents qui ont un impact significatif sur la continuité des services essentiels qu'ils fournissent.

(6) Sur la base des informations fournies dans la notification de l'opérateur de services essentiels, l'autorité compétente concernée signale aux autres Etats membres touchés si l'incident est susceptible d'avoir un impact significatif sur la continuité des services essentiels dans ces Etats membres. Sur demande de l'autorité compétente concernée, ce signalement est effectué par le point de contact national unique qui transmettra la notification aux points de contact nationaux des autres Etats membres touchés. Ce faisant, l'autorité compétente concernée doit~~, dans le respect de du droit de l'Union ou de la législation nationale conforme au droit de l'Union,~~ préserver la sécurité et les intérêts commerciaux de l'opérateur de services essentiels ainsi que la confidentialité des informations communiquées dans sa notification.

Lorsque les circonstances le permettent, l'autorité compétente concernée fournit à l'opérateur de services essentiels qui est à l'origine de la notification des informations utiles au suivi de sa notification.

~~À la demande de l'autorité compétente concernée, le point de contact national transmet les notifications visées au premier alinéa aux points de contact nationaux des autres Etats membres touchés.~~

(7) Une fois par an, l'autorité compétente concernée transmet au point de contact ~~national~~ unique un rapport de synthèse sur les notifications reçues, y compris le nombre de notifications et la nature des incidents notifiés, ainsi que sur les mesures prises conformément aux paragraphes ~~(~~4~~)~~ et ~~(~~6~~)~~.

Tous les ans, le point de contact national unique transmet au groupe de coopération un rapport de synthèse sur les notifications reçues, y compris le nombre de notifications et la nature des incidents notifiés, ainsi que sur les mesures prises conformément aux paragraphes ~~(~~4~~)~~ et ~~(~~6~~)~~.

(8) Après avoir consulté l'opérateur de services essentiels qui est à l'origine de la notification, l'autorité compétente concernée peut informer le public d'incidents particuliers ou imposer à l'opérateur de services essentiels de le faire, lorsque la sensibilisation du public est nécessaire pour prévenir un incident ou gérer un incident en cours, ou lorsque la divulgation de l'incident est dans l'intérêt public à d'autres égards.

Art. ~~8~~9. (1) A la demande de l'autorité compétente concernée, les opérateurs de services essentiels lui fournissent :

1° les informations nécessaires pour évaluer la sécurité de leurs réseaux et systèmes d'information, y compris les documents relatifs à leurs politiques de sécurité ;

2° des éléments prouvant la mise en oeuvre effective des politiques de sécurité, tels que les résultats d'un audit de sécurité exécuté par l'autorité compétente concernée ou un auditeur qualifié et, dans ce dernier cas, qu'ils en mettent les résultats, y compris les éléments probants, à la disposition de l'autorité compétente concernée. L'autorité compétente concernée peut charger un auditeur externe de contrôler la mise en oeuvre effective de la politique de sécurité à charge de l'opérateur de services essentiels ;

3° toute information nécessaire à l'accomplissement de ses missions en vertu de la présente loi.

Les opérateurs de services essentiels fournissent ces informations en respectant les délais et le niveau de détail exigés par l'autorité compétente concernée.

Au moment de formuler une telle demande d'informations et de preuves, l'autorité compétente concernée mentionne la finalité de la demande et précise quelles sont les informations exigées.

(2) Après évaluation des informations ou des résultats des audits de sécurité visés au paragraphe 1er, l'autorité compétente concernée peut donner des instructions contraignantes aux opérateurs de services essentiels pour remédier aux défaillances identifiées.

(3) Pour traiter des incidents notifiés donnant lieu à des violations des données à caractère personnel, l'autorité compétente concernée coopère étroitement avec la Commission nationale pour la protection des données et lui transmet les informations en relation avec ~~cette~~ ces violations.

Chapitre 4 – *Fournisseurs de service numérique*

Art. ~~9~~10. (1) Tombent ~~sous~~ dans le champ d'application de la présente loi, les fournisseurs de service numérique ayant leur établissement principal au Grand-Duché de Luxembourg. Un fournisseur de service numérique est réputé avoir son établissement principal au Grand-Duché de Luxembourg lorsque son siège social se trouve au Grand-Duché de Luxembourg. Le fournisseur de service numérique qui n'est pas établi dans l'Union européenne mais qui fournit un service numérique sur le territoire du Grand-Duché de Luxembourg et qui désigne un représentant au Grand-Duché de Luxembourg, relève de la compétence des autorités luxembourgeoises.

Le représentant peut être contacté par l'autorité compétente concernée à la place du fournisseur de service numérique concernant les obligations incombant audit fournisseur de service numérique en vertu de la présente loi.

La désignation d'un représentant par le fournisseur de service numérique est sans préjudice d'actions en justice qui pourraient être intentées contre le fournisseur de service numérique lui-même.

(2) Le chapitre 4 ne s'applique pas aux microentreprises et petites entreprises telles que définies dans ~~le règlement grand-ducal du 16 mars 2005 portant adaptation de la définition des micro, petites et moyennes entreprises~~la recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises.

Art. ~~10~~11. (1) Les fournisseurs de service numérique identifient les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'ils utilisent pour offrir, dans l'Union européenne, un service numérique et prennent les mesures techniques et organisationnelles nécessaires et proportionnées pour les gérer. Ces mesures garantissent, compte tenu de l'état des connaissances, un niveau de sécurité des réseaux et des systèmes d'information adapté au risque existant et prennent en considération les éléments suivants :

1° la sécurité des systèmes et des installations ;

2° la gestion des incidents ;

3° la gestion de la continuité des activités ;

4° le suivi, l'audit et le contrôle ;

5° le respect des normes internationales.

La gestion des risques qui menacent la sécurité des réseaux et des systèmes d'information des fournisseurs de service numérique se fait conformément au règlement d'exécution (UE) 2018/151 de la Commission du 30 janvier 2018 portant modalités d'application de la directive (UE) 2016/1148 du Parlement européen et du Conseil précisant les éléments à prendre en considération par les fournisseurs

de service numérique pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information ainsi que les paramètres permettant de déterminer si un incident a un impact significatif.

(2) Les fournisseurs de service numérique prennent des mesures pour éviter les incidents portant atteinte à la sécurité de leurs réseaux et systèmes d'information, et réduire au minimum l'impact de ces incidents sur les services numériques qui sont offerts dans l'Union européenne, de manière à garantir la continuité de ces services.

(3) Les fournisseurs de service numérique notifient à l'autorité compétente concernée, sans retard injustifié, tout incident ayant un impact significatif sur la fourniture d'un service numérique qu'ils offrent dans l'Union européenne. Les modalités de cette notification, le format et le délai, sont déterminés par l'autorité compétente concernée par voie de règlement. Ces notifications sont transmises au CERT Gouvernemental et au CIRCL en fonction de leurs compétences respectives. Les notifications contiennent des informations permettant à l'autorité compétente concernée d'évaluer l'ampleur de l'éventuel impact au niveau transfrontalier. Cette notification n'accroît pas la responsabilité de la partie qui en est à l'origine.

(4) L'importance de l'impact d'un incident est déterminée en tenant compte, en particulier, des paramètres suivants :

1. le nombre d'utilisateurs touchés par l'incident, en particulier ceux qui recourent au service pour la fourniture de leurs propres services ;
2. la durée de l'incident ;
3. la portée géographique eu égard à la zone touchée par l'incident ;
4. la gravité de la perturbation du fonctionnement du service ;
5. l'ampleur de l'impact sur les fonctions économiques et sociétales.

L'obligation de notifier un incident ne s'applique que lorsque le fournisseur de service numérique a accès aux informations nécessaires pour évaluer l'impact de l'incident eu égard aux paramètres visés au premier alinéa.

Les paramètres permettant de déterminer si un incident a un impact significatif sont précisés par le règlement d'exécution (UE) 2018/151 de la Commission du 30 janvier 2018 portant modalités d'application de la directive (UE) 2016/1148 du Parlement européen et du Conseil précisant les éléments à prendre en considération par les fournisseurs de service numérique pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information ainsi que les paramètres permettant de déterminer si un incident a un impact significatif.

(5) Lorsqu'un opérateur de services essentiels s'appuie sur un tiers fournisseur de service numérique pour la prestation d'un service essentiel au maintien de fonctions sociétales et économiques critiques, tout impact significatif sur la continuité des services essentiels en raison d'un incident touchant le fournisseur de service numérique est notifié par ledit opérateur.

(6) Lorsque l'incident visé au paragraphe 3 concerne deux Etats membres ou plus, l'autorité compétente concernée peut informer les autres Etats membres touchés. Ce faisant, l'autorité compétente concernée doit~~, dans le respect du droit de l'Union ou de la législation nationale conforme au droit de l'Union,~~ préserver la sécurité et les intérêts commerciaux du fournisseur de service numérique ainsi que la confidentialité des informations communiquées.

(7) Une fois par an, l'autorité compétente concernée transmet au point de contact national unique un rapport de synthèse sur les notifications reçues, y compris le nombre de notifications et la nature des incidents notifiés, ainsi que sur les mesures prises conformément aux paragraphes ~~(~~3~~)~~ et ~~(~~6~~)~~.

Tous les ans, le point de contact national unique transmet au groupe de coopération un rapport de synthèse sur les notifications reçues, y compris le nombre de notifications et la nature des incidents notifiés, ainsi que sur les mesures prises conformément aux paragraphes ~~(~~3~~)~~ et ~~(~~6~~)~~.

(8) Après avoir consulté le fournisseur de service numérique concerné, l'autorité compétente concernée, et les autorités ou les CSIRT des autres Etats membres concernés peuvent informer le public

d'incidents particuliers ou imposer au fournisseur de service numérique de le faire, dans le cas où la sensibilisation du public est nécessaire pour prévenir un incident ou pour gérer un incident en cours, ou lorsque la divulgation de l'incident est dans l'intérêt public à d'autres égards.

Art. ~~11~~12. (1) L'autorité compétente concernée peut imposer aux fournisseurs de service numérique :

1~~.~~° de lui communiquer les informations nécessaires pour évaluer la sécurité de leurs réseaux et systèmes d'information, y compris les documents relatifs à leurs politiques de sécurité ;

2~~.~~° de corriger tout manquement aux obligations fixées à l'article 11~~10~~ ;

3~~.~~° de lui communiquer toute information nécessaire à l'accomplissement de ses missions en vertu de la présente loi.

(2) Si un fournisseur de service numérique a son établissement principal ou un représentant au Grand-Duché de Luxembourg alors que ses réseaux et systèmes d'information sont situés dans un ou plusieurs autres Etats membres, les autorités compétentes concernées luxembourgeoises et étrangère coopèrent étroitement et se prêtent mutuellement assistance dans la mesure nécessaire à l'application de la présente loi ~~l'autorité compétente concernée luxembourgeoise coopère avec l'autorité compétente de ces autres Etats membres~~.

L'obligation au secret professionnel posée par l'article 16 de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier ne fait pas obstacle à cette coopération.

Chapitre 5 – *Notification volontaire*

Art. ~~12~~13. (1) Les entités qui n'ont pas été identifiées en tant qu'opérateurs de services essentiels et qui ne sont pas des fournisseurs de service numérique peuvent notifier, à titre volontaire, les incidents ayant un impact significatif sur la continuité des services qu'elles fournissent.

(2) Lorsqu'elle traite des notifications, l'autorité compétente concernée agit conformément à la procédure énoncée à l'article 8~~7~~. L'autorité compétente concernée peut traiter les notifications obligatoires en leur donnant la priorité par rapport aux notifications volontaires. Les notifications volontaires ne sont traitées que lorsque leur traitement ne fait pas peser de charge disproportionnée ou inutile sur l'autorité~~s~~ compétente concernée.

Une notification volontaire n'a pas pour effet d'imposer à l'entité qui est à l'origine de la notification des obligations auxquelles elle n'aurait pas été soumise en vertu de la présente loi si elle n'avait pas procédé à ladite notification.

Chapitre 6 – *Sanctions*

Art. ~~13~~14. (1) Lorsque l'autorité compétente concernée constate une violation des obligations prévues par les articles 8~~7~~, 9~~8~~, 11~~10~~ et 12~~11~~ ou par des mesures prises en exécution de ~~cette~~ la présente loi, elle peut frapper l'opérateur de services essentiels ou le fournisseur de service numérique concerné d'une ou de plusieurs des sanctions suivantes :

1~~.~~° un avertissement ;

2~~.~~° un blâme ;

3~~.~~° une amende d'ordre, dont le montant est proportionné à la gravité du manquement, à la situation de l'intéressé, à l'ampleur du dommage et aux avantages qui en sont tirés sans pouvoir excéder 125~~.~~ 000 euros.

L'amende ne peut être prononcée que pour autant que les manquements visés ne fassent pas l'objet d'une sanction pénale.

~~Les sanctions sont effectives, proportionnées et dissuasives.~~

(2) En cas de constatation d'un fait susceptible de constituer un manquement visé au paragraphe 1er, l'autorité compétente concernée engage une procédure contradictoire dans laquelle l'opérateur de services essentiels ou le fournisseur de service numérique concerné a la possibilité de consulter le

dossier et de présenter ses observations écrites ou verbales. L'opérateur de services essentiels ou le fournisseur de service numérique concerné peut se faire assister ou représenter par une personne de son choix. A l'issue de la procédure contradictoire, l'autorité compétente concernée peut prononcer à l'encontre de l'opérateur de services essentiels ou du fournisseur de service numérique concerné une ou plusieurs des sanctions visées au paragraphe 1er.

(3) Les décisions prises par l'autorité compétente concernée à l'issue de la procédure contradictoire sont motivées et notifiées à l'opérateur de services essentiels ou au fournisseur de service numérique concerné.

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

(5) La perception des amendes d'ordre prononcées par l'ILR est confiée à l'Administration de ~~l'Enregistrement~~ l'enregistrement et des ~~Domaines~~domaines.

Chapitre 7 – *Dispositions modificatives*

Art. ~~14~~15. A l'article 2, ~~point~~ lettre y), de la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat, le point final est remplacé par un point-virgule et l'article 2 de la même loi est complété comme suit :

« z) l'exercice, dans le cadre de ces attributions, de la fonction d'Autorité d'agrément cryptographique, chargée de veiller à ce que les produits cryptographiques soient conformes aux politiques de sécurité respectives en matière cryptographique; d'évaluer et d'agréer les produits cryptographiques pour la protection des informations classifiées jusqu'à un certain niveau de classification dans leur environnement opérationnel; de conserver et de gérer les données techniques relatives aux produits cryptographiques. »

~~**Art. 15.** (1) A l'article 2, point 4., de loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale, le point final est remplacé par un point-virgule et l'article 2 de la même loi est complété comme suit :~~

~~« 5. «stratégie nationale en matière de sécurité des réseaux et des systèmes d'information»: un cadre prévoyant des objectifs et priorités stratégiques en matière de sécurité des réseaux et des systèmes d'information au niveau national. »~~

~~(2) A l'article 3, paragraphe 1er, lettre b, de la même loi, il est ajouté un point 4., rédigé comme suit :~~

~~« de coordonner et d'élaborer une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information; »~~

~~(3) Dans l'article 8, paragraphe 1er, de la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale, les mots « l'article 5 » sont remplacés par ceux de « l'article 4 ».~~

~~(4) Dans la même loi, il est inséré un chapitre 4bis libellé comme suit :~~

~~« Chapitre 4bis – *La stratégie nationale en matière de sécurité des réseaux et des systèmes d'information*~~

~~Art. 9bis. Le Haut-Commissariat à la Protection nationale élabore une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information, qui porte, en particulier, sur les points suivants :~~

~~a) les objectifs et les priorités de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information ;~~

~~b) un cadre de gouvernance permettant d'atteindre les objectifs et les priorités de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information, prévoyant notamment les rôles et les responsabilités des organismes publics et des autres acteurs pertinents ;~~

~~c) l'inventaire des mesures en matière de préparation, d'intervention et de récupération, y compris la coopération entre les secteurs public et privé ;~~

~~d) un aperçu des programmes d'éducation, de sensibilisation et de formation en rapport avec la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information ;~~

~~e) un aperçu des plans de recherche et de développement en rapport avec la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information ;~~

~~f) un plan d'évaluation des risques permettant d'identifier les risques ;~~

~~g) une liste des différents acteurs concernés par la mise en œuvre de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information. »~~

Art. 16. La loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale est modifiée comme suit :

1° A l'article 2, point 4, le point final est remplacé par un point-virgule et il est inséré à la suite du point 4 un nouveau point 5, libellé comme suit :

« 5. «stratégie nationale en matière de sécurité des réseaux et des systèmes d'information»: un cadre prévoyant des objectifs et priorités stratégiques en matière de sécurité des réseaux et des systèmes d'information au niveau national. » ;

2° A l'article 3, paragraphe 1er, lettre b), il est ajouté un nouveau point 4, libellé comme suit :

« 4. de coordonner et d'élaborer une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information; » ;

3° A l'article 8, paragraphe 1er, les termes « l'article 5 » sont remplacés par les termes « l'article 4 » ;

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

« Chapitre 4*bis* – La stratégie nationale en matière de sécurité des réseaux et des systèmes d'information

Art. 9*bis*. Le Haut-Commissariat à la Protection nationale élabore une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information, qui porte, en particulier, sur les points suivants:

a) les objectifs et les priorités de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information;

b) un cadre de gouvernance permettant d'atteindre les objectifs et les priorités de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information, prévoyant notamment les rôles et les responsabilités des organismes publics et des autres acteurs pertinents;

c) l'inventaire des mesures en matière depréparation, d'intervention et de récupération, y compris la coopération entre les secteurs public et privé;

d) un aperçu des programmes d'éducation, de sensibilisation et de formation en rapport avec la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information;

e) un aperçu des plans de recherche et de développement en rapport avec la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information;

f) un plan d'évaluation des risques permettant d'identifier les risques;

g) une liste des différents acteurs concernés par la mise en oeuvre de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information. »

Art. ~~16~~17. La présente loi entre en vigueur le premier jour du deuxième mois qui suit celui de sa publication au Journal officiel du Grand-Duché de Luxembourg.

~~Mandons et ordonnons que la présente loi soit insérée au Journal officiel du Grand-Duché de Luxembourg pour être exécutée et observée par tous ceux que la chose concerne.~~

*

ANNEXE

Types d'entités aux fins de l'article ~~1~~2, point 3.

Secteur	*Sous-secteur*	*Type d'entités*
1. Energie	a) Electricité	– Entreprises d'électricité au sens de l'article 1er, paragraphe 14, de la loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité, qui remplit la fonction de « fourniture » au sens de l'article 1er, paragraphe 21, de la même loi
		– Gestionnaires de réseau de distribution au sens de l'article 1er, paragraphe 24, de la loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité
		– Gestionnaires de réseau de transport au sens de l'article 1er, paragraphe 25, de la loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité
	b) Pétrole	– Exploitants d'oléoducs
		– Exploitants d'installations de production, de raffinage, de traitement, de stockage et de transport de pétrole
	c) Gaz	– Entreprises de fourniture au sens de l'article 1er, paragraphe 14, de la loi modifiée du 1er août 2007 relative à l'organisation du marché du gaz naturel
		– Gestionnaires de réseau de distribution au sens de l'article 1er, paragraphe 22, de la loi modifiée du 1er août 2007 relative à l'organisation du marché du gaz naturel
		– Gestionnaires de réseau de transport au sens de l'article 1er, paragraphe 24, de la loi modifiée du 1er août 2007 relative à l'organisation du marché du gaz naturel
		– Gestionnaires d'installation de stockage au sens de l'article 1er, paragraphe 25, de la loi modifiée du 1er août 2007 relative à l'organisation du marché du gaz naturel
		– Gestionnaires d'installation de GNL au sens de l'article 1er, paragraphe 23, de la loi modifiée du 1er août 2007 relative à l'organisation du marché du gaz naturel
		– Entreprises de gaz naturel au sens de l'article 1er, paragraphe 15, de la loi modifiée du 1er août 2007 relative à l'organisation du marché du gaz naturel
		– Exploitants d'installations de raffinage et de traitement de gaz naturel

Secteur	*Sous-secteur*	*Type d'entités*
2. Transports	a) Transport aérien	– Transporteurs aériens au sens de l'article 3, point 4), du règlement (CE) n° 300/2008 du Parlement européen et du Conseil du 11 mars 2008 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile et abrogeant le règlement (CE) no 2320/2002
		– Entités gestionnaires d'aéroports au sens de l'article 2, point 1), de la loi du 23 mai 2012 portant transposition de la directive 2009/12/CE du Parlement européen et du Conseil du 11 mars 2009 sur les redevances aéroportuaires et portant modification: 1) de la loi modifiée du 31 janvier 1948 relative à la réglementation de la navigation aérienne; 2) de la loi modifiée du 19 mai 1999 ayant pour objet a) de réglementer l'accès au marché de l'assistance en escale à l'aéroport de Luxembourg, b) de créer un cadre réglementaire dans le domaine de la sûreté de l'aviation civile, et c) d'instituer une Direction de l'Aviation Civile, aéroports, y compris les aéroports du réseau central énumérés à l'annexe II, section 2, du règlement (UE) n° 1315/2013 du Parlement européen et du Conseil du 11 décembre 2013 sur les orientations de l'Union pour le développement du réseau transeuropéen de transport et abrogeant la décision no 661/2010/UE, et entités exploitant les installations annexes se trouvant dans les aéroports
		– Services du contrôle de la circulation aérienne au sens de l'article 2, point 1), du règlement (CE) n° 549/2004 du Parlement européen et du Conseil du 10 mars 2004 fixant le cadre pour la réalisation du ciel unique européen (« règlement-cadre »)
	b) Transport ferroviaire	– Gestionnaires de l'infrastructure au sens de l'article 2, point 3), de la loi modifiée du 10 mai 1995 relative à la gestion de l'infrastructure ferroviaire
		– Entreprises ferroviaires au sens de l'article 2, point 7), de la loi modifiée du 11 juin 1999 relative à l'accès à l'infrastructure ferroviaire et à son utilisation, y compris les exploitants d'installations de services au sens de l'article 2, point 2), de la loi modifiée du 10 mai 1995 relative à la gestion de l'infrastructure ferroviaire
	c) Transport par voie d'eau	– Sociétés de transport terrestre, maritime et côtier de passagers et de fret au sens de l'annexe I du règlement (CE) n° 725/2004 du Parlement européen et du Conseil du 21 novembre 2012 établissant un espace ferroviaire unique européen, à l'exclusion des navires exploités à titre individuel par ces sociétés
		– Entités gestionnaires des ports au sens de l'article 3, point 1), de la directive 2005/65/CE du Parlement européen et du Conseil du 26 octobre 2005 relative à l'amélioration de la sûreté des ports, y compris les installations portuaires au sens de l'article 2, point 11), du règlement (CE) n° 725/2004, ainsi que les entités exploitant des ateliers et des équipements à l'intérieur des ports
		– Exploitants de services de trafic maritime au sens de l'article 2, lettre o), du règlement grand–ducal modifié du 27 février 2011 relatif à la mise en place d'un système communautaire de suivi du trafic des navires et d'information

Secteur	*Sous-secteur*	*Type d'entités*
	d) Transport routier	– Autorités routières au sens de l'article 2, point 12~~.~~, du règlement délégué (UE) 2015/962 de la Commission du 18 décembre 2014 complétant la directive 2010/40/UE du Parlement européen et du Conseil en ce qui concerne la mise à disposition, dans l'ensemble de l'Union, de services d'informations en temps réel sur la circulation, chargées du contrôle de gestion du trafic
		– Exploitants de systèmes de transport intelligents au sens de la lettre circulaire du 22 février 2012 concernant la directive 2010/40/UE du Parlement européen et du Conseil du 7 juillet 2010 concernant le cadre pour le déploiement de systèmes de transport intelligents dans le domaine du transport routier et d'interfaces avec d'autres modes de transport
3. ~~Banques~~ Etablissements de crédit		– Etablissements de crédit au sens de l'article 1er, point 12~~)~~, de la loi modifiée du 5 avril 1993 relative au secteur financier
4. Infrastructures de marchés financiers		– Exploitants de plate-forme de négociation au sens de l'article 4, point 24~~.~~, de la directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE
		– Contreparties centrales au sens de l'article 2, point 1~~.~~, du règlement (UE) n° 648/2012 du Parlement européen et du Conseil du 4 juillet 2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux
5. Secteur de la santé	Etablissements de soins de santé (y compris les hôpitaux et les cliniques privées)	– Prestataires de soins de santé au sens de l'article 2, lettre f), de la loi du 24 juillet 2014 relative aux droits et obligations du patient, portant création d'un service national d'information et de médiation dans le domaine de la santé et modifiant: – la loi modifiée du 28 août 1998 sur les établissements hospitaliers; – la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel; – le Code civil
6. Fourniture et distribution d'eau potable		– Fournisseurs et distributeurs d'eaux destinées à la consommation humaine au sens de l'article 3, point 1~~)~~, lettre a), du règlement grand–ducal modifié du 7 octobre 2002 relatif à la qualité des eaux destinées à la consommation humaine
7. Infrastructures numériques		– IXP
		– Fournisseurs de services DNS
		– Registres de noms de domaines de haut niveau

*

TEXTE COORDONNE

PROJET DE LOI

portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne et modifiant

1° la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat et

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

Chapitre 1er – *Définitions et champ d'application*

Art. 1er. (1) Les exigences en matière de sécurité et de notification prévues par la présente loi ne s'appliquent pas aux entreprises soumises aux exigences énoncées aux articles 45 et 46 de la loi modifiée du 27 février 2011 sur les réseaux et les services de communications électroniques ni aux prestataires de services de confiance soumis aux exigences à l'article 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.

(2) Lorsqu'une loi ou un acte juridique sectoriel de l'Union européenne exige des opérateurs de services essentiels ou des fournisseurs de service numérique qu'ils assurent la sécurité de leurs réseaux et systèmes d'information ou qu'ils procèdent à la notification des incidents, à condition que les exigences en question aient un effet au moins équivalent à celui des obligations prévues par la présente loi, les dispositions de cette loi ou de cet acte juridique sectoriel de l'Union européenne s'appliquent.

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

1° « Réseau et système d'information » :

a) un réseau de communications électroniques au sens de l'article 2, paragraphe 24, de la loi modifiée du 27 février 2011 sur les réseaux et les services de communications électroniques ;

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

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

2° « Sécurité des réseaux et des systèmes d'information » : la capacité des réseaux et des systèmes d'information de résister, à un niveau de confiance donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles ;

3° « Opérateur de services essentiels » : une entité publique ou privée dont le type figure en annexe et qui répond aux critères énoncés à l'article 7, paragraphe 2 ;

4° « Service numérique » : un service au sens de l'article 1er, paragraphe 1er, lettre b), de la loi du 8 novembre 2016 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information du type « place de marché en ligne », « moteur de recherche en ligne » ou « service d'informatique en nuage » ;

5° « Fournisseur de service numérique » : une personne morale qui fournit un service numérique ;

6° « Incident » : tout événement ayant un impact négatif réel sur la sécurité des réseaux et des systèmes d'information;

7° « Gestion d'incident » : toutes les procédures utiles à la détection, à l'analyse et au confinement d'un incident et toutes les procédures utiles à l'intervention en cas d'incident ;

8° « Risque » : toute circonstance ou tout événement raisonnablement identifiable ayant un impact négatif potentiel sur la sécurité des réseaux et des systèmes d'information ;

9° « Représentant » : une personne physique ou morale établie dans l'Union européenne qui est expressément désignée pour agir pour le compte d'un fournisseur de service numérique non établi dans l'Union européenne ;

10° « Norme » : une norme au sens de l'article 2, point 1, du règlement (UE) n° 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision n° 1673/2006/CE du Parlement européen et du Conseil ;

11° « Spécification » : une spécification technique au sens de l'article 2, point 4, du règlement (UE) n° 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision n° 1673/2006/CE du Parlement européen et du Conseil ;

12° « Point d'échange internet », ci-après « IXP » : une structure de réseau qui permet l'interconnexion de plus de deux systèmes autonomes indépendants, essentiellement aux fins de faciliter l'échange de trafic internet ; un IXP n'assure l'interconnexion que pour des systèmes autonomes ; un IXP n'exige pas que le trafic internet passant entre une paire quelconque de systèmes autonomes participants transite par un système autonome tiers, pas plus qu'il ne modifie ou n'altère par ailleurs un tel trafic ;

13° « Système de noms de domaine », ci-après « DNS » : un système hiérarchique et distribué d'affectation de noms dans un réseau qui résout les questions liées aux noms de domaines ;

14° « Fournisseur de services DNS » : une entité qui fournit des services DNS sur l'internet ;

15° « Registre de noms de domaine de haut niveau » : une entité qui administre et gère l'enregistrement de noms de domaine internet dans un domaine de haut niveau donné ;

16° « Place de marché en ligne » : un service numérique qui permet à des consommateurs ou à des professionnels au sens de l'article L. 010-1, point 1 ou point 2 respectivement, du Code de la consommation de conclure des contrats de vente ou de service en ligne avec des professionnels soit sur le site internet de la place de marché en ligne, soit sur le site internet d'un professionnel qui utilise les services informatiques fournis par la place de marché en ligne ;

17° « Moteur de recherche en ligne » : un service numérique qui permet aux utilisateurs d'effectuer des recherches sur, en principe, tous les sites internet ou sur les sites internet dans une langue donnée, sur la base d'une requête lancée sur n'importe quel sujet sous la forme d'un mot clé, d'une phrase ou d'une autre entrée, et qui renvoie des liens à partir desquels il est possible de trouver des informations en rapport avec le contenu demandé ;

18° « Service informatique en nuage » : un service numérique qui permet l'accès à un ensemble modulable et variable de ressources informatiques pouvant être partagées ;

19° « CERT Gouvernemental » : Centre de traitement des urgences informatiques, tel que défini à l'arrêté grand-ducal du 9 mai 2018 déterminant l'organisation et les attributions du Centre de traitement des urgences informatiques, dénommé « CERT Gouvernemental » ;

20° « CIRCL » : Computer Incident Response Center Luxembourg, opéré par le groupement d'intérêt économique Security Made in Lëtzebuerg ;

21° « CSIRT » : centre de réponse aux incidents de sécurité informatiques ;

22° « Groupe de coopération » : groupe institué aux fins de soutenir et de faciliter la coopération stratégique et l'échange d'informations entre les Etats membres et de renforcer la confiance, et de parvenir à un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne ;

23° « Réseau des CSIRT » : groupe institué aux fins de contribuer au renforcement de la confiance entre les Etats membres et de promouvoir une coopération opérationnelle rapide et effective ;

24° « Point de contact national unique » : autorité qui exerce une fonction de liaison pour assurer une coopération transfrontalière entre les autorités des Etats membres, ainsi qu'avec les autorités concernées des autres Etats membres, le groupe de coopération et le réseau des CSIRT.

Chapitre 2 – *Autorités compétentes concernées et point de contact national unique*

Art. 3. La Commission de surveillance du secteur financier, ci-après « la CSSF », est l'autorité compétente en matière de sécurité des réseaux et des systèmes d'information couvrant les secteurs des établissements de crédits et des infrastructures de marchés financiers tels que définis aux points 3 et 4 de l'annexe, ainsi que les services numériques fournis par une entité tombant sous la surveillance de la CSSF.

L'Institut luxembourgeois de régulation, ci-après « l'ILR », est l'autorité compétente en matière de sécurité des réseaux et des systèmes d'information couvrant les autres secteurs visés en annexe, ainsi que les services numériques fournis par une entité pour laquelle la CSSF n'est pas l'autorité compétente.

L'obligation au secret professionnel posée par l'article 16 de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier ne fait pas obstacle à l'échange d'informations entre autorités compétentes.

Art. 4. L'ILR constitue le point de contact national unique en matière de sécurité des réseaux et des systèmes d'information.

Art. 5. Dans l'exercice de sa mission, l'ILR bénéficie d'une contribution financière à charge du budget de l'Etat, afin de couvrir l'intégralité de ses frais de fonctionnement.

Art. 6. Dans la mesure nécessaire à l'accomplissement de leur mission en vertu de la présente loi, les autorités compétentes et le point de contact national unique consultent les services répressifs nationaux compétents et les autorités nationales chargées de la protection des données et coopèrent avec eux.

L'obligation au secret professionnel posée par l'article 16 de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier ne fait pas obstacle à cette coopération.

Chapitre 3 – *Opérateurs de services essentiels*

Art. 7. (1) Tombent sous le champ d'application de la présente loi, les opérateurs de services essentiels ayant un établissement sur le territoire luxembourgeois.

(2) L'identification des opérateurs de services essentiels par l'autorité compétente concernée se fait au moyen des critères d'identification suivants :

1° une entité fournit un service qui est essentiel au maintien d'activités sociétales ou économiques critiques ;

2° la fourniture de ce service est tributaire des réseaux et des systèmes d'information ; et

3° un incident a un effet disruptif important sur la fourniture dudit service.

L'autorité compétente concernée notifie la décision d'identification à l'opérateur de services essentiels.

(3) L'importance de l'effet disruptif visé au paragraphe 2, point 3, est déterminée sur base de facteurs transsectoriels et sectoriels, dont au moins :

1° le nombre d'utilisateurs tributaires du service fourni par l'entité concernée ;

2° la dépendance des autres secteurs visés en annexe à l'égard du service fourni par cette entité ;

3° les conséquences que des incidents pourraient avoir, en termes de degré et de durée, sur les fonctions économiques ou sociétales ou sur la sûreté publique ;

4° la part de marché de cette entité ;

5° la portée géographique eu égard à la zone susceptible d'être touchée par un incident ;

6° l'importance que revêt l'entité pour garantir un niveau de service suffisant, compte tenu de la disponibilité de solutions de rechange pour la fourniture de ce service.

(4) La liste des services essentiels est fixée par l'autorité compétente concernée par voie de règlement.

(5) Lorsqu'une entité fournit un service visé au paragraphe 2, point 1, dans un autre Etat membre, l'autorité compétente concernée consulte l'autorité compétente de l'autre Etat membre. La consultation intervient avant que l'identification ne fasse l'objet d'une décision.

Art. 8. (1) Les opérateurs de services essentiels prennent les mesures techniques et organisationnelles nécessaires et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'ils utilisent dans le cadre de leurs activités. Ces mesures garantissent, pour les réseaux et les systèmes d'information, un niveau de sécurité adapté au risque existant, compte tenu de l'état des connaissances. Afin d'identifier les risques, les opérateurs de services essentiels utilisent un cadre d'analyse de risques approprié pouvant être précisé par l'autorité compétente concernée par voie de règlement.

(2) Les opérateurs de services essentiels prennent des mesures appropriées en vue de prévenir les incidents qui compromettent la sécurité des réseaux et des systèmes d'information utilisés pour la fourniture de ces services essentiels ou d'en limiter l'impact, en vue d'assurer la continuité de ces services.

(3) Les mesures prises sur base des paragraphes 1er et 2 sont notifiées à l'autorité compétente concernée. Les modalités de cette notification, le format et le délai, sont déterminées par l'autorité compétente concernée par voie de règlement.

(4) Les opérateurs de services essentiels notifient à l'autorité compétente concernée, sans retard injustifié, les incidents qui ont un impact significatif sur la continuité des services essentiels qu'ils fournissent. Ces notifications sont transmises au CERT Gouvernemental et au CIRCL en fonction de leurs compétences respectives. Les notifications contiennent des informations permettant à l'autorité compétente concernée de déterminer si l'incident a un impact au niveau transfrontalier. Cette notification n'accroît pas la responsabilité de la partie qui en est à l'origine.

(5) L'ampleur de l'impact d'un incident est déterminée en tenant compte, en particulier, des paramètres suivants :

1° le nombre d'utilisateurs touchés par la perturbation du service essentiel ;

2° la durée de l'incident ;

3° la portée géographique eu égard à la zone touchée par l'incident.

L'autorité compétente concernée peut préciser, par voie de règlement, les paramètres, les modalités et délais des notifications des incidents qui ont un impact significatif sur la continuité des services essentiels qu'ils fournissent.

(6) Sur la base des informations fournies dans la notification de l'opérateur de services essentiels, l'autorité compétente concernée signale aux autres Etats membres touchés si l'incident est susceptible d'avoir un impact significatif sur la continuité des services essentiels dans ces Etats membres. Sur demande de l'autorité compétente concernée, ce signalement est effectué par le point de contact national unique qui transmettra la notification aux points de contact nationaux des autres Etats membres touchés. Ce faisant, l'autorité compétente concernée doit préserver la sécurité et les intérêts commerciaux de l'opérateur de services essentiels ainsi que la confidentialité des informations communiquées dans sa notification.

Lorsque les circonstances le permettent, l'autorité compétente concernée fournit à l'opérateur de services essentiels qui est à l'origine de la notification des informations utiles au suivi de sa notification.

(7) Une fois par an, l'autorité compétente concernée transmet au point de contact national unique un rapport de synthèse sur les notifications reçues, y compris le nombre de notifications et la nature des incidents notifiés, ainsi que sur les mesures prises conformément aux paragraphes 4 et 6.

Tous les ans, le point de contact national unique transmet au groupe de coopération un rapport de synthèse sur les notifications reçues, y compris le nombre de notifications et la nature des incidents notifiés, ainsi que sur les mesures prises conformément aux paragraphes 4 et 6.

(8) Après avoir consulté l'opérateur de services essentiels qui est à l'origine de la notification, l'autorité compétente concernée peut informer le public d'incidents particuliers ou imposer à l'opérateur de services essentiels de le faire, lorsque la sensibilisation du public est nécessaire pour prévenir un incident ou gérer un incident en cours, ou lorsque la divulgation de l'incident est dans l'intérêt public à d'autres égards.

Art. 9. (1) A la demande de l'autorité compétente concernée, les opérateurs de services essentiels lui fournissent :

1° les informations nécessaires pour évaluer la sécurité de leurs réseaux et systèmes d'information, y compris les documents relatifs à leurs politiques de sécurité ;

2° des éléments prouvant la mise en oeuvre effective des politiques de sécurité, tels que les résultats d'un audit de sécurité exécuté par l'autorité compétente concernée ou un auditeur qualifié et, dans ce dernier cas, qu'ils en mettent les résultats, y compris les éléments probants, à la disposition de l'autorité compétente concernée. L'autorité compétente concernée peut charger un auditeur externe de contrôler la mise en oeuvre effective de la politique de sécurité à charge de l'opérateur de services essentiels ;

3° toute information nécessaire à l'accomplissement de ses missions en vertu de la présente loi.

Les opérateurs de services essentiels fournissent ces informations en respectant les délais et le niveau de détail exigés par l'autorité compétente concernée.

Au moment de formuler une telle demande d'informations et de preuves, l'autorité compétente concernée mentionne la finalité de la demande et précise quelles sont les informations exigées.

(2) Après évaluation des informations ou des résultats des audits de sécurité visés au paragraphe 1er, l'autorité compétente concernée peut donner des instructions contraignantes aux opérateurs de services essentiels pour remédier aux défaillances identifiées.

(3) Pour traiter des incidents notifiés donnant lieu à des violations des données à caractère personnel, l'autorité compétente concernée coopère étroitement avec la Commission nationale pour la protection des données et lui transmet les informations en relation avec ces violations.

Chapitre 4 – *Fournisseurs de service numérique*

Art. 10. (1) Tombent dans le champ d'application de la présente loi, les fournisseurs de service numérique ayant leur établissement principal au Grand-Duché de Luxembourg. Un fournisseur de service numérique est réputé avoir son établissement principal au Grand-Duché de Luxembourg lorsque son siège social se trouve au Grand-Duché de Luxembourg. Le fournisseur de service numérique qui n'est pas établi dans l'Union européenne mais qui fournit un service numérique sur le territoire du Grand-Duché de Luxembourg et qui désigne un représentant au Grand-Duché de Luxembourg, relève de la compétence des autorités luxembourgeoises.

Le représentant peut être contacté par l'autorité compétente concernée à la place du fournisseur de service numérique concernant les obligations incombant audit fournisseur de service numérique en vertu de la présente loi.

La désignation d'un représentant par le fournisseur de service numérique est sans préjudice d'actions en justice qui pourraient être intentées contre le fournisseur de service numérique lui-même.

(2) Le chapitre 4 ne s'applique pas aux microentreprises et petites entreprises telles que définies dans la recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises.

Art. 11. (1) Les fournisseurs de service numérique identifient les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'ils utilisent pour offrir, dans l'Union européenne, un service numérique et prennent les mesures techniques et organisationnelles nécessaires et proportion-

nées pour les gérer. Ces mesures garantissent, compte tenu de l'état des connaissances, un niveau de sécurité des réseaux et des systèmes d'information adapté au risque existant et prennent en considération les éléments suivants :

1° la sécurité des systèmes et des installations ;

2° la gestion des incidents ;

3° la gestion de la continuité des activités ;

4° le suivi, l'audit et le contrôle ;

5° le respect des normes internationales.

La gestion des risques qui menacent la sécurité des réseaux et des systèmes d'information des fournisseurs de service numérique se fait conformément au règlement d'exécution (UE) 2018/151 de la Commission du 30 janvier 2018 portant modalités d'application de la directive (UE) 2016/1148 du Parlement européen et du Conseil précisant les éléments à prendre en considération par les fournisseurs de service numérique pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information ainsi que les paramètres permettant de déterminer si un incident a un impact significatif.

(2) Les fournisseurs de service numérique prennent des mesures pour éviter les incidents portant atteinte à la sécurité de leurs réseaux et systèmes d'information, et réduire au minimum l'impact de ces incidents sur les services numériques qui sont offerts dans l'Union européenne, de manière à garantir la continuité de ces services.

(3) Les fournisseurs de service numérique notifient à l'autorité compétente concernée, sans retard injustifié, tout incident ayant un impact significatif sur la fourniture d'un service numérique qu'ils offrent dans l'Union européenne. Les modalités de cette notification, le format et le délai, sont déterminés par l'autorité compétente concernée par voie de règlement. Ces notifications sont transmises au CERT Gouvernemental et au CIRCL en fonction de leurs compétences respectives. Les notifications contiennent des informations permettant à l'autorité compétente concernée d'évaluer l'ampleur de l'éventuel impact au niveau transfrontalier. Cette notification n'accroît pas la responsabilité de la partie qui en est à l'origine.

(4) L'importance de l'impact d'un incident est déterminée en tenant compte, en particulier, des paramètres suivants :

1° le nombre d'utilisateurs touchés par l'incident, en particulier ceux qui recourent au service pour la fourniture de leurs propres services ;

2° la durée de l'incident ;

3° la portée géographique eu égard à la zone touchée par l'incident ;

4° la gravité de la perturbation du fonctionnement du service ;

5° l'ampleur de l'impact sur les fonctions économiques et sociétales.

L'obligation de notifier un incident ne s'applique que lorsque le fournisseur de service numérique a accès aux informations nécessaires pour évaluer l'impact de l'incident eu égard aux paramètres visés au premier alinéa.

Les paramètres permettant de déterminer si un incident a un impact significatif sont précisés par le règlement d'exécution (UE) 2018/151 de la Commission du 30 janvier 2018 portant modalités d'application de la directive (UE) 2016/1148 du Parlement européen et du Conseil précisant les éléments à prendre en considération par les fournisseurs de service numérique pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information ainsi que les paramètres permettant de déterminer si un incident a un impact significatif.

(5) Lorsqu'un opérateur de services essentiels s'appuie sur un tiers fournisseur de service numérique pour la prestation d'un service essentiel au maintien de fonctions sociétales et économiques critiques, tout impact significatif sur la continuité des services essentiels en raison d'un incident touchant le fournisseur de service numérique est notifié par ledit opérateur.

(6) Lorsque l'incident visé au paragraphe 3 concerne deux Etats membres ou plus, l'autorité compétente concernée peut informer les autres Etats membres touchés. Ce faisant, l'autorité compétente

concernée doit préserver la sécurité et les intérêts commerciaux du fournisseur de service numérique ainsi que la confidentialité des informations communiquées.

(7) Une fois par an, l'autorité compétente concernée transmet au point de contact national unique un rapport de synthèse sur les notifications reçues, y compris le nombre de notifications et la nature des incidents notifiés, ainsi que sur les mesures prises conformément aux paragraphes 3 et 6.

Tous les ans, le point de contact national unique transmet au groupe de coopération un rapport de synthèse sur les notifications reçues, y compris le nombre de notifications et la nature des incidents notifiés, ainsi que sur les mesures prises conformément aux paragraphes 3 et 6.

(8) Après avoir consulté le fournisseur de service numérique concerné, l'autorité compétente concernée, et les autorités ou les CSIRT des autres Etats membres concernés peuvent informer le public d'incidents particuliers ou imposer au fournisseur de service numérique de le faire, dans le cas où la sensibilisation du public est nécessaire pour prévenir un incident ou pour gérer un incident en cours, ou lorsque la divulgation de l'incident est dans l'intérêt public à d'autres égards.

Art. 12. (1) L'autorité compétente concernée peut imposer aux fournisseurs de service numérique :

1° de lui communiquer les informations nécessaires pour évaluer la sécurité de leurs réseaux et systèmes d'information, y compris les documents relatifs à leurs politiques de sécurité ;

2° de corriger tout manquement aux obligations fixées à l'article 11 ;

3° de lui communiquer toute information nécessaire à l'accomplissement de ses missions en vertu de la présente loi.

(2) Si un fournisseur de service numérique a son établissement principal ou un représentant au Grand-Duché de Luxembourg alors que ses réseaux et systèmes d'information sont situés dans un ou plusieurs autres Etats membres, les autorités compétentes concernées luxembourgeoises et étrangère coopèrent étroitement et se prêtent mutuellement assistance dans la mesure nécessaire à l'application de la présente loi.

L'obligation au secret professionnel posée par l'article 16 de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier ne fait pas obstacle à cette coopération.

Chapitre 5 – *Notification volontaire*

Art. 13. (1) Les entités qui n'ont pas été identifiées en tant qu'opérateurs de services essentiels et qui ne sont pas des fournisseurs de service numérique peuvent notifier, à titre volontaire, les incidents ayant un impact significatif sur la continuité des services qu'elles fournissent.

(2) Lorsqu'elle traite des notifications, l'autorité compétente concernée agit conformément à la procédure énoncée à l'article 8. L'autorité compétente concernée peut traiter les notifications obligatoires en leur donnant la priorité par rapport aux notifications volontaires. Les notifications volontaires ne sont traitées que lorsque leur traitement ne fait pas peser de charge disproportionnée ou inutile sur l'autorité compétente concernée.

Une notification volontaire n'a pas pour effet d'imposer à l'entité qui est à l'origine de la notification des obligations auxquelles elle n'aurait pas été soumise en vertu de la présente loi si elle n'avait pas procédé à ladite notification.

Chapitre 6 – *Sanctions*

Art. 14. (1) Lorsque l'autorité compétente concernée constate une violation des obligations prévues par les articles 8, 9, 11 et 12 ou par des mesures prises en exécution de la présente loi, elle peut frapper l'opérateur de services essentiels ou le fournisseur de service numérique concerné d'une ou de plusieurs des sanctions suivantes :

1° un avertissement ;

2° un blâme ;

3° une amende d'ordre, dont le montant est proportionné à la gravité du manquement, à la situation de l'intéressé, à l'ampleur du dommage et aux avantages qui en sont tirés sans pouvoir excéder 125 000 euros.

L'amende ne peut être prononcée que pour autant que les manquements visés ne fassent pas l'objet d'une sanction pénale.

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

(3) Les décisions prises par l'autorité compétente concernée à l'issue de la procédure contradictoire sont motivées et notifiées à l'opérateur de services essentiels ou au fournisseur de service numérique concerné.

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

(5) La perception des amendes d'ordre prononcées par l'ILR est confiée à l'Administration de l'enregistrement et des domaines.

Chapitre 7 – *Dispositions modificatives*

Art. 15. A l'article 2, lettre y), de la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat, le point final est remplacé par un point-virgule et l'article 2 de la même loi est complété comme suit :

« z) l'exercice, dans le cadre de ces attributions, de la fonction d'Autorité d'agrément cryptographique, chargée de veiller à ce que les produits cryptographiques soient conformes aux politiques de sécurité respectives en matière cryptographique; d'évaluer et d'agréer les produits cryptographiques pour la protection des informations classifiées jusqu'à un certain niveau de classification dans leur environnement opérationnel; de conserver et de gérer les données techniques relatives aux produits cryptographiques. »

Art. 16. La loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale est modifiée comme suit :

1° A l'article 2, point 4, le point final est remplacé par un point-virgule et il est inséré à la suite du point 4 un nouveau point 5, libellé comme suit :

« 5. «stratégie nationale en matière de sécurité des réseaux et des systèmes d'information»: un cadre prévoyant des objectifs et priorités stratégiques en matière de sécurité des réseaux et des systèmes d'information au niveau national. » ;

2° A l'article 3, paragraphe 1er, lettre b), il est ajouté un nouveau point 4, libellé comme suit :

« 4. de coordonner et d'élaborer une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information; » ;

3° A l'article 8, paragraphe 1er, les termes « l'article 5 » sont remplacés par les termes « l'article 4 » ;

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

« Chapitre 4*bis* – La stratégie nationale en matière de sécurité des réseaux et des systèmes d'information

Art. 9*bis*. Le Haut-Commissariat à la Protection nationale élabore une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information, qui porte, en particulier, sur les points suivants:

a) les objectifs et les priorités de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information;

b) un cadre de gouvernance permettant d'atteindre les objectifs et les priorités de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information, prévoyant notamment les rôles et les responsabilités des organismes publics et des autres acteurs pertinents;

c) l'inventaire des mesures en matière de préparation, d'intervention et de récupération, y compris la coopération entre les secteurs public et privé;

d) un aperçu des programmes d'éducation, de sensibilisation et de formation en rapport avec la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information;

e) un aperçu des plans de recherche et de développement en rapport avec la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information;

f) un plan d'évaluation des risques permettant d'identifier les risques;

g) une liste des différents acteurs concernés par la mise en oeuvre de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information. »

Art. 17. La présente loi entre en vigueur le premier jour du deuxième mois qui suit celui de sa publication au Journal officiel du Grand-Duché de Luxembourg.

*

ANNEXE

Types d'entités aux fins de l'article 2, point 3

Secteur	*Sous-secteur*	*Type d'entités*
1. Energie	a) Electricité	– Entreprises d'électricité au sens de l'article 1er, paragraphe 14, de la loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité, qui remplit la fonction de « fourniture » au sens de l'article 1er, paragraphe 21, de la même loi
		– Gestionnaires de réseau de distribution au sens de l'article 1er, paragraphe 24, de la loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité
		– Gestionnaires de réseau de transport au sens de l'article 1er, paragraphe 25, de la loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité
	b) Pétrole	– Exploitants d'oléoducs
		– Exploitants d'installations de production, de raffinage, de traitement, de stockage et de transport de pétrole
	c) Gaz	– Entreprises de fourniture au sens de l'article 1er, paragraphe 14, de la loi modifiée du 1er août 2007 relative à l'organisation du marché du gaz naturel
		– Gestionnaires de réseau de distribution au sens de l'article 1er, paragraphe 22, de la loi modifiée du 1er août 2007 relative à l'organisation du marché du gaz naturel
		– Gestionnaires de réseau de transport au sens de l'article 1er, paragraphe 24, de la loi modifiée du 1er août 2007 relative à l'organisation du marché du gaz naturel
		– Gestionnaires d'installation de stockage au sens de l'article 1er, paragraphe 25, de la loi modifiée du 1er août 2007 relative à l'organisation du marché du gaz naturel
		– Gestionnaires d'installation de GNL au sens de l'article 1er, paragraphe 23, de la loi modifiée du 1er août 2007 relative à l'organisation du marché du gaz naturel
		– Entreprises de gaz naturel au sens de l'article 1er, paragraphe 15, de la loi modifiée du 1er août 2007 relative à l'organisation du marché du gaz naturel

Secteur	*Sous-secteur*	*Type d'entités*
		– Exploitants d'installations de raffinage et de traitement de gaz naturel
2. Transports	a) Transport aérien	– Transporteurs aériens au sens de l'article 3, point 4, du règlement (CE) n° 300/2008 du Parlement européen et du Conseil du 11 mars 2008 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile et abrogeant le règlement (CE) no 2320/2002
		– Entités gestionnaires d'aéroports au sens de l'article 2, point 1, de la loi du 23 mai 2012 portant transposition de la directive 2009/12/CE du Parlement européen et du Conseil du 11 mars 2009 sur les redevances aéroportuaires et portant modification: 1) de la loi modifiée du 31 janvier 1948 relative à la réglementation de la navigation aérienne; 2) de la loi modifiée du 19 mai 1999 ayant pour objet a) de réglementer l'accès au marché de l'assistance en escale à l'aéroport de Luxembourg, b) de créer un cadre réglementaire dans le domaine de la sûreté de l'aviation civile, et c) d'instituer une Direction de l'Aviation Civile, aéroports, y compris les aéroports du réseau central énumérés à l'annexe II, section 2, du règlement (UE) n° 1315/2013 du Parlement européen et du Conseil du 11 décembre 2013 sur les orientations de l'Union pour le développement du réseau transeuropéen de transport et abrogeant la décision no 661/2010/UE, et entités exploitant les installations annexes se trouvant dans les aéroports
		– Services du contrôle de la circulation aérienne au sens de l'article 2, point 1, du règlement (CE) n° 549/2004 du Parlement européen et du Conseil du 10 mars 2004 fixant le cadre pour la réalisation du ciel unique européen (« règlement-cadre »)
	b) Transport ferroviaire	– Gestionnaires de l'infrastructure au sens de l'article 2, point 3, de la loi modifiée du 10 mai 1995 relative à la gestion de l'infrastructure ferroviaire
		– Entreprises ferroviaires au sens de l'article 2, point 7, de la loi modifiée du 11 juin 1999 relative à l'accès à l'infrastructure ferroviaire et à son utilisation, y compris les exploitants d'installations de services au sens de l'article 2, point 2, de la loi modifiée du 10 mai 1995 relative à la gestion de l'infrastructure ferroviaire
	c) Transport par voie d'eau	– Sociétés de transport terrestre, maritime et côtier de passagers et de fret au sens de l'annexe I du règlement (CE) n° 725/2004 du Parlement européen et du Conseil du 21 novembre 2012 établissant un espace ferroviaire unique européen, à l'exclusion des navires exploités à titre individuel par ces sociétés
		– Entités gestionnaires des ports au sens de l'article 3, point 1, de la directive 2005/65/CE du Parlement européen et du Conseil du 26 octobre 2005 relative à l'amélioration de la sûreté des ports, y compris les installations portuaires au sens de l'article 2, point 11, du règlement (CE) n° 725/2004, ainsi que les entités exploitant des ateliers et des équipements à l'intérieur des ports
		– Exploitants de services de trafic maritime au sens de l'article 2, lettre o), du règlement grand–ducal modifié du 27 février 2011 relatif à la mise en place d'un système communautaire de suivi du trafic des navires et d'information

Secteur	*Sous-secteur*	*Type d'entités*
	d) Transport routier	– Autorités routières au sens de l'article 2, point 12, du règlement délégué (UE) 2015/962 de la Commission du 18 décembre 2014 complétant la directive 2010/40/UE du Parlement européen et du Conseil en ce qui concerne la mise à disposition, dans l'ensemble de l'Union, de services d'informations en temps réel sur la circulation, chargées du contrôle de gestion du trafic
		– Exploitants de systèmes de transport intelligents au sens de la lettre circulaire du 22 février 2012 concernant la directive 2010/40/UE du Parlement européen et du Conseil du 7 juillet 2010 concernant le cadre pour le déploiement de systèmes de transport intelligents dans le domaine du transport routier et d'interfaces avec d'autres modes de transport
3. Etablissements de crédit		– Etablissements de crédit au sens de l'article 1er, point 12, de la loi modifiée du 5 avril 1993 relative au secteur financier
4. Infrastructures de marchés financiers		– Exploitants de plate-forme de négociation au sens de l'article 4, point 24, de la directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE
		– Contreparties centrales au sens de l'article 2, point 1, du règlement (UE) n° 648/2012 du Parlement européen et du Conseil du 4 juillet 2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux
5. Secteur de la santé	Etablissements de soins de santé (y compris les hôpitaux et les cliniques privées)	– Prestataires de soins de santé au sens de l'article 2, lettre f), de la loi du 24 juillet 2014 relative aux droits et obligations du patient, portant création d'un service national d'information et de médiation dans le domaine de la santé et modifiant: – la loi modifiée du 28 août 1998 sur les établissements hospitaliers; – la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel; – le Code civil
6. Fourniture et distribution d'eau potable		– Fournisseurs et distributeurs d'eaux destinées à la consommation humaine au sens de l'article 3, point 1, lettre a), du règlement grand–ducal modifié du 7 octobre 2002 relatif à la qualité des eaux destinées à la consommation humaine
7. Infrastructures numériques		– IXP
		– Fournisseurs de services DNS
		– Registres de noms de domaines de haut niveau

Impression: CTIE – Division Imprimés et Fournitures de bureau