LOIS, DECRETS, ORDONNANCES ET REGLEMENTS
WETTEN, DECRETEN, ORDONNANTIES EN VERORDENINGEN

SERVICE PUBLIC FEDERAL
CHANCELLERIE DU PREMIER MINISTRE

[C − 2019/11507]

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 2005 relative aux communications électroniques, et, pour leurs activités de services de 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.

FEDERALE OVERHEIDSDIENST
KANSELARIJ VAN DE EERSTE MINISTER

[C − 2019/11507]

7 APRIL 2019. — Wet tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (1)

FILIP, Koning der Belgen,

Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

De Kamer van volksvertegenwoordigers heeft aangenomen en Wij bekrachtigen hetgeen volgt :

TITEL 1. — *Definities en algemene bepalingen*

HOOFDSTUK 1. — *Onderwerp en toepassingsgebied*

Afdeling 1. — Onderwerp

Artikel 1. Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.

Art. 2. Deze wet voorziet met name in de omzetting van de Europese Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, hierna de "NIS-richtlijn" genoemd.

Afdeling 2. — Toepassingsgebied

Art. 3. § 1. Deze wet is van toepassing op de aanbieders van essentiële diensten, zoals gedefinieerd in artikel 6, 11°, die minstens één vestiging op Belgisch grondgebied hebben en daadwerkelijk een activiteit uitoefenen die betrekking heeft op de verlening van minstens één essentiële dienst op Belgisch grondgebied.

De bepalingen van titel 1, de artikelen 13, 14 en 30, alsook hoofdstuk 3 van titel 4 zijn van toepassing op de potentiële aanbieders van essentiële diensten.

§ 2. Deze wet is van toepassing op de digitaledienstverleners, zoals gedefinieerd in artikel 6, 21°, die hun hoofdkantoor in België hebben. Een digitaledienstverlener wordt geacht zijn hoofdkantoor in België te hebben als zijn maatschappelijke zetel zich daar bevindt.

Deze wet is ook van toepassing op de digitaledienstverleners die niet in de Europese Unie gevestigd zijn wanneer zij in België diensten verlenen als bedoeld in bijlage II en hun vertegenwoordiger in België gevestigd is in het kader van de NIS-richtlijn.

Art. 4. § 1. De beveiligings- en meldingseisen bedoeld in deze wet zijn niet van toepassing op ondernemingen die onderworpen zijn aan de eisen van de artikelen 114 en 114/1 van de wet van 13 juni 2005 betreffende de elektronische communicatie, wat hun activiteiten betreft op het gebied van het aanbieden van openbare elektronischecommunicatienetwerken of openbare elektronischecommunicatiediensten, en op verleners van vertrouwensdiensten die onderworpen zijn aan de eisen van artikel 19 van de Europese Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, wat hun activiteiten inzake vertrouwensdiensten betreft.

§ 2. Wanneer een sectorspecifieke rechtshandeling van de Europese Unie vereist dat aanbieders van essentiële diensten of digitaledienstverleners zorgen voor de beveiliging van hun netwerk- en informatiesystemen of voor de melding van incidenten, en op voorwaarde dat die eisen ten minste feitelijk gelijkwaardig zijn aan de verplichtingen van deze wet, kunnen de bepalingen betreffende de beveiliging van netwerk- en informatiesystemen en de melding van incidenten van deze handeling afwijken van de bepalingen van deze wet.

De Koning is ermee belast de eventuele gelijkwaardige sectorspecifieke handelingen, als bedoeld in het eerste lid, nader te bepalen.

§ 3. Deze wet is niet van toepassing op de aanbieders die behoren tot de sector financiën in de zin van bijlage I bij deze wet, met uitzondering van de bepalingen van titel I, hoofdstuk 1 van titel II en van artikel 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 46*bis* de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers ou à l'article 12*quater* 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 259*bis*, 314*bis*, 380, 382*quinquies*, 383*bis*, 383*bis*/1, 433*septies*, 433*novies*/1, 458*bis*, 550*bis* et 550*ter* 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 1998 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 ;

In afwijking van het eerste lid is artikel 52 van toepassing op de aanbieders die behoren tot de sector financiën in de zin van bijlage I bij deze wet, met uitzondering van de exploitanten van een handelsplatform in de zin van artikel 3, 6°, van de wet van 21 november 2017 over de infrastructuren voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU.

De sectorale overheden en de aanbieders die behoren tot de sector financiën in de zin van bijlage I bij deze wet zijn onderworpen aan de artikelen 65 tot 73.

In afwijking op wat voorafgaat zijn de artikelen 65 tot 73 niet van toepassing op de betrokken sectorale overheid wanneer deze laatste optreedt in de gevallen bedoeld in artikel 46*bis* van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten, of in artikel 12*quater* van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België.

§ 4. Deze wet is niet van toepassing wanneer en voor zover er maatregelen voor de beveiliging van netwerk- en informatiesystemen bestaan krachtens de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle.

In afwijking van het eerste lid is deze wet van toepassing op de elementen van een nucleaire installatie bestemd voor de industriële productie van elektriciteit die dienen voor de transmissie van de elektriciteit.

Art. 5. § 1. Onder voorbehoud van de bepalingen van titel 6 doet deze wet geen afbreuk aan de toepassing van Verordening EU 2016/679 of aan de wettelijke en reglementaire bepalingen die deze verordening aanvullen of verduidelijken.

§ 2. Deze wet doet geen afbreuk aan de toepassing van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, aan de artikelen 259*bis*, 314*bis*, 380, 382*quinquies*, 383*bis*, 383*bis*/1, 433*septies*, 433*novies*/1, 458*bis*, 550*bis* en 550*ter* van het Strafwetboek, of aan andere bepalingen van het Belgisch recht tot omzetting van Richtlijn 2011/92/EU van het Europees Parlement en de Raad van 13 december 2011 ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie, en ter vervanging van Kaderbesluit 2004/68/JBZ van de Raad, en van Richtlijn 2013/40/EU van het Europees Parlement en de Raad van 12 augustus 2013 over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad.

§ 3. Deze wet doet geen afbreuk aan de regels die van toepassing zijn op de verwerking van informatie, documenten of gegevens, materieel, materialen of stoffen, in welke vorm ook, die geclassificeerd zijn overeenkomstig de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.

§ 4. Deze wet doet geen afbreuk aan de regels die van toepassing zijn op de nucleaire documenten, in de zin van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle.

HOOFDSTUK 2. — *Definities*

Art. 6. Voor de toepassing van deze wet moet worden verstaan onder:

1° "nationaal CSIRT": het nationale computer security incident response team, aangewezen door de Koning;

2° "sectorale overheid": de overheid aangewezen door de wet of de Koning bij besluit vastgesteld na overleg in de Ministerraad;

3° "sectoraal CSIRT": het sectorale computer security incident response team, aangewezen door de Koning;

4° "toezichthoudende autoriteit persoonsgegevens": toezichthoudende autoriteit in de zin van artikel 4, 21°, van Verordening EU 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming);

5° "instelling voor de conformiteitsbeoordeling": instelling bedoeld in artikel I.9.7° van het Wetboek van economisch recht;

6° "certificeringsaudit": een audit uitgevoerd in het kader van een certificering bedoeld in artikel 22, § 2;

7° "nationale accreditatieautoriteit": instelling die door de Koning is opgericht in uitvoering van artikel VIII.30 van het Wetboek van economisch recht;

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 2005 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° "opérateur de services essentiels potentiel " : une entité publique ou privée active en Belgique dans l'un des secteurs repris à l'annexe I de la présente loi, mais qui n'a pas été désignée comme opérateur de services essentiels ;

13° "incident" : tout événement ayant un impact négatif réel sur la sécurité des réseaux et des systèmes d'information ;

14° "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 ;

15° "risque" : toute circonstance ou tout événement raisonnablement identifiable ayant un impact négatif potentiel sur la sécurité des réseaux et des systèmes d'information ;

16° "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) ;

17° "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) ;

18° "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 ;

19° "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.

20° "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 ;

21° "fournisseur de service numérique" : une personne morale qui fournit un service numérique visé à l'annexe II de la présente loi ;

22° "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

8° "netwerk- en informatiesysteem":

a) een elektronische-communicatienetwerk in de zin van artikel 2, 3°, van de wet van 13 juni 2005 betreffende de elektronische communicatie;

b) een apparaat of groep van permanent of tijdelijk gekoppelde of bij elkaar behorende apparaten, waarvan een of meer elementen, in uitvoering van een programma, digitale gegevens automatisch verwerken, met inbegrip van de digitale, elektronische of mechanische componenten van dat apparaat die met name de automatisering van het operationele proces, de controle op afstand of het verkrijgen van werkingsgegevens in real time mogelijk maken;

c) of digitale gegevens die via in de bepalingen onder a) en b), bedoelde elementen worden opgeslagen, verwerkt, opgehaald of verzonden met het oog op de werking, het gebruik, de beveiliging en het onderhoud ervan;

9° "beveiliging van netwerk- en informatiesystemen": het vermogen van netwerk- en informatiesystemen om met een bepaalde mate van betrouwbaarheid bestand te zijn tegen acties die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van de opgeslagen, verzonden of verwerkte gegevens of de daaraan gerelateerde diensten die via die netwerk- en informatiesystemen worden aangeboden of toegankelijk zijn, in gevaar brengen;

10° "nationale strategie voor de beveiliging van netwerk- en informatiesystemen": een kader met strategische doelstellingen en prioriteiten op het gebied van de beveiliging van netwerk- en informatiesystemen op nationaal niveau;

11° "aanbieder van essentiële diensten": een publieke of private entiteit die actief is in België in een van de sectoren opgenomen in bijlage I bij deze wet, die aan de criteria bedoeld in artikel 12, § 1, voldoet en die als dusdanig is aangewezen door de sectorale overheid;

12° "potentiële aanbieder van essentiële diensten": een publieke of private entiteit die in België actief is in een van de sectoren opgenomen in bijlage I bij deze wet, maar niet is aangewezen als aanbieder van essentiële diensten;

13° "incident": elke gebeurtenis met een reële negatieve impact op de beveiliging van netwerk- en informatiesystemen;

14° "incidentenbehandeling": alle procedures ter ondersteuning van de opsporing, analyse en beheersing van en reactie op een incident;

15° "risico": elke redelijkerwijs vast te stellen omstandigheid of gebeurtenis met een mogelijke negatieve impact op de beveiliging van netwerk- en informatiesystemen;

16° "intersectoraal criterium": factor die gemeenschappelijk is voor alle sectoren bedoeld in bijlage I bij deze wet en die het belang van een verstorend effect voor de verlening van een essentiële dienst in de zin van artikel 12, § 1, c), bepaalt;

17° "sectoraal criterium": factor die eigen is aan een sector of deelsector bedoeld in bijlage I bij deze wet en die het belang van een verstorend effect voor de verlening van een essentiële dienst in de zin van artikel 12, § 1, c), bepaalt;

18° "beveiligingsbeleid voor de netwerk- en informatiesystemen (I.B.B.)" : een document als bedoeld in artikel 21, § 1, met de maatregelen voor de beveiliging van de netwerk- en informatiesystemen die een aanbieder van essentiële diensten heeft genomen;

19° "contactpunt voor de beveiliging van netwerk- en informatiesystemen": het contactpunt aangewezen door de aanbieder van essentiële diensten of de digitaledienstverlener dat de functie van contactpunt uitoefent ten aanzien van de autoriteiten bedoeld in artikel 7, voor elke vraag in verband met de beveiliging van de netwerk- en informatiesystemen waarvan de verleende essentiële diensten afhankelijk zijn.

20° "digitale dienst": een dienst in de zin van artikel 1, lid 1, punt b), van de Europese Richtlijn 2015/1535 van het Europees Parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij, en waarvan de soort is vermeld in de lijst in bijlage II;

21° "digitaledienstverlener": elke rechtspersoon die een digitale dienst aanbiedt als bedoeld in bijlage II bij deze wet;

22° "vertegenwoordiger van een digitaledienstverlener": elke in België gevestigde natuurlijke of rechtspersoon die uitdrukkelijk is aangewezen om voor rekening van een niet in de Unie gevestigde digitaledienstverlener op te treden en die door de nationale autoriteit bedoeld in artikel 7, § 1, de bevoegde sectorale overheid of de bevoegde inspectiedienst kan worden gecontacteerd in plaats van

service numérique concernant ses obligations découlant de la présente loi ;

23° "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 ;

24° "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 ;

25° "fournisseur de services DNS" : une entité qui fournit des services DNS sur l'internet ;

26° "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 ;

27° "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 ;

28° "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 ;

29° "service d'informatique en nuage" : un service numérique qui permet l'accès à un ensemble modulable et variable de ressources informatiques pouvant être partagées ;

30° "loi du 1er juillet 2011" : la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques ;

31° "loi du 11 décembre 1998" : la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité ;

32° "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 ;

33° "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 œuvre de la présente loi.

L'autorité visée à l'alinéa 1er est également le point de contact national unique en matière de sécurité 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 États 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 œuvre des dispositions de la présente loi.

de digitaledienstverlener, wat de uit deze wet voortvloeiende verplichtingen van deze laatste betreft;

23° "internetknooppunt (IXP)": een netwerkinfrastructuur die de onderlinge verbinding van meer dan twee onafhankelijke autonome systemen mogelijk maakt, voornamelijk met als doel de uitwisseling van internetverkeer te vergemakkelijken; een internetknooppunt zorgt enkel voor onderlinge verbinding voor autonome systemen; een internetknooppunt vereist niet dat het internetverkeer tussen twee deelnemende autonome systemen via een derde autonoom systeem verloopt, noch dat het internetknooppunt dergelijk verkeer wijzigt of anderszins daartussen komt;

24° "domeinnaamsysteem" of "DNS": een hiërarchisch opgebouwd adresseringssysteem in een netwerk dat een zoekvraag naar een domeinnaam beantwoordt;

25° "DNS-dienstverlener": een entiteit die DNS-diensten op het internet verleent;

26° "register voor topleveldomeinnamen": een entiteit die de internetdomeinnamen van een specifiek topleveldomein registreert en beheert;

27° "onlinemarktplaats": een digitale dienst die het consumenten, zoals gedefinieerd in artikel I.1., eerste lid, 2°, van het Wetboek van economisch recht, en/of ondernemingen, zoals gedefinieerd in artikel I.8, 39°, van hetzelfde Wetboek, mogelijk maakt online verkoop- of dienstenovereenkomsten met ondernemingen te sluiten op de website van de onlinemarktplaats of op de website van een onderneming die gebruikmaakt van door de onlinemarktplaats aangeboden informaticadiensten;

28° "onlinezoekmachine": een digitale dienst die het gebruikers mogelijk maakt zoekacties uit te voeren op in principe alle websites of websites in een bepaalde taal op basis van een zoekvraag over om het even welk onderwerp in de vorm van een trefwoord, een zin of andere input; het resultaat zijn hyperlinks naar informatie over de opgevraagde inhoud;

29° "cloudcomputerdienst": een digitale dienst die toegang mogelijk maakt tot een schaalbare en elastische pool van deelbare computercapaciteit;

30° "wet van 1 juli 2011": de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren;

31° "wet van 11 december 1998": de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen;

32° "wet van 15 april 1994": de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle.

33° "Verordening EU 2016/679": de Europese Verordening 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

HOOFDSTUK 3. — *Bevoegde autoriteiten en samenwerking op nationaal niveau*

Afdeling 1. — Bevoegde autoriteiten

Art. 7. § 1. De Koning wijst de autoriteit aan die, als nationale autoriteit, belast is met de opvolging en coördinatie van de uitvoering van deze wet.

De autoriteit bedoeld in het eerste lid is ook het centraal nationaal contactpunt voor de beveiliging van netwerk- en informatiesystemen, voor alle aanbieders van essentiële diensten en digitaledienstverleners, voor België in zijn relatie met de Europese Commissie, de lidstaten van de Europese Unie, de in artikel 11 van de NIS-richtlijn bedoelde Samenwerkingsgroep en het CSIRT-netwerk. Daartoe vertegenwoordigt het contactpunt België binnen de Samenwerkingsgroep.

§ 2. De Koning wijst de autoriteit aan die de rol van nationaal CSIRT vervult.

Het nationale CSIRT vertegenwoordigt België binnen het CSIRT-netwerk bedoeld in artikel 12 van de NIS-richtlijn. Het werkt op doeltreffende, efficiënte en beveiligde wijze mee aan de opdrachten van het CSIRT-netwerk.

§ 3. De Koning wijst, bij besluit vastgesteld na overleg in de Ministerraad, de sectorale overheden aan die, voor hun respectievelijke sector, belast zijn met het toezicht op de uitvoering van de bepalingen van deze wet.

Le Roi peut créer des autorités sectorielles, composées de représentants de l'État fédéral, des Communautés et des Régions, conformément aux modalités prévues à l'article 92*ter* 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'État, les autorités administratives, les autorités judiciaires, les services de renseignement et de sécurité visés par la loi du 30 novembre 1998 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 1998, 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.

De Koning kan sectorale overheden oprichten, bestaande uit vertegenwoordigers van de Federale Staat, de Gemeenschappen en de Gewesten, overeenkomstig de nadere regels bepaald in artikel 92*ter* van de bijzondere wet van 8 augustus 1980 tot hervorming der instellingen.

In afwijking van het eerste lid wijst de wet zelf de bij wet opgerichte en geregelde sectorale overheden aan.

§ 4. De Koning wijst de autoriteit aan die, in samenwerking met de nationale autoriteit bedoeld in paragraaf 1, de identificatie van aanbieders van essentiële diensten coördineert.

§ 5. Per sector of, in voorkomend geval, per deelsector wordt een inspectiedienst opgericht die toeziet op de naleving van de bepalingen van deze wet en van de uitvoeringsbesluiten ervan door aanbieders van essentiële diensten of digitaledienstverleners.

De Koning wijst voor een welbepaalde sector of, in voorkomend geval, per deelsector de inspectiedienst aan die bevoegd is voor het toezicht.

In afwijking van het tweede lid wijst de wet de door haar opgerichte en geregelde inspectiediensten aan.

Afdeling 2. — Samenwerking op nationaal niveau

Art. 8. § 1. De autoriteiten bedoeld in artikel 7 werken nauw samen om de in deze wet vastgestelde verplichtingen te vervullen.

§ 2. Naargelang de behoeften die nodig zijn voor de uitvoering van de wet en overeenkomstig de toepasselijke wettelijke bepalingen werken de in paragraaf 1 bedoelde autoriteiten, op nationaal niveau, ook samen met de administratieve diensten van de Staat, de administratieve autoriteiten, de gerechtelijke autoriteiten, de inlichtingen- en veiligheidsdiensten bedoeld in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, de politiediensten bedoeld in de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus, en met de toezichthoudende autoriteiten persoonsgegevens.

§ 3. De aanbieder van essentiële diensten, de digitaledienstverlener en de autoriteiten bedoeld in artikel 7 werken te allen tijde samen door een adequate uitwisseling van informatie over de beveiliging van de netwerk- en informatiesystemen.

HOOFDSTUK 4. — *Informatie-uitwisseling*

Art. 9. § 1. Dit artikel doet geen afbreuk aan de toepassing van de wet van 11 december 1998, de wet van 15 april 1994, de wet van 11 april 1994 betreffende de openbaarheid van bestuur of andere wettelijke bepalingen die de vertrouwelijkheid van de informatie m.b.t. de wezenlijke belangen van de nationale openbare veiligheid waarborgen.

De autoriteiten bedoeld in artikel 7, de aanbieder van essentiële diensten, de digitaledienstverlener, of hun onderaannemers, beperken de toegang tot de informatie over de uitvoering van deze wet tot de personen die er de kennis van nodig hebben en er toegang toe moeten hebben voor de uitoefening van hun functie of opdracht die verband houdt met deze wet.

§ 2. De personeelsleden van de aanbieder van essentiële diensten, de digitaledienstverlener, of hun onderaannemers, zijn gebonden aan het beroepsgeheim wat de informatie over de uitvoering van deze wet betreft.

Personen die uit hoofde van hun staat of beroep kennis dragen van geheimen die hun zijn toevertrouwd, mogen deze geheimen bekendmaken voor de uitvoering van deze wet.

§ 3. De informatie die door aanbieders van essentiële diensten en digitaledienstverleners aan de autoriteiten bedoeld in artikel 7 wordt bezorgd, mag worden uitgewisseld met autoriteiten van de Europese Unie, Belgische of buitenlandse autoriteiten, wanneer die uitwisseling noodzakelijk is voor de toepassing van wettelijke bepalingen.

De uitgewisselde informatie wordt beperkt tot hetgeen relevant is voor en evenredig is met het doel van die uitwisseling, met name overeenkomstig Verordening EU 2016/679. Bij die uitwisseling van informatie wordt de vertrouwelijkheid van de informatie gewaarborgd en worden de veiligheid en de commerciële belangen van de aanbieders van essentiële diensten en de digitaledienstverleners beschermd.

HOOFDSTUK 5. — *Nationale strategie voor de beveiliging van netwerk- en informatiesystemen*

Art. 10. § 1. De Koning wijst, bij besluit vastgesteld na overleg in de Ministerraad, de autoriteit aan die belast is met de actualisering van de bestaande nationale strategie voor de beveiliging van netwerk- en informatiesystemen.

§ 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 œuvre 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.

§ 2. De in paragraaf 1 bedoelde strategie wordt geactualiseerd na advies van de autoriteiten bedoeld in artikel 7 en, in voorkomend geval, van de toezichthoudende autoriteiten persoonsgegevens. Ze heeft minstens betrekking op de sectoren bedoeld in bijlage I en de diensten bedoeld in bijlage II.

In deze strategie worden passende strategische en regelgevingsdoelstellingen bepaald om een hoog niveau van beveiliging van netwerk- en informatiesystemen tot stand te brengen en te handhaven.

§ 3. De nationale strategie voor de beveiliging van netwerk- en informatiesystemen betreft onder meer de volgende punten:

a) de doelstellingen en de prioriteiten van de nationale strategie voor de beveiliging van netwerk- en informatiesystemen;

b) een governancekader ter verwezenlijking van de doelstellingen en de prioriteiten van de nationale strategie voor de beveiliging van netwerk- en informatiesystemen, met inbegrip van de taken en verantwoordelijkheden van de overheidsorganen en de andere betrokken actoren;

c) de bepaling van maatregelen inzake paraatheid, reactie en herstel, met inbegrip van samenwerking tussen de publieke en de particuliere sector;

d) een overzicht van de onderwijs-, bewustmakings- en opleidingsprogramma's met betrekking tot de nationale strategie voor de beveiliging van netwerk- en informatiesystemen;

e) een overzicht van de plannen voor onderzoek en ontwikkeling met betrekking tot de nationale strategie voor de beveiliging van netwerk- en informatiesystemen;

f) een risicobeoordelingsplan om risico's te identificeren;

g) een lijst van de verschillende actoren die betrokken zijn bij de uitvoering van de nationale strategie voor de beveiliging van netwerk- en informatiesystemen.

TITEL 2. — *Netwerk- en informatiesystemen van de aanbieders van essentiële diensten*

HOOFDSTUK 1. — *Identificatie van de aanbieders van essentiële diensten*

Art. 11. § 1. De sectorale overheid identificeert de aanbieders van essentiële diensten van haar sector en houdt hierbij minstens rekening met de soorten aanbieders bedoeld in bijlage I van deze wet.

Binnen de grenzen van hun respectievelijke bevoegdheden overleggen de autoriteiten bedoeld in artikel 7, §§ 1 en 4, met de sectorale overheid om over te gaan tot deze identificatie.

De sectorale overheid raadpleegt, in voorkomend geval, de betrokken gewesten of gemeenschappen en de vertegenwoordigers van de in bijlage I bedoelde entiteiten.

§ 2. Na raadpleging van de potentiële aanbieder van essentiële diensten deelt de sectorale overheid deze aanbieder mee welke door hem verleende dienst of diensten als essentieel worden beschouwd.

§ 3. De sectorale overheid zorgt voor een permanente opvolging van het identificatie- en aanwijzingsproces van de aanbieders van essentiële diensten en van hun essentiële diensten, volgens de in dit hoofdstuk beschreven procedures. Dit proces vindt voor het eerst plaats uiterlijk binnen zes maanden na de inwerkingtreding van deze wet.

De sectorale overheid evalueert en, in voorkomend geval, actualiseert minstens om de twee jaar de identificatie van de aanbieders van essentiële diensten en van hun essentiële diensten.

De actualiseringen worden naar de autoriteiten bedoeld in artikel 7, §§ 1 en 4, gestuurd.

Art. 12. § 1. Om de in artikel 11 bedoelde aanbieders te identificeren, past de sectorale overheid de volgende criteria toe:

a) de entiteit verleent een dienst die van essentieel belang is voor de instandhouding van kritieke maatschappelijke en/of economische activiteiten;

b) de verlening van die dienst is afhankelijk van netwerk- en informatiesystemen; en

c) een incident kan aanzienlijke verstorende effecten hebben voor de verlening van die dienst, rekening houdend met de in artikel 13 bedoelde criteria en weerslagniveaus of drempelwaarden.

§ 2. Behoudens tegenbewijs wordt de verlening van een essentiële dienst geacht afhankelijk te zijn van netwerk- en informatiesystemen.

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 État 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. 13. § 1. Om het belang van het in artikel 12, § 1, c), bedoelde verstorende effect vast te stellen, bepaalt de sectorale overheid sectorale en/of intersectorale criteria, weerslagniveaus of drempelwaarden voor haar sector.

Het aanzienlijke verstorende effect staat vast zodra de potentiële aanbieder van essentiële diensten aan een drempelwaarde of weerslagniveau voldoet.

Binnen de grenzen van hun respectievelijke bevoegdheden overleggen de autoriteiten bedoeld in artikel 7, §§ 1 en 4, met de sectorale overheid om de criteria, weerslagniveaus en drempelwaarden te bepalen, in voorkomend geval na raadpleging van de betrokken gewesten of gemeenschappen en van de vertegenwoordigers van de in bijlage I bedoelde entiteiten.

§ 2. De sectorale overheid houdt minstens rekening met de volgende intersectorale criteria op basis van de beschikbare informatie:

a) het aantal gebruikers dat afhankelijk is van de door de betrokken entiteit verleende dienst;

b) de afhankelijkheid van de andere in bijlage I bedoelde sectoren van de door die entiteit verleende dienst;

c) de gevolgen die incidenten kunnen hebben, wat betreft mate en duur, voor economische of maatschappelijke activiteiten of de openbare veiligheid;

d) het marktaandeel van die entiteit;

e) de omvang van het geografische gebied dat door een incident kan worden getroffen;

f) het belang van de entiteit voor de instandhouding van een toereikend dienstverleningsniveau, rekening houdend met de beschikbare alternatieven voor het verlenen van die dienst.

§ 3. Na advies van de autoriteiten bedoeld in artikel 7 en raadpleging van de betrokken gewesten en gemeenschappen kan de Koning deze intersectorale criteria aanvullen.

Art. 14. De potentiële aanbieder van essentiële diensten bezorgt, op verzoek van een autoriteit bedoeld in artikel 7, alle nuttige informatie over zijn eventuele identificatie als aanbieder van essentiële diensten, met inbegrip van de informatie die toelaat te objectiveren of de verlening van de essentiële dienst al dan niet afhankelijk is van netwerk- en informatiesystemen.

De door de potentiële aanbieder overgezonden relevante informatie wordt meegedeeld aan de andere autoriteiten bedoeld in artikel 7.

Art. 15. § 1. De sectorale overheid bezorgt de autoriteiten bedoeld in artikel 7, §§ 1 en 4, een met redenen omkleed voorstel van lijst van aanbieders van essentiële diensten van haar sector, samen met een of meer toegepaste identificatiecriteria.

Wanneer de sectorale overheid geen enkele aanbieder van essentiële diensten binnen een sector of deelsector heeft voorgesteld, licht ze de redenen hiervoor schriftelijk toe.

De autoriteiten bedoeld in artikel 7, §§ 1 en 4, brengen, binnen de grenzen van hun respectievelijke bevoegdheden, advies uit over het met redenen omklede voorstel van lijst, in voorkomend geval na raadpleging van de gewesten en gemeenschappen.

§ 2. Wanneer de sectorale overheid vaststelt dat de entiteit die zij voornemens is aan te wijzen als aanbieder van essentiële diensten een of meer essentiële diensten in minstens één andere lidstaat van de Europese Unie verleent, brengt ze de autoriteiten bedoeld in artikel 7, §§ 1 en 4, daarvan op de hoogte. Deze laatsten organiseren, in samenwerking met de betrokken sectorale overheden, de besprekingen met de betrokken buitenlandse nationale autoriteit of autoriteiten en, in voorkomend geval, met de betrokken gewesten of gemeenschappen.

§ 3. De sectorale overheid stelt de aanbieder in kennis van haar met redenen omklede beslissing betreffende zijn aanwijzing als aanbieder van essentiële diensten. Deze kennisgeving gebeurt op beveiligde wijze.

Ze bezorgt ook een kopie van deze beslissing aan de autoriteiten bedoeld in artikel 7, §§ 1 en 4.

In voorkomend geval brengt de sectorale overheid de betrokken gewesten en/of gemeenschappen hiervan op de hoogte.

Art. 16. Binnen drie maanden na zijn aanwijzing bezorgt de aanbieder van essentiële diensten de sectorale overheid een beschrijving van de netwerk- en informatiesystemen waarvan de verlening van de betrokken essentiële dienst of diensten afhankelijk is.

De sectorale overheid bezorgt deze beschrijving aan de autoriteit bedoeld in artikel 7, § 1.

Art. 17. Sans préjudice de l'application éventuelle de la loi du 11 décembre 1998, 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 œuvre 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

Art. 17. Onverminderd de eventuele toepassing van de wet van 11 december 1998 worden de bestuursdocumenten betreffende de toepassing van dit hoofdstuk als bestuursdocumenten beschouwd die verband houden met de veiligheid van de bevolking, de openbare orde en de veiligheid, in de zin van artikel 6, § 1, van de wet van 11 april 1994 betreffende de openbaarheid van bestuur, en die niet het voorwerp mogen uitmaken van inzage, uitleg of mededeling in afschrift voor het publiek.

Art. 18. § 1. In afwijking van artikel 11 wijst de sectorale overheid de exploitanten van kritieke infrastructuren aan, zoals aangeduid krachtens artikel 8 van de wet van 1 juli 2011 en artikel 6 van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer, als aanbieders van essentiële diensten, wanneer hun sector is opgenomen in bijlage I van deze wet en de verlening van hun essentiële diensten afhankelijk is van netwerk- en informatiesystemen.

Deze aanwijzing gebeurt in overleg met de autoriteiten bedoeld in artikel 7, §§ 1 en 4, binnen de grenzen van hun respectievelijke bevoegdheden.

§ 2. Behoudens tegenbewijs wordt de exploitatie van een kritieke infrastructuur geacht afhankelijk te zijn van netwerk- en informatiesystemen.

§ 3. De exploitant bezorgt de sectorale overheid, op haar verzoek of op verzoek van de autoriteiten bedoeld in artikel 7, §§ 1 en 4, alle nuttige informatie over zijn eventuele identificatie als aanbieder van essentiële diensten, met inbegrip van de informatie die toelaat te objectiveren of hij al dan niet afhankelijk is van netwerk- en informatiesystemen.

De sectorale overheid bezorgt de door de exploitant meegedeelde relevante informatie aan de autoriteiten bedoeld in artikel 7, §§ 1 en 4.

§ 4. Artikel 15, § 3, is van toepassing op de met redenen omklede beslissing tot aanwijzing van een exploitant van een kritieke infrastructuur als aanbieder van essentiële diensten.

Art. 19. De Koning kan, bij besluit vastgesteld na overleg in de Ministerraad, andere sectoren of soorten aanbieders toevoegen aan bijlage I van deze wet.

HOOFDSTUK 2. — *Beveiligingsmaatregelen*

Art. 20. De aanbieder van essentiële diensten neemt passende en evenredige technische en organisatorische maatregelen om de risico's voor de beveiliging van netwerk- en informatiesystemen waarvan zijn essentiële diensten afhankelijk zijn, te beheersen.

Deze maatregelen zorgen, rekening houdend met de stand van de technische kennis, voor een niveau van fysieke en logische beveiliging van netwerk- en informatiesystemen dat is afgestemd op de risico's die zich voordoen.

De aanbieder neemt ook passende maatregelen om incidenten die de beveiliging van de voor de verlening van die essentiële diensten gebruikte netwerk- en informatiesystemen aantasten, te voorkomen of de gevolgen ervan te minimaliseren, teneinde de continuïteit van deze diensten te waarborgen.

Art. 21. § 1. De aanbieder van essentiële diensten werkt een beveiligingsbeleid uit voor zijn netwerk- en informatiesystemen (hierna "I.B.B." genoemd) dat minstens de in artikel 20 bedoelde concrete beveiligingsdoelstellingen en -maatregelen bevat.

§ 2. De aanbieder van essentiële diensten werkt zijn I.B.B. uiterlijk uit binnen een termijn van twaalf maanden na de kennisgeving van zijn aanwijzing. Hij implementeert de in zijn I.B.B. beschreven maatregelen uiterlijk binnen een termijn van vierentwintig maanden na de kennisgeving van zijn aanwijzing.

Voor een welbepaalde sector of, in voorkomend geval, per deelsector kan de bevoegde sectorale overheid deze termijn aanpassen in functie van het soort maatregelen waarin het I.B.B. voorziet.

§ 3. Na advies van de autoriteiten bedoeld in artikel 7 en, in voorkomend geval, na raadpleging van de betrokken gewesten of gemeenschappen kan de Koning de aanbieders van essentiële diensten van een of meer sectoren beveiligingsmaatregelen opleggen.

§ 4. In overleg met de autoriteit bedoeld in artikel 7, § 1, en, in voorkomend geval, na raadpleging van de gewesten of gemeenschappen kan de sectorale overheid, bij individuele administratieve beslissing, bijkomende beveiligingsmaatregelen opleggen.

§ 5. De maatregelen voor de fysieke en logische beveiliging van netwerk- en informatiesystemen die zijn opgenomen in het beveiligingsplan van de exploitant (B.P.E.) bedoeld in artikel 13 van de wet van 1 juli 2011 en in artikel 11 van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het

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.

luchtvervoer, worden gelijkgesteld met het I.B.B. indien alle in paragraaf 2 bedoelde informatie erin opgenomen is.

Art. 22. § 1. Het I.B.B. bedoeld in artikel 21, § 1, wordt tot bewijs van het tegendeel geacht conform te zijn met de beveiligingseisen bedoeld in artikel 20, indien de beveiligingsmaatregelen die het invoert voldoen aan de eisen van de norm ISO/IEC 27001 of aan een nationale, buitenlandse of internationale norm die door de Koning als gelijkwaardig wordt erkend, bij besluit vastgesteld na overleg in de Ministerraad.

Het in het eerste lid bedoelde besluit wordt genomen na advies van de nationale accreditatieautoriteit, de sectorale overheid en de autoriteit bedoeld in artikel 7, § 1.

§ 2. De naleving van de eisen bedoeld in paragraaf 1 wordt aangetoond aan de hand van een certificaat uitgereikt door een instelling voor de conformiteitsbeoordeling die volgens de norm ISO/IEC 17021 of ISO/IEC 17065 geaccrediteerd is door de nationale accreditatieautoriteit of door een instelling die de erkenningsakkoorden van de "European Cooperation for Accreditation" medeondertekend heeft.

Het uitgereikte certificaat moet betrekking hebben op het certificeringsdomein waarvoor de instelling voor de conformiteitsbeoordeling geaccrediteerd is en op de volledige inhoud van het I.B.B.

Art. 23. § 1. De aanbieder van essentiële diensten wijst zijn contactpunt aan voor de beveiliging van netwerk- en informatiesystemen en deelt de gegevens ervan mee aan de bevoegde sectorale overheid binnen een termijn van drie maanden na de kennisgeving van de aanwijzing als aanbieder van essentiële diensten, en, onverwijld, na elke actualisering van deze gegevens.

De sectorale overheid stelt deze gegevens ter beschikking van de autoriteiten bedoeld in artikel 7, §§ 1, en 4.

§ 2. Indien er reeds een beveiligingscontactpunt bestaat krachtens nationale of internationale bepalingen die van toepassing zijn in een sector of een deelsector, bezorgt de aanbieder van essentiële diensten de contactgegevens ervan aan de sectorale overheid binnen de in paragraaf 1 bedoelde termijnen.

§ 3. Het in paragraaf 1 bedoelde contactpunt voor de beveiliging van netwerk- en informatiesystemen is te allen tijde beschikbaar.

HOOFDSTUK 3. — *Melding van incidenten*

Art. 24. § 1. De aanbieder van essentiële diensten meldt onverwijld alle incidenten die aanzienlijke gevolgen hebben voor de beschikbaarheid, vertrouwelijkheid, integriteit of authenticiteit van de netwerk- en informatiesystemen waarvan de door hem verleende essentiële dienst of diensten afhankelijk zijn.

§ 2. Na advies van het nationale CSIRT, de autoriteit bedoeld in artikel 7, § 4, de sectorale overheid en, in voorkomend geval, van de betrokken gewesten of gemeenschappen, kan de Koning, per sector of deelsector, de weerslagniveaus en/of de drempelwaarden bepalen die minstens aanzienlijke gevolgen hebben in de zin van paragraaf 1.

§ 3. Indien geen weerslagniveaus en/of drempelwaarden als bedoeld in paragraaf 2 zijn bepaald, meldt de aanbieder alle incidenten die gevolgen hebben voor de beschikbaarheid, vertrouwelijkheid, integriteit of authenticiteit van de netwerk- en informatiesystemen waarvan de door hem verleende essentiële dienst of diensten afhankelijk zijn.

§ 4. De Koning kan verschillende meldingscategorieën creëren volgens de mate van impact van het incident.

Art. 25. De melding bedoeld in artikel 24 gebeurt tegelijkertijd bij het nationale CSIRT, de sectorale overheid of haar sectorale CSIRT, en de autoriteit bedoeld in artikel 7, § 4.

De meldingsplicht is van toepassing zelfs wanneer de aanbieder van essentiële diensten slechts gedeeltelijk over de relevante informatie beschikt om te bepalen of het incident een aanzienlijke impact heeft.

Art. 26. § 1. Dit hoofdstuk is van toepassing op de exploitanten van een handelsplatform in de zin van artikel 3, 6°, van de wet van 21 november 2017 over de infrastructuren voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU.

§ 2. Aanbieders die behoren tot de sector financiën in de zin van bijlage I van de wet, met uitzondering van de exploitanten van een handelsplatform, melden onverwijld aan de Nationale Bank van België (NBB) alle incidenten die aanzienlijke gevolgen hebben voor de beschikbaarheid, vertrouwelijkheid, integriteit of authenticiteit van de netwerk- en informatiesystemen waarvan de door hen verleende essentiële dienst of diensten afhankelijk zijn. De NBB bepaalt de aanzienlijke gevolgen bedoeld in dit lid.

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 États membres de l'Union européenne touchés, si l'incident a un impact significatif sur la continuité des services essentiels dans ces États 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 États 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 volontaires.

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.

De NBB bezorgt de melding vervolgens onverwijld aan het nationale CSIRT en de autoriteit bedoeld in artikel 7, § 4.

Art. 27. De onderneming die een digitale dienst verleent aan een aanbieder van essentiële diensten en die onderworpen is aan deze wet, meldt deze aanbieder onverwijld alle incidenten die aanzienlijke gevolgen, in de zin van artikel 24, hebben voor de continuïteit van zijn essentiële diensten.

Vervolgens meldt de aanbieder van essentiële diensten dit incident volgens de in dit hoofdstuk beschreven procedures.

Art. 28. § 1. Wanneer een aanbieder van essentiële diensten getroffen is door een incident met aanzienlijke gevolgen in de zin van artikel 24, is hij verplicht het incident aan te pakken en reactieve maatregelen te nemen om het op te lossen.

De aanbieder van essentiële diensten blijft verantwoordelijk voor de aanpak van het incident.

§ 2. De aanbieder van essentiële diensten onderzoekt incidenten of verdachte gebeurtenissen die hem door het nationale CSIRT, de sectorale overheid of de autoriteit bedoeld in artikel 7, § 4, worden gemeld.

Art. 29. Op basis van de informatie in de melding van de aanbieder van essentiële diensten informeert het nationale CSIRT de andere getroffen lidstaten van de Europese Unie als het incident aanzienlijke gevolgen heeft voor de continuïteit van essentiële diensten in die lidstaten. Het nationale CSIRT beschermt daarbij, overeenkomstig het Unierecht of nationale wetgeving die met het Unierecht in overeenstemming is, de veiligheids- en commerciële belangen van de aanbieder van essentiële diensten alsook de vertrouwelijkheid van de informatie in diens melding.

Het nationale CSIRT bezorgt de in het eerste lid bedoelde meldingen aan de centrale contactpunten van de andere getroffen lidstaten.

Art. 30. § 1. De potentiële aanbieders van essentiële diensten mogen op vrijwillige basis incidenten melden die aanzienlijke gevolgen hebben voor de continuïteit van de door hen in België verleende diensten.

Vrijwillige melding mag niet leiden tot het opleggen aan de meldende entiteit van verplichtingen waaraan zij niet zou zijn onderworpen als zij die melding niet had gedaan.

§ 2. Bij de behandeling van meldingen mogen het nationale CSIRT, de sectorale overheid of haar sectorale CSIRT, en de autoriteit bedoeld in artikel 7, § 4, de door deze wet opgelegde verplichte meldingen prioritair verwerken ten opzichte van vrijwillige meldingen.

Vrijwillige meldingen worden enkel verwerkt wanneer die verwerking geen onevenredige of overmatige belasting vormt voor het nationale CSIRT, de sectorale overheid of haar sectorale CSIRT, en de autoriteit bedoeld in artikel 7, § 4.

Art. 31. § 1. De Koning is ermee belast de nadere regels voor de melding en rapportering van incidenten te bepalen, en een beveiligd meldingsplatform op te richten.

Via dit platform kunnen aanbieders van essentiële diensten ook inbreuken in verband met persoonsgegevens melden aan de toezichthoudende autoriteiten, zoals opgelegd door artikel 33, eerste alinea, van Verordening EU 2016/679.

§ 2. Wanneer publieke bewustwording nodig is om een incident te voorkomen of een lopend incident te beheersen, kan het nationale CSIRT na raadpleging van de aanbieder die de melding heeft ingediend en van de bevoegde sectorale overheid, het publiek over afzonderlijke incidenten informeren. Hierbij wordt uitsluitend algemene informatie over het incident meegedeeld.

TITEL 3. — *Netwerk- en informatiesystemen van digitaledienstverleners*

HOOFDSTUK 1. — *Toepassingsgebied*

Art. 32. Deze titel is niet van toepassing op micro- en kleine ondernemingen zoals gedefinieerd in de aanbeveling van de Europese Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (2003/361/EG).

HOOFDSTUK 2. — *De beveiligingseisen*

Art. 33. § 1. De digitaledienstverleners identificeren de risico's voor de beveiliging van de netwerk- en informatiesystemen die zij gebruiken voor het aanbieden in de Europese Unie van de in bijlage II bedoelde diensten en nemen passende en evenredige technische en organisatorische maatregelen om die risico's te beheersen.

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 État membre de l'Union européenne, le CSIRT national informe le ou les autres États 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 États 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.

Deze maatregelen zorgen, rekening houdend met de stand van de technische kennis, voor een niveau van beveiliging van netwerk- en informatiesystemen dat is afgestemd op de risico's die zich voordoen, en houden rekening met de volgende aspecten:

a) de beveiliging van systemen en voorzieningen;

b) de behandeling van incidenten;

c) het beheer van de bedrijfscontinuïteit;

d) toezicht, controle en testen;

e) de inachtneming van de internationale normen.

§ 2. De digitaledienstverleners nemen ook maatregelen om incidenten die de beveiliging van hun netwerk- en informatiesystemen aantasten, voor de in bijlage II van deze wet bedoelde diensten die in de Europese Unie worden aangeboden, te voorkomen en te minimaliseren, teneinde de continuïteit van deze diensten te waarborgen.

Art. 34. De digitaledienstverleners wijzen een contactpunt aan voor de computerbeveiliging en delen de gegevens ervan mee aan de sectorale overheid die bevoegd is voor de digitaledienstverleners, alsook na elke actualisering van deze gegevens. De sectorale overheid bezorgt deze informatie aan de nationale autoriteit bedoeld in artikel 7, § 1.

HOOFDSTUK 3. — *Melding van incidenten*

Art. 35. § 1. De digitaledienstverleners melden onverwijld ieder incident dat aanzienlijke gevolgen heeft voor de verlening van een door hen in de Europese Unie aangeboden dienst als bedoeld in bijlage II.

Incidenten worden tegelijkertijd gemeld aan het nationale CSIRT, de sectorale overheid of haar sectorale CSIRT, en de autoriteit bedoeld in artikel 7, § 4, via het meldingsplatform bedoeld in artikel 31.

§ 2. De melding gebeurt overeenkomstig de uitvoeringsverordeningen van de Europese Commissie, waaronder de Uitvoeringsverordening (EU) 2018/151 van 30 januari 2018 tot vaststelling van toepassingsbepalingen voor Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad wat betreft de nadere specificatie van de door digitaledienstverleners in aanmerking te nemen elementen voor het beheer van de risico's in verband met de beveiliging van netwerk- en informatiesystemen en van de parameters om te bepalen of een incident aanzienlijke gevolgen heeft.

De meldingen bevatten informatie om te bepalen of de eventuele grensoverschrijdende impact van het incident aanzienlijk is. Melding leidt voor de meldende partij niet tot een verhoogde aansprakelijkheid.

§ 3. De verplichting om een incident te melden geldt alleen wanneer de digitaledienstverlener toegang heeft tot de informatie die nodig is om de gevolgen van een incident volledig of gedeeltelijk te beoordelen.

Art. 36. § 1. Deze melding gebeurt overeenkomstig de door de Koning bepaalde nadere regels en via het platform bedoeld in artikel 31.

§ 2. Via het platform bedoeld in artikel 31 kunnen digitaledienstverleners ook inbreuken in verband met persoonsgegevens melden aan de toezichthoudende autoriteiten, zoals opgelegd door artikel 33, eerste alinea, van Verordening EU 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

Art. 37. § 1. Het nationale CSIRT stelt in voorkomend geval, en in het bijzonder indien het in artikel 35, paragraaf 1 bedoelde incident op minstens één andere lidstaat van de Europese Unie betrekking heeft, de andere getroffen lidstaat of lidstaten in kennis. Het nationale CSIRT beschermt daarbij, overeenkomstig de nationale wetgeving en het Unierecht, de veiligheids- en commerciële belangen van de digitaledienstverlener alsook de vertrouwelijkheid van de verstrekte informatie.

§ 2. Na raadpleging van de betrokken digitaledienstverlener, de sectorale overheid en, in voorkomend geval, de autoriteiten of CSIRT's van de andere betrokken lidstaten van de Europese Unie kan het nationale CSIRT het publiek informeren over afzonderlijke incidenten of eisen dat de digitaledienstverlener dit doet. Het verstrekken van deze informatie kan met name nodig zijn wanneer publieke bewustwording zou toelaten een incident te voorkomen of een lopend incident te beheersen, of wanneer de openbaarmaking van het incident anderszins in het algemeen belang is.

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.

TITEL 4. — *Toezicht en sancties*

HOOFDSTUK 1. — *Toezicht op de aanbieders van essentiële diensten*

Afdeling 1. — Audits

Art. 38. § 1. De aanbieder van essentiële diensten voert, jaarlijks en op zijn kosten, een interne audit uit van de netwerk- en informatiesystemen waarvan de door hem verleende essentiële diensten afhankelijk zijn. Deze interne audit moet de aanbieder van essentiële diensten toelaten zich ervan te vergewissen dat de in zijn I.B.B. bepaalde maatregelen en processen goed worden toegepast en regelmatig worden gecontroleerd.

De aanbieder van essentiële diensten bezorgt de interne auditverslagen binnen de dertig dagen aan de sectorale overheid.

§ 2. De aanbieder van essentiële diensten laat, minstens om de drie jaar en op zijn kosten, een externe audit uitvoeren door een instelling voor de conformiteitsbeoordeling die geaccrediteerd is door de nationale accreditatieautoriteit of door een instelling die de erkenningsakkoorden van de "European Cooperation for Accreditation" medeondertekend heeft.

De aanbieder van essentiële diensten bezorgt de externe auditverslagen binnen de dertig dagen aan de sectorale overheid.

§ 3. De aanbieder van essentiële diensten voert zijn eerste interne audit uit uiterlijk binnen de drie maanden na de uitwerking van zijn I.B.B. Hij voert zijn eerste externe audit uit uiterlijk binnen de vierentwintig maanden na de uitvoering van zijn eerste interne audit.

Art. 39. § 1. Na advies van de sectorale overheid en de autoriteit bedoeld in artikel 7, § 1, bepaalt de Koning:

1° de algemene accreditatievoorwaarden op basis van de eisen van de normen ISO/IEC 17021 of ISO/IEC 17065;

2° de bijkomende sectorale eisen waaraan de instelling voor de conformiteitsbeoordeling onderworpen kan zijn;

3° de regels die van toepassing zijn op de interne audit;

4° de regels die van toepassing zijn op de externe audit.

§ 2. Bij besluit vastgesteld na overleg in de Ministerraad kan de Koning, na advies van de sectorale overheid en de autoriteit bedoeld in artikel 7, § 1, ook de voorwaarden bepalen voor een eventuele erkenning die door de sectorale overheid aan een instelling voor de conformiteitsbeoordeling wordt verleend.

§ 3. De lijst van de geaccrediteerde of erkende instellingen voor de conformiteitsbeoordeling is beschikbaar bij de sectorale overheid die ze actueel houdt.

Art. 40. § 1. Certificeringsaudits kunnen door de inspectiedienst of de sectorale overheid worden gelijkgesteld met de verplichte jaarlijkse interne audit bedoeld in artikel 39, § 1. De verslagen van deze audits worden binnen de dertig dagen door de aanbieder van essentiële diensten aan de sectorale overheid bezorgd.

§ 2. Certificeringsaudits kunnen door de inspectiedienst of de sectorale overheid worden gelijkgesteld met de verplichte externe audit bedoeld in artikel 39, § 2. De verslagen van deze audits worden binnen de dertig dagen door de aanbieder van essentiële diensten aan de sectorale overheid bezorgd.

Art. 41. De autoriteit bedoeld in artikel 7, § 1, kan de sectorale overheid of de inspectiedienst, mits motivering, vragen haar de certificerings- of auditverslagen van een aanbieder van essentiële diensten te bezorgen.

Afdeling 2. — Inspectiedienst

Art. 42. § 1. De inspectiediensten kunnen op elk ogenblik controles uitvoeren op de naleving door de aanbieder van essentiële diensten van de beveiligingsmaatregelen en de regels voor het melden van incidenten.

§ 2. De autoriteit bedoeld in artikel 7, § 1, of de sectorale overheid kan de inspectiedienst, mits motivering, aanbevelen om controles uit te voeren.

Na advies van de sectorale overheid en de autoriteit bedoeld in artikel 7, § 1, kan de Koning de eventuele sectorale praktische controlemodaliteiten bepalen.

§ 3. Bij het formuleren van een verzoek om informatie of bewijzen vermeldt de inspectiedienst het doel van het verzoek en de termijn waarbinnen de informatie of bewijzen moeten worden verstrekt.

De inspectiedienst kan een beroep doen op experten.

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 États. 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. À 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.

Art. 43. Wanneer de netwerk- en informatiesystemen van een aanbieder van essentiële diensten zich buiten het Belgische grondgebied bevinden, kan de inspectiedienst, in overleg met de autoriteit bedoeld in artikel 7, § 1, de bevoegde toezichthoudende autoriteiten van deze andere landen om samenwerking en bijstand verzoeken. Deze bijstand en samenwerking kunnen betrekking hebben op informatie-uitwisseling en verzoeken om toezichtmaatregelen.

Art. 44. § 1. De leden van de inspectiedienst beschikken over een legitimatiekaart waarvan het model, per sector of, in voorkomend geval, per deelsector, door de Koning wordt bepaald.

§ 2. De leden van de inspectiedienst of de experten die deelnemen aan de inspectie, mogen geen enkel rechtstreeks of onrechtstreeks belang hebben in de ondernemingen of instellingen waarop zij toezicht dienen uit te oefenen, waardoor hun objectiviteit in het gedrang zou kunnen komen. Ze leggen de eed af bij de leidend ambtenaar van hun dienst.

§ 3. Onverminderd de bevoegdheden van de officieren van gerechtelijke politie bedoeld in artikel 8 van het Wetboek van strafvordering beschikken de beëdigde leden van de inspectiedienst op elk ogenblik over de volgende toezichtbevoegdheden bij de uitoefening van hun opdracht, en dit zowel in het kader van administratieve handelingen als in het kader van de vaststelling van inbreuken bij proces-verbaal:

1° zonder voorafgaande verwittiging, op vertoon van hun legitimatiekaart, alle plaatsen betreden die de aanbieder van essentiële diensten gebruikt; zij hebben slechts toegang tot bewoonde lokalen mits een machtiging die vooraf is uitgereikt door de onderzoeksrechter;

2° ter plaatse kennis nemen van het I.B.B., de auditverslagen, alle bescheiden, documenten en andere informatiebronnen die nodig zijn voor de uitoefening van hun opdracht en hiervan een kopie verkrijgen;

3° overgaan tot elk onderzoek, elke controle en elk verhoor, alsook alle inlichtingen inwinnen die zij nodig achten voor de uitoefening van hun opdracht;

4° de identiteit opnemen van de personen die zich bevinden op de plaatsen die de aanbieder van essentiële diensten gebruikt en van wie ze het verhoor noodzakelijk achten voor de uitoefening van hun opdracht. Daartoe kunnen ze van deze personen eisen dat ze hun officiële identiteitsdocumenten voorleggen;

5° de bijstand vorderen van de federale of lokale politiediensten;

6° inlichtingen inwinnen bij de personeelsleden bedoeld in artikel 9 van de wet van 15 april 1994 voor de uitvoering van de bepalingen van deze wet en van de wet van 1 juli 2011.

§ 4. Om een machtiging tot betreding van bewoonde lokalen te bekomen, richten de personeelsleden van de inspectiedienst een met redenen omkleed verzoek aan de onderzoeksrechter. Dit verzoek bevat minstens de volgende gegevens:

1° de identificatie van de bewoonde ruimten waartoe de personeelsleden van de inspectiedienst of van de sectorale overheid toegang wensen te hebben;

2° de eventuele inbreuken die het voorwerp zijn van het toezicht;

3° alle documenten en inlichtingen waaruit blijkt dat het gebruik van dit middel nodig is.

De onderzoeksrechter beslist binnen een termijn van maximum 48 uur na ontvangst van het verzoek. De beslissing van de onderzoeksrechter is met redenen omkleed. Bij gebrek aan een beslissing binnen de voorgeschreven termijn wordt het plaatsbezoek geacht te zijn geweigerd. De inspectiedienst kan beroep instellen tegen de weigeringsbeslissing of het gebrek aan een beslissing bij de kamer van inbeschuldigingstelling binnen vijftien dagen na de kennisgeving van de beslissing of het verstrijken van de termijn.

Bezoeken aan bewoonde lokalen zonder toestemming van de bewoner gebeuren tussen vijf en eenentwintig uur door minstens twee leden van de inspectiedienst die samen optreden.

§ 5. Bij het begin van elk verhoor wordt aan de ondervraagde persoon meegedeeld:

1° dat zijn verklaringen voor een rechtbank als bewijs kunnen worden gebruikt;

2° dat hij kan vragen dat alle vragen die hem worden gesteld en de antwoorden die hij geeft, worden genoteerd in de gebruikte bewoordingen;

3° dat hij het recht heeft om te zwijgen en niet bij te dragen tot zijn eigen beschuldiging.

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 interviennent lors 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 État 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 États, le service d'inspection, en concertation avec l'autorité visée à l'article 7,

Elke ondervraagde persoon mag de documenten in zijn bezit gebruiken, zonder dat daardoor het verhoor uitgesteld wordt. Hij mag tijdens het verhoor of later vragen om die documenten bij het verhoor te voegen.

Het verhoor vermeldt nauwkeurig het tijdstip waarop het wordt aangevat, eventueel onderbroken en hervat, alsook beëindigd. Het vermeldt de identiteit van de personen die tussenkomen tijdens het verhoor of een deel ervan.

Aan het einde van het verhoor heeft de ondervraagde persoon het recht om zijn verhoor te lezen of het te laten voorlezen. Hij mag zijn verklaringen laten verbeteren of er iets aan laten toevoegen.

De personeelsleden van de inspectiedienst die een persoon ondervragen, delen hem mee dat hij een kopie mag vragen van de tekst van zijn verhoor. Deze kopie wordt gratis verstrekt.

§ 6. De leden van de inspectiedienst mogen alle informatiedragers en de erin opgenomen gegevens raadplegen. Zij mogen zich ter plaatse het informaticasysteem en de erin opgenomen gegevens die zij nodig hebben voor hun onderzoeken en vaststellingen doen voorleggen en er kosteloos uittreksels, duplicaten of kopieën van nemen of vragen in een door hen gevraagde leesbare en verstaanbare vorm.

Indien het niet mogelijk is om ter plaatse kopieën te nemen, mogen de leden van de inspectiedienst, tegen een ontvangstbewijs dat een inventaris bevat, het informaticasysteem en de erin opgenomen gegevens in beslag nemen.

§ 7. Om de zoekactie in een informaticasysteem of een deel hiervan die op basis van paragraaf 6 werd opgestart, uit te breiden naar een informaticasysteem of een deel hiervan dat zich op een andere plaats bevindt dan die van de zoekactie, kan de inspectiedienst een onderzoeksrechter verzoeken op te treden.

Art. 45. § 1. Na elke inspectie stellen de leden van de inspectiedienst een verslag op en bezorgen ze een kopie daarvan aan de geïnspecteerde aanbieder van essentiële diensten en aan de bevoegde sectorale overheid.

§ 2. De autoriteit bedoeld in artikel 7, § 1, en de sectorale overheid kunnen de inspectiedienst, mits motivering, vragen om zijn inspectieverslagen te bezorgen.

Art. 46. § 1. De aanbieder van essentiële diensten verleent zijn volledige medewerking aan de leden van de inspectiedienst bij de uitoefening van hun functie en met name om deze zo goed mogelijk te informeren over alle bestaande beveiligingsmaatregelen.

Indien nodig stelt de aanbieder van essentiële diensten het nodige materiaal ter beschikking van de leden van de inspectiedienst of van de sectorale overheid zodat ze de veiligheidsvoorschriften kunnen naleven tijdens de inspecties.

§ 2. Voor iedere sector of deelsector kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad en na advies van de sectorale overheid, retributies bepalen voor de inspectieprestaties. Deze retributies zijn ten laste van de aanbieders van essentiële diensten. De Koning bepaalt de nadere regels inzake berekening en betaling.

HOOFDSTUK 2. — *Toezicht op de digitaledienstverleners*

Art. 47. § 1. De Koning bepaalt de praktische nadere regels van het toezicht op de digitaledienstverleners.

§ 2. De digitaledienstverlener moet met name:

a) de bevoegde inspectiedienst binnen de gestelde termijn de informatie verstrekken die nodig is om de beveiliging van zijn netwerk- en informatiesystemen te beoordelen, met inbegrip van gedocumenteerde beleidsmaatregelen op het gebied van beveiliging;

b) elke niet-inachtneming van de beveiligingseisen en de eisen inzake het melden van incidenten rechtzetten binnen de gestelde termijn.

§ 3. Overeenkomstig de door de Koning bepaalde regels kan de inspectiedienst, indien nodig, door middel van toezichtmaatregelen achteraf, maatregelen nemen wanneer ze het bewijs in handen krijgt dat een digitaledienstverlener niet voldoet aan de beveiligingseisen of de eisen inzake het melden van incidenten. Dit bewijs kan worden voorgelegd door een bevoegde autoriteit van een andere lidstaat van de Europese Unie waar de dienst wordt verleend.

§ 4. In het kader van haar controles achteraf beschikt de inspectiedienst over dezelfde bevoegdheden als deze bedoeld in artikel 44.

§ 5. Wanneer een digitaledienstverlener zijn hoofdvestiging of een vertegenwoordiger in België heeft maar zijn netwerk- en informatiesystemen in een of meer andere landen, kan de inspectiedienst, in overleg met de autoriteit bedoeld in artikel 7, § 1, de bevoegde

§ 1er, peut solliciter la coopération et l'assistance des autorités de contrôle compétentes de ces autres États. 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 État 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 œuvre.

§ 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.

toezichthoudende autoriteiten van deze andere landen om samenwerking en bijstand verzoeken. Deze bijstand en samenwerking kunnen betrekking hebben op informatie-uitwisseling en verzoeken om toezichtmaatregelen.

§ 6. Overeenkomstig de door de Koning bepaalde regels kan de inspectiedienst de in dit artikel bedoelde bevoegdheden ook uitoefenen op verzoek van bevoegde autoriteiten van een andere lidstaat van de Europese Unie.

§ 7. De autoriteit bedoeld in artikel 7, § 1, kan de inspectiedienst vragen haar de inspectieverslagen van een digitaledienstverlener te bezorgen.

§ 8. De Koning kan, bij besluit vastgesteld na overleg in de Ministerraad en na advies van de sectorale overheid, retributies bepalen voor de controleprestaties. Deze retributies zijn ten laste van de digitale dienstverleners. De Koning bepaalt de nadere regels inzake berekening en betaling.

HOOFDSTUK 3. — *De sancties*

Afdeling 1. — Procedure

Art. 48. § 1. Wanneer een of meer inbreuken op de eisen van de wet, de uitvoeringsbesluiten ervan of de eraan verbonden individuele administratieve beslissingen worden vastgesteld, stelt de inspectiedienst de betrokken aanbieder van essentiële diensten of digitaledienstverlener in gebreke om zijn verplichtingen na te komen binnen een door hem vastgestelde termijn.

De termijn wordt bepaald rekening houdend met de werkingsvoorwaarden van de aanbieder van essentiële diensten of digitaledienstverlener en met de te nemen maatregelen.

§ 2. De inspectiedienst deelt de overtreder vooraf, op een met redenen omklede wijze, mee dat hij van plan is hem een ingebrekestelling te sturen en laat hem weten dat hij het recht heeft om, binnen de vijftien dagen na ontvangst van deze informatie, zijn verweermiddelen schriftelijk in te dienen of te vragen om te worden gehoord. De informatie wordt geacht te zijn ontvangen door de overtreder de zesde dag na de verzending ervan door de inspectiedienst.

§ 3. Op basis van de elementen waarover zij beschikt, kan de autoriteit bedoeld in artikel 7, § 1, mits motivering, de inspectiedienst ook aanbevelen om de aanbieder van essentiële diensten of digitaledienstverlener in gebreke te stellen.

Art. 49. § 1. Als de inspectiedienst vaststelt dat de aanbieder van essentiële diensten of digitaledienstverlener geen gevolg geeft aan de ingebrekestelling binnen de vastgestelde termijn, worden de feiten vastgesteld in een door de beëdigde leden van de inspectiedienst opgesteld proces-verbaal. Dat proces-verbaal wordt naar de bevoegde sectorale overheid gestuurd.

§ 2. Het feit dat iemand de uitvoering van een controle door de leden van de inspectiedienst vrijwillig verhindert of belemmert, de informatie die hem gevraagd wordt naar aanleiding van deze controle weigert mee te delen, of opzettelijk foutieve of onvolledige informatie meedeelt, wordt vastgesteld in een proces-verbaal door de beëdigde leden van de inspectiedienst.

§ 3. De paragrafen 1 en 2 zijn ook van toepassing op de potentiële aanbieder van essentiële diensten of op de exploitant van een kritieke infrastructuur die de informatieverplichtingen bedoeld in artikel 14 of in artikel 18, § 3, niet nakomt.

§ 4. De processen-verbaal opgesteld door de beëdigde leden van de inspectiedienst hebben bewijskracht tot het tegendeel is bewezen.

Art. 50. Inbreuken op deze wet of de uitvoeringsbesluiten ervan kunnen aanleiding geven tot strafrechtelijke of administratieve sancties.

Afdeling 2. — Strafrechtelijke sancties

Art. 51. § 1. Niet-naleving van een van de meldingsverplichtingen bedoeld in artikel 24 of 35 wordt bestraft met een gevangenisstraf van acht dagen tot een jaar en een geldboete van 26 euro tot 20 000 euro of met een van deze straffen alleen.

§ 2. Niet-naleving van een van de beveiligingsverplichtingen opgelegd door de Koning of de sectorale overheid krachtens artikel 21 of 33 wordt bestraft met een gevangenisstraf van acht dagen tot een jaar en een geldboete van 26 euro tot 30 000 euro of met een van deze straffen alleen.

§ 3. Niet-naleving van een van de toezichtverplichtingen bedoeld in hoofdstuk 1 en 2 van titel 4 wordt bestraft met een gevangenisstraf van acht dagen tot een jaar en een geldboete van 26 euro tot 50 000 euro of met een van deze straffen alleen.

§ 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 présent 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. Niet-naleving van een van de informatieverplichtingen bedoeld in artikel 14 of in artikel 18, § 3, wordt bestraft met een gevangenisstraf van acht dagen tot een jaar en een geldboete van 26 euro tot 50 000 euro of met een van deze straffen alleen.

§ 5. Iedere vrijwillige verhindering of belemmering van de uitvoering van de controle door de leden van de inspectiedienst, weigering om de informatie mee te delen die naar aanleiding van deze controle is gevraagd, of opzettelijke mededeling van foutieve of onvolledige informatie wordt bestraft met een gevangenisstraf van acht dagen tot twee jaar en een geldboete van 26 euro tot 75 000 euro of met een van deze straffen alleen.

§ 6. In geval van herhaling van dezelfde feiten binnen een termijn van drie jaar wordt de geldboete verdubbeld en de overtreder gestraft met een gevangenisstraf van vijftien dagen tot drie jaar.

§ 7. De bepalingen van Boek 1 van het Strafwetboek, met inbegrip van hoofdstuk VII en artikel 85, zijn van toepassing op de inbreuken bedoeld in dit artikel.

De artikelen 269 tot 274 en 276 van het Strafwetboek zijn van toepassing op de leden van de inspectiedienst die handelen in de uitoefening van hun functie.

§ 8. Inbreuken op artikel 9, §§ 2 en 3, van deze wet worden bestraft met de straffen bepaald in artikel 458 van het Strafwetboek.

Afdeling 3. — Administratieve sancties

Art. 52. § 1. Elke inbreuk op deze wet, op de uitvoeringsbesluiten ervan of op de administratieve beslissingen die krachtens deze wet genomen worden, kan aanleiding geven tot een administratieve sanctie.

§ 2. Niet-naleving van de meldingsverplichtingen bedoeld in artikel 24 of 35 wordt bestraft met een geldboete van 500 tot 75 000 euro.

§ 3. Niet-naleving van de beveiligingsverplichtingen opgelegd door de Koning of de sectorale overheid krachtens artikel 21 of 33 wordt bestraft met een geldboete van 500 tot 100 000 euro.

§ 4. Niet-naleving van de informatieverplichtingen bedoeld in artikel 14 of in artikel 18, § 3, wordt bestraft met een geldboete van 500 tot 125 000 euro.

§ 5. Niet-naleving van de toezichtverplichtingen bedoeld in hoofdstuk 1 en 2 van titel 4 wordt bestraft met een geldboete van 500 tot 200 000 euro.

§ 6. Iedere handeling waarbij een persoon die optreedt voor rekening van een aanbieder van essentiële diensten of digitaledienstverlener nadelige gevolgen ondervindt bij de uitvoering, te goeder trouw en in het kader van zijn functie, van de verplichtingen die voortvloeien uit deze wet, wordt bestraft met een geldboete van 500 tot 200 000 euro.

Art. 53. De inspectiedienst stuurt het origineel van het proces-verbaal naar de procureur des Konings.

Tegelijk wordt een kopie van het proces-verbaal naar de overtreder gestuurd.

Art. 54. De procureur des Konings beschikt over een termijn van twee maanden, te rekenen vanaf de dag van ontvangst van het proces-verbaal, om de sectorale overheid in te lichten dat strafrechtelijke vervolging is ingesteld.

De sectorale overheid mag de procedure voor het opleggen van een administratieve geldboete niet opstarten vóór het verstrijken van voormelde termijn, behalve wanneer de procureur des Konings vooraf meedeelt dat hij geen gevolg aan het feit wenst te geven.

Wanneer de procureur des Konings geen kennis geeft van zijn beslissing binnen de vastgestelde termijn of van strafvervolging afziet, kan de sectorale overheid beslissen de administratieve procedure op te starten.

Art. 55. § 1. De beslissing om een administratieve geldboete op te leggen wordt met redenen omkleed. Ze vermeldt ook het bedrag van de administratieve geldboete en de bedoelde inbreuken.

§ 2. De sectorale overheid bezorgt de overtreder op voorhand haar met redenen omkleed voorstel van administratieve sanctie en laat hem weten dat hij het recht heeft om, binnen de vijftien dagen na ontvangst van het voorstel, zijn verweermiddelen schriftelijk in te dienen of te vragen om te worden gehoord. Het voorstel wordt geacht te zijn ontvangen door de overtreder de zesde dag na de verzending ervan door de sectorale overheid.

§ 3. Rekening houdend met de aangevoerde verweermiddelen binnen de in paragraaf 2 bedoelde termijn of bij gebrek aan een antwoord van de overtreder binnen diezelfde termijn, kan de sectorale overheid een in artikel 52 bedoelde administratieve sanctie opleggen.

§ 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.

§ 4. De administratieve geldboete staat in verhouding tot de ernst, de duur, de gebruikte middelen, de veroorzaakte schade en de omstandigheden van de feiten.

De administratieve geldboete wordt verdubbeld in geval van herhaling van dezelfde feiten binnen een termijn van drie jaar.

§ 5. De samenloop van meerdere inbreuken kan aanleiding geven tot één enkele administratieve geldboete die in verhouding staat tot de ernst van het geheel van de feiten.

Art. 56. De beslissing wordt bij aangetekende zending ter kennis gebracht van de overtreder.

Een verzoek tot betaling van de geldboete binnen een maand wordt bij de beslissing gevoegd.

Art. 57. De overtreder kan de beslissing van de sectorale overheid betwisten bij het Marktenhof bedoeld in artikel 101 van het Gerechtelijk Wetboek.

De vordering wordt ingesteld bij verzoekschrift op tegenspraak dat, op straffe van verval, binnen zestig dagen na kennisgeving van de beslissing van de sectorale overheid wordt ingediend.

De zaak wordt behandeld zoals in kort geding overeenkomstig de artikelen 1035 tot 1038, 1040 en 1041 van het Gerechtelijk Wetboek.

Dit beroep schorst de uitvoering van de beslissing niet.

Art. 58. § 1. Als de overtreder de administratieve geldboete niet betaalt binnen de gestelde termijn, is de beslissing om een administratieve geldboete op te leggen uitvoerbaar en kan de sectorale overheid een dwangbevel uitvaardigen.

Het dwangbevel wordt uitgevaardigd door de wettelijke vertegenwoordiger van de sectorale overheid of door een daartoe gemachtigd personeelslid.

§ 2. Het dwangbevel wordt aan de overtreder bij gerechtsdeurwaarderexploot betekend. De betekening bevat een bevel om te betalen binnen vierentwintig uur op straffe van tenuitvoerlegging door beslag, alsook een boekhoudkundige verantwoording van de gevorderde bedragen en een afschrift van de uitvoerbaarverklaring.

§ 3. De overtreder kan tegen het dwangbevel verzet aantekenen bij de beslagrechter.

Het verzet is, op straffe van nietigheid, met redenen omkleed. Het dient gedaan te worden door middel van een dagvaarding aan de sectorale overheid bij deurwaardersexploot binnen vijftien dagen te rekenen vanaf de betekening van het dwangbevel.

De bepalingen van hoofdstuk VIII van het eerste deel van het Gerechtelijk Wetboek zijn van toepassing op deze termijn, met inbegrip van de verlengingen bepaald in artikel 50, tweede lid, en artikel 55 van dit Wetboek.

De uitoefening van verzet tegen het dwangbevel schorst de tenuitvoerlegging van het dwangbevel, alsook de verjaring van de schuldvorderingen opgenomen in het dwangbevel, tot uitspraak is gedaan over de gegrondheid ervan. De reeds eerder gelegde beslagen behouden hun bewarend karakter.

§ 4. De sectorale overheid mag bewarend beslag laten leggen en het dwangbevel uitvoeren met gebruikmaking van de middelen tot tenuitvoerlegging bepaald in het vijfde deel van het Gerechtelijk Wetboek.

De gedeeltelijke betalingen gedaan ingevolge de betekening van een dwangbevel verhinderen de voortzetting van de vervolging niet.

§ 5. De betekeningskosten van het dwangbevel evenals de kosten van tenuitvoerlegging of van bewarende maatregelen zijn ten laste van de overtreder.

Ze worden bepaald volgens de regels die gelden voor de akten van gerechtsdeurwaarders in burgerlijke zaken en handelszaken.

Art. 59. De sectorale overheid kan geen administratieve geldboete opleggen na het verstrijken van een termijn van drie jaar, te rekenen vanaf de dag waarop het feit werd gepleegd.

De betaling volgens de administratieve procedure doet ook de mogelijkheid vervallen om strafrechtelijke vervolging in te stellen voor de bedoelde feiten.

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. À 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.

TITEL 5. — *CSIRT*

HOOFDSTUK 1. — *Het nationale CSIRT*

Afdeling 1. — Taken van het nationale CSIRT

Art. 60. De taken van het nationale CSIRT omvatten ten minste het volgende:

a) monitoren van incidenten op nationaal en internationaal niveau, met inbegrip van de verwerking van persoonsgegevens met betrekking tot het monitoren van deze incidenten;

b) ten behoeve van de betrokken belanghebbende partijen zorgen voor vroegtijdige waarschuwingen, alarmmeldingen, aankondigingen en verspreiding van informatie over risico's en incidenten;

c) reageren op incidenten;

d) zorgen voor een dynamische risico- en incidentanalyse en situatiekennis;

e) computerbeveiligingsproblemen opsporen, observeren en analyseren;

f) stimuleren van de vaststelling en het gebruik van gemeenschappelijke of gestandaardiseerde praktijken op het gebied van procedures voor de behandeling van incidenten en risico's, en van systemen voor de classificatie van incidenten, risico's en informatie;

g) zorgen voor op samenwerking gerichte contacten met de particuliere sector en met andere administratieve diensten of publiek overheden;

h) deelnemen aan het CSIRT-netwerk bedoeld in artikel 12 van de NIS-richtlijn.

Na advies van het nationale CSIRT kan de Koning dit CSIRT bijkomende taken toevertrouwen.

Afdeling 2 - Voorschriften voor het nationale CSIRT

Art. 61. De voorschriften voor het nationale CSIRT omvatten ten minste het volgende:

a) een hoge mate van beschikbaarheid van zijn communicatiediensten garanderen door zwakke punten (single points of failure) te voorkomen, en beschikken over diverse kanalen waarlangs te allen tijde contact met hen kan worden opgenomen en contact met anderen kan worden opgenomen;

b) beschikken over lokalen en informatiesystemen die zich op beveiligde locaties bevinden;

c) de bedrijfscontinuïteit garanderen met een adequaat systeem voor het beheren en routeren van verzoeken met het oog op vlotte overdrachten;

d) deelnemen aan de vergaderingen van het CSIRT-netwerk bedoeld in artikel 12 van de NIS-richtlijn;

e) een beroep doen op infrastructuur waarvan de continuïteit gewaarborgd is. Hiertoe wordt voorzien in redundante systemen en reservewerkruimten;

f) ervoor zorgen dat zijn communicatiekanalen duidelijk worden gespecificeerd en bekend zijn bij zijn partners.

Art. 62. In het kader van de uitoefening van zijn bevoegdheden neemt het nationale CSIRT alle passende maatregelen om de in de artikelen 60 en 61 bepaalde doelstellingen te verwezenlijken. Deze maatregelen moeten evenredig zijn met die doelstellingen en in overeenstemming met de beginselen van objectiviteit, transparantie en non-discriminatie.

Bij de verwezenlijking van die doelstellingen mag het nationale CSIRT alle beschikbare gegevens onder zich houden, aan een andere persoon onthullen of verspreiden, of er enig gebruik van maken, zelfs als die gegevens voortkomen uit een ongerechtigde toegang tot een informaticasysteem door een derde.

Het nationale CSIRT vervult zijn opdrachten met de nodige behoedzaamheid die verwacht mag worden van een overheid. Er moet steeds bij voorrang voor worden gezorgd dat de werking van het informaticasysteem niet wordt verstoord en alle redelijke voorzorgen moeten worden genomen om te voorkomen dat het informaticasysteem materiële schade oploopt.

De leidende ambtenaren van het nationale CSIRT zorgen voor de naleving van de in dit artikel vermelde voorwaarden. Daartoe werken zij interne procedures uit.

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. À 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 œuvre 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.

HOOFDSTUK 2. — *Het sectoraal CSIRT*

Afdeling 1. — Taken van het sectoraal CSIRT

Art. 63. De taken van een sectoraal CSIRT omvatten, in samenwerking met het nationale CSIRT, ten minste het volgende:

a) monitoren van sectorale incidenten;

b) ten behoeve van de betrokken belanghebbende partijen van de sector zorgen voor vroegtijdige waarschuwingen, alarmmeldingen, aankondigingen en verspreiding van informatie over risico's en incidenten;

c) reageren op sectorale incidenten;

d) zorgen voor een dynamische analyse van sectorale risico's en incidenten en situatiekennis;

e) zorgen voor op samenwerking gerichte contacten met de aanbieders van zijn sector;

f) kunnen deelnemen aan vergaderingen van het CSIRT-netwerk bedoeld in artikel 12 van de NIS-richtlijn, die gewijd zijn aan zijn sector.

Na advies van het sectorale CSIRT kan de Koning dit CSIRT bijkomende taken toevertrouwen.

Afdeling 2. — Voorschriften voor een sectoraal CSIRT

Art. 64. De voorschriften voor een sectoraal CSIRT omvatten het volgende:

a) een hoge mate van beschikbaarheid van zijn communicatiekanalen garanderen door zwakke punten (single points of failure) te voorkomen, en beschikken over diverse kanalen waarlangs te allen tijde contact met hen kan worden opgenomen en contact met anderen kan worden opgenomen.

b) beschikken over lokalen en informatiesystemen die zich op beveiligde locaties bevinden.

c) de bedrijfscontinuïteit garanderen met een adequaat systeem voor het beheren en routeren van verzoeken met het oog op vlotte overdrachten.

d) een beroep doen op infrastructuur waarvan de continuïteit gewaarborgd is. Hiertoe wordt voorzien in redundante systemen en reservewerkruimten.

f) ervoor zorgen dat zijn communicatiekanalen duidelijk worden gespecificeerd en bekend zijn bij zijn partners.

TITEL 6. — *Verwerking van persoonsgegevens*

HOOFDSTUK 1. — *Beginselen inzake verwerking, wettelijke basis en doeleinden*

Art. 65. § 1. Overeenkomstig artikel 5.1.c) van Verordening EU 2016/679 zorgt de verwerkingsverantwoordelijke, bij de verwerking van persoonsgegevens in het kader van de uitvoering van deze wet, ervoor dat de verwerking tot het noodzakelijke minimum beperkt blijft en in verhouding staat tot het nagestreefde doeleinde.

§ 2. Overeenkomstig dat beginsel kunnen de verwerkte persoonsgegevens allerhande gegevens zijn in verband met de beveiliging van netwerk- en informatiesystemen, namelijk in voorkomend geval nominatieve informatie, gegevens over de medewerkers van een organisatie of externe personen, verbindingsgegevens of -identificatoren, locatiegegevens, identificatie- of authenticatiegegevens, in voorkomend geval met behulp van beveiligde systemen.

§ 3. De belangrijkste verwerkingen van persoonsgegevens in het kader van deze wet kunnen als volgt worden ingedeeld:

— algemene informatie-uitwisseling tussen aanbieders van essentiële diensten en digitaledienstverleners, enerzijds, en de autoriteit bedoeld in artikel 7, anderzijds;

— de verwerking van specifieke informatie tussen de entiteiten bedoeld in het eerste streepje in het kader van incidentmeldingen of andere specifieke uitwisselingen;

— de verwerking door inspectiediensten overeenkomstig titel 4;

— de verwerking door hoven en rechtbanken of sectorale overheden in het kader van de uitvoering van de wet en met name de opsporing, vervolging en bestraffing van inbreuken;

— de uitwisseling en andere verwerking van informatie door het nationale en sectorale CSIRT voor hun opdrachten respectievelijk bedoeld in de artikelen 60 tot 62, 63 en 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 œuvre 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

Art. 66. § 1. Indien mogelijk worden de verwerkte gegevens gepseudonimiseerd of geaggregeerd om het risico te verkleinen dat persoonsgegevens worden gebruikt op een wijze die onverenigbaar is met de Verordening EU 2016/679 of de wetten en reglementen die ze aanvullen of verduidelijken.

§ 2. De bijzondere gegevenscategorieën in de zin van de artikelen 9 en 10 van Verordening EU 2016/679 worden verwerkt overeenkomstig deze verordening en de wetten en reglementen die ze aanvullen of verduidelijken.

§ 3. De verwerkingsverantwoordelijke kan ofwel een van de autoriteiten bedoeld in artikel 7 zijn, ofwel de aanbieders van essentiële diensten of de digitaledienstverleners, ofwel de politionele of gerechtelijke autoriteiten.

§ 4. De ontvangers van persoonsgegevens kunnen alle personen zijn die betrokken zijn bij de uitvoering van de bepalingen van de wet, voor zover noodzakelijk voor de informatie-uitwisseling waarin de wet voorziet.

Art. 67. Overeenkomstig de artikelen 6.1, c), en 6.1, e), van Verordening EU 2016/679, moeten de verwerkingen bedoeld in artikel 65, § 3, noodzakelijk blijven om te voldoen aan een wettelijke verplichting van de verwerkingsverantwoordelijke of voor de invulling van een taak van algemeen belang die aan deze laatste is opgedragen. Deze verwerkingen moeten noodzakelijk zijn enkel wat deze wettelijke basis betreft en beperkt blijven tot wat noodzakelijk is om eraan te voldoen.

Art. 68. § 1. De verwerkingen bedoeld in artikel 65, § 3, moeten beperkt zijn tot en verenigbaar blijven met de doeleinden bepaald door de verwerkingsverantwoordelijke.

§ 2. Deze doeleinden kunnen onder meer zijn: een betere bescherming van de netwerk- en informatiesystemen, een krachtiger preventie- en veiligheidsbeleid, de preventie van beveiligingsincidenten, de continuïteit van de in deze wet bedoelde essentiële of digitale diensten, het toezicht op aanbieders van essentiële diensten en digitaledienstverleners, nationale en internationale samenwerking, de evaluatie van de uitvoering van de wet, de voorbereiding, de organisatie, het beheer en de opvolging van onderzoek of vervolging, alsook de andere opdrachten die bij wet zijn toegewezen aan de verschillende betrokken autoriteiten.

§ 3. Wat de relevante doeleinden en subdoeleinden betreft, bepaalt elke verwerkingsverantwoordelijke de betrokken gegevens- en persoonscategorieën, de ontvangers of categorieën van ontvangers van gegevens, de bewaartermijnen en de andere eventuele kenmerken van de verwerking, alsook de regels en praktijken voor de naleving van de toepasselijke regelgeving.

HOOFDSTUK 2. — *Bewaartermijn*

Art. 69. § 1. Onverminderd de bewaring die noodzakelijk is voor de verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, bedoeld in artikel 89 van Verordening EU 2016/679, worden de in uitvoering van de wet verwerkte persoonsgegevens door de autoriteiten bedoeld in artikel 7 niet langer bewaard dan nodig is voor de doeleinden waarvoor ze worden verwerkt.

§ 2. Overeenkomstig de eerste paragraaf kan de Koning de maximale bewaartermijn van dezelfde gegevens bepalen bij besluit vastgesteld na overleg in de Ministerraad.

HOOFDSTUK 3. — *Functionaris voor gegevensbescherming*

Art. 70. Elke aanbieder van essentiële diensten, digitaledienstverlener en autoriteit bedoeld in artikel 7 van de wet die persoonsgegevens verwerkt, wijst een functionaris voor gegevensbescherming aan.

HOOFDSTUK 4. — *Beperking van de rechten van de betrokken personen*

Art. 71. § 1. Met toepassing van artikel 23.1, a), b), c), d), e), h), van Verordening EU 2016/679 worden bepaalde verplichtingen en rechten van deze verordening beperkt of uitgesloten, overeenkomstig de bepalingen van dit hoofdstuk. Deze beperkingen of uitsluitingen mogen geen afbreuk doen aan de wezenlijke inhoud van de grondrechten en fundamentele vrijheden en moeten worden toegepast voor zover dit strikt noodzakelijk is voor het nagestreefde doel.

§ 2. De artikelen 12 tot 22 van voormelde verordening zijn niet van toepassing op de verwerking van persoonsgegevens door een aanbieder van essentiële diensten, een digitaledienstverlener of een autoriteit bedoeld in artikel 7, overeenkomstig deze wet en om te voldoen aan de verplichtingen die deze oplegt inzake het melden van incidenten, als bedoeld in hoofdstuk 3 van titel 2 en hoofdstuk 3 van titel 3. Deze artikelen zijn evenmin van toepassing op het toezicht bedoeld in titel 4. De vrijstelling geldt enkel indien en voor zover deze verwerking

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.

noodzakelijk is voor de hierboven bepaalde doeleinden, met name voor zover de toepassing van de rechten bepaald in de voormelde verordening nadelig zou zijn voor de controle, het onderzoek of de voorbereidende werkzaamheden, of het geheim van het strafonderzoek of de veiligheid van personen zou kunnen schaden.

§ 3. De verwerkingsverantwoordelijke die de in paragraaf 2 bedoelde vrijstelling kan genieten, is ofwel de aanbieder van essentiële diensten, ofwel de digitaledienstverlener, ofwel de autoriteit bedoeld in artikel 7, elk voor de gegevens die hij of zij bezit in het kader van de opdrachten bedoeld in paragraaf 2.

§ 4. De vrijstelling geldt, onder voorbehoud van het evenredigheidsbeginsel en in voorkomend geval van het beginsel van minimale gegevensverwerking, voor alle categorieën van persoonsgegevens, voor zover de verwerking van deze gegevens in overeenstemming is met de doeleinden bedoeld in paragraaf 2. Deze vrijstelling geldt ook voor voorbereidende werkzaamheden of procedures met het oog op de eventuele toepassing van een administratieve sanctie.

§ 5. Persoonsgegevens die voortkomen uit de in paragraaf 2 bedoelde vrijstelling worden niet langer bewaard dan nodig is voor de doeleinden waarvoor ze worden verwerkt, met een maximale bewaartermijn die de duur van de verjaringstermijn van eventuele inbreuken bedoeld in artikelen 51 en 52 niet mag overschrijden, overeenkomstig de toepasselijke wetgeving.

§ 6. De verwerkingsverantwoordelijke die niet alle bepalingen van de wet en met name van artikel 72 naleeft, kan de vrijstelling niet genieten.

§ 7. Bovendien moet elke verwerkingsverantwoordelijke de vertrouwelijkheid van de persoonsgegevens die het voorwerp uitmaken van de vrijstelling waarborgen, en ervoor zorgen dat ze enkel toegankelijk zijn voor personen die ze nodig hebben voor de uitvoering van de bepalingen van deze wet. Ook moet elke betrokken verwerkingsverantwoordelijke de Gegevensbeschermingsautoriteit minstens één keer per jaar schriftelijk een lijst bezorgen van de verzoeken tot uitoefening van de rechten bedoeld in de artikelen 12 tot 22 van de verordening die volgens deze verantwoordelijke onder de vrijstelling vallen. Onverminderd de bepalingen van deze wet moet elke betrokken verwerkingsverantwoordelijke daarenboven elke andere passende maatregel nemen om elke vorm van misbruik of onrechtmatige toegang of doorgifte van persoonsgegevens die onder de vrijstelling vallen te voorkomen, met name en zonder enige beperking de maatregelen van artikel 32 van Verordening EU 2016/679.

Art. 72. § 1. De betrokkenen kunnen een verzoek in verband met hun rechten bepaald in de artikelen 12 tot 22 van Verordening EU 2016/679 naar de functionaris voor gegevensbescherming sturen die de ontvangst ervan bevestigt.

§ 2. De functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke informeert de betrokkene schriftelijk en dit onverwijld, en in ieder geval binnen een maand na ontvangst van het verzoek, over iedere weigering of beperking van zijn rechten bepaald in de artikelen 12 tot 22 van Verordening EU 2016/679, alsook over de redenen voor deze weigering of beperking. De informatie over de weigering of beperking kan achterwege worden gelaten wanneer de verstrekking ervan een van de doelstellingen vermeld in artikel 71, § 2, zou ondermijnen. Afhankelijk van de complexiteit van de verzoeken en van het aantal ervan kan die termijn indien nodig met twee maanden worden verlengd. De verwerkingsverantwoordelijke stelt de betrokkene binnen één maand na ontvangst van het verzoek in kennis van deze verlenging en van de redenen voor het uitstel.

§ 3. De functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke licht de betrokkene in over de mogelijkheid om klacht in te dienen bij de Gegevensbeschermingsautoriteit en om beroep in rechte in te stellen.

De functionaris voor gegevensbescherming van de verwerkingsverantwoordelijke vermeldt de feitelijke of juridische redenen waarop zijn beslissing steunt. Deze inlichtingen worden ter beschikking gesteld van de Gegevensbeschermingsautoriteit.

§ 4. De betrokken verwerkingsverantwoordelijke verleent de betrokkene evenwel toegang tot beperkte informatie over de verwerking van zijn persoonsgegevens, voor zover deze kennisgeving de verwezenlijking van de doelstellingen van deze wet niet in het gedrang brengt. Hierbij is het voor betrokkene onmogelijk om na te gaan of hij al dan niet het voorwerp uitmaakt van een onderzoek, en kan hij in geen geval persoonsgegevens rechtzetten, wissen, beperken, meedelen, of aan derden overdragen, noch enige vorm van verwerking van voormelde gegevens die in het bovenvermelde kader noodzakelijk is, stopzetten.

§ 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. À 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 ;

§ 5. De maatregel van weigering of beperking van de rechten bepaald in de artikelen 12 tot 22 van Verordening EU 2016/679 moet worden opgeheven:

— voor maatregelen die gerechtvaardigd zijn door de verplichtingen inzake het melden van incidenten, bij het afsluiten van de verwerking van een incident door de autoriteiten bedoeld in artikel 24 of 34;

— voor maatregelen die gerechtvaardigd zijn door de verplichtingen krachtens titel 4, bij het afsluiten van de controle of het onderzoek of de voorbereidende werkzaamheden ervan door de inspectiedienst, alsook in de periode tijdens dewelke de sectorale overheid de stukken verwerkt die afkomstig zijn van de inspectiedienst met het oog op de vervolging;

— uiterlijk één jaar vanaf de ontvangst van het verzoek ingediend overeenkomstig de artikelen 12 tot 22 van Europese Verordening EU 2016/679, behalve indien een controle of onderzoek loopt.

§ 6. De betrokken verwerkingsverantwoordelijke heft ook de maatregel van weigering of beperking van de rechten bepaald in de artikelen 12 tot 22 van Verordening EU 2016/679 op zodra deze maatregel niet meer nodig is voor het nakomen van een van de doeleinden bedoeld in artikel 68, § 2.

§ 7. In alle toepassingsgevallen van de paragrafen 5 en 6 informeert de functionaris voor gegevensbescherming de betrokken persoon of personen schriftelijk dat de maatregel van weigering of beperking is opgeheven.

HOOFDSTUK 5. — *Beperkingen inzake de verplichte melding van inbreuken in verband met persoonsgegevens*

Art. 73. De betrokken verwerkingsverantwoordelijke is vrijgesteld van het meedelen van een inbreuk in verband met persoonsgegevens aan een of meer welbepaalde betrokkenen, in de zin van artikel 34 van Verordening EU 2016/679, mits toestemming van de autoriteit bedoeld in artikel 7, § 1, voor zover deze individuele kennisgeving de verwezenlijking van de doeleinden bedoeld in artikel 71, § 2, in het gedrang zou brengen.

TITEL 7. — *Slotbepalingen*

HOOFDSTUK 1. — *Wijzigingen van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren*

Art. 74. Artikel 2 van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren wordt aangevuld met een lid, luidende:

"Deze wet voorziet in de gedeeltelijke omzetting van Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie.".

Art. 75. In artikel 3 van dezelfde wet gewijzigd bij de wetten van 25 april 2014 en 15 juli 2018, worden de volgende wijzigingen aangebracht:

1° in de bepaling onder 3° worden de bepalingen onder c) en d) vervangen als volgt:

–"c) voor de sector financiën, met uitzondering van de exploitanten van een handelsplatform in de zin van artikel 3, 6°, van de wet van 21 november 2017 over de infrastructuren voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU: de Nationale Bank van België (NBB);

d) voor de exploitanten van een handelsplatform in de zin van artikel 3, 6°, van de wet van 21 november 2017 over de infrastructuren voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU: de Autoriteit voor Financiële Diensten en Markten (FSMA);";

2° de bepaling onder 3° wordt aangevuld met de bepalingen onder e) tot g), luidende:

e) voor de sectoren elektronische communicatie en digitale infrastructuren: het Belgisch Instituut voor postdiensten en telecommunicatie (B.I.P.T.);

f) voor de sector gezondheidszorg: de overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad;

g) voor de sector drinkwater: de overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad;";

3° het artikel wordt aangevuld met de bepalingen onder 13° tot 17°, luidende:

— "13° "de wet van 7 april 2019": de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;

— 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. À 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 5*bis*, 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. À l'article 22*bis* de la même loi, inséré par la loi du 25 avril 2004, 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.".

— 14° "beveiliging van netwerk- en informatiesystemen": de beveiliging van netwerk- en informatiesystemen als bedoeld in artikel 6, 8° en 9°, van de wet van 7 april 2019;

— 15° " de sector digitale infrastructuren": de sector bedoeld in punt 6 van bijlage 1 van de wet van 7 april 2019;

— 16° " de sector drinkwater": de sector bedoeld in punt 5 van bijlage 1 van de wet van 7 april 2019;

— 17° " de sector gezondheidszorg": de sector bedoeld in punt 4 van bijlage 1 van de wet van 7 april 2019.".

Art. 76. In artikel 4 van dezelfde wet, gewijzigd bij de wet van 15 juli 2018, wordt paragraaf 4 vervangen als volgt:

"§ 4. Dit hoofdstuk is van toepassing op de sector financiën, met inbegrip van de exploitanten van een handelsplatform bedoeld in artikel 3, 3°, d), de sector elektronische communicatie, de sector digitale infrastructuren, de sector gezondheidszorg en de sector drinkwater, wat de beveiliging en de bescherming van de nationale kritieke infrastructuren betreft.".

Art. 77. Artikel 5 van dezelfde wet, gewijzigd bij de wet van 15 juli 2018, wordt aangevuld met een paragraaf 3, luidende:

"§ 3. Tijdens het hele identificatieproces als bedoeld in deze afdeling wordt de autoriteit bedoeld in artikel 7, § 1, van de wet van 7 april 2019 betrokken bij het door de sectorale overheden en de ADCC gevoerde nationale en internationale overleg voor de identificatie van de kritieke infrastructuren met betrekking tot de beveiliging van netwerk- en informatiesystemen.".

Art. 78. In artikel 13 van dezelfde wet, gewijzigd bij de wetten van 25 april 2014 en 15 juli 2018 worden de volgende wijzigingen aangebracht:

1° in paragraaf 5*bis* worden de woorden "met uitzondering van die welke worden uitgebaat door een exploitant van een handelsplatform," ingevoegd tussen de woorden "vallen," en het woord "worden".

2° in paragraaf 6, eerste lid, worden de woorden ", met uitzondering van de kritieke infrastructuren die worden uitgebaat door een exploitant van een handelsplatform," ingevoegd tussen de woorden "de sector financiën" en de woorden "worden".

Art. 79. In artikel 14 van dezelfde wet, gewijzigd bij de wet van 15 juli 2018, wordt paragraaf 2 aangevuld met de woorden "en, in voorkomend geval, de autoriteit bedoeld in artikel 7, § 1, van de wet van 7 april 2019 wat de beveiliging van netwerk- en informatiesystemen betreft.".

Art. 80. In artikel 18 van dezelfde wet, gewijzigd bij de wet van 15 juli 2018, worden de woorden "De ADCC, de politiediensten en het OCAD" vervangen door de woorden "De ADCC, de politiediensten, het OCAD en, in voorkomend geval, de autoriteit bedoeld in artikel 7, § 1, van de wet van 7 april 2019, wat de beveiliging van netwerk- en informatiesystemen betreft".

Art. 81. In artikel 19 van dezelfde wet worden de woorden "De exploitant, het beveiligingscontactpunt, de sectorale overheid, de ADCC, het OCAD en de politiediensten" vervangen door de woorden "De exploitant, het beveiligingscontactpunt, de sectorale overheid, de ADCC, het OCAD, de politiediensten en, in voorkomend geval, de autoriteit bedoeld in artikel 7, § 1, van de wet van 7 april 2019, wat de beveiliging van netwerk- en informatiesystemen betreft,".

Art. 82. In artikel 22 van dezelfde wet, vervangen bij de wet van 15 juli 2018, worden de woorden "De sectorale overheid, de ADCC, het OCAD en de politiediensten" vervangen door de woorden "De sectorale overheid, de ADCC, het OCAD, de politiediensten en de autoriteit bedoeld in artikel 7, § 1, van de wet van 7 april 2019,".

Art. 83. In artikel 22*bis* van dezelfde wet, ingevoegd bij de wet van 25 april 2004, worden de volgende wijzigingen aangebracht:

1° in het eerste lid worden de woorden ", met uitzondering van de deelsector van de exploitanten van een handelsplatform," ingevoegd tussen de woorden "de sector financiën" en het woord "maakt".

2° het artikel wordt aangevuld met een lid, luidende:

"Voor de exploitanten van een handelsplatform bezorgt de FSMA de minister van Financiën een verslag met betrekking tot de taken die zij krachtens deze wet vervult, volgens een passende frequentie van ten hoogste drie jaar. De FSMA brengt hem echter onmiddellijk op de hoogte van elke concrete en nakende dreiging voor een kritieke infrastructuur die onder de bevoegdheid van haar sectoor valt.".

Art. 84. À 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 15*ter*, rédigé comme suit :

"Art. 15*ter*. 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 2003 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 2003 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 2005 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 ;

Art. 84. In artikel 24 van dezelfde wet, gewijzigd bij de wetten van 25 april 2014 en 15 juli 2018, worden de volgende wijzigingen aangebracht:

1° in paragraaf 2, derde lid, worden de woorden ", met uitzondering van de deelsector van de exploitanten van een handelsplatform," ingevoegd tussen de woorden "de sector financiën" en het woord "wordt".

2° paragraaf 2 wordt aangevuld met een lid, luidende:

"De Autoriteit voor Financiële Diensten en Markten wordt aangewezen als inspectiedienst belast met het toezicht op de toepassing van de bepalingen van deze wet en van de uitvoeringsbesluiten ervan, voor de exploitanten van een handelsplatform in de zin van artikel 3, 6°, van de wet van 21 november 2017 over de infrastructuren voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU. Dit artikel doet geen afbreuk aan de mogelijkheid voor de FSMA om, voor de uitvoering van de opdrachten die haar door deze wet worden toevertrouwd, een gespecialiseerde externe dienstverlener te belasten met de uitvoering van welbepaalde taken of de bijstand van een dergelijke dienstverlener te verkrijgen.".

HOOFDSTUK 2. — *Wijzigingen van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle*

Art. 85. Artikel 1 van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniseerde stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire controle, laatstelijk gewijzigd bij de wet van 13 december 2017, wordt aangevuld als volgt:

— "de wet van 7 april 2019": de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;".

Art. 86. In afdeling 1 van hoofdstuk III van dezelfde wet wordt een artikel 15*ter* ingevoegd, luidende:

"Art. 15*ter*. Het Agentschap wordt aangewezen als inspectiedienst, in de zin van artikel 42 van de wet van 7 april 2019, en is belast met het controleren van de toepassing van de bepalingen van deze wet en de uitvoeringsbesluiten ervan door de aanbieders van essentiële diensten, die krachtens bovengenoemde wet geïdentificeerd zijn, wat betreft de elementen van een nucleaire installatie bestemd voor de industriële productie van elektriciteit die dienen voor de transmissie van de elektriciteit.

De Koning bepaalt de praktische inspectiemodaliteiten, na advies van het Agentschap.".

HOOFDSTUK 3. — *Wijzigingen van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector*

Art. 87. Artikel 1/1 van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector, ingevoegd bij de wet van 10 juli 2012, wordt aangevuld met een lid, luidende:

"Deze wet voorziet in de gedeeltelijke omzetting van Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie.".

Art. 88. In artikel 14, § 1, eerste lid, van dezelfde wet, gewijzigd bij de wetten van 13 december 2010, 10 juli 2012, 27 maart 2014, 18 april 2017, 5 mei 2017 en 31 juli 2017, worden de volgende wijzigingen aangebracht:

1° in het eerste lid worden de woorden ", met betrekking tot de sector digitale infrastructuren in de zin van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, met betrekking tot de sectoren elektronische communicatie en digitale infrastructuren in de zin van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren," ingevoegd tussen het woord "radioapparatuur" en de woorden "en met betrekking tot";

2° de bepaling onder 3° wordt vervangen als volgt:

"3° het toezicht op de naleving van de volgende normen en van de uitvoeringsbesluiten ervan:

a) de wet van 13 juni 2005 betreffende de elektronische communicatie;

b) Titel I, hoofdstuk X, en Titel III van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven;

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 2003 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 2003 concernant les recours et le traitement des litiges à l'occasion de la loi du 17 janvier 2003 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 mesures relatives 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 2002 relative à la surveillance du secteur financier et aux services financiers*

Art. 92. L'article 75, § 1er, 15°, de la loi du 2 août 2002 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 ;".

c) de wet van 26 januari 2018 betreffende de postdiensten;

d) de artikelen 14, § 2, 2°, en 21, §§ 5 tot en met 7, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector;

e) de artikelen 4 en 4/1 van de wet van 17 januari 2003 betreffende de rechtsmiddelen en de geschillenbehandeling naar aanleiding van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector;

f) de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad;

g) de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, wat de sectoren elektronische communicatie en digitale infrastructuren betreft;

h) de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, met betrekking tot de sector digitale infrastructuren;

i) de Verordening (EU) 611/2013 van de Commissie van 24 juni 2013 betreffende maatregelen voor het melden van inbreuken in verband met persoonsgegevens op grond van Richtlijn 2002/58/EG van het Europees Parlement en de Raad betreffende privacy en elektronische communicatie.

Voor de toepassing van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, wordt het Instituut aangewezen als sectorale overheid en inspectiedienst voor de sector digitale infrastructuren. De Koning kan de praktische inspectiemodaliteiten voor deze sector bepalen, na advies van het Instituut.".

Art. 89. In artikel 24, eerste lid, van dezelfde wet, gewijzigd bij de wetten van 27 maart 2014 en 26 januari 2018, worden de woorden ", de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, wat de sector elektronische communicatie en de sector digitale infrastructuren betreft, en de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, wat de sector digitale infrastructuren betreft", ingevoegd tussen de woorden "in het tweetalig gebied Brussel-Hoofdstad" en de woorden "en hun uitvoeringsbesluiten".

HOOFDSTUK 4. — *Wijzigingen van de wet van 21 november 2017 over de infrastructuren voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU*

Art. 90. Artikel 71 van de wet van 21 november 2017 over de infrastructuren voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU wordt aangevuld met de woorden "en van titel 2 van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid. Voor de uitvoering van de voormelde opdrachten betreffende de wet van 7 april 2019 kan de FSMA niettemin een gespecialiseerde externe dienstverlener belasten met de uitvoering van welbepaalde toezichtsopdrachten of de bijstand van een dergelijke dienstverlener verkrijgen.".

Art. 91. Artikel 79 van dezelfde wet wordt aangevuld met een paragraaf 4, luidende:

"§ 4. In geval van schending van de toepasselijke bepalingen van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid kan de FSMA de in artikel 52 van voormelde wet bepaalde administratieve sancties opleggen.".

HOOFDSTUK 5. — *Wijziging van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten*

Art. 92. Artikel 75, § 1, 15°, van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten, opgeheven door de wet van 5 december 2017 houdende diverse financiële bepalingen, wordt hersteld in de volgende lezing:

"15° binnen de grenzen van het recht van de Europese Unie, aan de autoriteiten bedoeld in artikel 7 van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid voor de uitvoering van de bepalingen van deze wet en van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren;".

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. À 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.

HOOFDSTUK 6. — *Wijzigingen van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België*

Art. 93. Artikel 36/1 van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België, ingevoegd bij het koninklijk besluit van 3 maart 2011, wordt aangevuld met de bepaling onder 28°, luidende:

"28° "de wet van 7 april 2019": de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.".

Art. 94. In artikel 36/14, § 1, van dezelfde wet, laatstelijk gewijzigd bij de wet van 30 juli 2018, worden de volgende wijzigingen aangebracht:

1° in de bepaling onder 20° worden de woorden "aan de autoriteit bedoeld in artikel 7, § 1, van de wet van 7 april 2019" ingevoegd tussen de woorden "de analyse van de dreiging," en de woorden "en aan de politiediensten";

2° de paragraaf wordt aangevuld met de bepaling onder 24°, luidende:

"24° binnen de grenzen van het recht van de Europese Unie, aan de autoriteiten bedoeld in artikel 7 van de wet van 7 april 2019 voor de uitvoering van de bepalingen van de wet van 7 april 2019 en van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren.".

Art. 95. In dezelfde wet wordt een hoofdstuk IV/4 ingevoegd, dat artikel 36/47 bevat, luidende:

"Hoofdstuk IV/4. Toezicht door de Bank in het kader van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.

Art. 36/47. "Voor de toepassing van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid wordt de Bank aangewezen als sectorale overheid en inspectiedienst voor de aanbieders van de sector financiën, met uitzondering van de exploitanten van een handelsplatform in de zin van artikel 3, 6°, van de wet van 21 november 2017 over de infrastructuren voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU.

De artikelen 36/19 en 36/20 zijn van toepassing.

De Sanctiecommissie oordeelt over het opleggen van de administratieve geldboetes bedoeld in artikel 52 van voormelde wet van 7 april 2019. De artikelen 36/8 tot 36/12/3 en artikel 36/21 zijn van toepassing.

De Bank deelt relevante informatie over incidentmeldingen die zij ontvangt krachtens de wet van 7 april 2019 zo snel mogelijk met de ECB.".

HOOFDSTUK 7. — *Inwerkingtreding*

Art. 96. Deze wet treedt in werking de dag waarop ze in het *Belgisch Staatsblad* wordt bekendgemaakt.

Kondigen deze wet af, bevelen dat zij met 's Lands zegel zal worden bekleed en door het *Belgisch Staatsblad* zal worden bekendgemaakt.

Gegeven te Brussel, 7 april 2019.

FILIP

Van Koningswege :

De Eerste Minister,
Ch. MICHEL

De Minister van Veiligheid en Binnenlandse Zaken,
P. DE CREM

Met 's Lands zegel gezegeld :

De Minister van Justitie,

K. GEENS

Nota

(1) Kamer van volksvertegenwoordigers (www.dekamer.be):
Stukken: 54 3340
Integraal verslag: 21 maart 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. Énergie	a) Électricité	Entreprises d'électricité au sens de l'article 2, 15°*ter* de la loi du 29 avril 1999 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 1999 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 1999 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 1965 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 1965 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 1965 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 1965 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 1965 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.

Secteur	Sous-secteur	Type d'entités
	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 2007 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	Établissements 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 12*bis* 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	Établissements 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

Bijlage 1 bij de wet van 7 april 2019 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid

Soorten aanbieders van essentiële diensten bedoeld in artikel 11, § 1

Sector	**Deelsector**	**Soort entiteit**
1. Energie	a) Elektriciteit	Elektriciteitsbedrijven in de zin van artikel 2, 15°*ter*, van de wet van 29 april 1999 betreffende de organisatie van de elektriciteitsmarkt.
		Distributienetbeheerders in de zin van artikel 2, 11°, van de wet van 29 april 1999 betreffende de organisatie van de elektriciteitsmarkt.
		Netbeheerders in de zin van artikel 2, 8°, van de wet van 29 april 1999 betreffende de organisatie van de elektriciteitsmarkt.
	b) Aardolie	Exploitanten van oliepijpleidingen.
		Exploitanten van installaties voor de productie, raffinage, verwerking, opslag en het vervoer van aardolie.
	c) Gas	Aardgasondernemingen in de zin van artikel 1, 5°*bis*, van de wet van 12 april 1965 betreffende het vervoer van gasachtige produkten en andere door middel van leidingen.
		Distributienetbeheerders in de zin van artikel 1, 13°, van de wet van 12 april 1965 betreffende het vervoer van gasachtige produkten en andere door middel van leidingen.
		Beheerders van het aardgasvervoersnet in de zin van artikel 1, 31°, van de wet van 12 april 1965 betreffende het vervoer van gasachtige produkten en andere door middel van leidingen.
		Beheerders van de opslag in de zin van artikel 1, 33°, van de wet van 12 april 1965 betreffende het vervoer van gasachtige produkten en andere door middel van leidingen.
		Beheerders van de LNG-installatie in de zin van artikel 1, 35°, van de wet van 12 april 1965 betreffende het vervoer van gasachtige produkten en andere door middel van leidingen.
		Exploitanten van raffinage- en verwerkingsinstallaties van aardgas.
2. Vervoer	a) Luchtvervoer	Luchtvaartmaatschappijen in de zin van artikel 3, punt 4) van de verordening (EG) nr. 300/2008 van het Europees Parlement en de Raad van 11 maart 2008 inzake gemeenschappelijke regels op het gebied van de beveiliging van de burgerluchtvaart en tot intrekking van verordening (EG) nr. 2320/2002.
		Luchthavenbeheerders in de zin van in artikel 2, punt 2), van het KB van 6 november 2010 betreffende de toegang tot de grondafhandelingsmarkt op de luchthaven Brussel-Nationaal, luchthavens in de zin van artikel 2, punt 1), van richtlijn 2009/12/EG van het Europees Parlement en de Raad, met inbegrip van de luchthavens die tot het kernnetwerk behoren, opgesomd in bijlage II, afdeling 2, van verordening (EU) nr. 1315/2013 van het Europees Parlement en de Raad, alsook entiteiten die bijbehorende installaties bedienen welke zich op luchthavens bevinden.
		Luchtvaartnavigatiediensten in de zin van artikel 2, punt 4), van de verordening (EG) nr. 549/2004 van het Europees Parlement en de Raad van 10 maart 2004 tot vaststelling van het kader voor de totstandbrenging van het gemeenschappelijke Europese luchtruim ("de kaderverordening").

Sector	Deelsector	Soort entiteit
		De netwerkbeheerder in de zin van artikel 2, punt 22), van de verordening (EU) nr. 677/2011 van de Commissie van 7 juli 2011 tot vaststelling van nadere regels ter uitvoering van de netwerkfuncties voor luchtverkeersbeheer en tot wijziging van Verordening (EU) nr. 691/2010.
	b) Spoorvervoer	Infrastructuurbeheerders in de zin van artikel 3, 29°, van de Spoorcodex.
		Spoorwegondernemingen in de zin van artikel 3, 27°, van de Spoorcodex.
	c) Vervoer over water	Bedrijven voor land-, zee- en kustvervoer van passagiers en goederen in de zin van bijlage I van de verordening (EG) nr. 725/2004 van het Europees Parlement en de Raad, behalve schepen die individueel worden geëxploiteerd door die bedrijven.
		Beheerders van havens in de zin van artikel 5, punt 7), van de wet van 5 februari 2007 betreffende de maritieme beveiliging, met inbegrip van hun havenfaciliteiten in de zin van artikel 2, punt 11), van verordening (EG) nr. 725/2004, alsook entiteiten die werken en uitrusting in havens beheren.
		Exploitanten van verkeersbegeleidingssystemen (VBS) in de zin van artikel 1, punt 12), van het KB van 17 september 2005 tot omzetting van richtlijn 2002/59/EG van 27 juni 2002.
	d) Vervoer over de weg	Wegenautoriteiten in de zin van artikel 2, punt 12), van de gedelegeerde verordening (EU) 2015/962 van de Commissie van 18 december 2014 ter aanvulling van Richtlijn 2010/40/EU van het Europees Parlement en de Raad wat de verlening van EU-wijde realtimeverkeersinformatiediensten betreft, belast met de verkeerbeheerscontrole.
		Exploitanten van intelligente vervoerssystemen in de zin van artikel 3, punt 1), van de wet van 17 augustus 2013 tot creatie van het kader voor het invoeren van intelligente vervoerssystemen en tot wijziging van de wet van 10 april 1990 tot regeling van de private en bijzondere veiligheid (geciteerd als "ITS-kaderwet").
3. Financiën	a) Financiële instellingen	Kredietinstellingen in de zin van artikel 4, punt 1), van de verordening (EU) nr. 575/2013 van het Europees Parlement en de Raad van 26 juni 2013 betreffende prudentiële vereisten voor kredietinstellingen en beleggingsondernemingen en tot wijziging van verordening (EU) nr. 648/2012.
		Centrale tegenpartijen in de zin van artikel 2, punt 1), van de verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad van 4 juli 2012 betreffende otc-derivaten, centrale tegenpartijen en transactieregisters.
		Financiële instellingen (andere dan de kredietinstellingen en de centrale tegenpartijen) die onderworpen zijn aan het toezicht van de Nationale Bank van België, krachtens de artikelen 8 en 12*bis* van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België.
	b) Financiële handelsplatformen	Exploitanten van een handelsplatform in de zin van artikel 3, 6°, van de wet van 21 november 2017 over de infrastructuren voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU.
4. Gezondheidszorg	Zorginstellingen (waaronder ziekenhuizen en privéklinieken)	Zorgverleners in de zin van artikel 3, punt g), van de richtlijn 2011/24/EU van het Europees Parlement en de Raad van 9 maart 2011 betreffende de toepassing van de rechten van patiënten bij grensoverschrijdende gezondheidszorg.
5. Drinkwater		Leveranciers en distributeurs van water bestemd voor menselijke consumptie in de zin van artikel 2, punt 1) a), van de richtlijn 98/83/EG van de Raad van 3 november 1998 betreffende de kwaliteit van voor menselijke consumptie bestemd water, behalve de distributeurs voor wie de distributie van water bestemd voor menselijke consumptie slechts een deel is van hun algemene distributieactiviteit van andere producten en goederen die niet worden beschouwd als essentiële diensten.

Sector	Deelsector	Soort entiteit
6.Digitale infrastructuren		IXP.
		Leveranciers van DNS-diensten.
		Registers van topleveldomeinnamen.

Gezien om te worden gevoegd bij de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.

FILIP

Van Koningswege :

De Eerste Minister,

Ch. MICHEL

De Minister van Veiligheid en Binnenlandse Zaken,

P. DE CREM

Bijlage 2 bij de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid

Soorten digitale diensten

1. Onlinemarktplaats
2. Onlinezoekmachines
3. Cloudcomputerdiensten

Gezien om te worden gevoegd bij de wet van 7 april 2019 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.

FILIP

Van Koningswege :

De Eerste Minister,

Ch. MICHEL

De Minister van Veiligheid en Binnenlandse Zaken,

P. DE CREM

SERVICE PUBLIC FEDERAL AFFAIRES ETRANGERES, COMMERCE EXTERIEUR ET COOPERATION AU DEVELOPPEMENT

[C − 2018/12850]

29 JUILLET 1971. — Loi portant approbation de la Convention entre le Royaume de Belgique et la République d'Indonésie relative à l'encouragement et à la protection réciproque des investissements, et du Protocole, signés à Djakarta le 15 janvier 1970. — Addendum (1)

Conformément à son article 12, la Convention a pris fin le 16 juin 2002.

Note

(1) Voir *Moniteur belge* du 31/08/1972

FEDERALE OVERHEIDSDIENST BUITENLANDSE ZAKEN, BUITENLANDSE HANDEL EN ONTWIKKELINGSSAMENWERKING

[C − 2018/12850]

29 JULI 1971. — Wet houdende goedkeuring van de Overeenkomst tussen het Koninkrijk België en de Republiek Indonesië inzake de aanmoediging en de wederzijdse bescherming van investeringen, en van het Protocol, ondertekend te Djakarta op 15 januari 1970. — Addendum (1)

Overeenkomstig haar artikel 12, is de Overeenkomst beëindigd op 16 juni 2002.

Nota

(1) Zie het *Belgisch Staatsblad* d.d. 31/08/1972

SERVICE PUBLIC FEDERAL AFFAIRES ETRANGERES, COMMERCE EXTERIEUR ET COOPERATION AU DEVELOPPEMENT

[C − 2019/40863]

1er MARS 1991. — Loi portant approbation de l'Accord entre le Gouvernement du Royaume de Belgique et le Gouvernement du Grand-Duché de Luxembourg, d'une part, et le Gouvernement de la République populaire de Pologne, d'autre part, concernant l'encouragement et la protection réciproques des investissements, et de l'échange de lettres, signés à Varsovie le 19 mai 1987. — Addendum (1)

Les autorités polonaises ont dénoncé cet Accord le 19 juillet 2018, conformément à l'article 10.1 de l'Accord.

FEDERALE OVERHEIDSDIENST BUITENLANDSE ZAKEN, BUITENLANDSE HANDEL EN ONTWIKKELINGSSAMENWERKING

[C − 2019/40863]

1 MAART 1991. — Wet houdende goedkeuring van de Overeenkomst tussen de Regering van het Koninkrijk België en de Regering van het Groothertogdom Luxemburg, enerzijds, en de Regering van de Volksrepubliek Polen, anderzijds, inzake de wederzijdse bevordering en bescherming van investeringen, en van de wisseling van brieven, ondertekend te Warschau op 19 mei 1987. — Addendum (1)

De Poolse autoriteiten hebben deze Overeenkomst op 19 juli 2018 opgezegd, overeenkomstig artikel 10.1 van de Overeenkomst.