Member State: Belgium

Loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique

Source: service public federal chancellerie du premier ministre
Numac: 2019011507
Pub: 03/05/2019
Prom: 07/04/2019

Monitor: https://www.ejustice.just.fgov.be/cgi/article_body.pl?language=fr& (...)

SERVICE PUBLIC FEDERAL CHANCELLERIE DU PREMIER MINISTRE

7 AVRIL 2019. - Loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (1)

PHILIPPE, Roi des Belges, A tous, présents et à venir, Salut.La Chambre des représentants a adopté et Nous sanctionnons ce qui suit : TITRE 1er. - Définitions et dispositions générales

CHAPITRE 1er. - Objet et champ d'application

Section 1re. – Objet

Article 1er. La présente loi règle une matière visée à l'article 74 de la Constitution.

Art. 2. La présente loi vise notamment à transposer la Directive européenne (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 dénommée la "directive NIS".

Section 2. - Champ d'application

Art. 3.

§ 1er. La présente loi s'applique aux opérateurs de services essentiels, tels que définis à l'article 6, 11°, ayant au moins un établissement sur le territoire belge et exerçant effectivement une activité liée à la fourniture d'au moins un service essentiel sur le territoire belge. Les dispositions du titre 1er, des articles 13, 14 et 30, ainsi que du chapitre 3 du titre 4 sont applicables aux opérateurs de services essentiels potentiels.

§ 2. La présente loi s'applique aux fournisseurs de service numérique, tels que définis à l'article 6, 21°, dont le siège principal est situé en Belgique. Un fournisseur de service numérique est réputé avoir son siège principal en Belgique lorsque son siège social s'y trouve. La présente loi est également applicable aux fournisseurs de service numérique qui ne disposent pas d'un établissement dans l'Union européenne lorsque ceux-ci fournissent en Belgique des services visés à l'annexe II et qu'ils établissent en Belgique leur représentant pour les besoins de la directive NIS.

Art. 4.

§ 1er. Les exigences en matière de sécurité et de notification prévues par la présente loi ne s'appliquent pas, pour leurs activités de fourniture de réseaux publics de communications électroniques ou de services de communications électroniques accessibles au public, aux entreprises soumises aux exigences énoncées aux articles 114 et 114/1 de la loi du 13 juin 20052 relative aux communications électroniques, et, pour leurs activités de servicesde confiance, aux prestataires de services de confiance soumis aux exigences énoncées à l'article 19 du Règlement européen (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'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, et à condition que les exigences en question aient un effet au moins équivalent à celui des obligations prévues par la présente loi, les dispositions relatives à la sécurité des réseaux et des systèmes d'information et à la notification d'incidents de cet acte peuvent déroger aux dispositions de la présente loi. Le Roi est chargé de préciser les éventuels actes sectoriels équivalents visés à l'alinéa 1er.

§ 3. La présente loi n'est pas applicable aux opérateurs relevant du secteur des finances au sens de l'annexe I de la présente loi, à l'exception des dispositions du titre I, du chapitre 1er du titre II et de l'article 26. Par dérogation à l'alinéa 1er, l'article 52 est applicable aux opérateurs relevant du secteur des finances au sens de l'annexe I de la présente loi, à l'exception des opérateurs de plate-forme de négociation au sens de l'article 3, 6°, de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la Directive 2014/65/UE. Les autorités sectorielles et les opérateurs relevant du secteur des finances au sens de l'annexe I de la présente loi sont soumis aux articles 65 à 73. Par dérogation à ce qui précède, les articles 65 à 73 ne sont pas applicables à l'autorité sectorielle concernée lorsque cette dernière agit dans les hypothèses visées à l'article 46bis de la loi du 2 août 20026 relative à la surveillance du secteur financier et aux services financiers ou à l'article 12quater de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique.

§ 4. La présente loi n'est pas applicable lorsque et dans la mesure où des mesures pour la sécurité des réseaux et des systèmes d'information existent en vertu de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire. Par dérogation à l'alinéa 1er, la présente loi est applicable aux éléments d'une installation nucléaire destinée à la production industrielle d'électricité et qui servent au transport de l'électricité.

Art. 5. § 1er. Sous réserve des dispositions du titre 6, la présente loi ne porte pas préjudice à l'application du Règlement UE 2016/679, ni aux dispositions légales et réglementaires qui complètent ou précisent ledit règlement.

§ 2. La présente loi ne porte pas préjudice à l'application de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques, des articles 259bis, 314bis, 380, 382quinquies, 383bis, 383bis/1, 433septies, 433novies/1, 458bis, 550bis et 550ter du Code pénal, ou d'autres dispositions du droit belge transposant la Directive 2011/92/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil, ainsi que la Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil.

§ 3. La présente loi ne porte pas préjudice aux règles applicables au traitement des informations, documents ou données, au matériel, aux matériaux ou matières, sous quelque forme que ce soit, qui sont classifiés en application de la loi du 11 décembre 19984 relative à la classification et aux habilitations, attestations et avis de sécurité.

§ 4. La présente loi ne porte pas préjudice aux règles applicables aux documents nucléaires, au sens de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire.

CHAPITRE 2. - Définitions

Art. 6. Pour l'application de la présente loi, il faut entendre par:

(1) "CSIRT national" : le centre national de réponse aux incidents de sécurité informatique, désigné par le Roi ;

(2) "autorité sectorielle" : l'autorité publique désignée par la loi ou par le Roi par arrêté délibéré en Conseil des ministres ;

(3) "CSIRT sectoriel" : le centre sectoriel de réponse aux incidents de sécurité informatique, désigné par le Roi ;

(4) "autorité de contrôle des données à caractère personnel" : autorité de contrôle au sens de l'article 4, 21°, du Règlement UE 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) ;

(5) "organisme d'évaluation de la conformité" : organisme visé à l'article I.9.7° du Code de droit économique ;

(6) "audit de certification" : un audit réalisé dans le cadre d'une certification visée à l'article 22, § 2 ;

(7) "autorité nationale d'accréditation" : organisme créé par le Roi en exécution de l'article VIII.30 du Code de droit économique ;

(8) "réseau et système d'information" :
a) un réseau de communications électroniques au sens de l'article 2, 3°, de la loi du 13 juin 20052 relative aux communications électroniques ;
b) tout dispositif, tout ensemble de dispositifs interconnectés ou apparentés, de manière permanente ou temporaire, dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques, en ce compris les composants numériques, électroniques ou mécaniques de ce dispositif permettant notamment l'automatisation du processus opérationnel, le contrôle à distance, ou l'obtention de données de fonctionnement en temps réel ;
c) ou les données numériques stockées, traitées, récupérées ou transmises par les éléments visés aux points a) et b), en vue de leur fonctionnement, utilisation, protection et maintenance ;

(9) "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 ;

(10) "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 ;

(11) "opérateur de services essentiels" : une entité publique ou privée active en Belgique dans l'un des secteurs repris à l'annexe I de la présente loi, qui répond aux critères visés à l'article 12, § 1er, et qui est désignée comme telle par l'autorité sectorielle ;

(12) "incident" : tout événement ayant un impact négatif réel sur la sécurité des réseaux et des systèmes d'information ;

(13) "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 ;

(14) "risque" : toute circonstance ou tout événement raisonnablement identifiable ayant un impact négatif potentiel sur la sécurité des réseaux et des systèmes d'information ;

(15) "critère intersectoriel" : facteur commun à tous les secteurs visés à l'annexe I de la présente loi et déterminant l'importance d'un effet perturbateur sur la fourniture d'un service essentiel au sens de l'article 12, § 1er, c) ;

(16) "critère sectoriel" : facteur propre à un secteur ou sous-secteur visé à l'annexe I de la présente loi et déterminant l'importance d'un effet perturbateur sur la fourniture d'un service essentiel au sens de l'article 12, § 1er, c) ;

(17) "politique de sécurité des systèmes et réseaux d'information (P.S.I.)" : un document visé à l'article 21, § 1er, reprenant les mesures de sécurité des réseaux et des systèmes d'information adoptées par un opérateur de services essentiels ;

(18) "point de contact pour la sécurité des systèmes et réseaux d'information" : le point de contact désigné par l'opérateur de services essentiels ou le fournisseur de service numérique et qui exerce la fonction de point de contact vis-à-vis des autorités visées à l'article 7 pour toute question liée à la sécurité des réseaux et des systèmes d'information dont sont tributaires les services essentiels fournis.

(19) "service numérique" : un service au sens de l'article 1er, paragraphe 1er, point b), de la directive européenne 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information et dont le type figure dans la liste de l'annexe II ;

(20) "fournisseur de service numérique" : une personne morale qui fournit un service numérique visé à l'annexe II de la présente loi ;

(21) "représentant d'un fournisseur de service numérique" : une personne physique ou morale établie en Belgique qui est expressément désignée pour agir pour le compte d'un fournisseur de service numérique non établi dans l'Union, qui peut être contactée par l'autorité nationale visée à l'article 7, § 1er, par l'autorité sectorielle ou par le service d'inspection compétent à la place du fournisseur de service numérique concernant ses obligations découlant de la présente loi ;

(22) "point d'échange internet (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 point d'échange internet n'assure l'interconnexion que pour des systèmes autonomes; un point d'échange internet n'exige pas que le trafic internet passant entre deux systèmes autonomes participants transite par un système autonome tiers, pas plus qu'il ne modifie ou n'altère par ailleurs un tel trafic ;

(23) "système de noms de domaine" ou "DNS" : un système hiérarchique et distribué d'affectation de noms dans un réseau qui résout les questions liées aux noms de domaines ;

(24) "fournisseur de services DNS" : une entité qui fournit des services DNS sur l'internet ;

(25) "registre de noms de domaine de haut niveau" : une entité qui enregistre et gère les noms de domaine internet dans un domaine de haut niveau donné ;

(26) "place de marché en ligne" : un service numérique qui permet à des consommateurs au sens de l'article I.1., alinéa 1er, 2°, du Code de droit économique et/ou à des entreprises, au sens de l'article I.8, 39°, du même Code, de conclure des contrats de vente ou de service en ligne avec des entreprises, soit sur le site internet de la place de marché en ligne, soit sur le site internet d'une entreprise qui utilise les services informatiques fournis par la place de marché en ligne ;

(27) "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 ;

(28) "service d'informatique en nuage" : un service numérique qui permet l'accès à un ensemble modulable et variable de ressources informatiques pouvant être partagées ;

(29) " loi du 1er juillet 2011" : la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques ;

(30) " loi du 11 décembre 19984" : la loi du 11 décembre 19984 relative à la classification et aux habilitations, attestations et avis de sécurité ;

(31) " loi du 15 avril 1994" : la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire ;

(32) "Règlement UE 2016/679" : le Règlement européen 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la Directive 95/46/CE (règlement général sur la protection des données).

CHAPITRE 3. - Autorités compétentes et coopération au niveau national

Section 1re. - Autorités compétentes

Art. 7. § 1er. Le Roi désigne l'autorité chargée, au titre d'autorité nationale, du suivi et de la coordination de la mise en oeuvre de la présente loi. L'autorité visée à l'alinéa 1er est également le point de contact national unique en matière desécurité des réseaux et des systèmes d'information, pour l'ensemble des opérateurs de services essentiels et des fournisseurs de services numériques, pour la Belgique dans ses relations avec la Commission européenne, les Etats membres de l'Union européenne, le Groupe de coopération visé à l'article 11 de la directive NIS et le réseau des CSIRT. A cette fin, le point de contact représente la Belgique au sein du Groupe de coopération.

§ 2. Le Roi désigne l'autorité chargée d'assurer le rôle de CSIRT national. Le CSIRT national représente la Belgique au sein du réseau des CSIRT visé à l'article 12 de la directive NIS. Il coopère de manière effective, efficace et sécurisée aux missions du réseau des CSIRT.

§ 3. Le Roi désigne, par arrêté délibéré en Conseil des ministres, les autorités sectorielles chargées, pour leur secteur respectif, de veiller à la mise en oeuvre des dispositions de la présente loi. Le Roi peut créer des autorités sectorielles, composées de représentants de l'Etat fédéral, des Communautés et des Régions, conformément aux modalités prévues à l'article 92ter de la loi spéciale du 8 août 1980 de réformes institutionnelles. Par dérogation à l'alinéa 1er, la loi désigne elle-même les autorités sectorielles créés et régies par la loi.

§ 4. Le Roi désigne l'autorité chargée, en coopération avec l'autorité nationale visée au paragraphe 1er, de coordonner l'identification des opérateurs de services essentiels.

§ 5. Un service d'inspection par secteur, ou, le cas échéant, par sous-secteur, est mis en place, chargé du contrôle du respect des dispositions de la présente loi et de ses actes d'exécution par les opérateurs de services essentiels ou par les fournisseurs de service numérique.

Le Roi désigne, pour un secteur déterminé ou, le cas échéant, par sous-secteur, le service d'inspection compétent pour effectuer le contrôle.

Par dérogation à l'alinéa 2, la loi désigne les services d'inspection créés et régis par elle.

Section 2. - Coopération au niveau national

Art. 8. § 1er. Les autorités visées à l'article 7 coopèrent étroitement aux fins du respect des obligations énoncées dans la présente loi.

§ 2. En fonction des besoins nécessaires à l'exécution de la loi et conformément aux dispositions légales applicables, les autorités visées au paragraphe 1er coopèrent également, au niveau national, avec les services administratifs de l'Etat, les autorités administratives, les autorités judiciaires, les services de renseignement et de sécurité visés par la loi du 30 novembre 19983 organique des services de renseignement et de sécurité, les services de police visés par la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux et avec les autorités de contrôle des données à caractère personnel.

§ 3. L'opérateur de services essentiels, le fournisseur de service numérique et les autorités visées à l'article 7 collaborent en tout temps, par un échange adéquat d'informations concernant la sécurité des systèmes et réseaux d'informations.

CHAPITRE 4. - Echanges d'information

Art. 9. § 1er. Le présent article ne porte pas préjudice à l'application de la loi du 11 décembre 19984, de la loi du 15 avril 1994, de la loi du 11 avril 1994 relative à la publicité de l'administration ou d'autres dispositions légales garantissant la confidentialité des informations liées aux intérêts essentiels de la sécurité publique nationale.

Les autorités visées à l'article 7, l'opérateur de services essentiels, le fournisseur de service numérique, ou leurs sous-traitants limitent l'accès aux informations relatives à l'exécution de la présente loi aux personnes ayant besoin d'en connaître et d'y avoir accès pour l'exercice de leurs fonctions ou de leur mission en lien avec la présente loi.

§ 2. Les membres du personnel de l'opérateur de services essentiels, le fournisseur de service numérique, ou leurs sous-traitants sont tenus au secret professionnel en ce qui concerne les informations en rapport à l'exécution de la présente loi.

Les personnes dépositaires, par état ou par profession, des secrets qu'on leur confie sont autorisés à faire connaître ces secrets pour l'exécution de la présente loi.

§ 3. Les informations fournies aux autorités visées à l'article 7 par les opérateurs de services essentiels et les fournisseurs de service numérique, peuvent être échangées avec des autorités de l'Union européenne, avec des autorités belges ou étrangères, lorsque cet échange est nécessaire à l'application de dispositions légales.

Les informations échangées se limitent à ce qui est pertinent et sont proportionnées à l'objectif de cet échange, notamment dans le respect du Règlement UE 2016/679. Cet échange d'informations préserve la confidentialité des informations concernées et protège la sécurité et les intérêts commerciaux des opérateurs de services essentiels et des fournisseurs de service numérique.

CHAPITRE 5. - Stratégie nationale en matière de sécurité des réseaux et des systèmes d'information

Art. 10. § 1er. Le Roi désigne, par arrêté délibéré en Conseil des ministres, l'autorité chargée de maintenir à jour la stratégie nationale existante en matière de sécurité des réseaux et des systèmes d'information.

§ 2. La stratégie visée au paragraphe 1er est mise à jour, après avis des autorités visées à l'article 7 et, le cas échéant, des autorités de contrôle des données à caractère personnel. Elle couvre au moins les secteurs visés à l'annexe I et les services visés à l'annexe II. Cette stratégie définit les objectifs stratégiques et réglementaires appropriées en vue de parvenir à un niveau élevé de sécurité des réseaux et des systèmes d'information et de le maintenir.

§ 3. La stratégie nationale en matière de sécurité des réseaux et des systèmes d'information porte, entre autres, 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 tâches et les responsabilités des organismes publics et des autres acteurs concernés ;
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.

TITRE 2. - Réseaux et systèmes d'information des opérateurs de services essentiels

CHAPITRE 1er. - Identification des opérateurs de services essentiels

Art. 11. § 1er. L'autorité sectorielle identifie les opérateurs de services essentiels de son secteur, en prenant au minimum en compte les types d'opérateurs qui figurent à l'annexe I de la présente loi. Dans les limites de leurs compétences respectives, les autorités visées à l'article 7, §§ 1er et 4, se concertent avec l'autorité sectorielle pour procéder à cette identification. L'autorité sectorielle consulte, le cas échéant, les régions ou les communautés concernées, et les représentants des entités visées à l'annexe I.

§ 2. Après consultation de l'opérateur de services essentiels potentiel, l'autorité sectorielle lui précise le ou les services désignés comme essentiels parmi les différents services qu'il fournit.

§ 3. L'autorité sectorielle assure le suivi permanent du processus d'identification et de désignation des opérateurs de services essentiels et de leurs services essentiels, selon les procédures décrites au présent chapitre, ce processus étant effectué pour la première fois, au plus tard dans les six mois de l'entrée en vigueur de la présente loi. L'autorité sectorielle évalue et, le cas échéant, met à jour l'identification des opérateurs de services essentiels et de leurs services essentiels au moins tous les deux ans. Les actualisations sont adressées aux autorités visées à l'article 7, §§ 1er et 4.

Art. 12. § 1er. Pour identifier les opérateurs visés à l'article 11, l'autorité sectorielle applique les critères suivants :
a) l'entité fournit un service qui est essentiel au maintien d'activités sociétales et/ou économiques critiques ;
b) la fourniture de ce service est tributaire des réseaux et des systèmes d'information ;et
c) un incident serait susceptible d'avoir un effet perturbateur important sur la fourniture dudit service, en tenant compte des critères et des niveaux d'incidence ou seuils visés à l'article 13.

§ 2. Sauf preuve contraire, la fourniture d'un service essentiel est présumée être tributaire des réseaux et systèmes d'information.

Art. 13. § 1er. Afin de déterminer l'importance de l'effet perturbateur visé à l'article 12, § 1er, c), l'autorité sectorielle établit, pour son secteur, des critères sectoriels et/ou intersectoriels, des niveaux d'incidence ou des seuils. L'effet perturbateur important est établi dès que l'opérateur de services essentiels potentiel répond soit à un seuil soit à un niveau d'incidence. Dans les limites de leurs compétences respectives, les autorités visées à l'article 7, §§ 1er et 4, se concertent avec l'autorité sectorielle pour déterminer les critères, les niveaux d'incidence et les seuils, le cas échéant, après consultation des régions ou des communautés concernées et des représentants des entités visées à l'annexe I.

§ 2. L'autorité sectorielle prend au moins en compte les critères intersectoriels suivants, à partir des informations disponibles :

a) le nombre d'utilisateurs tributaires du service fourni par l'entité concernée ;

b) la dépendance des autres secteurs visés à l'annexe I à l'égard du service fourni par cette entité ;

c) les conséquences que des incidents pourraient avoir, en termes de degré et de durée, sur les fonctions économiques ou sociétales ou sur la sécurité publique ;

d) la part de marché de cette entité ;

e) l'ampleur de la zone géographique susceptible d'être touchée par un incident ;

f) 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. Après avis des autorités visées à l'article 7, consultation des régions et des communautés concernées, le Roi peut compléter ces critères intersectoriels.

Art. 14. L'opérateur de services essentiels potentiel transmet à la demande d'une autorité visée à l'article 7, toutes les informations utiles quant à son éventuelle identification en tant qu'opérateur de services essentiels, en ce compris celles permettant d'objectiver la dépendance ou non de la fourniture du service essentiel aux réseaux et systèmes de l'information. Les informations pertinentes transmises par l'opérateur potentiel sont portées à la connaissance des autres autorités visées à l'article 7.

Art. 15.

§ 1er. L'autorité sectorielle communique aux autorités visées à l'article 7, §§ 1er et 4, une proposition motivée de liste des opérateurs de services essentiels de son secteur avec le ou les critères d'identification retenus. Lorsqu'elle n'a proposé aucun opérateur de services essentiels au sein d'un secteur ou d'un sous-secteur, l'autorité sectorielle en expose par écrit les raisons. Les autorités visées à l'article 7, §§ 1er et 4, dans les limites de leurs compétences respectives, rendent un avis sur la proposition motivée de liste, le cas échéant après consultation des régions et des communautés.

§ 2. Lorsque l'autorité sectorielle constate que l'entité qu'elle envisage de désigner comme opérateur de services essentiels fournit un ou des services essentiels dans au moins un autre Etat membre de l'Union européenne, elle en informe les autorités visées à l'article 7, §§ 1er et 4. Ces derniers, en collaboration avec les autorités sectorielles concernées, organisent les discussions avec la ou les autorités nationales étrangères concernées et, le cas échéant, avec les régions ou les communautés concernées.

§ 3. L'autorité sectorielle notifie à l'opérateur sa décision motivée de désignation en qualité d'opérateur de services essentiels. Cette notification est réalisée de manière sécurisée. Elle communique également copie de cette décision aux autorités visées à l'article 7, §§ 1er et 4. L'autorité sectorielle en informe, le cas échéant, les régions et/ou les communautés concernées.

Art. 16. Dans les trois mois de sa désignation, l'opérateur de services essentiels transmet à l'autorité sectorielle un descriptif des réseaux et des systèmes d'information dont la fourniture du ou des services essentiels concernés est tributaire. L'autorité sectorielle communique ce descriptif à l'autorité visée à l'article 7, § 1er.

Art. 17. Sans préjudice de l'application éventuelle de la loi du 11 décembre 1998 4, les documents administratifs liés à l'application du présent chapitre, sont considérés comme des documents administratifs liés à la sécurité de la population, à l'ordre public et la sûreté, au sens de l'article 6, § 1er, de la loi du 11 avril 1994 relative à la publicité de l'administration, qui ne peuvent être consultés, faire l'objet d'explications ou être communiqués sous forme de copie pour le public.

Art. 18.

§ 1er. Par dérogation à l'article 11, l'autorité sectorielle désigne les exploitants d'infrastructures critiques, telles que désignées en vertu de l'article 8 de la loi du 1er juillet 2011 et de l'article 6 de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien, comme des opérateurs de services essentiels lorsque leur secteur est repris dans l'annexe I de la présente loi et que la fourniture des services essentiels qu'ils délivrent est tributaire des réseaux et des systèmes d'information. Cette désignation se fait en concertation avec les autorités visées à l'article 7, §§ 1er et 4, dans les limites de leurs compétences respectives.

§ 2. Sauf preuve contraire, l'exploitation d'une infrastructure critique est présumée être tributaire des réseaux et systèmes d'information.

§ 3. L'exploitant transmet à l'autorité sectorielle, à la demande de celle-ci ou des autorités visées à l'article 7, §§ 1er et 4, toutes les informations utiles quant à son éventuelle identification en tant qu'opérateur de services essentiels, en ce compris celles permettant d'objectiver sa dépendance ou non aux réseaux et systèmes de l'information. Les informations pertinentes transmises par l'exploitant sont communiquées par l'autorité sectorielle aux autorités visées à l'article 7, §§ 1er et 4.

§ 4. L'article 15, § 3, est applicable à la décision motivée de désignation d'un exploitant d'une infrastructure critique en qualité d'opérateur de services essentiels.

Art. 19.Le Roi peut, par arrêté délibéré en Conseil des ministres, ajouter d'autres secteurs ou types d'opérateurs à l'annexe I de la présente loi.

CHAPITRE 2. - Mesures de sécurité

Art. 20. L'opérateur de services essentiels prend les mesures techniques et organisationnelles nécessaires et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information dont sont tributaires ses services essentiels. Ces mesures garantissent, pour les réseaux et les systèmes d'information, un niveau de sécurité physique et logique adapté aux risques existants, compte tenu de l'état des connaissances techniques. L'opérateur prend également les 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.

Art. 21.

§ 1er. L'opérateur de services essentiels élabore une politique de sécurité de ses systèmes et réseaux d'information (ci-après dénommé "P.S.I.") reprenant au moins les objectifs et les mesures de sécurité concrètes, visés à l'article 20.

§ 2. L'opérateur de services essentiels élabore sa P.S.I. au plus tard dans un délai de douze mois à dater de la notification de sa désignation. Dans un délai de vingt-quatre mois au plus tard à dater de la notification de sa désignation, il met en oeuvre les mesures prévues dans sa P.S.I. Pour un secteur déterminé ou le cas échéant par sous-secteur, l'autorité sectorielle compétente peut moduler ce délai en fonction du type de mesures prévues dans la P.S.I.

§ 3. Après avis des autorités visées à l'article 7 et, le cas échéant, après consultation des régions ou des communautés concernées, le Roi peut imposer certaines mesures de sécurité applicables aux opérateurs de services essentiels d'un ou plusieurs secteurs.

§ 4. L'autorité sectorielle, en concertation avec l'autorité visée à l'article 7, § 1er, et, le cas échéant, après consultation des régions ou des communautés, peut, par décision administrative individuelle, imposer des mesures complémentaires de sécurité.

§ 5. Les mesures de sécurité physique et logique des réseaux et systèmes d'information contenues dans le plan de sécurité de l'exploitant (P.S.E.) visé à l'article 13 de la loi du 1er juillet 2011 et à l'article 11 de l'arrêté royal du 2

décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien sont assimilées à la P.S.I. lorsque toutes les informations visées au paragraphe 2 y sont reprises.

Art. 22.

§ 1er. La P.S.I. visée à l'article 21, § 1er, est, jusqu'à preuve du contraire, présumée conforme aux exigences de sécurité, visées à l'article 20, lorsque les mesures de sécurité qu'elle comporte répondent aux exigences de la norme ISO/IEC 27001 ou à une norme nationale, étrangère ou internationale reconnue équivalente par le Roi, par arrêté délibéré en Conseil des ministres. L'arrêté visé à l'alinéa 1er est pris après avis de l'autorité nationale d'accréditation, de l'autorité sectorielle et de l'autorité visée à l'article 7, § 1er.

§ 2. Le respect des exigences visées au paragraphe 1er est établi par un certificat délivré par un organisme d'évaluation de la conformité accrédité selon la norme ISO/IEC 17021 ou ISO/IEC 17065 par l'autorité nationale d'accréditation ou par une institution qui est co-signataire des accords de reconnaissance du "European Cooperation for Accreditation". Le certificat délivré doit relever du domaine de certification pour lequel l'organisme d'évaluation de la conformité a été accrédité et porter sur l'ensemble du contenu de la P.S.I.

Art. 23.

§ 1er. L'opérateur de services essentiels désigne son point de contact pour la sécurité des systèmes et réseaux d'information et en communique les données à l'autorité sectorielle compétente dans un délai de trois mois à dater de la notification de la désignation comme opérateur de services essentiels, et, sans délai, après chaque mise à jour de ces données. L'autorité sectorielle met ces données à disposition des autorités visées à l'article 7, §§ 1er, et 4.

§ 2. Lorsqu'il existe déjà un point de contact pour la sécurité en vertu de dispositions nationales ou internationales applicables dans un secteur ou un sous-secteur, l'opérateur de services essentiels en communique les coordonnées à l'autorité sectorielle dans les délais visés au paragraphe 1er.

§ 3. Le point de contact pour la sécurité des systèmes et réseaux d'information visé au paragraphe 1er est disponible à tout moment.

CHAPITRE 3. - Notification d'incidents

Art. 24.

§ 1er. L'opérateur de services essentiels notifie, sans retard, tous les incidents ayant un impact significatif sur la disponibilité, la confidentialité, l'intégrité ou l'authenticité des réseaux et des systèmes d'information dont sont tributaires le ou les services essentiels qu'il fournit.

§ 2. Après avis du CSIRT national, de l'autorité visée à l'article 7, § 4, de l'autorité sectorielle et, le cas échéant, des régions ou des communautés concernées, le Roi peut établir des niveaux d'incidence et/ou des seuils, par secteur ou sous-secteur, constituant au minimum un impact significatif au sens du § 1er.

§ 3. En l'absence de niveaux d'incidence et/ou de seuils visés au paragraphe 2, l'opérateur notifie tous les incidents ayant un impact sur la disponibilité, la confidentialité, l'intégrité ou l'authenticité des réseaux et des systèmes d'information dont sont tributaires le ou les services essentiels qu'il fournit.

§ 4. Le Roi peut créer différentes catégories de notification en fonction du degré d'impact de l'incident.

Art. 25. La notification visée à l'article 24 est faite simultanément au CSIRT national, à l'autorité sectorielle ou à son CSIRT sectoriel, et à l'autorité visée à l'article 7, § 4. L'obligation de notification s'applique même si l'opérateur de services essentiels ne dispose que d'une partie des informations pertinentes pour évaluer le caractère significatif de l'impact de l'incident.

Art. 26.

§ 1er. Le présent chapitre s'applique aux opérateurs de plate-forme de négociation au sens de l'article 3, 6°, de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la Directive 2014/65/UE.

§ 2. Les opérateurs relevant du secteur des finances au sens de l'annexe I de la loi, à l'exception des opérateurs de plate-forme de négociation, notifient à la Banque nationale de Belgique (BNB), sans retard, tous les incidents ayant un impact significatif sur la disponibilité, la confidentialité, l'intégrité ou l'authenticité des réseaux et des systèmes d'information dont sont tributaires le ou les services essentiels qu'ils fournissent. La Banque nationale de Belgique détermine l'impact significatif visé par cet alinéa. La BNB transmet alors la notification, sans retard, au CSIRT national et à l'autorité visée à l'article 7, § 4.

Art. 27. L'entreprise qui fournit un service numérique à un opérateur de services essentiels et qui est soumise à la présente loi lui notifie, sans retard, tous les incidents ayant un impact significatif, au sens de l'article 24, sur la continuité des services essentiels de ce dernier. L'opérateur de services essentiels notifie ensuite cet incident, selon les procédures décrites au présent chapitre.

Art. 28.

§ 1er. Lorsqu'un opérateur de services essentiels est touché par un incident ayant un impact significatif au sens de l'article 24, ce dernier est obligé de gérer l'incident et de prendre les mesures réactives afin de le résoudre. La gestion de l'incident demeure de la responsabilité de l'opérateur de services essentiels.

§ 2. L'opérateur de services essentiels examine les incidents ou évènements suspects qui lui sont notifiés par le CSIRT national, l'autorité sectorielle ou l'autorité visée à l'article 7, § 4.

Art. 29. Sur la base des informations fournies dans la notification de l'opérateur de services essentiels, le CSIRT national signale aux autres Etats membres de l'Union européenne touchés, si l'incident a un impact significatif sur la continuité des services essentiels dans ces Etats membres. Ce faisant, le CSIRT national préserve, dans le respect du droit de l'Union ou de la législation nationale conforme au droit de l'Union, la sécurité et les intérêts commerciaux de l'opérateur de services essentiels ainsi que la confidentialité des informations communiquées dans sa notification. Le CSIRT national transmet les notifications visées à l'alinéa 1er aux points de contact uniques des autres Etats membres touchés.

Art. 30.

§ 1er. Les opérateurs de services essentiels potentiels peuvent notifier, à titre volontaire, les incidents ayant un impact significatif sur la continuité des services qu'elles fournissent. 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 si elle n'avait pas procédé à ladite notification.

§ 2. Lors du traitement des notifications, le CSIRT national, l'autorité sectorielle ou son CSIRT sectoriel, et l'autorité visée à l'article 7, § 4, peuvent donner la priorité aux notifications obligatoires imposées par la présente loi par rapport aux notifications Les notifications volontaires ne sont traitées que lorsque leur traitement ne fait pas peser de charge disproportionnée ou inutile à charge du CSIRT national, de l'autorité sectorielle ou de son CSIRT sectoriel, et de l'autorité visée à l'article 7, § 4.

Art. 31.

§ 1er. Le Roi est chargé de déterminer les modalités de notification et de rapportage des incidents, et de créer une plate-forme sécurisée de notification. Cette plate-forme peut permettre également aux opérateurs de services essentiels de notifier aux autorités de contrôle les violations de données à caractère personnel, comme imposé par l'article 33, alinéa 1er, du Règlement UE 2016/679.

§ 2. Après avoir consulté l'opérateur qui est à l'origine de la notification et l'autorité sectorielle compétente, le CSIRT national peut informer le public concernant des incidents particuliers, lorsque la sensibilisation du public est nécessaire pour prévenir un incident ou gérer un incident en cours. Cette information concerne uniquement des informations générales sur l'incident.

TITRE 3. - Réseaux et systèmes d'information des fournisseurs de service numérique

CHAPITRE 1er. - Champ d'application

Art. 32. Le présent titre ne s'applique pas aux micro et petites entreprises telles qu'elles sont définies dans la recommandation de la Commission européenne du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises (2003/361/CE).

CHAPITRE 2. - Les exigences de sécurité

Art. 33.

§ 1er. 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, les services visés à l'annexe II et prennent les mesures techniques et organisationnelles nécessaires et proportionnées pour les gérer. Ces mesures garantissent, compte tenu de l'état des connaissances techniques, un niveau de sécurité des réseaux et des systèmes d'information adapté au risque existant et prennent en considération les éléments suivants :

a) la sécurité des systèmes et des installations ;

b) la gestion des incidents ;

c) la gestion de la continuité des activités ;

d) le suivi, l'audit et le contrôle ;

e) le respect des normes internationales.

§ 2. Les fournisseurs de service numérique prennent également 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 visés à l'annexe II de la présente loi qui sont offerts dans l'Union européenne, de manière à garantir la continuité de ces services.

Art. 34. Les fournisseurs de service numérique renseignent un point de contact pour la sécurité informatique et en communiquent les données à l'autorité sectorielle compétente pour les fournisseurs de services numériques, ainsi qu'après chaque mise à jour de ces données. L'autorité sectorielle communique ces informations à l'autorité nationale visée à l'article 7, § 1er.

CHAPITRE 3. - Notification d'incidents

Art. 35.

§ 1er. Les fournisseurs de service numérique notifient, sans retard, tout incident ayant un impact significatif sur la fourniture d'un service visé à l'annexe II qu'ils offrent dans l'Union européenne. La notification est faite simultanément au CSIRT national, à l'autorité sectorielle ou à son CSIRT sectoriel et à l'autorité visée à l'article 7, § 4, via la plate-forme de notification visée à l'article 31.

§ 2. La notification se fait conformément aux règlements d'exécution de la Commission européenne, dont celui du 30 janvier 2018 2018/151 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. Les notifications contiennent les informations permettant 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.

§ 3. L'obligation de notifier un incident ne s'applique que lorsque le fournisseur de service numérique a accès aux informations nécessaires pour évaluer, complètement ou partiellement, l'impact de l'incident.

Art. 36.

§ 1er. Cette notification est réalisée conformément aux modalités prévues par le Roi et via la plate-forme visée à l'article 31.

§ 2. La plate-forme visée à l'article 31 peut permettre également aux fournisseurs de service numérique de notifier aux autorités de contrôle les violations de données à caractère personnel, comme imposé par l'article 33, alinéa 1er, du Règlement UE 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Art. 37.

§ 1er. Le cas échéant, et notamment si l'incident visé à l'article 35, paragraphe 1er concerne au moins un autre Etat membre de l'Union européenne, le CSIRT national informe le ou les autres Etats membres touchés. Ce faisant, le CSIRT national doit, dans le respect du droit national et de l'Union, préserver la sécurité et les intérêts commerciaux du fournisseur de service numérique ainsi que la confidentialité des informations communiquées.

§ 2. Après avoir consulté le fournisseur de service numérique concerné, l'autorité sectorielle et, le cas échéant, les autorités ou les CSIRT des autres Etats membres de l'Union européenne concernés, le CSIRT national peut informer le public d'incidents particuliers ou imposer au fournisseur de service numérique de le faire. Cette information peut notamment s'avérer nécessaire lorsque la sensibilisation du public permettrait de prévenir un incident ou de gérer un incident en cours ou lorsque la divulgation de l'incident est dans l'intérêt public à d'autres égards.

TITRE 4. - Contrôle et sanctions

CHAPITRE 1er. - Les contrôles des opérateurs de services essentiels

Section 1re. - Audits

Art. 38.

§ 1er. L'opérateur de services essentiels réalise, chaque année et à ses frais, un audit interne des réseaux et systèmes d'information dont sont tributaires les services essentiels qu'il fournit. Cet audit interne doit permettre à l'opérateur de services essentiels de s'assurer que les mesures et les processus définis dans sa P.S.I. sont bien appliqués et font l'objet de contrôles réguliers. L'opérateur de services essentiels transmet les rapports d'audit interne, dans les trente jours, à l'autorité sectorielle.

§ 2. L'opérateur de services essentiels fait réaliser, au moins tous les trois ans et à ses frais, un audit externe réalisé par un organisme d'évaluation de la conformité accrédité par l'autorité nationale d'accréditation, ou par une institution qui est co-signataire des accords de reconnaissance du "European Cooperation for Accreditation". L'opérateur de services essentiels transmet les rapports d'audit externe, dans les trente jours, à l'autorité sectorielle.

§ 3. Au plus tard dans les trois mois de l'élaboration de sa P.S.I., l'opérateur de services essentiels réalise son premier audit interne. Au plus tard vingt-quatre mois après la réalisation de son premier audit interne, l'opérateur de services essentiels réalise son premier audit externe.

Art. 39.

§ 1er. Après avis de l'autorité sectorielle et de l'autorité visée à l'article 7, § 1er, le Roi fixe : 1° les conditions générales d'accréditation sur base des exigences des normes ISO/IEC 17021 ou ISO/IEC 17065 ;2° les exigences supplémentaires

sectorielles auxquelles peut être soumis l'organisme d'évaluation de la conformité ;3° les règles applicables à l'audit interne ;4° les règles applicables à l'audit externe.

§ 2. Par arrêté délibéré en Conseil des ministres, le Roi peut également déterminer, après avis de l'autorité sectorielle et de l'autorité visée à l'article 7, § 1er, les conditions d'un éventuel agrément accordé par l'autorité sectorielle à un organisme d'évaluation de la conformité.

§ 3. La liste des organismes d'évaluation de la conformité accrédités ou agréés est disponible auprès de l'autorité sectorielle qui la tient à jour.

Art. 40.

§ 1er. Les audits de certification peuvent être assimilés, par le service d'inspection ou l'autorité sectorielle, à l'audit interne annuel obligatoire visé au 39, § 1er. Les rapports de ces audits sont transmis, par l'opérateur de services essentiels, dans les trente jours, à l'autorité sectorielle.

§ 2. Les audits de certification peuvent être assimilés, par le service d'inspection ou l'autorité sectorielle, à l'audit externe obligatoire visé à l'article 39, § 2. Les rapports de ces audits sont transmis, dans les trente jours, par l'opérateur de services essentiels, à l'autorité sectorielle.

Art. 41. L'autorité visée à l'article 7, § 1er, peut solliciter, de manière motivée, de l'autorité sectorielle ou du service d'inspection la transmission des rapports de certification ou d'audits d'un opérateur de services essentiels.

Section 2. - Service d'inspection

Art. 42.

§ 1er. Les services d'inspection peuvent à tout moment réaliser des contrôles du respect par l'opérateur de services essentiels des mesures de sécurité et des règles de notification des incidents.

§ 2. L'autorité visée à l'article 7, § 1er, ou l'autorité sectorielle peut recommander, de manière motivée, au service d'inspection de réaliser des contrôles. Après avis de l'autorité sectorielle et de l'autorité visée à l'article 7, § 1er, le Roi peut fixer les éventuelles modalités sectorielles pratiques du contrôle.

§ 3. Au moment de formuler une demande d'informations ou de preuves, le service d'inspection mentionne la finalité de la demande et précise le délai dans lequel les informations ou preuves doivent être fournies. Le service d'inspection peut faire appel à des experts.

Art. 43. Lorsque les réseaux et les systèmes d'information d'un opérateur de services essentiels sont situés en dehors du territoire belge, le service d'inspection, en concertation avec l'autorité visée à l'article 7, § 1er, peut solliciter la coopération et l'assistance des autorités de contrôle compétentes de ces autres Etats. Cette assistance et cette coopération peuvent porter sur des échanges d'informations et sur des demandes de prise de mesures de contrôle.

Art. 44.

§ 1er. Les membres du service d'inspection sont dotés d'une carte de légitimation dont le modèle est fixé par le Roi, par secteur, ou, le cas échéant, par sous-secteur.

§ 2. Les membres du service d'inspection ou les experts appelés à participer à l'inspection ne peuvent avoir un intérêt quelconque, direct ou indirect, dans les entreprises ou institutions qu'ils sont chargés de contrôler, susceptible de compromettre leur objectivité. Ils prêtent serment auprès du fonctionnaire dirigeant de leur service.

§ 3. Sans préjudice des attributions des officiers de police judiciaire visées à l'article 8 du Code d'instruction criminelle, les membres assermentés du service d'inspection disposent, à tout moment, des compétences de contrôle suivantes dans l'exercice de leur mission, tant dans le cadre de démarches administratives, que dans le cadre de la constatation d'infractions par procès-verbal :

1° pénétrer sans avertissement préalable, sur présentation de leur carte de légitimation, dans tous les lieux utilisés par l'opérateur de services essentiels ;ils n'ont accès aux locaux habités que moyennant autorisation préalable délivrée par le juge d'instruction ;

2° prendre connaissance sur place et obtenir une copie de la P.S.I., des rapports d'audits, de tout acte, tout document et toute autre source d'informations nécessaires à l'exercice de leur mission ;

3° procéder à tout examen, contrôle et audition, et requérir toutes les informations qu'ils estiment nécessaires à l'exercice de leur mission ;

4° prendre l'identité des personnes qui se trouvent sur les lieux utilisés par l'opérateur de services essentiels et dont ils estiment l'audition nécessaire pour l'exercice de leur mission.A cet effet, ils peuvent exiger de ces personnes la présentation de documents officiels d'identification ;

5° requérir l'assistance des services de la police fédérale ou locale ;

6° solliciter des informations auprès des membres du personnel visé à l'article 9 de la loi du 15 avril 1994, pour les besoins de l'exécution des dispositions de la présente loi et de la loi du 1er juillet 2011.

§ 4. Pour obtenir l'autorisation de pénétrer dans des locaux habités, les membres du personnel du service d'inspection adressent une demande motivée au juge d'instruction. Cette demande contient au moins les données suivantes :

1° l'identification des espaces habités auxquels les membres du personnel du service d'inspection ou de l'autorité sectorielle souhaitent avoir accès ;

2° les infractions éventuelles qui font l'objet du contrôle ;

3° tous les documents et renseignements desquels il ressort que l'utilisation de ce moyen est nécessaire. Le juge d'instruction décide dans un délai de 48 heures maximum après réception de la demande. La décision du juge d'instruction est motivée. En l'absence de décision dans le délai prescrit, la visite des lieux est réputée être refusée. Le service d'inspection peut introduire un recours contre la décision de refus ou l'absence de décision devant la chambre des mises en accusation dans les quinze jours de la notification de la décision ou de l'expiration du délai. Les visites sans autorisation de l'occupant dans des locaux habités se font entre cinq et vingt-et-une heures par au moins deux membres du service d'inspection agissant conjointement.

§ 5. Au début de toute audition, il est communiqué à la personne interrogée :

1° que ses déclarations peuvent être utilisées comme preuve en justice ;

2° qu'elle peut demander que toutes les questions qui lui sont posées et les réponses qu'elle donne soient actées dans les termes utilisés ;

3° qu'elle a le droit de garder le silence et de ne pas contribuer à sa propre incrimination. Toute personne interrogée peut utiliser les documents en sa possession, sans que cela puisse entraîner le report de l'audition. Elle peut, lors de l'audition ou ultérieurement, exiger que ces documents soient joints à l'audition. L'audition mentionne avec précision l'heure à laquelle elle a pris cours, est éventuellement interrompue et reprise, et prend fin. Elle mentionne l'identité des personnes qui interviennentlors de l'audition ou à une partie de celle-ci. A la fin de l'audition, la personne interrogée a le droit de relire celle-ci ou de demander que lecture lui en soit faite. Elle peut demander à ce que ses déclarations soient corrigées ou complétées. Les membres du personnel du service d'inspection qui interrogent une personne l'informent qu'elle peut demander une copie du texte de son audition. Cette copie lui est délivrée gratuitement.

§ 6. Les membres du service d'inspection peuvent consulter tous les supports d'information et les données qu'ils contiennent. Ils peuvent se faire produire sur place le système informatique et les données qu'il contient dont ils ont besoin pour leurs examens et constatations, et en prendre ou en demander gratuitement des extraits, des duplicatas ou des copies, sous une forme lisible et intelligible qu'ils ont demandée. S'il n'est pas possible de prendre des copies sur place,

les membres du service d'inspection peuvent saisir, contre récépissé contenant un inventaire, le système informatique et les données qu'il contient.

§ 7. Pour étendre les recherches dans un système informatique ou une partie de celui-ci, entamées sur la base du paragraphe 6, vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée, le service d'inspection peut solliciter l'intervention d'un juge d'instruction.

Art. 45.

§ 1er. Après chaque inspection, les membres du service d'inspection rédigent un rapport et en transmettent une copie à l'opérateur de services essentiels inspecté et à l'autorité sectorielle compétente.

§ 2. L'autorité visée à l'article 7, § 1er, et l'autorité sectorielle peuvent solliciter, de manière motivée, du service d'inspection la transmission de ses rapports d'inspection.

Art. 46.

§ 1er. L'opérateur de services essentiels apporte son entière collaboration aux membres du service d'inspection dans l'exercice de leurs fonctions et notamment pour informer ceux-ci au mieux de toutes les mesures de sécurité existantes. Si nécessaire, l'opérateur de services essentiels met à disposition des membres du service d'inspection ou de l'autorité sectorielle le matériel nécessaire de manière à ce qu'ils remplissent les consignes de sécurité lors des inspections.

§ 2. Le Roi peut déterminer, par secteur ou sous-secteur, par arrêté délibéré en Conseil des ministres et après avis de l'autorité sectorielle, des rétributions relatives aux prestations d'inspections. Ces rétributions sont à charge des opérateurs de services essentiels.

Il fixe les modalités de calcul et de paiement.

CHAPITRE 2. - Contrôle des fournisseurs de service numérique

Art. 47.

§ 1er. Le Roi fixe les modalités pratiques du contrôle des fournisseurs de service numérique.

§ 2. Le fournisseur de service numérique est tenu notamment :

a) de communiquer, dans le délai requis, au service d'inspection compétent les informations nécessaires pour évaluer la sécurité de ses réseaux et systèmes d'information, y compris les documents relatifs à ses politiques de sécurité ;

b) de corriger tout manquement aux exigences de sécurité et de notification d'incidents, dans le délai requis.

§ 3. Conformément aux règles fixées par le Roi, le service d'inspection peut adopter des mesures, au besoin, dans le cadre de mesures de contrôle a posteriori, lorsque, selon les éléments communiqués, un fournisseur de service numérique ne satisfait pas aux exigences de sécurité ou de notification d'incidents. Ces éléments peuvent être communiqués par une autorité compétente d'un autre Etat membre de l'Union européenne dans lequel le service est fourni.

§ 4. Dans le cadre de ses contrôles a posteriori, le service d'inspection dispose des mêmes pouvoirs que ceux prévues à l'article 44.

§ 5. Si un fournisseur de service numérique a son établissement principal ou un représentant en Belgique alors que ses réseaux et systèmes d'information sont situés dans un ou plusieurs autres Etats, le service d'inspection, en concertation avec l'autorité visée à l'article 7, § 1er, peut solliciter la coopération et l'assistance des autorités de contrôle compétentes de ces autres Etats. Cette assistance et cette coopération peuvent porter sur les échanges d'informations et sur les demandes de prise de mesures de contrôle.

§ 6. Conformément aux règles fixées par le Roi, le service d'inspection peut exercer également les compétences prévues au présent article, à la demande d'autorités compétentes d'un autre Etat membre de l'Union européenne.

§ 7. L'autorité visée à l'article 7, § 1er, peut solliciter du service d'inspection la transmission des rapports d'inspection d'un fournisseur de service numérique.

§ 8. Le Roi peut déterminer, par arrêté délibéré en Conseil des ministres et après avis de l'autorité sectorielle, des rétributions relatives aux prestations de contrôles. Ces rétributions sont à charge des fournisseurs de service numérique. Le Roi fixe les modalités de calcul et de paiement.

CHAPITRE 3. - Les sanctions Section 1re. - Procédure

Art. 48.

§ 1er. Lorsqu'un ou plusieurs manquements aux exigences imposées par la loi, ses arrêtés d'exécution ou les décisions administratives individuelles y afférentes sont constatés, le service d'inspection met en demeure l'opérateur de services essentiels ou le fournisseur de service numérique concerné de se conformer, dans un délai qu'il fixe, aux obligations qui lui incombent.

Le délai est déterminé en tenant compte des conditions de fonctionnement de l'opérateur de services essentiels ou du fournisseur de service numérique et des mesures à mettre en oeuvre.

§ 2. Au préalable, le service d'inspection informe, de manière motivée, le contrevenant de son intention de lui adresser une mise en demeure et lui fait part de son droit, dans les quinze jours de la réception de cette information, de formuler par écrit ses moyens de défense ou de solliciter d'être d'entendu. L'information est présumée reçue par le contrevenant le sixième jour suivant son envoi par le service d'inspection.

§ 3. Sur base des éléments en sa possession, l'autorité visée à l'article 7, § 1er, peut également, de manière motivée, recommander au service d'inspection de mettre en demeure l'opérateur de services essentiels ou le fournisseur de service numérique.

Art. 49.

§ 1er. Lorsque le service d'inspection constate que l'opérateur de services essentiels ou le fournisseur de service numérique n'a pas respecté, dans le délai fixé, la mise en demeure, les faits sont constatés dans un procès-verbal rédigé par les membres assermentés du service d'inspection. Ce procès-verbal est adressé à l'autorité sectorielle compétente.

§ 2. Le fait pour quiconque d'empêcher ou entraver volontairement l'exécution d'un contrôle effectué par les membres du service d'inspection, de refuser de communiquer les informations qui lui sont demandées à l'occasion de ce contrôle, ou de communiquer sciemment des informations inexactes ou incomplètes est constaté par les membres assermentés du service d'inspection dans un procès-verbal.

§ 3. Les paragraphes 1er et 2 sont également applicables à l'opérateur de services essentiels potentiel ou à l'exploitant d'une infrastructure critique qui ne se conforme pas aux obligations d'information visées à l'article 14 ou à l'article 18, § 3.

§ 4. Les procès-verbaux rédigés par les membres assermentés du service d'inspection font foi jusqu'à preuve du contraire.

Art. 50. Les infractions à la présente loi ou à ses actes d'exécution peuvent faire l'objet soit de sanctions pénales, soit de sanctions administratives.

Section 2. - Sanctions pénales

Art. 51.

§ 1er. Est puni d'une peine d'emprisonnement de huit jours à un an et d'une amende de 26 euros à 20 000 euros ou de l'une de ces peines seulement quiconque ne se conforme pas à une des obligations de notification d'incidents visées aux articles 24 ou 35.

§ 2. Est puni d'une peine d'emprisonnement de huit jours à un an et d'une amende de 26 euros à 30 000 euros ou de l'une de ces peines seulement quiconque ne se conforme pas à une des obligations de sécurité imposées par le Roi ou l'autorité sectorielle en vertu des articles 21 ou 33.

§ 3. Est puni d'une peine d'emprisonnement de huit jours à un an et d'une amende de 26 euros à 50 000 euros ou de l'une de ces peines seulement quiconque ne se conforme pas à une des obligations de contrôle visées aux chapitres 1er et 2 du titre 4.

§ 4. Est puni d'une peine d'emprisonnement de huit jours à un an et d'une amende de 26 euros à 50 000 euros ou de l'une de ces peines seulement quiconque ne se conforme pas à une des obligations d'information visées à l'article 14 ou à l'article 18, § 3.

§ 5. Est puni d'une peine d'emprisonnement de huit jours à deux ans et d'une amende de 26 euros à 75 000 euros ou de l'une de ces peines seulement, quiconque empêche ou entrave volontairement l'exécution du contrôle effectué par les membres du service d'inspection, refuse de communiquer les informations qui lui sont demandées à l'occasion de ce contrôle, ou communique sciemment des informations inexactes ou incomplètes.

§ 6. En cas de récidive pour les mêmes faits dans un délai de trois ans, l'amende est doublée et le contrevenant puni d'une peine d'emprisonnement de quinze jours à trois ans.

§ 7. Les dispositions du Livre 1er du Code pénal, en ce compris le chapitre VII et l'article 85, sont applicables aux infractions visées au present article. Les articles 269 à 274 et 276 du Code pénal sont d'application à l'égard des membres du service d'inspection agissant dans l'exercice de leurs fonctions.

§ 8. Les infractions à l'article 9, §§ 2 et 3 de la présente loi sont punies des peines prévues à l'article 458 du Code pénal.

Section 3. - Sanctions administratives

Art. 52.

§ 1er. Toute infraction à la présente loi, à ses arrêtés d'exécution ou aux décisions administratives prises en vertu de cette dernière peut faire l'objet d'une sanction administrative.

§ 2. Est puni d'une amende de 500 à 75 000 euros quiconque ne se conforme pas aux obligations de notification d'incidents visées aux articles 24 ou 35.

§ 3. Est puni d'une amende de 500 à 100 000 euros quiconque ne se conforme pas aux obligations de sécurité imposées par le Roi ou l'autorité sectorielle en vertu des articles 21 ou 33.

§ 4. Est puni d'une amende de 500 à 125 000 euros quiconque ne se conforme pas aux obligations d'information visées à l'article 14 ou à l'article 18, § 3.

§ 5. Est puni d'une amende de 500 à 200 000 euros quiconque ne se conforme pas aux obligations de contrôle visées aux chapitres 1er et 2 du titre 4.

§ 6. Est puni d'une amende de 500 à 200 000 euros quiconque fait subir des conséquences négatives à une personne agissant pour le compte d'un opérateur de services essentiels ou d'un fournisseur de service numérique en raison de l'exécution, de bonne foi et dans le cadre de ses fonctions, des obligations découlant de la présente loi.

Art. 53. L'original du procès-verbal est envoyé par le service d'inspection au procureur du Roi. Une copie du procès-verbal est dans le même temps envoyée au contrevenant.

Art. 54. Le procureur du Roi dispose d'un délai de deux mois à compter du jour de la réception du procès-verbal pour informer l'autorité sectorielle que des poursuites pénales ont été engagées. L'autorité sectorielle ne peut diligenter la procédure pour infliger une amende administrative avant l'échéance du délai précité, sauf communication préalable par le procureur du Roi que celui-ci ne souhaite pas réserver de suite au fait. Dans le cas où le procureur du Roi omet de notifier

sa décision dans le délai fixé ou renonce à intenter des poursuites pénales, l'autorité sectorielle peut décider d'entamer la procédure administrative.

Art. 55.

§ 1er. La décision d'imposer une amende administrative est motivée. Elle mentionne également le montant de l'amende administrative et les infractions visées.

§ 2. L'autorité sectorielle informe au préalable le contrevenant de sa proposition motivée de sanction administrative et lui fait part de son droit, dans les quinze jours de la réception de la proposition, de formuler par écrit ses moyens de défense ou de solliciter d'être d'entendu. La proposition est présumée reçue par le contrevenant le sixième jour suivant son envoi par l'autorité sectorielle.

§ 3. En tenant compte des moyens de défense invoqués dans le délai visé au paragraphe 2 ou en l'absence de réaction du contrevenant dans ce même délai, l'autorité sectorielle peut adopter une sanction administrative visée à l'article 52.

§ 4. L'amende administrative est proportionnelle à la gravité, la durée, les moyens utilisés, les dommages causés et les circonstances des faits. L'amende administrative est doublée en cas de récidive pour les mêmes faits dans un délai de trois ans.

§ 5. Le concours de plusieurs infractions peut donner lieu à une amende administrative unique proportionnelle à la gravité de l'ensemble des faits.

Art. 56. La décision est notifiée par envoi recommandé au contrevenant. Une invitation à acquitter l'amende dans un délai d'un mois est jointe à la décision.

Art. 57. Le contrevenant peut contester la décision de l'autorité sectorielle devant la Cour des marchés visée à l'article 101 du Code judiciaire. La demande est introduite par requête contradictoire introduite, à peine de déchéance, dans les soixante jours de la notification de la décision de l'autorité sectorielle. La cause est traitée selon les formes du référé conformément aux articles 1035 à 1038, 1040 et 1041 du Code judiciaire. Ce recours ne suspend pas l'exécution de la décision.

Art. 58.

§ 1er. Lorsque le contrevenant reste en défaut de payer l'amende administrative dans le délai imparti, la décision d'infliger une amende administrative a force exécutoire et l'autorité sectorielle peut décerner une contrainte. La contrainte est décernée par le représentant légal de l'autorité sectorielle ou par un membre du personnel habilité à cette fin.

§ 2. La contrainte est signifiée au contrevenant par exploit d'huissier de justice. La signification contient un commandement de payer dans les vingt-quatre heures, à peine d'exécution par voie de saisie, de même qu'une justification comptable des sommes exigées ainsi que copie de l'exécutoire.

§ 3. Le contrevenant peut former opposition à la contrainte devant le juge des saisies. L'opposition est motivée à peine de nullité. Elle est formée au moyen d'une citation à l'autorité sectorielle par exploit d'huissier dans les quinze jours à partir de la signification de la contrainte. Les dispositions du chapitre VIII de la première partie du Code judiciaire sont applicables à ce délai, y compris les prorogations prévues à l'article 50, alinéa 2, et l'article 55 de ce Code. L'exercice de l'opposition à la contrainte suspend l'exécution de la contrainte, ainsi que la prescription des créances contenues dans la contrainte, jusqu'à ce qu'il ait été statué sur son bien-fondé. Les saisies déjà pratiquées antérieurement conservent leur caractère conservatoire.

§ 4. L'autorité sectorielle peut faire pratiquer la saisie conservatoire et exécuter la contrainte en usant des voies d'exécution prévues à la cinquième partie du Code judiciaire. Les paiements partiels effectués en suite de la signification d'une contrainte ne font pas obstacle à la continuation des poursuites.

§ 5. Les frais de signification de la contrainte de même que les frais de l'exécution ou des mesures conservatoires sont à charge du contrevenant. Ils sont déterminés suivant les règles établies pour les actes accomplis par les huissiers de justice en matière civile et commerciale.

Art. 59. L'autorité sectorielle ne peut imposer d'amende administrative à l'échéance d'un délai de trois ans, à compter du jour où le fait a été commis. Le paiement selon la procédure administrative éteint également la possibilité d'engager des poursuites pénales pour les faits visés.

TITRE 5. - CSIRT

CHAPITRE 1er. - Le CSIRT national

Section 1re. - Tâches du CSIRT national

Art. 60. Les tâches du CSIRT national sont au moins les suivantes :

a) le suivi des incidents au niveau national et international, en ce compris le traitement de données à caractère personnel lié au suivi de ces incidents ;

b) l'activation du mécanisme d'alerte précoce, la diffusion de messages d'alerte, les annonces et la diffusion d'informations sur les risques et incidents auprès des parties intéressées ;

c) l'intervention en cas d'incident ;

d) l'analyse dynamique des risques et incidents et conscience situationnelle ;

e) la détection, l'observation et l'analyse des problèmes de sécurité informatique ;

f) la promotion de l'adoption et de l'utilisation de pratiques communes ou normalisées pour les procédures de gestion des risques et incidents, ainsi que des systèmes de classification des incidents, risques et informations ;

g) l'établissement de relations de coopération avec le secteur privé, d'autres services administratifs ou autorités publiques ;

h) la participation au réseau des CSIRT visé à l'article 12 de la directive NIS. Après avis du CSIRT national, le Roi peut lui confier des tâches supplémentaires.

Section 2. - Obligations du CSIRT national

Art. 61. Les obligations du CSIRT national sont au moins les suivantes :

a) garantir un niveau élevé de disponibilité de ses services de communication en évitant les points uniques de défaillance et disposer de plusieurs moyens pour être contacté et contacter autrui à tout moment ;

b) disposer de locaux et de systèmes d'information se trouvant sur des sites sécurisés ;

c) assurer la continuité des opérations avec un système approprié de gestion et de routage des demandes afin de faciliter les transferts ;

d) participer aux réunions du réseau des CSIRT visé à l'article 12 de la directive NIS ;

e) s'appuyer sur une infrastructure dont la continuité est garantie.A cette fin, des systèmes redondants et un espace de travail de secours sont disponibles ;

f) faire en sorte que ses canaux de communication soient clairement précisés et bien connus de ses partenaires.

Art. 62. Dans le cadre de l'exercice de ses compétences, le CSIRT national prend toutes les mesures adéquates afin de réaliser les objectifs définis aux articles 60 et 61. Ces mesures doivent être proportionnelles à ces objectifs, et respecter les principes d'objectivité, de transparence et de non-discrimination. Pour atteindre ces objectifs, le CSIRT national est autorisé à détenir, à divulguer à une autre personne, à diffuser ou à faire usage de toutes les informations disponibles, même si celles-ci sont issues d'un accès non autorisé à un système informatique par un tiers. Dans l'accomplissement de ses missions, le CSIRT national use de la prudence que l'on est en droit d'attendre d'une autorité publique, en veillant toujours en priorité à ne pas perturber le fonctionnement du système informatique et en prenant toutes précautions raisonnables afin qu'aucun dommage matériel ne soit causé au système informatique. Les fonctionnaires dirigeants du CSIRT national veillent, par l'adoption de procédures internes, au respect des conditions visées au présent article.

CHAPITRE 2. - Le CSIRT sectoriel

Section 1re. - Tâches du CSIRT sectoriel

Art. 63. Les tâches d'un CSIRT sectoriel sont, en collaboration avec le CSIRT national, au moins les suivantes :

a) le suivi des incidents sectoriels ;

b) l'activation du mécanisme d'alerte précoce, la diffusion de messages d'alerte, les annonces et la diffusion d'informations sur les risques et les incidents auprès des parties intéressées du secteur ;

c) l'intervention en cas d'incident sectoriel ;

d) l'analyse dynamique des risques et incidents sectoriels et conscience situationnelle ;

e) l'établissement de relations de coopération avec les opérateurs de son secteur ;

f) pouvoir participer aux réunions, relatives à son secteur, du réseau des CSIRT visé à l'article 12 de la directive NIS. Après avis du CSIRT sectoriel, le Roi peut lui confier des tâches supplémentaires.

Section 2. - Obligations d'un CSIRT sectoriel

Art. 64. Les obligations d'un CSIRT sectoriel sont les suivantes :

a) garantir un niveau élevé de disponibilité de ses canaux de communication en évitant les points uniques de défaillance et disposer de plusieurs moyens pour être contactés et contacter autrui à tout moment.

b) disposer de locaux et de systèmes d'information se trouvant sur des sites sécurisés.

c) assurer la continuité des opérations avec un système approprié de gestion et de routage des demandes afin de faciliter les transferts.

d) s'appuyer sur une infrastructure dont la continuité est garantie. A cette fin, des systèmes redondants et un espace de travail de secours sont disponibles.

f) faire en sorte que ses canaux de communication soient clairement précisés et bien connus de ses partenaires. TITRE 6. - Traitement des données à caractère personnel

CHAPITRE 1er. - Principes relatifs au traitement, base légale et finalités

Art. 65.

§ 1er. Conformément à l'article 5.1.c) du Règlement UE 2016/679, lors du traitement de données à caractère personnel dans le cadre de l'exécution de la présente loi, le responsable de traitement veille à limiter le traitement au minimum nécessaire et de manière proportionnée à la finalité poursuivie.

§ 2. Dans le respect de ce principe, les données personnelles traitées peuvent être des données de tout type en rapport avec la sécurité des réseaux et systèmes d'information, à savoir le cas échéant des informations nominatives, des données concernant les collaborateurs d'une organisation ou des personnes extérieures, des données ou des identifiants de connexion, des données de géolocalisation, des données d'identification ou d'authentification, le cas échéant au moyen de dispositifs sécurisés.

§ 3. Les principaux traitements de données personnelles dans le cadre de la présente loi peuvent être regroupés comme suit : - l'échange général d'informations entre les opérateurs de services essentiels et les fournisseurs de services numériques, d'une part, et les autorités visées à l'article 7, d'autre part ; - le traitement d'informations spécifiques entre les entités visées au premier tiret dans le cadre des notifications d'incidents ou d'autres échanges ponctuels ; - le traitement par les services d'inspection conformément au titre 4 ; - le traitement par les cours et tribunaux ou les autorités sectorielles dans le cadre de la mise en oeuvre de la loi et particulièrement de la recherche, la poursuite et la répression d'infractions ; - les échanges et autres traitements d'informations par le CSIRT national et par le CSIRT sectoriel pour leurs missions visées respectivement aux articles 60 à 62 et 63 et 64.

Art. 66.

§ 1er. Chaque fois que possible, les données traitées sont pseudonymisées ou agrégées de façon à diminuer le risque d'une utilisation de données personnelles incompatible avec le Règlement UE 2016/679 ou les lois et règlements qui le complètent ou le précisent.

§ **2.** Les catégories particulières de données au sens des articles 9 et 10 du Règlement UE 2016/679 sont traitées dans le respect dudit règlement et des lois et règlements qui le complètent ou le précisent.

§ 3. Le responsable du traitement peut être soit l'une des autorités visées à l'article 7, soit les opérateurs de services essentiels ou les fournisseurs de services numériques, soit les autorités policières ou judiciaires.

§ 4. Les destinataires de données personnelles peuvent être toutes les personnes impliquées dans l'exécution des dispositions de la loi, dans la mesure nécessaire pour les échanges d'informations prévus par la loi.

Art. 67. Conformément aux articles 6.1, c), et 6.1, e), du Règlement UE 2016/679, les traitements visés à l'article 65, § 3, doivent demeurer nécessaires au respect d'une obligation légale du responsable du traitement ou à l'exécution d'une mission d'intérêt public dont ce dernier est investi. Ces traitements doivent être nécessaires au regard de ces seules bases juridiques et demeurer limités à ce qui est nécessaire pour y satisfaire.

Art. 68.

§ 1er. Les traitements visés à l'article 65, § 3, doivent être limités à et demeurer compatibles avec les finalités déterminées par le responsable du traitement.

§ 2. Ces finalités peuvent notamment être la recherche d'un niveau accru de protection des réseaux et systèmes d'information, le renforcement des politiques de prévention et de sécurité, la prévention des incidents de sécurité, la continuité des services essentiels ou des services numériques visés par la présente loi, le contrôle des opérateurs de services essentiels et fournisseurs de services numériques, la coopération sur les plan national et international, l'évaluation de la mise en oeuvre de la loi, la préparation, l'organisation, la gestion et le suivi d'enquêtes ou de poursuites, ainsi que les autres missions dévolues par la loi aux différentes autorités concernés.

§ 3. Il appartient à chaque responsable du traitement de déterminer pour ce qui le concerne les finalités ou sous-finalités pertinentes, les catégories de données et de personnes concernées, les destinataires ou catégories de destinataires de données, les durées de conservation ainsi que les autres caractéristiques éventuelles du traitement ainsi que les règles et pratiques de mise en conformité à la réglementation applicable.

CHAPITRE 2. - Durée de conservation

Art. 69.

§ 1er. Sans préjudice de la conservation nécessaire pour le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, visé à l'article 89 du Règlement UE 2016/679, les données à caractère personnel traitées en exécution de la loi, ne sont pas conservées par les autorités visées à l'article 7 plus longtemps que nécessaire au regard des finalités pour lesquelles elles sont traitées.

§ 2. Dans le respect du paragraphe 1er, le Roi peut fixer la durée maximale de conservation des mêmes données par arrêté délibéré en conseil des Ministres.

CHAPITRE 3. - Délégué à la protection des données

Art. 70. Tout opérateur de services essentiels, tout fournisseur de service numérique et toute autorité visée à l'article 7 de la loi qui traitent des données à caractère personnel, désignent un délégué à la protection des données.

CHAPITRE 4. - Limitation des droits des personnes concernées

Art. 71.

§ 1er. En application des articles 23.1, a), b), c), d), e), h), du Règlement UE 2016/679, certaines obligations et droits prévus par ledit règlement sont limités ou exclus, conformément aux dispositions du présent chapitre. Ces limitations ou exclusions ne peuvent porter préjudice à l'essence des libertés et droits fondamentaux et doivent être appliquées dans la stricte mesure nécessaire au but poursuivi.

§ 2. Les articles 12 à 22 dudit règlement ne sont pas applicables au traitement de données à caractère personnel effectué par un opérateur de services essentiels, un fournisseur de service numérique ou une autorité visée à l'article 7, qui est effectué dans le respect de la présente loi et pour satisfaire aux obligations que celle-ci impose en matière de notifications d'incidents visées au chapitre 3 du titre 2 et au chapitre 3 du titre 3, ainsi que de contrôles visés au titre 4. L'exemption ne vaut que si et dans la mesure où ce traitement nécessaire pour les finalités définies ci-avant, notamment dans la mesure où l'application des droits prévus par le règlement précité nuirait aux besoins du contrôle, de l'enquête ou des actes préparatoires, ou risquerait de violer le secret de l'enquête pénale ou la sécurité des personnes.

§ 3. Le responsable du traitement susceptible de bénéficier de l'exemption prévue au paragraphe 2, est soit l'opérateur de services essentiels, soit le fournisseur de service numérique, soit l'autorité visée à l'article 7, chacun pour les données qu'il détient dans le cadre des missions visées au paragraphe 2.

§ 4. L'exemption vaut, sous réserve du principe de proportionnalité et le cas échéant de minimisation des données, pour toutes les catégories de données à caractère personnel, dans la mesure où le traitement de ces données n'est pas étranger aux finalités visées au paragraphe 2. Cette exemption vaut également pour les actes préparatoires ou pour les procédures visant à l'application éventuelle d'une sanction administrative.

§ 5. Les données à caractère personnel qui résultent de l'exemption visée au paragraphe 2 ne sont pas conservées plus longtemps que nécessaire au regard des finalités pour lesquelles elles sont traitées, avec une durée maximale de conservation ne pouvant excéder la durée du délai de prescription des infractions éventuelles visées aux articles 51 et 52, conformément à la législation applicable.

§ 6. Le responsable du traitement qui ne se conforme pas à toutes les dispositions de la loi et en particulier de l'article 72, ne peut bénéficier de l'exemption.

§ 7. Chaque responsable du traitement est tenu en outre de préserver la confidentialité des données personnelles qui font l'objet de l'exemption, et de faire en sorte qu'elles ne soient accessibles qu'aux personnes qui en ont besoin pour l'exécution des dispositions de la présente loi. Chaque responsable du traitement concerné doit aussi adresser par écrit à

l'Autorité de protection des données, au moins une fois par an, une liste des demandes d'exercice des droits visés aux articles 12 à 22 du règlement qui relèvent, selon ledit responsable, de l'exemption. Sans préjudice des dispositions de la présente loi, chaque responsable du traitement concerné est par ailleurs tenu de prendre toute autre mesure appropriée pour éviter toute forme d'abus, d'accès ou de transfert illicites des données à caractère personnel qui relèvent de l'exemption, à savoir notamment et sans limitation aucune les mesures prévues à l'article 32 du Règlement UE 2016/679.

Art. 72.

§ 1er. Les personnes concernées peuvent adresser une demande concernant leurs droits prévus aux articles 12 à 22 du Règlement UE 2016/679, au délégué à la protection des données, lequel en accuse réception.

§ 2. Le délégué à la protection des données du responsable du traitement informe la personne concernée par écrit, dans les meilleurs délais, et en tout état de cause dans un délai d'un mois à compter de la réception de la demande, de tout refus ou de toute limitation de ses droits prévus aux articles 12 à 22 du Règlement UE 2016/679, ainsi que des motifs du refus ou de la limitation. Ces informations concernant le refus ou la limitation peuvent ne pas être fournies lorsque leur communication risque de compromettre l'une des finalités énoncées à l'article 71, § 2. Au besoin, ce délai peut être prolongé de deux mois, compte tenu de la complexité et du nombre de demandes.

Le responsable du traitement informe la personne concernée de cette prolongation et des motifs du report dans un délai d'un mois à compter de la réception de la demande.

§ 3. Le délégué à la protection des données du responsable du traitement informe la personne concernée des possibilités d'introduire une réclamation auprès de l'Autorité de protection des données et de former un recours juridictionnel. Le délégué à la protection des données du responsable du traitement consigne les motifs de fait ou de droit sur lesquels se fonde la décision. Ces informations sont mises à la disposition de l'Autorité de protection des données.

§ 4. Le responsable du traitement concerné donne toutefois accès à la personne concernée à des informations limitées concernant le traitement de ses données à caractère personnel, pour autant que cette communication ne compromette pas la réalisation des objectifs de la présente loi et de manière telle que la personne concernée se trouve dans l'impossibilité de savoir si elle fait l'objet d'une enquête ou pas, et sans pouvoir en aucun cas rectifier, effacer, limiter, notifier, transmettre à un tiers des données personnelles, ni cesser toute forme de traitement desdites données qui soit nécessaire dans le cadre défini ci-avant.

§ 5. La mesure de refus ou de limitation des droits prévus aux articles 12 à 22 du Règlement UE 2016/679, doit être levée : - pour les mesures justifiées par les obligations en matière de notification d'incidents, lors de la clôture du traitement d'un incident par les autorités visées à l'article 24 ou 34 ; - pour les mesures justifiées par les obligations en vertu du titre 4, lors de la clôture du contrôle ou de l'enquête ou des actes préparatoires à ceux-ci effectués par le service d'inspection, ainsi que pendant la période durant laquelle l'autorité sectorielle traite les pièces provenant du service d'inspection en vue d'exercer des poursuites ; - au plus tard un an à partir de la réception de la demande introduite en application des articles 12 à 22 du Règlement européen UE 2016/679, sauf si un contrôle ou une enquête sont en cours.

§ 6. Le responsable du traitement concerné lève également la mesure de refus ou de limitation des droits prévus aux articles 12 à 22 du Règlement UE 2016/679, dès qu'une telle mesure n'est plus nécessaire au respect d'une des finalités visées à l'article 68, § 2.

§ 7. Dans tous les cas d'application des paragraphes 5 et 6, le délégué à la protection des données informe par écrit la ou les personnes concernées de la levée de la mesure de refus ou de limitation.

CHAPITRE 5. - Limitations aux obligations de notification des violations de données à caractère personnel

Art. 73. Le responsable du traitement concerné est dispensé de communiquer une violation de données à caractère personnel à une ou des personnes concernées bien déterminées, au sens de l'article 34 du Règlement UE 2016/679,

moyennant l'autorisation de l'autorité visée à l'article 7, § 1er, pour autant que et dans la mesure où une telle notification individuelle risque de compromettre la réalisation des finalités visées à l'article 71, § 2.

TITRE 7. - Dispositions finales

CHAPITRE 1er. - Modifications de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques

Art. 74. L'article 2 de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques est complété par un alinéa rédigé comme suit : "La présente loi transpose partiellement 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.".

Art. 75. A l'article 3 de la même loi, modifié par les lois du 25 avril 2014 et du 15 juillet 2018, les modifications suivantes sont apportées :

1° dans le 3°, les c) et d) sont remplacés par ce qui suit : "c) pour le secteur des finances, à l'exception des opérateurs de plate-forme de négociation au sens de l'article 3, 6°, de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la Directive 2014/65/UE : la Banque nationale de Belgique (BNB) ;

d) pour les opérateurs de plate-forme de négociation au sens de l'article 3, 6°, de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la Directive 2014/65/UE : l'Autorité des services et marchés financiers (FSMA) ;" ; 2° le 3° est complété par les e) à g) rédigés comme suit : **e)** pour les secteurs des communications électroniques et des infrastructures numériques : l'Institut belge des services postaux et des télécommunications (I.B.P.T.) ;

f) pour le secteur de la santé : l'autorité publique désignée par le Roi par arrêté délibéré en Conseil des ministres ;

g) pour le secteur de l'eau potable : l'autorité publique désignée par le Roi par arrêté délibéré en Conseil des ministres ;" ;

3° l'article est complété par les 13° à 17° rédigés comme suit : - "13° "la loi du 7 avril 2019" : la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique ;

- 14° "sécurité des réseaux et systèmes d'information" : la sécurité des réseaux et systèmes d'information au sens de l'article 6, 8° et 9°, de la loi du 7 avril 2019 ;

- 15° "le secteur des infrastructures numériques" : le secteur visé au point 6 de l'annexe 1 de la loi du 7 avril 2019 ;

- 16° "le secteur de l'eau potable" : le secteur visé au point 5 de l'annexe 1 de la loi du 7 avril 2019 ; - 17° "le secteur de la santé" : le secteur visé au point 4 de l'annexe 1 de la loi du 7 avril 2019.".

Art. 76. Dans l'article 4 de la même loi, modifié par la loi du 15 juillet 2018, le paragraphe 4 est remplacé par ce qui suit : " § 4. Le présent chapitre s'applique au secteur des finances, en ce compris aux opérateurs de plate-forme de négociation visés à l'article 3, 3°, d), au secteur des communications électroniques, au secteur des infrastructures numériques, au secteur de la santé et au secteur de l'eau potable, en ce qui concerne la sécurité et la protection des infrastructures critiques nationales.".

Art. 77. L'article 5 de la même loi, modifié par la loi du 15 juillet 2018, est complété par le paragraphe 3 rédigé comme suit : " § 3. Tout au long du processus d'identification visé à la présente section, l'autorité visée à l'article 7, § 1er, de la loi du 7 avril 2019 est associée aux concertations nationales et internationales menées par les autorités sectorielles et la

DGCC, pour les aspects de l'identification des infrastructures critiques liés à la sécurité des réseaux et systèmes d'information.".

Art. 78. A l'article 13 de la même loi, modifié par les lois du 25 avril 2014 et du 15 juillet 2018, les modifications suivantes sont apportées :

1° dans le paragraphe 5bis, les mots "à l'exception de celles exploitées par un opérateur de plate-forme de négociation" sont insérés entre les mots "du secteur des finances" et les mots", les mesures de sécurité".

2° dans le paragraphe 6, alinéa 1er, les mots "à l'exception des infrastructures critiques exploitées par un opérateur de plate-forme de négociation" sont insérés entre les mots "le secteur des finances" et les mots", les exercices".

Art. 79. Dans l'article 14 de la même loi, modifié par la loi du 15 juillet 2018, le paragraphe 2 est complété par les mots "et, le cas échéant, l'autorité visée à l'article 7, § 1er, de la loi du 7 avril 2019, pour ce qui concerne la sécurité des réseaux et systèmes d'information.".

Art. 80. Dans l'article 18 de la même loi, modifié par la loi du 15 juillet 2018, les mots "La DGCC, les services de police et l'OCAM" sont remplacés par les mots "La DGCC, les services de police, l'OCAM et, le cas échéant, l'autorité visée à l'article 7, § 1er, de la loi du 7 avril 2019 pour ce qui concerne la sécurité des réseaux et systèmes d'information".

Art. 81. à l'article 19 de la même loi, les mots "L'exploitant, le point de contact pour la sécurité, l'autorité sectorielle, la DGCC, l'OCAM et les services de police" sont remplacés par les mots "L'exploitant, le point de contact pour la sécurité, l'autorité sectorielle, la DGCC, l'OCAM, les services de police et, le cas échéant, l'autorité visée à l'article 7, § 1er, de la loi du 7 avril 2019 pour ce qui concerne la sécurité des réseaux et systèmes d'information,".

Art. 82. à l'article 22 de la même loi, remplacé par la loi du 15 juillet 2018, les mots "L'autorité sectorielle, la DGCC, l'OCAM et les services de police" sont remplacés par : "L'autorité sectorielle, la DGCC, l'OCAM, les services de police et l'autorité visée à l'article 7, § 1er, de la loi du 7 avril 2019,".

Art. 83. A l'article 22bis de la même loi, inséré par la loi du 25 avril 20048, les modifications sont apportées : 1° dans l'alinéa 1er, les mots "à l'exception du sous-secteur des opérateurs de plate-forme de négociation" sont insérés entre les mots "le secteur des finances" et les mots ", la Banque nationale de Belgique".2° l'article est complété par un alinéa rédigé comme suit : "Pour les opérateurs de plate-forme de négociation, la FSMA communique au ministre des Finances un rapport relatif aux tâches qu'elle accomplit en vertu de la présente loi selon une périodicité appropriée n'excédant toutefois pas trois ans.La FSMA l'informe toutefois sans délai de toute menace concrète et imminente pesant sur une infrastructure critique relevant de son secteur.".

Art. 84. A l'article 24 de la même loi, modifié par les lois du 25 avril 2014 et du 15 juillet 2018, les modifications suivantes sont apportées :

1° dans le paragraphe 2, alinéa 3, les mots "à l'exception du sous-secteur des opérateurs de plate-forme de négociation" sont insérés entre les mots "le secteur des finances" et les mots ", la Banque nationale de Belgique".

2° le paragraphe 2 est complété par un alinéa rédigé comme suit : "L'Autorité des services et marchés financiers est désignée en tant que service d'inspection chargé de contrôler l'application des dispositions de la présente loi et de ses arrêtés d'exécution, pour les opérateurs de plate-forme de négociation au sens de l'article 3, 6°, de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la Directive 2014/65/UE.Le présent article ne porte pas préjudice à la possibilité pour la FSMA, pour l'exécution des missions qui lui sont confiées par la présente loi de charger un prestataire externe spécialisé de l'exécution de tâches déterminées ou d'obtenir l'assistance d'un tel prestataire.".

CHAPITRE 2. - Modifications de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire

Art. 85. L'article 1er de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire, modifié en dernier lieu par la loi du 13 décembre 2017, est complété comme suit : - "la loi du 7 avril 2019" : la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique ;".

Art. 86. Dans la section 1re du chapitre III de la même loi, il est inséré un article 15ter, rédigé comme suit : "

Art. 15ter. L'Agence est désignée comme service d'inspection, au sens de l'article 42 de la loi du 7 avril 2019 et est chargée du contrôle de l'application des dispositions de ladite loi et de ses arrêtés d'exécution par les opérateurs de services essentiels, identifiés en vertu de la loi susmentionnée, pour ce qui concerne les éléments d'une installation nucléaire destinée à la production industrielle d'électricité et qui servent au transport de l'électricité.

Le Roi fixe les modalités pratiques des inspections, après avis de l'Agence.".

CHAPITRE 3. - Modifications de la loi du 17 janvier 20037 relative au statut du régulateur des secteurs des postes et des télécommunications belges

Art. 87. L'article 1er/1 de la loi du 17 janvier 20037 relative au statut du régulateur des secteurs des postes et des télécommunications belges, inséré par la loi du 10 juillet 2012, est complété par un alinéa rédigé comme suit : "La présente loi transpose partiellement 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.".

Art. 88. Dans l'article 14, § 1er, alinéa 1er, de la même loi, modifié par les lois du 13 décembre 2010, 10 juillet 2012, 27 mars 2014, 18 avril 2017, 5 mai 2017 et 31 juillet 2017, les modifications suivantes sont apportées :

1° à l'alinéa 1er, les mots ", en ce qui concerne le secteur des infrastructures numériques au sens de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, en ce qui concerne les secteurs des communications électroniques et des infrastructures numériques au sens de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques," sont insérés entre les mots "équipement hertzien" et les mots "et en ce qui concerne" ;

2° le 3° est remplacé par ce qui suit : "3° le contrôle du respect des normes suivantes et de leurs arrêtés d'exécution :

a) la loi du 13 juin 20052 relative aux communications électroniques ;

b) le Titre Ier, chapitre X et le Titre III de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques ;

c) la loi du 26 janvier 2018 relative aux services postaux ;

d) les articles 14, § 2, 2°, et 21, §§ 5 à 7, de la loi du 17 janvier 20037 relative au statut du régulateur des secteurs des postes et télécommunications belges ;

e) les articles 4 et 4/1 de la loi du 17 janvier 20037 concernant les recours et le traitement des litiges à l'occasion de la loi du 17 janvier 20037 relative au statut du régulateur des secteurs des postes et des télécommunications belges ;

f) la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale ;

g) la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, pour ce qui concerne les secteurs des communications électroniques et des infrastructures numériques ;

h) la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, en ce qui concerne le secteur des infrastructures numériques ;

i) le Règlement (UE) 611/2013 de la Commission du 24 juin 2013 concernant les mesuresrelatives à la notification des violations de données à caractère personnel en vertu de la Directive 2002/58/CE du Parlement européen et du Conseil sur la vie privée et les communications électroniques. Pour l'application de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, l'Institut est désigné comme autorité sectorielle et service d'inspection pour le secteur des infrastructures numériques. Le Roi peut fixer les modalités pratiques des inspections pour ce secteur, après avis de l'Institut.".

Art. 89. Dans l'article 24, alinéa 1er, de la même loi, modifié par les lois du 27 mars 2014 et du 26 janvier 2018, les mots ", ainsi qu' à la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, pour ce qui concerne le secteur des communications électroniques et le secteur des infrastructures numériques, et à la loi 7 april 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, pour ce qui concerne le secteur des infrastructures numériques," sont insérés entre les mots "dans la région bilingue de Bruxelles-Capitale" et les mots "et à leurs arrêtés d'exécution".

CHAPITRE 4. - Modifications de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la Directive 2014/65/UE

Art. 90. L'article 71 de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la Directive 2014/65/UE est complété par les mots "et du titre 2 de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique. Pour l'exécution des missions précitées concernant la loi du 7 avril 2019, la FSMA peut néanmoins charger un prestataire externe spécialisé de l'exécution de tâches déterminées de contrôle ou obtenir l'assistance d'un tel prestataire. ".

Art. 91. L'article 79 de la même loi est complété par un paragraphe 4, rédigé comme suit : " § 4. En cas de violation des dispositions applicables de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, la FSMA peut infliger les sanctions administratives prévues par l'article 52 de ladite loi.".

CHAPITRE 5. - Modification de la loi du 2 août 20026 relative à la surveillance du secteur financier et aux services financiers

Art. 92. L'article 75, § 1er, 15°, de la loi du 2 août 20026 relative à la surveillance du secteur financier et aux services financiers, abrogé par la loi du 5 décembre 2017 portant des dispositions financières diverses, est rétabli dans la rédaction suivante : "15° dans les limites du droit de l'Union européenne, les autorités visées à l'article 7 de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique pour les besoins de l'exécution des dispositions de cette loi et de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques ;".

CHAPITRE 6. - Modifications de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique

Art. 93. L'article 36/1 de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique, inséré par l'arrêté royal du 3 mars 2011, est complété par le 28° rédigé comme suit : "28° "la loi du 7 avril 2019" : la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.".

Art. 94. A l'article 36/14, § 1er, de la même loi, modifié en dernier lieu par la loi du 30 juillet 2018, les modifications suivantes sont apportées :

1° dans le 20° les mots "à l'autorité visée à l'article 7, § 1er, de la loi du 7 avril 2019";sont insérés entre les mots "l'analyse de la menace" et "et aux service de police" ;

2° le paragraphe est complété par le 24° rédigé comme suit : "24° dans les limites du droit de l'Union européenne, aux autorités visées à l'article 7 de la loi du 7 avril 2019 pour les besoins de l'exécution des dispositions de la loi du 7 avril 2019 et de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.".

Art. 95. Dans la même loi, il est inséré un chapitre IV/4, comportant l'article 36/47 rédigé comme suit : "Chapitre IV/4. Surveillance par la Banque dans le cadre de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.

Art. 36/47. "Pour l'application de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, la Banque est désignée comme autorité sectorielle et service d'inspection pour les opérateurs du secteur des finances, à l'exception des opérateurs de plate-forme de négociation au sens de l'article 3, 6°, de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la Directive 2014/65/UE. Les articles 36/19 et 36/20 sont applicables. La Commission des sanctions statue sur l'imposition des amendes administratives prévues à l'article 52 de la loi précitée du 7 avril 2019. Les articles 36/8 à 36/12/3 et l'article 36/21 sont applicables. La Banque partage avec la BCE le plus vite possible les informations pertinentes sur les notifications d'incident qu'elle reçoit en vertu de la loi du 7 avril 2019".

CHAPITRE 7. - Entrée en vigueur

Art. 96. La présente loi entre en vigueur le jour de sa publication au Moniteur belge.

Promulguons la présente loi, ordonnons qu'elle soit revêtue du sceau de l'Etat et publiée par le Moniteur belge.

Donné à Bruxelles, le 7 avril 2019.

PHILIPPE Par le Roi : Le Premier Ministre, Ch. MICHEL Le Ministre de la Sécurité et de l'Intérieur, P. DE CREM Scellé du sceau de l'Etat : Le Ministre de la Justice, K. GEENS _____ Note (1) Chambres des représentants (www.lachambre.be) : Documents : 54 - 3340 Compte rendu intégral : 21 mars 2019.

Annexe 1 à la loi du 7 avril 2019 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique Types d'opérateurs de services essentiels visés à l'article 11, § 1er

Secteur

Sous-secteur

Type d'entités

1. Energie

a) Electricité

Entreprises d'électricité au sens de l'article 2, 15° ter de la loi du 29 avril 19995 relative à l'organisation du marché de l'électricité. Gestionnaires de réseau de distribution au sens de l'article 2, 11° de la loi du 29 avril 19995 relative à l'organisation du marché de l'électricité.

Gestionnaires de réseau au sens de l'article 2, 8° de la loi du 29 avril 19995 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 gaz naturel au sens de l'article 1, 5° bis de la loi du 12 avril 19651 relative au transport de produits gazeux et autres par canalisations. Gestionnaires de réseau de distribution au sens de l'article 1, 13° de la loi du 12 avril 19651 relative au transport de produits gazeux et autres par canalisations.

Gestionnaires du réseau de transport de gaz naturel au sens de l'article 1, 31° de la loi du 12 avril 19651 relative au transport de produits gazeux et autres par canalisations.

Gestionnaires de stockage au sens de l'article 1, 33° de la loi du 12 avril 19651 relative au transport de produits gazeux et autres par canalisations.

Gestionnaires d'installation de GNL au sens de l'article 1, 35° de la loi du 12 avril 19651 relative au transport de produits gazeux et autres par canalisations.

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) n° 2320/2002. Entités gestionnaires d'aéroports au sens de l'article 2, point 2), de l'AR du 6 novembre 2010 réglementant l'accès au marché de l'assistance en escale à l'aéroport de Bruxelles-National, aéroports au sens de l'article 2, point 1), de la directive 2009/12/CE du Parlement européen et du Conseil, 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, et entités exploitant les installations annexes se trouvant dans les aéroports.

Services de navigation aérienne au sens de l'article 2, point 4), 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 »).

Le gestionnaire de réseau au sens de l'article 2, point 22), du règlement (UE) n° 677/2011 de la Commission du 7 juillet 2011 établissant les modalités d'exécution des fonctions de réseau de la gestion du trafic aérien et modifiant le règlement (UE) n° 691/2010.

b) Transport ferroviaire

Gestionnaires de l'infrastructure au sens de l'article 3, 29° du Code ferroviaire. Entreprises ferroviaires au sens de l'article 3, 27° du Code 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, à l'exclusion des navires exploités à titre individuel par ces sociétés. Entités gestionnaires des ports au sens de l'article 5 point 7) de la loi du 5 février 20070 relative à la sûreté maritime, 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 (STM) au sens de l'article 1er, point 12), de l'AR du 17 septembre 2005 transposant la directive 2002/59/CE du 27 juin 2002.

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 l'article 3, point 1), de la loi du 17 août 2013 portant création du cadre pour le déploiement de systèmes de transport intelligents et modifiant la loi du 10 avril 1990 réglementant la sécurité privée et particulière (dénommée : " loi-cadre STI ").

3. Finances

a) Etablissements financiers

Etablissements de crédit au sens de l'article 4, point 1), du règlement (UE) n° 575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement et modifiant le règlement (UE) n° 648/2012. 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.

Etablissements financiers (autres que les établissements de crédit et les contreparties centrales) soumis au contrôle de la Banque nationale de Belgique, en vertu des articles 8 et 12bis de la loi du 22 février 1998 fixant le statut organique de la Banque nationale de Belgique.

b) Plates-formes de négociation financière

Opérateurs de plate-forme de négociation au sens de l'article 3, 6° de la loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la Directive 2014/65/UE. 4. Santé

Etablissements de soins de santé (y compris les hôpitaux et les cliniques privées)

Prestataires de soins de santé au sens de l'article 3, point g), de la directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers. 5. Eau potable Fournisseurs et distributeurs d'eaux destinées à la consommation humaine au sens de l'article 2, point 1) a), de la directive 98/83/CE du Conseil du 3 novembre 1998 relative à la qualité des eaux destinées à la consommation humaine, à l'exclusion des distributeurs pour lesquels la distribution d'eaux destinées à la consommation humaine ne constitue qu'une partie de leur activité générale de distribution d'autres produits et biens qui ne sont pas considérés comme des services essentiels. 6.Infrastructures numériques

IXP. Fournisseurs de services DNS. Registres de noms de domaines de haut niveau.

Vu pour être annexé à la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.

PHILIPPE Par le Roi : Le Premier Ministre, CH. MICHEL Le Ministre de la Sécurité et de l'Intérieur, P. DE CREM

Annexe 2 à la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique Types de services numériques

1. Place de marché en ligne

2. Moteurs de recherche en ligne

3. Service d'informatique en nuage Vu pour être annexé à la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.

PHILIPPE Par le Roi : Le Premier Ministre, CH. MICHEL Le Ministre de la Sécurité et de l'Intérieur, P. DE CREM