DOC 54 **3340/001**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

12 november 2018

# WETSONTWERP

## tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid

**INHOUD**

Blz.



OVEREENKOMSTIG ARTIKEL 8, § 2, 1°, VAN DE WET VAN 15 DECEMBER 2013 WERD DE IMPACTANALYSE NIET GEVRAAGD.

**DE SPOEDBEHANDELING WORDT DOOR DE REGERING GEVRAAGD OVEREENKOMSTIG ARTIKEL 51 VAN HET REGLEMENT.**

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

12 novembre 2018

# PROJET DE LOI

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

**SOMMAIRE**

Pages



CONFORMÉMENT À L'ARTICLE 8, § 2, 1°, DE LA LOI DU 15 DÉCEMBRE 2013, L'ANALYSE D'IMPACT N'A PAS ÉTÉ DEMANDÉE.

**LE GOUVERNEMENT DEMANDE L'URGENCE CONFORMÉMENT À L'ARTICLE 51 DU RÈGLEMENT.**

| | |
|---|---|
| *De regering heeft dit wetsontwerp op 12 november 2018 ingediend.* | *Le gouvernement a déposé ce projet de loi le 12 novembre 2018.* |
| *De "goedkeuring tot drukken" werd op 12 november 2018 door de Kamer ontvangen.* | *Le "bon à tirer" a été reçu à la Chambre le 12 novembre 2018.* |

| | | |
|---|---|---|
| *N-VA* | : | *Nieuw-Vlaamse Alliantie* |
| *PS* | : | *Parti Socialiste* |
| *MR* | : | *Mouvement Réformateur* |
| *CD&V* | : | *Christen-Democratisch en Vlaams* |
| *Open Vld* | : | *Open Vlaamse liberalen en democraten* |
| *sp.a* | : | *socialistische partij anders* |
| *Ecolo-Groen* | : | *Ecologistes Confédérés pour l'organisation de luttes originales – Groen* |
| *cdH* | : | *centre démocrate Humaniste* |
| *VB* | : | *Vlaams Belang* |
| *PTB-GO!* | : | *Parti du Travail de Belgique – Gauche d'Ouverture* |
| *DéFI* | : | *Démocrate Fédéraliste Indépendant* |
| *PP* | : | *Parti Populaire* |
| *Vuye&Wouters* | : | *Vuye&Wouters* |

| *Afkortingen bij de nummering van de publicaties:* | | *Abréviations dans la numérotation des publications:* | |
|---|---|---|---|
| *DOC 54 0000/000:* | *Parlementair document van de 54e zittingsperiode + basisnummer en volgnummer* | *DOC 54 0000/000:* | *Document parlementaire de la 54e législature, suivi du n° de base et du n° consécutif* |
| *QRVA:* | *Schriftelijke Vragen en Antwoorden* | *QRVA:* | *Questions et Réponses écrites* |
| *CRIV:* | *Voorlopige versie van het Integraal Verslag* | *CRIV:* | *Version Provisoire du Compte Rendu intégral* |
| *CRABV:* | *Beknopt Verslag* | *CRABV:* | *Compte Rendu Analytique* |
| *CRIV:* | *Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaald beknopt verslag van de toespraken (met de bijlagen)* | *CRIV:* | *Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)* |
| *PLEN:* | *Plenum* | *PLEN:* | *Séance plénière* |
| *COM:* | *Commissievergadering* | *COM:* | *Réunion de commission* |
| *MOT:* | *Moties tot besluit van interpellaties (beigekleurig papier)* | *MOT:* | *Motions déposées en conclusion d'interpellations (papier beige)* |

*Officiële publicaties, uitgegeven door de Kamer van volksvertegenwoordigers*

*Bestellingen:*
*Natieplein 2*
*1008 Brussel*
*Tel. : 02/ 549 81 60*
*Fax : 02/549 82 74*
*www.dekamer.be*
*e-mail : publicaties@dekamer.be*

*De publicaties worden uitsluitend gedrukt op FSC gecertificeerd papier*

*Publications officielles éditées par la Chambre des représentants*

*Commandes:*
*Place de la Nation 2*
*1008 Bruxelles*
*Tél. : 02/ 549 81 60*
*Fax : 02/549 82 74*
*www.lachambre.be*
*courriel : publications@lachambre.be*

*Les publications sont imprimées exclusivement sur du papier certifié FSC*

**SAMENVATTING**

*Dit wetsontwerp beoogt met name 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 "NIS-richtlijn" genoemd.*

*De NIS-richtlijn heeft tot doel ervoor te zorgen dat technische en organisatorische beveiligingsmaatregelen worden genomen door de aanbieders van essentiële diensten om incidenten te voorkomen of de impact ervan te beperken, teneinde de continuïteit en de openbare veiligheid van essentiële diensten te waarborgen. In dezelfde geest heeft de in de richtlijn vervatte meldingsplicht van incidenten betrekking op incidenten die een aanzienlijke impact hebben op de verleende essentiële diensten.*

*De verplichtingen vervat in de NIS-richtlijn gelden voornamelijk voor entiteiten die, in geval van een incident dat de beveiliging van hun netwerk- en informatiesystemen aantast, de verlening van essentiële diensten voor het behoud van kritieke maatschappelijke of economische activiteiten aanzienlijk kunnen verstoren. De NIS-richtlijn bepaalt ook dat bij de beoordeling van het belang van het verstorende effect van een incident met name rekening moet worden gehouden met de gevolgen ervan voor economische of maatschappelijke activiteiten of voor de openbare veiligheid.*

*De verstoring van de in de wet bedoelde digitale diensten (de digitaledienstverleners) kan ook verhinderen dat diezelfde essentiële diensten worden verleend.*

*Dit wetsontwerp een gemeenschappelijke aanpak van de door de verschillende soorten aanbieders toegepaste beveiligingsmaatregelen uitwerken, de doelgroep van de beveiligingsverplichtingen uitbreiden, de definities herzien en verplichtingen invoeren voor het melden van beveiligingsincidenten bij netwerk- en informatiesystemen.*

**RÉSUMÉ**

*Ce projet de 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".*

*L'objectif de la directive NIS est d'assurer la prise de mesures de sécurité techniques et organisationnelles par les opérateurs de services essentiels pour prévenir les incidents ou en limiter l'impact, en vue d'assurer la continuité et la sécurité publique des services essentiels. Dans le même esprit, les obligations de notification des incidents contenues dans la directive portent sur les incidents qui ont un impact significatif sur les services essentiels fournis.*

*Les principaux destinataires des obligations de la directive NIS sont les entités susceptibles, en cas d'incident affectant la sécurité de leurs réseaux et systèmes d'information, de perturber de manière importante la fourniture de services essentiels au maintien d'activités sociétales ou économiques critiques. La directive NIS précise également que l'importance de l'effet perturbateur d'un incident doit s'apprécier notamment au regard de ses conséquences sur les fonctions économiques ou sociétales ou sur la sûreté publique.*

*La perturbation des services numériques visés par la loi (les fournisseur de services numériques) est également susceptible d'empêcher la fourniture de ces mêmes services essentiels.*

*Le présent projet de loi entend mettre en œuvre une approche commune des mesures de sécurité appliquées par les différents types d'opérateurs, élargir les destinataires des obligations de sécurité, revoir les définitions et prévoir des obligations de notification des incidents de sécurité sur les réseaux et des systèmes d'information.*

## MEMORIE VAN TOELICHTING

DAMES EN HEREN,

### ALGEMENE TOELICHTING

Dit wetsontwerp beoogt met name 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 "NIS-richtlijn" genoemd.

Netwerk- en informatiesystemen spelen een cruciale rol in onze moderne maatschappij. Een groot deel van de entiteiten die essentiële diensten verlenen voor het behoud van kritieke maatschappelijke of economische activiteiten in België zijn afhankelijk van netwerk- en informatiesystemen. De verstoring van de in de wet bedoelde digitale diensten kan ook verhinderen dat diezelfde essentiële diensten worden verleend. Ook tal van overheden gebruiken de in de wet bedoelde digitale diensten in het kader van hun opdrachten van algemeen belang.

De verplichtingen vervat in de NIS-richtlijn gelden voornamelijk voor entiteiten die, in geval van een incident dat de beveiliging van hun netwerk- en informatiesystemen aantast, de verlening van essentiële diensten voor het behoud van kritieke maatschappelijke of economische activiteiten aanzienlijk kunnen verstoren. De NIS-richtlijn bepaalt ook dat bij de beoordeling van het belang van het verstorende effect van een incident met name rekening moet worden gehouden met de gevolgen ervan voor economische of maatschappelijke activiteiten of voor de openbare veiligheid.

De NIS-richtlijn heeft tot doel ervoor te zorgen dat technische en organisatorische beveiligingsmaatregelen worden genomen door de aanbieders van essentiële diensten om incidenten te voorkomen of de impact ervan te beperken, teneinde de continuïteit van essentiële diensten te waarborgen. In dezelfde geest heeft de in de richtlijn vervatte meldingsplicht van incidenten betrekking op incidenten die een aanzienlijke impact hebben op de verleende essentiële diensten.

De omvang, de frequentie en de gevolgen van incidenten die netwerk- en informatiesystemen aantasten, nemen almaar toe en vormen een grote bedreiging voor de goede werking van de essentiële diensten ervan. De informatiesystemen kunnen met name een doelwit worden van opzettelijke schadelijke acties die bedoeld zijn om de werking van de systemen te verstoren of te onderbreken.

## EXPOSÉ DES MOTIFS

MESDAMES, MESSIEURS,

### EXPOSÉ GÉNÉRAL

Ce projet de 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".

Les réseaux et systèmes d'information jouent un rôle crucial dans nos sociétés modernes. Une grande partie des entités fournissant des services essentiels au maintien d'activités sociétales ou économiques critiques en Belgique sont tributaires de réseaux et systèmes d'information. La perturbation des services numériques visés par la loi est également susceptible d'empêcher la fourniture de ces mêmes services essentiels. De même, de nombreuses autorités publiques utilisent les services numériques visés par la loi, dans le cadre de leurs missions d'intérêt général.

Les principaux destinataires des obligations de la directive NIS sont les entités susceptibles, en cas d'incident affectant la sécurité de leurs réseaux et systèmes d'information, de perturber de manière importante la fourniture de services essentiels au maintien d'activités sociétales ou économiques critiques. La directive NIS précise également que l'importance de l'effet perturbateur d'un incident doit s'apprécier notamment au regard de ses conséquences sur les fonctions économiques ou sociétales ou sur la sûreté publique.

L'objectif de la directive NIS est d'assurer la prise de mesures de sécurité techniques et organisationnelles par les opérateurs de services essentiels pour prévenir les incidents ou en limiter l'impact, en vue d'assurer la continuité des services essentiels. Dans le même esprit, les obligations de notification des incidents contenues dans la directive portent sur les incidents qui ont un impact significatif sur les services essentiels fournis.

L'ampleur, la fréquence et l'impact des incidents affectant les réseaux et les systèmes d'information ne cessent de croître et représentent une menace considérable pour le bon fonctionnement de ses services essentiels. Les systèmes d'information peuvent notamment devenir des cibles pour des actions intentionnelles malveillantes qui visent à la détérioration ou à l'interruption de leur fonctionnement.

De bescherming, de beveiliging en de betrouwbaarheid van de netwerk- en informatiesystemen van aanbieders van essentiële diensten en van sommige digitaledienstverleners zijn voortaan overwegingen van algemeen belang voor de bescherming van de bevolking en de ondernemingen van ons land. De beveiligingsvoorschriften voor hun netwerk- en informatiesystemen vallen bijgevolg onder de openbare orde en veiligheid in ruime zin.

In het licht van deze beschouwingen moeten eisen inzake beveiliging en melding van incidenten van toepassing zijn op aanbieders van essentiële diensten en sommige digitaledienstverleners om een cultuur van risicobeheer te bevorderen en ervoor te zorgen dat de ernstigste incidenten worden gemeld.

Bovendien blijkt het noodzakelijk om een nationale strategie te ontwikkelen waarin passende strategische en reglementaire doelstellingen worden bepaald met het oog op het tot stand brengen van een hoog beveiligingsniveau van netwerk- en informatiesystemen, ten minste voor de aanbieders van essentiële diensten en digitaledienstverleners bedoeld in de NIS-richtlijn die actief zijn in België.

Momenteel voorziet het Belgische wetgevende kader enkel in algemene beveiligingsverplichtingen, die ook gelden voor netwerk- en informatiesystemen, voor de exploitanten van zogenaamde “kritieke” infrastructuren in de zin van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, die voorziet in de omzetting van Richtlijn 2008/114/EG van 8 december 2008 inzake de identificatie van Europese kritieke infrastructuren, de aanmerking van infrastructuren als Europese kritieke infrastructuren en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuren te verbeteren.

Zoals bepaald in de NIS-richtlijn, wil dit wetsontwerp een gemeenschappelijke aanpak van de door de verschillende soorten aanbieders toegepaste beveiligingsmaatregelen uitwerken, de doelgroep van de beveiligingsverplichtingen uitbreiden, de definities herzien en verplichtingen invoeren voor het melden van beveiligingsincidenten bij netwerk- en informatiesystemen.

Tot op heden beschikte ons land niet over een volledig arsenaal aan wetgeving over de beveiliging van netwerk- en informatiesystemen. Dit ontwerp heeft ook tot doel om deze leemte op te vullen, op een gebied waarvan het strategische belang almaar toeneemt.

Het wetsontwerp wil een aanpak van het beheer van beveiligingsrisico’s bevorderen die aansluit bij

La protection, la sécurité et la fiabilité des réseaux et systèmes d’information des opérateurs fournissant des services essentiels et de certains fournisseurs de service numérique sont désormais des considérations d’intérêt général pour la protection de la population et des entreprises du pays. Les règles de sécurité de leurs réseaux et systèmes d’information relèvent dès lors de l’ordre et de la sécurité publique au sens large.

Ces considérations imposent donc de soumette les opérateurs de services essentiels et certains fournisseurs de service numérique à des exigences en matière de sécurité et de notification des incidents, afin de promouvoir une culture de gestion des risques et de faire en sorte que les incidents les plus graves soient signalés.

De plus, il s’avère nécessaire de développer une stratégie nationale qui définit les objectifs stratégiques et réglementaires appropriées en vue de parvenir à un niveau élevé de sécurité des réseaux et des systèmes d’information, au moins pour les opérateurs de services essentiels et les fournisseurs de services numériques visés par la directive NIS et opérant en Belgique.

Actuellement, le cadre législatif belge prévoit seulement des obligations générales de sécurité, en ce compris des réseaux et systèmes d’information, aux exploitants d’infrastructures dites “critiques” au sens de la loi du 1 juillet 2011 relative à la sécurité et à la protection des infrastructures critiques, qui transpose la Directive 2008/114/CE du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l’évaluation de la nécessité d’améliorer leur protection.

Comme le prévoit la directive NIS, le présent projet de loi entend mettre en œuvre une approche commune des mesures de sécurité appliquées par les différents types d’opérateurs, élargir les destinataires des obligations de sécurité, revoir les définitions et prévoir des obligations de notification des incidents de sécurité sur les réseaux et des systèmes d’information.

Notre pays ne s’était jusqu’à présent pas doté d’un arsenal législatif complet sur la sécurité des réseaux et des systèmes d’information. Le présent projet vise aussi à combler cette lacune, dans un domaine qui devient de plus en plus stratégique.

Le projet de loi tend à promouvoir une approche de la gestion des risques de sécurité qui soit en harmonie

de bepalingen inzake de bescherming van persoonsgegevens, waaronder de Europese Verordening nr. 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 (Algemene Verordening Gegevensbescherming, hierna "AVG").

Eerst en vooral blijven de bepalingen van de AVG volledig van toepassing op de gegevensverwerking in uitvoering van het wetsontwerp, met name het beginsel van minimale gegevensverwerking, de inachtneming van de doeleinden, de beperking van de bewaartermijn, enz. De noodzaak om bepaalde doelstellingen van het wetsontwerp te waarborgen, heeft beperkte afwijkingen van de regels van de AVG gerechtvaardigd, die in de artikelsgewijze bespreking verder worden toegelicht.

Tot slot is het belangrijk om bepaalde dicht bij elkaar liggende maar toch verschillende begrippen, die zowel in de AVG als in het wetsontwerp vermeld worden, van elkaar te onderscheiden, en met name:

— de artikelen 24 en 35 van het ontwerp leggen een meldingsplicht op voor "incidenten die aanzienlijke gevolgen hebben" terwijl de artikelen 33 en 34 van de AVG voorzien in een meldingsplicht voor "inbreuken in verband met persoonsgegevens";

— de artikelen 23, § 1, en 34 van het ontwerp voorzien in de aanwijzing van een "contactpunt voor de beveiliging van netwerk- en informatiesystemen", terwijl artikel 37 van de AVG voorziet in de aanwijzing van een "functionaris voor gegevensbescherming".

Vanuit institutioneel oogpunt zullen de verschillende ingestelde of bestaande autoriteiten die door of krachtens dit wetsontwerp gemachtigd worden, een essentiële rol moeten vervullen bij de uitvoering van de wet. Het wetsontwerp beoogt hen daartoe de nodige bevoegdheden en middelen te verschaffen.

De inhoud van de verplichtingen vervat in de NIS-richtlijn heeft betrekking op het beveiligingsniveau van de netwerk- en informatiesystemen van entiteiten die diensten van algemeen belang verlenen voor de bevolking en de ondernemingen, of kritiek zijn voor het economisch potentieel van ons land. Zoals de Raad van State heeft opgemerkt in zijn advies van 2 mei 2018, leidt de omzetting van deze richtlijn hoofdzakelijk tot de tenuitvoerlegging van de aangelegenheid van de preventieve bescherming op het gebied van de openbare veiligheid, die tot de exclusieve restbevoegdheid van de federale wetgever behoort.

avec les dispositions concernant la protection des données à caractère personnel, dont le Règlement européen n°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 (Règlement Général sur la protection des données, ci-après "RGPD").

Tout d'abord, les dispositions du RGPD demeurent entièrement applicables aux traitements de données qui seront effectués en exécution du projet de loi, notamment le principe de minimisation des données, le respect des finalités, la limitation de la durée de conservation, etc. La nécessité de préserver certains objectifs du projet de loi a justifié des dérogations limitées aux règles du RGPD, que le commentaire par article explicite davantage.

Ensuite, il est important de ne pas confondre certaines notions, proches mais néanmoins distinctes, qui figurent tant dans le RGPD que dans le projet de loi, et notamment:

— les articles 24 et 35 du projet imposent une obligation de notification des "incidents ayant un impact significatif" alors que les articles 33 et 34 du RGPD prévoient une obligation de notification pour les "violations de données à caractère personnel";

— les articles 23, § 1er et 34 du projet prévoient la désignation d'un "point de contact pour la sécurité des réseaux et systèmes d'information" alors que l'article 37 du RGPD prévoit la désignation d'un "délégué à la protection des données".

D'un point de vue institutionnel, les différentes autorités instituées ou existantes habilitées en vertu du présent projet de loi auront un rôle essentiel à jouer dans la mise en œuvre de la loi. Le projet de loi vise à les investir des compétences et des moyens nécessaires à cette fin.

Le contenu des obligations de la directive NIS porte sur le niveau de sécurité des réseaux et des systèmes d'information des entités fournissant des services d'intérêt général pour la population et les entreprises, ou critiques pour le potentiel économique du pays. Comme l'a souligné le Conseil d'État dans son avis du 2 mai 2018, la transposition de cette directive met principalement en œuvre la matière de la protection préventive exercée dans le domaine de la sécurité publique, qui relève des compétences résiduelles exclusives du législateur fédéral.

Naar analogie van de bepalingen van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren bepaalt de wet niettemin dat de deelgebieden worden geraadpleegd wanneer sommige aanbieders van essentiële diensten (publiekrechtelijke of privaatrechtelijke personen) of digitaledienstverleners voor andere aspecten van hun activiteiten onderworpen zouden zijn aan gewestelijke of gemeenschapsregels. Deze raadpleging is facultatief en gebeurt op een zodanige wijze dat, indien de deelgebieden verzuimen om mee te werken, dit niet verhindert dat de federale overheid de voorgenomen maatregelen kan nemen.

Tot slot blijft de uitoefening van de federale bevoegdheid in het wetsontwerp in elk geval in verhouding en heeft ze niet tot gevolg dat het voor de gewesten of gemeenschappen onmogelijk of bovenmatig moeilijk zou zijn om hun bevoegdheden op de werkterreinen van sommige betrokken aanbieders van essentiële diensten of digitaledienstverleners gewoon uit te oefenen.

## ARTIKELSGEWIJZE TOELICHTING

TITEL 1

*Definities en algemene bepalingen*

HOOFDSTUK 1

**Onderwerp en toepassingsgebied**

**Afdeling 1**

*Onderwerp*

Artikel 1

Dit artikel bevat de grondwettelijke grondslag van de wet.

Artikel 2

Dit artikel vermeldt de richtlijn die door de wet wordt omgezet.

**Afdeling 2**

*Toepassingsgebied*

Artikel 3

Dit artikel verduidelijkt het territoriale toepassingsgebied van de wet. Het wijst erop dat sommige bepalingen

A l'instar des dispositions de la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques, il est néanmoins prévu dans la loi de consulter, de manière facultative et en manière telle que leur éventuelle abstention de collaborer n'empêche pas l'adoption des mesures envisagées par l'autorité fédérale, les entités fédérées lorsque certains opérateurs de services essentiels (personnes publiques ou privées) ou fournisseurs de services numériques seraient, pour d'autres aspects de leurs activités, soumis à des règles régionales ou communautaires.

Enfin, l'exercice de la compétence fédérale dans le projet de loi reste, en tout état de cause, proportionné et n'a pas pour conséquence de rendre impossible ou exagérément difficile l'exercice normal des compétences régionales ou communautaires dans les domaines d'activités de certains opérateurs de services essentiels ou fournisseurs de services numériques concernés.

## COMMENTAIRE DES ARTICLES

TITRE 1ER

*Définitions et dispositions générales*

CHAPITRE 1ER

**Objet et champ d'application**

**Section 1re**

*Objet*

Article 1er

Cet article précise le fondement constitutionnel de la loi.

Article 2

Cet article précise la directive transposée par la loi.

**Section 2**

*Champ d'application*

Article 3

Cet article précise le champ d'application territorial de la loi. Il est précisé que certaines dispositions de la

van de wet ook van toepassing zijn op potentiële aanbieders van essentiële diensten. Er bestaan immers twee categorieën van aanbieders die in de wet worden bedoeld: enerzijds de "potentiële aanbieders van essentiële diensten" bepaald in artikel 6, 12°, d.w.z. de publieke of private entiteiten die actief zijn in België in een van de sectoren opgenomen in bijlage I van de wet, maar die niet zijn aangewezen als aanbieders van essentiële diensten door de bevoegde sectorale overheid, en anderzijds, de "aanbieders van essentiële diensten" bepaald in artikel 6, 11°, die als dusdanig zijn aangewezen door de bevoegde sectorale overheid.

Het artikel somt de bepalingen van de wet op die van toepassing zijn op potentiële aanbieders van essentiële diensten: de bepalingen van titel 1 (definities en algemene bepalingen), artikel 13 (identificatiecriteria), artikel 14 (verplichting om nuttige informatie te bezorgen), artikel 30 (vrijwillige melding van incidenten) en hoofdstuk 3 van titel 4 (de strafrechtelijke of administratieve sancties).

De wet is van toepassing op aanbieders van essentiële diensten die minstens één vestiging hebben op Belgisch grondgebied en daadwerkelijk een activiteit uitoefenen die betrekking heeft op de verlening van minstens één essentiële dienst op Belgisch grondgebied.

Het begrip "vestiging" wordt gedefinieerd overeenkomstig het recht van de Europese Unie. De rechtsvorm van deze vestiging, of het nu om een bijkantoor of om een dochteronderneming met rechtspersoonlijkheid gaat, is daarbij niet doorslaggevend.

Deze wet is van toepassing op digitaledienstverleners die hun hoofdvestiging in België hebben. Een digitaledienstverlener wordt geacht zijn hoofdvestiging in België te hebben als zijn hoofdkantoor zich daar bevindt.

Wanneer een digitaledienstverlener niet in de Europese Unie gevestigd is maar binnen de Europese Unie diensten verleent zoals bedoeld in bijlage III van de wet, moet deze dienstverlener een vertegenwoordiger aanwijzen in de Europese Unie. De vertegenwoordiger moet gevestigd zijn in een van de lidstaten waar de diensten worden verleend. Krachtens deze wet valt de digitaledienstverlener onder de bevoegdheid van de Belgische overheid wanneer zijn vertegenwoordiger in België gevestigd is.

Artikel 4

Dit artikel heeft betrekking op het toepassingsgebied van de wet. Het verduidelijkt dat sommige aanbieders

loi s'appliquent également aux opérateurs de services essentiels potentiels. Il existe, en effet, deux catégories d'opérateurs visés par la loi: d'une part, les "opérateurs de services essentiels potentiels" définis à l'article 6, 12°, c'est-à-dire les entités publiques ou privées actives en Belgique dans l'un des secteurs repris à l'annexe I de la loi mais qui n'ont pas été désignés comme opérateurs de services essentiels par l'autorité sectorielle compétente, et d'autre part, les "opérateurs de services essentiels" définis à l'article 6, 11° et qui ont été désignés comme tels par l'autorité sectorielle compétente.

L'article énumère les dispositions de la loi qui s'appliquent aux opérateurs de services essentiels potentiels: les dispositions du titre 1er (définitions et dispositions générales), l'article 13 (critères d'identification), l'article 14 (obligation de transmission d'informations utiles), l'article 30 (notification volontaire des incidents) et chapitre 3 du titre 4 (les sanctions pénales ou administratives).

La loi s'applique aux opérateurs de services essentiels 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.

Cette notion d'établissement est définie conformément au droit de l'Union européenne. La forme juridique retenue pour un tel établissement, qu'il s'agisse d'une succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard.

La présente loi s'applique aux fournisseurs de service numérique dont l'établissement principal est situé en Belgique. Un fournisseur de service numérique est réputé avoir son établissement principal en Belgique lorsque son siège social s'y trouve.

Lorsqu'un fournisseur de service numérique n'est pas établi dans l'Union européenne mais fournit des services visés à l'annexe III de la loi à l'intérieur de l'Union européenne, ce fournisseur doit désigner un représentant dans l'Union européenne. Le représentant doit être établi dans l'un des États membres dans lesquels les services sont fournis. Le fournisseur de service numérique relève de la compétence des autorités belges en vertu de la présente loi lorsque son représentant est établi en Belgique.

Article 4

L'article porte sur le champ d'application de la loi. Il précise certains opérateurs qui dérogent aux

afwijken van de bepalingen van de wet zodat, overeenkomstig de richtlijn, andere specifieke Europese en Belgische wetgeving volledig of gedeeltelijk op hen van toepassing is.

De door de richtlijn opgelegde beveiligings- en meldingseisen zijn niet van toepassing op ondernemingen die onderworpen zijn aan de eisen van de artikelen 13 bis en 13 ter van Richtlijn 2002/21/EG van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronische-communicatienetwerken en -diensten, omgezet in Belgisch recht door de artikelen 114 en 114/1 van de wet van 13 juni 2005 betreffende de elektronische communicatie.

Deze uitzondering geldt vanzelfsprekend enkel voor de activiteiten van deze ondernemingen die werkelijk onderworpen zijn aan de artikelen 114 en 114/1 van de wet van 13 juni 2005 betreffende de elektronische communicatie, namelijk deze in verband met het aanbieden van openbare elektronische-communicatienetwerken of openbare elektronische-communicatiediensten.

De onderneming die, enerzijds, diensten aanbiedt als bedoeld in voormelde wet van 13 juni 2005 (openbare elektronische-communicatienetwerken of openbare elektronische-communicatiediensten) en, anderzijds, digitale infrastructuurdiensten als bedoeld in bijlage I van de wet of digitale diensten als bedoeld in bijlage II van de wet, is onderworpen aan de bepalingen van deze wet voor het aanbieden respectievelijk van de in bijlage II van de wet bedoelde digitale diensten of van de in bijlage I van de wet bedoelde digitale infrastructuurdiensten.

Hetzelfde geldt voor de verleners van vertrouwensdiensten die onderworpen zijn aan de eisen vervat in artikel 19 van de Europese Verordening (EU) nr. 910/2014 van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt.

Rekening houdend met de bestaande sectorale wetgevingen op Europees niveau (bedoeld in paragraaf 2 van dit artikel), vallen de aanbieders van essentiële diensten die deel uitmaken van de sector financiën enkel onder sommige bepalingen van deze wet. Ze blijven immers onderworpen aan de bepalingen van Europese en Belgische wetgeving die minstens feitelijk gelijkwaardig zijn aan de beveiligings- en meldingsverplichtingen van de wet.

De bepalingen van Titel 1 van de wet (toepassingsgebied, definities, samenwerking op nationaal niveau, informatie-uitwisseling en nationale strategie), van hoofdstuk 1 van Titel 2 (identificatie van de aanbieders

dispositions de la loi pour se voir appliquer entièrement ou partiellement d'autres législations européennes et belges spécifiques, conformément à la directive.

Les exigences en matière de sécurité et de notification prévues par la directive ne s'appliquent pas aux entreprises soumises aux exigences énoncées aux articles 13 bis et 13 ter de la Directive 2002/21/CE du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, transposée en droit belge par les articles 114 et 114/1 de la loi du 13 juin 2005 relative aux communications électroniques.

Cette exception ne vaut, bien entendu, que pour les activités de ces entreprises qui sont effectivement soumises aux articles 114 et 114/1 de la loi du 13 juin 2005 relative aux communications électroniques, à savoir celles de fourniture de réseaux publics de communications électroniques ou de services de communications électroniques accessibles au public.

L'entreprise qui fournit, d'une part, des services visés par la loi du 13 juin 2005 précitée (réseaux publics de communications électroniques ou services de communications électroniques accessibles au public) et, d'autre part, des services d'infrastructures numériques visés à l'annexe I de la loi ou des services numériques visés à l'annexe II de la loi sera soumise aux dispositions de la présente loi, pour la fourniture respectivement des services numériques visés à l'annexe II de la loi ou des services d'infrastructures numériques visés à l'annexe I de la loi.

Il en va de même pour les prestataires de services de confiance soumis aux exigences énoncées à l'article 19 du règlement européen (UE) n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.

Compte tenu des législations sectorielles existantes au niveau européen (visées au paragraphe 2 du présent article), les opérateurs de services essentiels appartenant au secteur des finances ne se voient appliquer que certaines des dispositions de la présente loi. En effet, ils demeurent soumis aux dispositions des législations européennes et belges qui ont un effet au moins équivalent à celui des obligations de sécurité et de notification prévues par la loi.

Les dispositions du Titre 1er de la loi (le champ d'application, les définitions, la coopération au niveau national, l'échange d'informations et la stratégie nationale), du chapitre 1er du Titre 2 (identification des opérateurs

van essentiële diensten) en van artikel 26 (modaliteiten inzake het melden van incidenten) en de artikelen 65 tot 73 (afwijkingen van de verplichtingen en rechten van de AVG) zijn echter wel van toepassing op de aanbieders van essentiële diensten die deel uitmaken van de sector financiën.

De artikelen 65 tot 73 zijn evenwel niet van toepassing op de Nationale Bank van België en de Autoriteit voor Financiële Diensten en Markten, wanneer zij een regeling toepassen die afwijkt van de AVG voor de verwerking van gegevens over het toezicht op de aanbieders (krachtens artikel 46*bis* van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten, of artikel 12*quater* van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België).

De bepalingen van de wet (hoofdstuk 3 van Titel 2) inzake het melden van incidenten waartoe alle aanbieders van essentiële diensten verplicht zijn, zijn niettemin volledig van toepassing op de exploitanten van een handelsplatform omdat zij nog niet onder een Europese sectorale verplichting voor het melden van incidenten vallen. Voor aanbieders van essentiële diensten die deel uitmaken van de sector financiën, is niettemin voorzien in een specifiek mechanisme voor het melden van beveiligingsincidenten aan de Nationale Bank van België, die de melding vervolgens onverwijld aan het CCB en de ADCC bezorgt.

De controles ten aanzien van aanbieders van essentiële diensten die deel uitmaken van de sector financiën blijven onderworpen aan specifieke sectorale wetgeving. Titel 4 van de wet is dus op hen niet van toepassing, met uitzondering van artikel 53 voor de aanbieders van de sector financiën die geen exploitanten van een handelsplatform zijn.

Tot slot en zoals bepaald in de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, wordt verduidelijkt dat de elementen van een nucleaire installatie bestemd voor de industriële productie van elektriciteit die dienen voor de transmissie van de elektriciteit onderworpen zijn aan de bepalingen van de wet.

Voor de andere nucleaire installaties worden de maatregelen voor de beveiliging van netwerk- en informatiesystemen genomen 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.

de services essentiels) et de l'article 26 (modalités relatives aux notification des incidents) ainsi que des articles 65 à 73 (dérogations aux obligations et droits prévus par le RGPD) sont néanmoins applicables aux opérateurs de services essentiels appartenant au secteur des finances.

Toutefois, les articles 65 à 73 ne sont pas applicables à la Banque nationale de Belgique et à l'Autorité des services et marchés financiers, lorsque celles-ci appliquent un régime dérogatoire au RGPD pour les traitements de données liées au contrôle des opérateurs (en vertu de l'article 46*bis* de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers, ou de l'article 12*quater* de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique).

Les dispositions de la loi (chapitre 3 du Titre 2) relatives aux notifications d'incident prévues pour l'ensemble des opérateurs de services essentiels s'appliquent néanmoins complètement aux opérateurs de plate-forme de négociation car ceux-ci ne sont pas encore couverts par une obligation sectorielle européenne de notification des incidents. Pour les opérateurs de services essentiels appartenant au secteur des finances, il est prévu néanmoins un mécanisme de notification spécifique des incidents de sécurité à la Banque nationale de Belgique, qui transmet ensuite la notification, sans retard injustifié, au CCB et à la DGCC.

Les contrôles des opérateurs de services essentiels appartenant au secteur des finances demeurent régis par les législations sectorielles spécifiques. Le Titre 4 de la loi ne leur est donc pas applicable, à l'exception de l'article 53 pour les opérateurs du secteur financier autres que les opérateurs de plate-forme de négociation.

Enfin et comme le prévoit la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques, il est précisé que les éléments d'une installation nucléaire destinée à la production industrielle d'électricité qui servent au transport de l'électricité sont soumis aux dispositions de la loi.

Pour les autres installations nucléaires, les mesures de sécurité des réseaux et des systèmes d'information seront adoptées 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.

De beveiligingsmaatregelen van deze wet zijn evenwel van toepassing op de nucleaire installaties gebruikt in de sectoren bedoeld in bijlage I, wanneer en voor zover er geen maatregelen voor de beveiliging van netwerk- en informatiesystemen bestaan krachtens voormelde wet van 15 april 1994.

Artikel 5

Dit artikel wijst erop dat, onder voorbehoud van de afwijkende bepalingen in titel 6 van het ontwerp, de wet geen afbreuk doet aan de toepassing van de AVG of aan de wetten en reglementen die deze aanvullen of verduidelijken.

Er wordt tevens aan herinnerd dat de bepalingen van deze wet geen afbreuk doen aan de toepassing van sommige andere wettelijke bepalingen, waaronder de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, de regels die van toepassing zijn op de verwerking van geclassificeerde informatie in de zin van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen en 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.

Bijvoorbeeld, indien bepaalde informatie die overeenkomstig het wetsontwerp moet worden uitgewisseld geheel of gedeeltelijk is geclassificeerd krachtens de voormelde wet van 11 december 1998, blijven die laatste en de uitvoeringsbesluiten ervan volledig van toepassing.

HOOFDSTUK 2

**Definities**

Artikel 6

Dit artikel bevat de definities zoals die vooraf zijn vastgesteld door de NIS-richtlijn, alsook sommige aspecten die specifiek betrekking hebben op het Belgische of Europese wetgevende kader.

De sectorale overheden die, voor hun respectievelijke sector, belast zijn met het toezicht op de uitvoering van de bepalingen van de wet, worden aangewezen door de wet (voor de sectoren financiën en digitale infrastructuren) of door de Koning bij in Ministerraad

Toutefois, les mesures de sécurité prévues par la présente loi s'appliquent, par défaut, aux installations nucléaires utilisées dans les secteurs visés à l'annexe I de la loi, lorsque et dans la mesure où aucune mesure pour la sécurité des réseaux et des systèmes d'information n'existe en vertu de la loi du 15 avril 1994 précitée.

Article 5

L'article précise que, sous réserve des dispositions dérogatoires reprises au titre 6 du projet, la loi ne porte pas préjudice à l'application du RGPD ainsi qu'aux lois et règlements qui le complètent ou le précisent.

Il est aussi rappelé que les dispositions de la présente loi ne portent pas préjudice de l'application de certaines autres dispositions légales, dont la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques, les règles applicables au traitement des informations classifiées au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité et les 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.

Par exemple, si certaines informations qui doivent être échangées en application du projet de loi sont classifiées en tout ou en partie en vertu de la loi du 11 décembre 1998 précitée, cette dernière et ses actes d'exécution demeurent entièrement applicables.

CHAPITRE 2

**Définitions**

Article 6

Cet article reprend les définitions telles que préalablement établies par la directive NIS ainsi que certains éléments spécifiques au cadre législatif belge ou européen.

Les autorités sectorielles chargées, pour leur secteur respectif, de veiller à la mise en œuvre des dispositions de la loi seront désignées par la loi (pour le secteur financier ou le secteur des infrastructures digitales) ou désignées par le Roi, par arrêté délibéré en conseil des

overlegd besluit. Aldus wordt rekening gehouden met de opmerkingen van de Raad van State, volgens dewelke de door de Koning opgerichte sectorale overheden enkel door de Koning moeten worden aangewezen en niet door de wet. Deze aanpak laat ook toe om nieuwe sectorale overheden op te richten, met name bestaande uit vertegenwoordigers van de Gemeenschappen en Gewesten, op basis van artikel 92*ter* van de bijzondere wet van 8 augustus 1980 tot hervorming der instellingen.

Er wordt bijvoorbeeld overwogen om de Koning een Nationaal Comité voor de beveiliging van netwerk- en informatiesystemen voor de levering en distributie van drinkwater te laten oprichten, dat zou zijn samengesteld uit vertegenwoordigers van de Federale Staat, het Vlaams Gewest, het Brussels Hoofdstedelijk Gewest en het Waals Gewest.

Het begrip "sectoraal CSIRT" is met name eigen aan de Belgische omzetting van de richtlijn en omvat niet alle bevoegdheden die in de richtlijn en de bijlagen ervan aan het CSIRT worden toegekend. Het betreft een dienst van de sectorale overheid die voor zijn sector sommige taken van een CSIRT vervult, maar in coördinatie met en met inachtneming van de bevoegdheden van het nationale CSIRT.

De nationale accreditatieautoriteit wordt gedefinieerd als "instelling die door de Koning is opgericht in uitvoering van artikel VIII.30 van het wetboek van economisch recht". Krachtens het koninklijk besluit van 31 januari 2006 tot oprichting van het BELAC accreditatiesysteem van instellingen voor de conformiteitsbeoordeling, wordt dit een taak van de accreditatie-instelling BELAC.

Om alle twijfel weg te nemen over de draagwijdte van het begrip "netwerk- en informatiesysteem", wordt de definitie ervan verduidelijkt in punt 8, b), om er onder meer uitdrukkelijk de permanent of tijdelijk gekoppelde netwerken en de digitale, elektronische of mechanische componenten van een apparaat in op te nemen die met name de automatisering van het operationele proces, de controle op afstand, of het verkrijgen van gegevens inzake de werking in real time mogelijk maken.

Het is de bedoeling om te verduidelijken dat het begrip "apparaat dat digitale gegevens verwerkt" onder meer de digitale, elektronische of mechanische componenten van met name SCADA-systemen bevat (van het Engels "*Supervisory Control And Data Acquisition*"), alsook permanent of tijdelijk gekoppelde apparaten.

Ministres. L'on tient ainsi compte des observations du Conseil d'État, qui faisait remarquer que les autorités sectorielles créés par le Roi devaient être uniquement désignées par le Roi et non par la loi. Cette approche permet aussi de créer de nouvelles autorités sectorielles, notamment composées de représentants des Communautés et des Régions, sur base de l'article 92*ter* de la loi spéciale du 8 août 1980 de réformes institutionnelles.

Il est envisagé, par exemple, la création par le Roi d'un Comité national de sécurité des systèmes et réseaux de l'information pour la fourniture et de la distribution d'eau potable, lequel serait composé de représentants de l'État fédéral, de la Région flamande, de la Région de Bruxelles-Capitale et de la Région wallonne.

Le CSIRT sectoriel est notamment une notion propre à la transposition belge de la directive, qui ne reprend pas toutes les compétences attribuées au CSIRT par la directive et ses annexes. Il s'agit d'un service de l'autorité sectorielle qui exerce pour son secteur certaines des tâches d'un CSIRT mais en coordination et dans le respect des compétences du CSIRT national.

L'autorité nationale d'accréditation est défini comme "l'organisme créé par le Roi en exécution de l'article VIII.30 du Code de droit économique." En vertu de l'arrêté royal du 31 janvier 2006 portant création du système BELAC d'accréditation des organismes d'évaluation de la conformité, cette mission incombera à l'organisme d'accréditation BELAC.

Afin de lever les doutes quant à l'étendue de la notion de réseau et système d'information, sa définition est précisée au point 8, b) pour inclure explicitement, entre autres choses, les réseaux interconnectés de manière permanente ou temporaire et les composants numériques, électroniques ou mécaniques d'un dispositif permettant notamment l'automatisation de processus opérationnel, le contrôle à distance, ou l'obtention de données de fonctionnement en temps réel.

Il s'agit de préciser que la notion de dispositif traitant des données numériques comprend entre autre chose les composants numériques, électroniques ou mécaniques notamment de systèmes d'acquisition et de contrôle de données industriels (en anglais "*Supervisory Control And Data Acquisition*", en abrégé "SCADA"), ainsi que les dispositifs interconnectés de manière permanente ou temporaire.

HOOFDSTUK 3

## Bevoegde autoriteiten en samenwerking op nationaal niveau

### Afdeling 1

*Bevoegde autoriteiten*

Artikel 7

Dit artikel bepaalt dat de Koning de nationale autoriteit aanwijst, die belast is met de opvolging en coördinatie van de uitvoering van deze wet. De aanwijzing door de Koning houdt rekening met het advies van de Raad van State inzake de scheiding van de wetgevende en de uitvoerende macht. Deze nationale autoriteit is ook het "centraal nationaal contactpunt". Het nationale contactpunt is een nieuwigheid ingevoerd door de NIS-richtlijn. Het gaat om een verbindingsfunctie die moet zorgen voor samenwerking tussen de autoriteiten van de lidstaten van de Europese Unie en met de betrokken autoriteiten van de andere lidstaten, de Samenwerkingsgroep bedoeld in artikel 11. Bij deze aanwijzing wordt rekening gehouden met de opdrachten die het Centrum voor Cybersecurity België (CCB), dat is opgericht bij het koninklijk besluit van 10 oktober 2014, reeds moet uitvoeren als nationale autoriteit.

De Koning wijst de sectorale overheden aan bij in Ministerraad overlegd koninklijk besluit. In voorkomend geval kan Hij sectorale overheden oprichten, met name met vertegenwoordigers van de deelgebieden.

Het is de taak van de sectorale overheden om, voor hun respectievelijke sector, toe te zien op de uitvoering van de bepalingen van deze wet. Ze voeren de door de wet voorgeschreven opdrachten uit in het kader van hun bevoegdheden, met name de identificatie van de aanbieders van essentiële diensten en het toezicht op de naleving van de beveiligingseisen door aanbieders en digitaledienstverleners, in samenwerking met de andere autoriteiten bedoeld in dit artikel.

De sectorale overheden die door een wet zijn opgericht en geregeld, worden daarentegen rechtstreeks aangewezen, voor hun respectievelijke sector, namelijk voor de sector digitale infrastructuren: het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT), voor de sector financiën: de Nationale Bank van België (NBB) en 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

CHAPITRE 3

## Autorités compétentes et coopération au niveau national

### Section 1re

*Autorités compétentes*

Article 7

Cet article charge le Roi de désigner l'autorité nationale, chargée du suivi et de la coordination de la mise en œuvre de la loi. La désignation par le Roi tient compte de l'avis rendu par le Conseil d'État en matière de séparation des pouvoirs législatif et exécutif. Cette autorité nationale est aussi le "point de contact national unique". Le point de contact national est une nouvelle figure introduite par la directive NIS. Il s'agit d'une fonction de liaison afin d'assurer une coopération entre les autorités des États membres de l'Union européenne, ainsi qu'avec les autorités concernées des autres États membres, le groupe de coopération visé à l'article 11. Cette désignation tiendra compte des missions, au titre d'autorité nationale, qui incombent déjà au Centre pour la Cybersécurité Belgique (CCB), créé par l'arrêté royal du 10 octobre 2014.

Le Roi est chargé de désigner les autorités sectorielles, par arrêté royal délibéré en Conseil des ministres. Le cas échéant, le Roi peut créer des autorités sectorielles avec notamment des représentants des entités fédérées.

Les autorités sectorielles ont pour mission, pour leur secteur respectif, de veiller à la mise en œuvre des dispositions de la présente loi. Elles exécutent les missions prévues par la loi dans le cadre de leurs compétences, notamment l'identification des opérateurs de services essentiels et le contrôle du respect des exigences de sécurité imposées aux opérateurs et fournisseurs de service numérique, en collaboration avec les autres autorités visés par l'article.

En revanche, les autorités sectorielles créées et régies par une loi sont directement désignées, pour leur secteur respectif, à savoir pour le secteur des infrastructures numériques: l'Institut belge des services postaux et des télécommunications (IBPT), pour le secteur financier: la Banque nationale de Belgique et 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:

omzetting van Richtlijn 2014/65/EU: de Autoriteit voor Financiële Diensten en Markten (FSMA), door specifieke bepalingen van deze wet.

Dit artikel verduidelijkt ook dat de Koning de autoriteit aanwijst die de rol van nationaal CSIRT vervult, namelijk het nationale computer security incident response team. Het nationale CSIRT is met name belast met de ontvangst van meldingen van incidenten door aanbieders van essentiële diensten en digitaledienstverleners, alsook van meldingen van andere landen. Het CSIRT is een begrip dat door de NIS-richtlijn is gecreëerd. Het moet de erin opgelegde voorwaarden naleven. De opdrachten van het nationale CSIRT worden dus door de wet bepaald, met inbegrip van de deelname aan het CSIRT-netwerk bedoeld in artikel 12 van de NIS-richtlijn.

Bij de aanwijzing van de autoriteit die, in samenwerking met de nationale autoriteit, de identificatie van aanbieders van essentiële diensten coördineert, wordt rekening gehouden met de opdrachten toevertrouwd aan de Algemene Directie Crisiscentrum van de Federale Overheidsdienst Binnenlandse Zaken, opgericht bij het koninklijk besluit van 18 april 1988 tot oprichting van het coördinatie- en Crisiscentrum van de regering.

Tot slot bepaalt het artikel dat de Koning de bevoegde inspectiediensten aanwijst voor een bepaalde sector of, in voorkomend geval, per deelsector.

**Afdeling 2**

*Samenwerking op nationaal niveau*

Artikel 8

Dit artikel voorziet in samenwerking op nationaal niveau, waarbij de in artikel 7 van de wet bedoelde autoriteiten, de aanbieders van essentiële diensten en de digitaledienstverleners nauw samenwerken om de door deze wet opgelegde verplichtingen na te komen, zoals bepaald in de richtlijn.

Naargelang de behoeften en overeenkomstig de toepasselijke wettelijke bepalingen wordt ook samengewerkt met de andere administratieve diensten van de Staat, de andere administratieve autoriteiten, de gerechtelijke autoriteiten en de toezichthoudende autoriteiten persoonsgegevens.

l'Autorité des services et marchés financiers (FSMA), au moyen de dispositions spécifiques de la présente loi.

L'article prévoit aussi que le Roi désigne l'autorité chargée d'assurer le rôle de CSIRT national, c'est-à-dire le centre national de réponse aux incidents de sécurité informatique. Le CSIRT national est notamment chargé de recevoir les notifications d'incidents des opérateurs de services essentiels et des fournisseurs de service numérique ainsi que celles émanant d'autres États. Le CSIRT est une notion créée par la directive NIS et qui doit respecter les conditions imposées par celle-ci. Les missions du CSIRT national sont donc définies par la loi, dont la participation au réseau des CSIRT visé à l'article 12 de la directive NIS.

La désignation de l'autorité chargée, en coopération avec l'autorité nationale, de coordonner l'identification des opérateurs de services essentiels tiendra compte des missions confiées à la Direction générale Centre de Crise du Service public fédéral Intérieur, créée par l'arrêté royal du 18 avril 1988 portant création du Centre gouvernemental de Coordination et de Crise.

Enfin, l'article charge le Roi de désigner les services d'inspection compétents, pour un secteur déterminé ou, le cas échéant, par sous-secteur.

**Section 2**

*Coopération au niveau national*

Article 8

Cet article prévoit la coopération au niveau national, à savoir que les autorités visées à l'article 7 de la loi, les opérateurs de services essentiels et les fournisseurs de service numérique coopèrent étroitement aux fins du respect des obligations énoncées dans la présente loi, comme le prévoit la directive.

En fonction des besoins nécessaires à l'exécution de la loi et conformément aux dispositions légales applicables, cette coopération s'étend également aux autres services administratifs de l'État, aux autres autorités administratives, aux autorités judiciaires et aux autorités de contrôle des données à caractère personnel.

HOOFDSTUK 4

**Informatie-uitwisseling**

Artikel 9

Dit artikel bepaalt dat de informatie-uitwisseling met de autoriteiten van de Europese Unie en met buitenlandse of nationale autoriteiten noodzakelijk moet zijn voor de toepassing van de wet en in overeenstemming met de wettelijke bepalingen die de vertrouwelijkheid van de informatie m.b.t. de wezenlijke belangen van de openbare veiligheid waarborgen. Deze bepaling heeft met name tot doel om de toepassing van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, van de wet van 15 april 1994 en van de wet van 11 april 1994 betreffende de openbaarheid van bestuur te waarborgen. De autoriteiten bedoeld in artikel 7 van de wet beperken de toegang tot de in de titels 2 en 3 bedoelde informatie en tot de informatie die hen wordt toevertrouwd door aanbieders van essentiële diensten of digitaledienstverleners, 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. De personeelsleden van de aanbieders van essentiële diensten, de digitaledienstverleners en hun onderaannemers zijn onderworpen aan het beroepsgeheim.

Om deze informatie-uitwisseling mogelijk te maken, blijkt het evenwel noodzakelijk om, in sommige gevallen en behoudens de informatie m.b.t. de wezenlijke belangen van de openbare veiligheid, af te wijken van de verplichtingen inzake beroepsgeheim bedoeld in deze wet of in andere specifieke wetgeving.

Dit artikel voorziet bijgevolg in een beperking van de toegang tot de door de aanbieder van essentiële diensten en digitaledienstverlener toevertrouwde informatie en in een beperking van de inhoud van de uitgewisselde informatie. Het idee is dat de informatie moet kunnen worden uitgewisseld met inachtneming van de andere wettelijke bepalingen met name inzake de classificatie van informatie (wet van 11 december 1998) of de bescherming van persoonsgegevens (AVG of nationale wetten ter zake).

CHAPITRE 4

**Echanges d'information**

Article 9

L'article prévoit que l'échange d'information avec des autorités de l'Union européenne, avec des autorités étrangères ou nationales, doit être nécessaire à l'application de la loi et respecter les dispositions légales garantissant la confidentialité des informations liées aux intérêts essentiels de la sécurité publique. Cette disposition vise à garantir notamment l'application de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, de la loi du 15 avril 1994 et de la loi du 11 avril 1994 relative à la publicité de l'administration. Les autorités visées à l'article 7 de la loi limitent l'accès aux informations visées aux titres 2 et 3 et aux informations qui leur sont confiées par l'opérateur de services essentiels ou le fournisseur de service numérique, 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. Les membres du personnel des opérateurs de services essentiels, fournisseurs de service numérique et de leurs sous-traitants, sont soumis au secret professionnel.

Pour permettre cet échange d'informations, il s'avère toutefois nécessaire de déroger, dans certains cas et en dehors des informations liées aux intérêts essentiels de la sécurité publique, aux obligations de secret professionnel visées par la présente loi ou d'autres législations spécifiques.

L'article prévoit, par voie de conséquence, une limitation de l'accès aux informations confiées par l'opérateur de services essentiels ou le fournisseur de service numérique et une limitation du contenu des informations échangées. L'idée est que les informations doivent pouvoir être échangées tout en respectant les autres dispositions légales en matière notamment de classification des informations (loi du 11 décembre 1998) ou de protection des données à caractère personnel (RGPD ou lois nationales en la matière).

HOOFDSTUK 5

**Nationale strategie voor de beveiliging van netwerk- en informatiesystemen**

Artikel 10

Dit artikel bepaalt dat de Koning, bij in Ministerraad overlegd besluit, de autoriteit aanwijst die belast is met de actualisering van de nationale strategie voor de beveiliging van netwerk- en informatiesystemen, die in 2012 door de regering is goedgekeurd.

Na advies van de in artikel 7 van de wet bedoelde autoriteiten en, in voorkomend geval, van de toezichthoudende autoriteiten persoonsgegevens wordt deze strategie geactualiseerd. Ze moet minstens betrekking hebben op de sectoren bedoeld in bijlage I en op de diensten bedoeld in bijlage II van deze wet.

De nationale strategie bepaalt de strategische doelstellingen en passende beleids- en regelgevingsmaatregelen om een hoog beveiligingsniveau van de netwerk- en informatiesystemen te bereiken en te handhaven, en behelst minstens de in bijlage III van de wet bedoelde sectoren.

Het artikel somt ook de punten op waarop de nationale strategie betrekking heeft.

Die punten omvatten een risicobeoordelingsplan om risico's te identificeren. Dat plan zal worden gecoördineerd in nauwe samenwerking met het Crisiscentrum, rekening houdend met de opdrachten van dit centrum wat de analyse van de nationale risico's betreft.

TITEL 2

*Netwerk- en informatiesystemen van de aanbieders van essentiële diensten*

HOOFDSTUK 1

**Identificatie van de aanbieders van essentiële diensten**

Artikel 11

Het identificatieproces van de aanbieders van essentiële diensten en van de door hen verleende essentiële diensten is beschreven in de artikelen 11 tot en met 16.

Volgens dit artikel identificeert de sectorale overheid de aanbieders van essentiële diensten in overleg met de autoriteiten bedoeld in artikel 7, §§ 1 en 4, van de wet

CHAPITRE 5

**Stratégie nationale en matière de sécurité des réseaux et des systèmes d'information**

Article 10

Cet article prévoit que le Roi désigne, par arrêté délibéré en Conseil des ministres, l'autorité chargée de maintenir à jour la stratégie nationale, adoptée par le gouvernement en 2012, en matière de sécurité des réseaux et des systèmes d'information.

Après avis des autorités visées à l'article 7 de la loi et, le cas échéant, des autorités de contrôle des données à caractère personnel, la dite stratégie est mise à jour et elle couvre au moins les secteurs visés à l'annexe I[er] et les services visés à l'annexe II de la loi.

La stratégie nationale définit les objectifs stratégiques et les mesures politiques et réglementaires appropriées permettant d'atteindre un niveau élevé de sécurité des réseaux et des systèmes d'information et de le maintenir, et de couvrir au moins les secteurs visés à l'annexe III de la loi.

L'article énumère également les points sur lesquels porte la stratégie nationale.

Parmi ces points, figure un plan d'évaluation des risques permettant d'identifier les risques. La coordination de ce plan se fera en collaboration étroite avec le Centre de crise, compte tenu de ses missions en matière d'analyse des risques nationaux.

TITRE 2

*Réseaux et systèmes d'information des opérateurs de services essentiels*

CHAPITRE 1ER

**Identification des opérateurs de services essentiels**

Article 11

Le processus d'identification des opérateurs de services essentiels et des services essentiels qu'ils fournissent est décrit aux articles 11 à 16.

L'article prévoit que l'autorité sectorielle identifie les opérateurs de services essentiels, en concertation avec les autorités visées à l'article 7, §§ 1[er] et 4 de la loi,

binnen de grenzen van hun respectievelijke bevoegdheden. De sectorale overheid houdt minstens rekening met de in bijlage I van de wet bedoelde soorten aanbieders.

De sectorale overheid raadpleegt ook de gewesten en gemeenschappen en, indien ze dit nuttig acht, de vertegenwoordigers van de sector en van de potentiële aanbieders van essentiële diensten.

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

Het in dit artikel bedoelde begrip "essentiële dienst" moet worden opgevat als een activiteit die van essentieel belang is voor de instandhouding van kritieke maatschappelijke en/of economische activiteiten en niet als een afzonderlijk afgebakend organisatorisch of juridisch deel van de aanbieder.

Ze zorgt ook voor de opvolging en actualisering van het identificatie- en aanwijzingsproces van de aanbieders van essentiële diensten. Dit proces vindt voor het eerst plaats uiterlijk binnen zes maanden na de inwerkingtreding van deze wet.

Artikel 12

Artikel 12 bepaalt dat de sectorale overheid de criteria toepast die voortvloeien uit artikel 5, 2 van de NIS-richtlijn, rekening houdend met de criteria, weerslagniveaus of drempelwaarden bedoeld in artikel 13 van de wet.

Rekening houdend met het feit dat de informatie- en communicatietechnologie voortaan aan de basis ligt van bijna alle economische systemen en van de moderne samenleving, werd beslist ervan uit te gaan dat de verlening van de geïdentificeerde essentiële diensten afhankelijk is van deze systemen.

Aangezien dit vermoeden weerlegbaar is, blijft het steeds mogelijk om het te weerleggen door het bewijs van het tegendeel te leveren.

Zo zal een potentiële aanbieder van essentiële diensten die dit vermoeden wenst te weerleggen, de objectieve redenen hiervoor moeten toelichten aan de sectorale overheid. Deze zal, in samenwerking met de andere in artikel 7, §§ 1 en 4, van de wet bedoelde autoriteiten, de ingeroepen argumenten onderzoeken en beslissen over dit verzoek, aangezien zij, krachtens artikel 11, § 1, de aanbieders van essentiële diensten die tot haar sector behoren dient te identificeren.

chacun dans les limites de leurs compétences respectives. L'autorité sectorielle doit prendre en compte au moins les types d'opérateurs visés à l'annexe I de la loi.

L'autorité sectorielle consultera aussi les régions et communautés, et si elle l'estime utile, les représentants du secteur et des opérateurs de services essentiels potentiels.

Après consultation de l'opérateur de services essentiels potentiel, l'autorité sectorielle lui fait connaître les services considérés comme essentiels parmi les différents services qu'il fournit.

La notion de service essentiel visée à cet article doit être comprise comme un activité qui est essentielle au maintien d'activités sociétales et/ou économiques critiques et non comme une partie organisationnelle ou juridique délimitée distincte de l'opérateur.

Elle assure aussi le suivi et l'actualisation du processus d'identification et de désignation des opérateurs de services essentiels. Ce processus est effectué pour la première fois, au plus tard dans les six mois de l'entrée en vigueur de la présente loi.

Article 12

L'article 12 dispose que l'autorité sectorielle applique les critères qui résultent de l'article 5, 2 de la directive NIS, en tenant compte des critères, niveaux d'incidence ou seuils visés à l'article 13 de la loi.

Compte tenu du fait que les technologies de l'information et des communications se trouvent désormais à la base de pratiquement tous les systèmes économiques et sociétés modernes, il a été décidé de présumer que la fourniture des services essentiels identifiés est dépendante de ces systèmes.

Cette présomption étant réfutable, il demeure toujours possible de la renverser en apportant la preuve du contraire.

Ainsi, dans le cas où un opérateur de service essentiel potentiel souhaite renverser cette présomption, il lui appartiendra d'en expliquer les raisons objectives à l'autorité sectorielle. Celle-ci, en collaboration avec les autres autorités visées à l'article 7, §§ 1er et 4 de la loi, examinera les arguments invoqués et statuera sur cette demande, puisque c'est à elle qu'il revient, en vertu de l'article 11, § 1er d'identifier les opérateurs de services essentiels relevant de son secteur.

Artikel 13

Artikel 13 handelt over de derde voorwaarde van artikel 5, 2 van de NIS-richtlijn, waarbij de entiteiten worden bepaald voor wie een incident betreffende de beveiliging van netwerk- en informatiesystemen aanzienlijke verstorende effecten kan hebben voor de verlening van hun essentiële dienst.

Om het belang van een in het vorige lid bedoeld verstorend effect te bepalen, stelt de sectorale overheid (sectorale en/of intersectorale) criteria, weerslagniveaus en drempelwaarden vast. Dit gebeurt in samenwerking met de in artikel 7, §§ 1 en 4, van de wet bedoelde autoriteiten, en desgevallend met de betrokken gewesten en gemeenschappen.

Deze fase gebeurt in overleg met de in artikel 7, §§ 1 en 4, van de wet bedoelde autoriteiten om voor de nodige coherentie te zorgen tussen de verschillende sectoren en de andere lidstaten van de Europese Unie.

De sectorale overheid raadpleegt ook de gewesten of gemeenschappen wanneer potentiële aanbieders van essentiële diensten onder hun bevoegdheden vallen voor andere aspecten dan de openbare veiligheid van informatiesystemen.

Het artikel bevat ook een niet-limitatieve opsomming van een aantal intersectorale criteria bedoeld in artikel 6, 1 van de richtlijn.

Verduidelijkt wordt dat de richtlijn de term “sectoroverschrijdende factoren” gebruikt, terwijl deze wet naar de term “intersectorale criteria” verwijst die gebruikt wordt in de wet op de kritieke infrastructuren aangezien beide termen hetzelfde doel nastreven, en om in dit verband te zorgen voor de nodige samenhang in de nationale wetgeving. De wet machtigt de Koning om de lijst van deze intersectorale criteria aan te vullen.

Artikel 14

Krachtens artikel 14 moet de potentiële aanbieder van essentiële diensten alle nuttige informatie bezorgen over zijn eventuele identificatie als aanbieder van essentiële diensten.

Op basis van deze informatie moeten de andere autoriteiten bedoeld in artikel 7 van de wet kunnen nagaan of de voorwaarden voor de identificatie van de aanbieder al dan niet vervuld zijn.

Article 13

L’article 13 concerne la troisième condition de l’article 5, 2 de la directive NIS qui consiste à déterminer les entités pour lesquelles un incident relatif à la sécurité des réseaux et des systèmes d’information pourrait avoir un effet perturbateur important sur la fourniture de leur service essentiel.

Afin de déterminer l’importance de l’effet perturbateur visé à l’alinéa précédent, l’autorité sectorielle établira des critères (sectoriels et/ou intersectoriels), des niveaux d’incidence et des seuils. Ceux-ci seront fixés, en collaboration avec les autorités visées à l’article 7, §§ 1er et 4, de la loi, et si nécessaire, les régions et les communautés concernées.

Cette étape se fera en concertation, avec les autorités visées à l’article 7, §§ 1er et 4, de la loi, afin d’assurer une cohérence entre les différents secteurs et les autres États membres de l’Union européenne.

L’autorité sectorielle consultera également les régions ou communautés lorsque des opérateurs de services essentiels potentiels relèveront de leurs compétences pour d’autres éléments que la sécurité publique des systèmes d’informations.

L’article énumère aussi de manière non exhaustive une série de critères intersectoriels, visés à l’article 6, 1. de la Directive.

Il convient de préciser que la Directive utilise les termes de “facteurs transsectoriels” alors que la présente loi se réfère à la terminologie de “critères intersectoriels” utilisée dans la loi sur les infrastructures critiques dès lors que la finalité de ces deux terminologies est identique, et pour s’assurer d’une cohérence à cet égard en droit interne. La loi habilite le Roi à compléter la liste desdits facteurs intersectoriels.

Article 14

En vertu de l’article 14, l’opérateur de services essentiels potentiel est tenu de transmettre toutes les informations utiles quant à son éventuelle identification en tant qu’opérateur de services essentiels.

Ces informations doivent permettre aux autres autorités visées à l’article 7 de la loi, de vérifier la réunion des conditions d’identification ou non de l’opérateur.

De door de potentiële aanbieder meegedeelde relevante informatie wordt overgemaakt aan de autoriteiten bedoeld in artikel 7.

Artikel 15

Artikel 15 verduidelijkt dat de sectorale overheid een voorstel van lijst van potentiële aanbieders van essentiële diensten, samen met haar motivering, aan de autoriteiten bedoeld in artikel 7, §§ 1 en 4, van de wet moet bezorgen.

Vervolgens brengen de autoriteiten bedoeld in artikel 7, §§ 1 en 4, van de wet, binnen de grenzen van hun respectievelijke bevoegdheden, samen advies uit over het gemotiveerde voorstel van lijst, desgevallend na raadpleging van de gewesten en gemeenschappen.

Wanneer de sectorale overheid vaststelt dat de entiteit die ze 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 andere autoriteiten bedoeld in artikel 7, §§ 1 en 4, van de wet daarvan op de hoogte. Volgens de op Europees niveau bepaalde procedures voeren deze laatsten en de betrokken sectorale overheden, desgevallend in samenwerking met de betrokken gewesten of gemeenschappen, besprekingen met de bevoegde buitenlandse nationale autoriteit of autoriteiten.

Vervolgens moet de sectorale overheid, op beveiligde wijze, de administratieve beslissingen betreffende de aanwijzing van de aanbieders van essentiële diensten, samen met de motivering ervan, aan de betrokken aanbieder alsook aan de autoriteiten bedoeld in artikel 7, §§ 1 en 4, van de wet en desgevallend aan de gewesten en gemeenschappen bezorgen.

Artikel 16

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

De sectorale overheid heeft dit soort informatie immers nodig om de mogelijke risico's en de noodzakelijke beveiligingsmaatregelen te bepalen.

Voor het overige kan deze informatie, in voorkomend geval, het identificatieproces een zekere coherentie en objectiviteit verlenen en de evaluatie van de opgestelde

Les informations pertinentes transmises par l'opérateur potentiel sont portées à la connaissance des autorités visées à l'article 7.

Article 15

L'article 15 précise qu'il appartient ensuite à l'autorité sectorielle de communiquer une proposition de liste des opérateurs de services essentiels potentiels, accompagnée de sa motivation, aux autorités visées à l'article 7, §§ 1er et 4, de la loi.

Ensuite, les autorités visées à l'article 7, §§ 1er et 4, de la loi, dans les limites de leurs compétences respectives, rendent ensemble un avis sur la proposition motivée de liste, le cas échéant après consultation des régions et des communautés.

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 autres autorités visées à l'article 7, §§ 1er et 4, de la loi. Selon les procédures définies au niveau européen, ces dernières sont chargées avec les autorités sectorielles concernées et le cas échéant, en collaboration avec les régions ou communautés concernées, de mener des discussions avec la ou les autorités nationales étrangères compétentes.

Il appartient ensuite à l'autorité sectorielle de communiquer, de manière sécurisée, les décisions administratives de désignation des opérateurs de services essentiels, accompagnées de leur motivation, à l'opérateur concerné ainsi qu'aux autorités visées à l'article 7, §§ 1er et 4, de la loi, et le cas échéant, aux régions et communautés.

Article 16

L'article 16 précise que dans les trois mois de sa désignation, l'opérateur de services essentiels transmet à l'autorité sectorielle un descriptif des réseaux et systèmes d'information dont la fourniture du ou des services essentiels concernés est tributaire.

Ce type d'informations est en effet nécessaire pour permettre à l'autorité sectorielle de déterminer les risques encourus et les mesures de sécurité nécessaires.

Cela permet, pour le surplus, d'apporter le cas échéant, une certaine cohérence et objectivité au processus d'identification et de faciliter le travail de

lijst vergemakkelijken die moet plaatsvinden overeenkomstig de vorige artikelen.

Artikel 17

Dit artikel bepaalt in welke mate de bestuursdocumenten betreffende de toepassing van hoofdstuk 1 van Titel 2 ontsnappen aan de regels inzake openbaarheid van bestuur.

Artikel 18

In afwijking van de artikelen 11 tot 16 is voorzien in een vereenvoudigd systeem voor de aanwijzing van exploitanten van kritieke infrastructuren. Zij worden als dusdanig aangewezen overeenkomstig de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren.

Zij worden door de sectorale overheid aangewezen als aanbieders van essentiële diensten, in overleg met de autoriteiten bedoeld in artikel 7, §§ 1 en 4, van de wet, binnen de grenzen van hun respectievelijke bevoegdheden, wanneer de verlening van hun kritieke diensten afhankelijk is van netwerk- en informatiesystemen. Deze afhankelijkheid wordt vermoed naar het voorbeeld van wat bepaald is voor de aanbieders van essentiële diensten die geen exploitanten van kritieke infrastructuren zijn.

Artikel 19

Dit artikel machtigt de Koning om de verplichte identificatie van aanbieders van essentiële diensten eventueel uit te breiden tot andere soorten aanbieders of andere sectoren.

HOOFDSTUK 2

**Beveiligingsmaatregelen**

Artikel 20

Paragraaf 1 van deze bepaling voorziet in een algemene verplichting voor de aanbieder van essentiële diensten om passende en evenredige technische en organisatorische maatregelen te nemen voor de beveiliging van de netwerk- en informatiesystemen waarvan de door hem verleende essentiële diensten afhankelijk zijn. Deze maatregelen zorgen voor een beveiligingsniveau

réexamen de la liste établie, qui doit intervenir, conformément aux articles précédents.

Article 17

Cet article précise dans quelle mesure les documents administratifs liés à l'application du chapitre 1er du Titre 2 échappent aux règles de la publicité de l'administration.

Article 18

Par dérogation aux articles 11 à 16, il est prévu un système de désignation simplifié pour les exploitants d'infrastructures critiques désignées comme telles en application de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.

Ceux-ci sont désignés par l'autorité sectorielle comme opérateurs de services essentiels, en concertation avec les autorités visées à l'article 7, §§ 1er et 4, de la loi dans les limites de leurs compétences respectives, lorsque la fourniture des services critiques qu'ils délivrent est tributaire de réseaux et des systèmes d'information. Il est entendu que cette dépendance est présumée, à l'instar de ce qui est prévu pour les opérateurs de services essentiels qui ne sont pas des exploitants d'infrastructures critiques.

Article 19

Cet article permet au Roi d'étendre éventuellement l'identification obligatoire d'opérateurs de services essentiels à d'autres types d'opérateurs ou à d'autres secteurs.

CHAPITRE 2

**Mesures de sécurité**

Article 20

Cette disposition prévoit, dans son paragraphe 1er, l'obligation générale pour l'opérateur de services essentiels de prendre les mesures techniques et organisationnelles nécessaires et proportionnées de sécurité des réseaux et des systèmes d'information dont sont tributaires les services essentiels qu'il fournit. Ces mesures doivent garantir un niveau de sécurité adapté aux

dat is afgestemd op de risico's en de stand van de kennis ter zake, teneinde de continuïteit van de diensten te waarborgen.

Artikel 21

De doelstellingen en maatregelen zijn opgenomen in een document genaamd "beveiligingsbeleid voor de netwerk- en informatiesystemen" (I.B.B.).

Naast de algemene beveiligingsverplichting is bepaald dat de Koning bepaalde beveiligingsmaatregelen kan opleggen aan de aanbieders van essentiële diensten van verschillende sectoren. Doel is, in voorkomend geval, bepaalde minimale en specifieke beveiligingsmaatregelen verplicht te maken voor de aanbieders van essentiële diensten van verschillende sectoren.

Na overleg met de autoriteiten bedoeld in artikel 7 van de wet kan de Koning, desgevallend na raadpleging van de betrokken gewesten of gemeenschappen, bepaalde beveiligingsmaatregelen opleggen aan de aanbieders van essentiële diensten van een of meer sectoren.

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

Wanneer de aanbieder van essentiële diensten een beroep doet op een onderaannemer, moet hij zich ervan vergewissen dat deze de beveiligingsmaatregelen waartoe hij krachtens deze wet gehouden is werkelijk toepast.

Om de uitwerking van het I.B.B. voor de exploitanten van kritieke infrastructuren te vergemakkelijken, worden de maatregelen voor de fysieke en logische beveiliging van netwerk- en informatiesystemen die reeds vervat zijn in hun beveiligingsplan van de exploitant gelijkgesteld met het I.B.B. wanneer deze maatregelen aan de verplichte inhoud van het I.B.B. voldoen.

Artikel 22

Om de uitvoering van de algemene beveiligingsverplichting te vergemakkelijken, bepaalt dit artikel dat aanbieders die erkende technische normen hanteren, zoals de norm ISO/IEC 27001, het vermoeden genieten dat de inhoud van hun I.B.B. conform is, wanneer voldaan is aan de eisen van deze norm of aan een nationale, buitenlandse of internationale norm die door de Koning als gelijkwaardig wordt erkend.

risques, compte tenu des connaissances en la matière, dans une perspective de continuité des services.

Article 21

Les objectifs et les mesures sont reprises dans un document dénommé politique de sécurité des systèmes et réseaux d'information (P.S.I.).

Outre l'obligation générale de sécurité, il est précisé que le Roi peut imposer certaines mesures de sécurité applicables aux opérateurs de services essentiels de plusieurs secteurs. L'objectif est de rendre obligatoire, le cas échéant, certaines mesures minimales et précises de sécurité pour les opérateurs de services essentiels de plusieurs secteurs.

Après concertation avec les autorités visées à l'article 7 de la loi, le Roi, au besoin après consultation des régions ou communautés concernées, peut imposer certaines mesures de sécurité applicables aux opérateurs de services essentiels d'un ou plusieurs secteurs.

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, également par décision administrative individuelle, imposer des mesures complémentaires de sécurité.

Lorsqu'il fait appel à un sous-traitant, l'opérateur de services essentiels doit s'assurer que son sous-traitant applique effectivement les mesures de sécurité imposées en vertu de la présente loi.

Afin de faciliter l'élaboration de la P.S.I. pour les exploitants d'infrastructures critiques, les mesures de sécurité physique et logique des réseaux et systèmes d'information déjà contenues dans leur plan de sécurité de l'exploitant sont assimilées à la P.S.I. lorsque celles-ci répondent au contenu exigé pour celle-ci.

Article 22

Afin de faciliter la mise en œuvre de l'obligation générale de sécurité, cet article énonce que les opérateurs utilisant des standards techniques reconnus, comme la norme ISO/IEC 27001, pourront bénéficier d'une présomption de conformité du contenu de leur P.S.I. lorsque celle-ci répond aux exigences de cette norme – ou à une norme nationale, étrangère ou internationale reconnue équivalente par le Roi.

Het vermoeden van conformiteit heeft enkel betrekking op de inhoud van het I.B.B., d.w.z. op de doelstellingen inzake beveiligingsbeheer die in dat document moeten staan, en niet op het afdoende karakter van de toegepaste beveiligingsmaatregelen. De beveiligingsmaatregelen kunnen immers door de Koning of de sectorale overheid worden aangevuld en moeten het voorwerp uitmaken van een controle door een externe auditeur of de inspectiedienst van de sectorale overheid.

In de wet wordt rechtstreeks verwezen naar de norm ISO/IEC 27001 om voor alle aanbieders een duidelijke en concrete richting aan te geven, wat de minimale maatregelen voor het beveiligingsbeheer van hun systemen betreft, zodat zij kunnen voldoen aan de eisen van artikel 20, zonder een latere tussenkomst van de Koning of van de sectorale overheden af te wachten.

De norm ISO/IEC 27001 is immers de internationaal erkende technische norm die de algemene en gestructureerde aanpak bepaalt voor het beveiligingsbeheer van eender welk informatiesysteem. Het betreft dus een basisnorm die de algemene beginselen bepaalt voor de uitvoering van elke beveiligingsmaatregel voor informatiesystemen en die van toepassing is in alle sectoren. Bij deze norm wordt geen datum vermeld zodat steeds de meest recente versie ervan kan worden toegepast.

Tegelijk krijgen de sectorale overheden de mogelijkheid om hun in de wet bepaalde opdrachten zowel op een effectieve als een doeltreffende manier uit te voeren, doordat ze over een duidelijk referentiekader inzake minimale beveiligingsmaatregelen beschikken. Dit kader is evenwel niet verplicht omdat ook rekening moet worden gehouden met de specifieke kenmerken van elke sector of betrokken aanbieder.

Niettemin kan de Koning de gelijkwaardigheid van andere technische normen erkennen om de houders van een certificaat op basis van vergelijkbare of eventueel verdergaande technische beveiligingsnormen niet te benadelen. In hun advies aan de Koning zullen de sectorale overheid en de autoriteit bedoeld in artikel 7, § 1, van de wet hun analyse van de eventuele gelijkwaardigheid tussen beide technische normen uiteenzetten. BELAC, de accreditatie-instelling aangewezen door de Koning om in België de instellingen voor de conformiteitsbeoordeling te accrediteren, zal advies uitbrengen over de accrediteerbaarheid van de als gelijkwaardig voorgestelde norm, met inbegrip van het bestaan van een technisch schema dat een accreditatie mogelijk maakt.

Aanbieders die wensen dat dit vermoeden van conformiteit voor hen zou gelden, moeten een certificaat

La présomption porte uniquement sur le contenu de la P.S.I., c'est-à-dire sur les objectifs de gestion de la sécurité qui doivent figurer dans ce document, et non sur le caractère suffisant des mesures de sécurité appliquées. En effet, les mesures de sécurité peuvent être complétées par le Roi ou l'autorité sectorielle et elles doivent faire l'objet d'un contrôle par un auditeur externe ou le service d'inspection de l'autorité sectorielle.

Le choix de la référence directe dans la loi à la norme ISO/IEC 27001 vise à donner une direction claire et prévisible à l'ensemble des opérateurs, en ce qui concerne les mesures minimales de gestion de la sécurité de leurs systèmes, afin de se conformer aux exigences de l'article 20, sans attendre une intervention ultérieure du Roi ou des autorités sectorielles.

La norme ISO/IEC 27001 est, en effet, la norme technique internationalement reconnue qui fixe l'approche générale et structurée à adopter pour disposer d'une gestion de la sécurité de n'importe quel système d'informations. Il s'agit donc d'une norme de base fixant les principes généraux pour la mise en œuvre de toute mesure de sécurité d'un système d'information et est applicable dans tous les secteurs. Celle-ci est reprise sans indication de date afin de permettre d'appliquer toujours sa version la plus récente.

En même temps, il s'agit de permettre aux autorités sectorielles d'exercer leur missions prévues par la loi de façon effective tout autant qu'efficace, en disposant d'un cadre de référence clair en matière de mesures minimales de sécurité, sans que ce cadre possède un caractère obligatoire pour autant car il convient aussi de tenir compte des particularités propres à chaque secteur ou opérateur concerné.

La reconnaissance de l'équivalence d'autres normes techniques par le Roi est néanmoins prévue pour ne pas pénaliser les détenteurs d'un certificat obtenu selon des normes techniques de sécurité comparables ou éventuellement plus poussées. Dans leur avis au Roi, l'autorité sectorielle et l'autorité visée à l'article 7, § 1er, de la loi exposeront leur analyse de l'équivalence éventuelle entre les deux normes techniques. De son côté, BELAC, qui est l'organisme d'accréditation désigné par le Roi pour accréditer en Belgique des organismes d'évaluation de la conformité, donnera un avis sur l'accréditabilité de la norme proposée à l'équivalence, en ce compris l'existence d'un schéma technique permettant d'effectuer une accréditation.

Les opérateurs qui souhaitent bénéficier de cette présomption de conformité devront obtenir un certificat

verkrijgen van een instelling voor de conformiteitsbeoordeling die op basis van de norm ISO/IEC 17021 (certificatie van managementsysteem) of ISO/IEC 17065 (certificatie van producten) geaccrediteerd is. De normen ISO/IEC 17021 en ISO/IEC 17065 zijn technische basisnormen die het technische schema bepalen dat moet worden gebruikt om certificaten te kunnen uitreiken voor alle soorten specifieke technische normen, waaronder, maar niet uitsluitend, de norm ISO/IEC 27001.

Dit certificaat moet uiteraard tot het certificeringsdomein behoren waarvoor de instelling geaccrediteerd is. Zo moet de instelling voor de conformiteitsbeoordeling die certificaten uitreikt aan een aanbieder van essentiële diensten geaccrediteerd zijn door BELAC of een andere erkende instelling die de erkenningsakkoorden van de "*European Cooperation for Accreditation*" dus medeondertekend heeft.

De accreditatie door BELAC volgens de norm ISO/IEC 17021 of ISO/IEC 17065 laat toe na te gaan of de instellingen voor de conformiteitsbeoordeling bij de uitreiking van een certificaat algemene regels inzake onafhankelijkheid, onpartijdigheid, vertrouwelijkheid en constante kwaliteit hebben nageleefd.

Artikel 23

De aanwijzing van een contactpunt voor de beveiliging van netwerk- en informatiesystemen laat de bevoegde sectorale overheid en de autoriteiten bedoeld in artikel 7, §§ 1 en 4, toe om gemakkelijk met de geïdentificeerde aanbieders te communiceren in geval van incidenten of deze te informeren over eventuele dreigingen.

HOOFDSTUK 3

**Melding van incidenten**

Artikel 24

Paragraaf 1 is gewijd aan de verplichting om incidenten die aanzienlijke gevolgen hebben aan de bevoegde autoriteiten te melden, namelijk de in artikel 25 van de wet bedoelde autoriteiten. Overeenkomstig de regels inzake arbeidsrecht mogen de personeelsleden van de aanbieder van essentiële diensten of van een digitaledienstverlener geen nadelige gevolgen ondervinden vanwege hun werkgever, wanneer deze voortvloeien uit de naleving, te goeder trouw, van de door deze wet opgelegde verplichtingen, met name inzake het melden van incidenten.

délivré par un organisme d'évaluation de la conformité accrédité sur base de la norme ISO/IEC 17021 (certification système de gestion) ou ISO/IEC 17065 (certification produits). Les normes ISO/IEC 17021 et ISO/IEC 17065 sont des normes techniques de base qui déterminent le schéma technique à utiliser pour pouvoir délivrer des certificats pour tous types de normes techniques spécifiques, dont entre autres la norme ISO/IEC 27001 mais pas seulement.

Ce certificat devra bien entendu faire partie du domaine de certification pour lequel l'organisme est accrédité. L'organisme d'évaluation de la conformité délivrant les certificats à un opérateur de services essentiels devra ainsi disposer d'une accréditation par BELAC ou par une autre institution reconnue et donc cosignataire des accords de reconnaissance du "*European Cooperation for Accreditation*".

L'accréditation par BELAC selon la norme ISO/IEC 17021 ou ISO/IEC 17065 permet de s'assurer du respect par les organismes d'évaluation de la conformité, lors de la délivrance d'un certificat, de règles générales d'indépendance, d'impartialité, de confidentialité et de qualité continue.

Article 23

La désignation d'un point de contact pour la sécurité des systèmes et réseaux d'information permettra à l'autorité sectorielle compétente, et aux autorités visées à l'article 7, §§ 1er et 4 de communiquer facilement avec les opérateurs identifiés en cas d'incidents ou de les informer de menaces éventuelles.

CHAPITRE 3

**Notification d'incidents**

Article 24

Le paragraphe 1er consacre l'obligation de notifier les incidents ayant un impact significatif aux autorités compétentes, à savoir les autorités précisées à l'article 25 de la loi. Conformément aux règles en matière de droit du travail, les membres du personnel de l'opérateur de services essentiels ou d'un fournisseur de service numérique ne pourront subir de conséquences négatives de la part de leur employeur, lorsque celles-ci découlent du respect, de bonne foi, des obligations imposées par la présente loi, notamment en matière de notification d'incidents.

De vraag of een incident aanzienlijke gevolgen heeft, moet worden beoordeeld rekening houdend met de gevolgen ervan voor de beschikbaarheid, vertrouwelijkheid, integriteit of authenticiteit van de informatiesystemen waarvan de door de aanbieder verleende essentiële diensten afhankelijk zijn.

Voor de meldingsplicht moet rekening worden gehouden met de impact van een incident op alle elementen vervat in de definitie van de beveiliging van netwerk- en informatiesystemen, vermeld in de richtlijn, zonder zich te beperken tot de impact op de continuïteit van de verleende essentiële diensten. Een incident dat een impact heeft op de beschikbaarheid, vertrouwelijkheid, integriteit of authenticiteit van informatiesystemen voor het verlenen van een essentiële dienst vormt immers een gebeurtenis die aan de bevoegde autoriteiten moet worden meegedeeld en een belangrijk risico kan vormen voor de beveiliging van de aanbieder van essentiële diensten. De continuïteit van een verleende essentiële dienst is slechts één aspect van de beveiliging van informatiesystemen waarvan een aanbieder van essentiële diensten afhankelijk kan zijn. Een cyberaanval verloopt evenwel vaak in verschillende fasen met diverse verstorende effecten en veroorzaakt pas op het einde problemen voor de continuïteit van de diensten.

Paragraaf 2 machtigt de Koning om, per sector of deelsector, de weerslagniveaus en/of de drempelwaarden te bepalen die minstens aanzienlijke gevolgen hebben in de zin van paragraaf 1.

Deze mogelijkheid waarover de Koning beschikt heeft tot doel om de aanbieders van essentiële diensten te verduidelijken in welke gevallen wordt aangenomen dat een incident noodzakelijkerwijs aanzienlijke gevolgen heeft.

Indien geen weerslagniveaus of drempelwaarden zijn bepaald, worden de aanbieders verzocht alle gebeurtenissen te melden die een impact hebben op de beschikbaarheid, vertrouwelijkheid, integriteit of authenticiteit van informatiesystemen voor het verlenen van een essentiële dienst. Dit wordt uitdrukkelijk bevestigd in paragraaf 3.

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

Artikel 25

In principe moet deze melding tegelijk gebeuren bij drie afzonderlijke autoriteiten, namelijk het nationale

Le caractère significatif de l'impact d'un incident doit être évalué au regard de son effet sur la disponibilité, la confidentialité, l'intégrité ou l'authenticité des systèmes d'information dont sont tributaires les services essentiels fournis par l'opérateur.

Il s'agit de prendre en compte, pour l'obligation de notification, de l'impact d'un incident sur l'ensemble des éléments inclus dans la définition donnée par la directive de la sécurité des réseaux et systèmes d'information, sans se limiter au seul impact sur la continuité des services essentiels fournis. En effet, un incident ayant un impact sur la disponibilité, la confidentialité, l'intégrité ou l'authenticité de systèmes d'information liés à la fourniture d'un service essentiel constitue un événement qui mérite d'être communiqué aux autorités compétentes et qui peut constituer potentiellement un risque important pour la sécurité de l'opérateur de services essentiels. La continuité de la fourniture d'un service essentiel n'est qu'un élément de la sécurité des systèmes d'information dont peut être tributaire un opérateur de services essentiels. Cependant, une attaque cyber est souvent menée en plusieurs phases avec des effets perturbateurs divers et ne se manifeste par un problème de continuité des services qu'en bout de course.

Le paragraphe 2 permet au Roi d'établir des niveaux d'incidence et/ou des seuils, par secteur ou sous-secteur, constituant au minimum un impact significatif au sens du § 1er.

Cette faculté laissée au Roi vise à préciser aux opérateurs de services essentiels les hypothèses dans lesquelles un incident doit nécessairement être considéré comme ayant un impact significatif.

En l'absence de tels niveaux d'incidence ou de seuils, les opérateurs seront invités à notifier tous les événements ayant un effet sur la disponibilité, la confidentialité, l'intégrité ou l'authenticité des systèmes d'information liés à la fourniture d'un service essentiel, ce que confirme explicitement le paragraphe 3.

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

Article 25

Dans son principe, cette notification doit se faire, en même temps, à trois autorités distinctes, à savoir le

CSIRT, de sectorale overheid of haar sectorale CSIRT, en de autoriteit bedoeld in artikel 7, § 4, van de wet.

De aanbieder van essentiële diensten moet niet wachten tot hij over alle relevante informatie over een incident beschikt om het te melden. Wanneer hij uit de hem ter beschikking staande informatie reeds kan afleiden dat het incident een aanzienlijke impact heeft, moet hij het melden.

Artikel 26

Zoals hierboven aangegeven is deze meldingsplicht bovendien van toepassing op de aanbieders van essentiële diensten bedoeld in de de wet van 21 november 2017 over de infrastructuren voor de markten voor financiële instrumenten.

De andere aanbieders van essentiële diensten die tot de sector financiën behoren, als bedoeld in bijlage I, moeten beveiligingsincidenten melden aan de Nationale Bank van België, die ze onverwijld aan het nationale CSIRT en de autoriteit bedoeld in artikel 7, § 4, bezorgt.

Article 27

Artikel 27 bepaalt bovendien dat een onderneming die een digitale dienst verleent aan een aanbieder van essentiële diensten, alle incidenten die aanzienlijke gevolgen hebben voor de continuïteit van de essentiële diensten van deze aanbieder, aan deze aanbieder moet melden.

Article 28

Artikel 28 wijst erop dat een aanbieder van essentiele diensten die door een incident wordt getroffen, niet alleen verplicht is om het te melden maar ook om het aan te pakken en alle nodige maatregelen te nemen om het op te lossen. Zo blijft hij verantwoordelijk voor de aanpak van het incident.

Aanbieders moeten ook incidenten of andere gebeurtenissen onderzoeken die hen door het nationale CSIRT, de sectorale overheid of de autoriteit bedoeld in artikel 7, § 4, worden gemeld.

Article 29

Volgens artikel 29 moet het nationale CSIRT incidenten melden aan de andere lidstaten van de Europese

CSIRT national, l'autorité sectorielle ou à son CSIRT sectoriel, et à l'autorité visée à l'article 7, § 4, de la loi.

L'opérateur de services essentiels ne doit pas attendre de disposer de toutes les informations pertinentes sur un incident pour procéder à la notification. Lorsque les informations à sa disposition lui permette déjà de savoir qu'il s'agit d'un incident ayant un impact significatif, il convient qu'il le notifie.

Article 26

Par ailleurs, comme indiqué ci-avant, cette obligation de notification s'applique aux opérateurs de services essentiels visés par la loi du 21 novembre 2017 relative aux infrastructures de marchés d'instruments financiers.

Quant aux autres opérateurs de services essentiels relevant du secteur des finances visés à l'annexe I, ils doivent notifier les incidents de sécurité à la Banque Nationale de Belgique, qui se charge de les transmettre sans retard, au CSIRT national et à l'autorité visée à l'article 7, § 4.

Article 27

L'article 27 impose en outre à l'entreprise qui fournit un service numérique à un opérateur de services essentiels, de notifier à ce dernier tous les incidents ayant un impact significatif sur la continuité des services essentiels de cet opérateur.

Article 28

L'article 28 dispose qu'un opérateur de services essentiels touché par un incident a l'obligation non seulement de le notifier mais également de le gérer et de prendre toutes les mesures nécessaires pour le résoudre. La gestion de l'incident demeure ainsi de sa responsabilité.

Les opérateurs doivent également examiner les incidents ou autres événements qui leur sont signalés par le CSIRT national, l'autorité sectorielle ou l'autorité visée à l'article 7, § 4.

Article 29

L'article 29 charge le CSIRT national de signaler aux autres États de l'Union européenne les incidents

Unie wanneer die aanzienlijke gevolgen hebben voor de continuïteit van essentiële diensten in die lidstaten.

Artikel 30

Het artikel verduidelijkt dat het steeds mogelijk is voor de private of publieke entiteiten die actief zijn in de sectoren opgenomen in bijlage I van de wet en die niet zijn geïdentificeerd als aanbieders van essentiële diensten, om op vrijwillige basis incidenten te melden die aanzienlijke gevolgen hebben voor de continuïteit van de door hen verleende diensten.

Artikel 31

De Koning is belast met de modaliteiten voor de melding en rapportering van incidenten, met inbegrip van de oprichting van een beveiligd meldingsplatform te bepalen.. Het is met name de bedoeling om Hem de mogelijkheid te bieden een gemeenschappelijk meldingsplatform op te richten teneinde de uitvoering en verwerking van de verplichte meldingen door aanbieders van essentiële diensten en digitaledienstverleners te vergemakkelijken, zodat in de praktijk slechts één enkele melding nodig is via dit unieke platform.

Indien de aanbieders van essentiële diensten en digitaledienstverleners dit wensen, kan dit platform ook worden gebruikt voor verplichte meldingen krachtens de AVG.

Het bestaan van dit platform wijzigt het in de AVG opgenomen “verantwoordingsbeginsel” van de verwerkingsverantwoordelijke niet. Volgens dat beginsel is het altijd aan de verwerkingsverantwoordelijke om te beslissen aan welke instantie(s) hij zijn melding al dan niet bezorgt. De oprichting van dit platform betekent dus niet dat deze verantwoordelijkheid wordt overgedragen aan een of meer instanties die via dit platform meldingen ontvangen. Bijgevolg moet de beheerder van dit platform niet zelf beslissen of een melding al dan niet voor de Gegevensbeschermingsautoriteit bestemd is, maar moet de aanbieder van essentiële diensten of digitaledienstverlener zich ervan vergewissen dat hij zijn wettelijke meldingsplicht volledig is nagekomen.

Tot slot kan het nationale CSIRT, zowel voor verplichte als voor vrijwillige meldingen, beslissen om, na raadpleging van de betrokken aanbieder en de bevoegde sectorale overheid, bepaalde geanonimiseerde algemene informatie aan het publiek mee te delen om redenen van sensibilisering en incidentpreventie of -beheer.

ayant un impact significatif sur la continuité des services essentiels dans ces États.

Article 30

L’article vise à clarifier qu’il est toujours possible pour les entités privées ou publiques, actives dans les secteurs repris à l’annexe I de la loi, qui n’ont pas été identifiées en tant qu’opérateurs de services essentiels de notifier, à titre volontaire, les incidents ayant un impact significatif sur la continuité des services qu’elles fournissent.

Article 31

Le Roi est chargé de déterminer les modalités de notification et de rapportage des incidents, en ce compris, créer une plate-forme sécurisée de notification. Il s’agit notamment de lui permettre de créer une plateforme commune de notification pour faciliter la mise en œuvre et le traitement des notifications imposées aux opérateurs de services essentiels et aux fournisseurs de service numérique de sorte que ces derniers pourront réaliser en pratique une seule démarche de notification via cette plateforme unique.

Cette plateforme pourra servir également, si les opérateurs de services essentiels et les fournisseurs de service numérique le souhaitent, pour les notifications imposées en vertu du RGPD.

L’existence de cette plateforme ne modifie pas le principe de “responsabilité” du responsable de traitement, prévu dans le RGPD. Ce principe implique que c’est toujours au responsable de traitement qu’incombe le choix de décider à quelle(s) instance(s) il adresse ou non sa notification. En d’autre termes, la réalisation de cette plateforme n’impliquera pas un report de cette responsabilité vers une ou plusieurs instances qui reçoivent des notifications via cette plateforme. Ainsi, il ne revient pas au gestionnaire de cette plateforme de décider lui-même lorsqu’une notification est destinée ou non à l’Autorité de protection des données, mais bien à l’opérateur de services essentiels ou au fournisseur de service numérique de s’assurer qu’il a pleinement exécuté toutes ses obligations légales de notification.

Enfin, tant pour les notifications obligatoires que les notifications volontaires, le CSIRT national peut décider, après consultation de l’opérateur concerné et de l’autorité sectorielle compétente, de diffuser certaines informations générales anonymisées au public à des fins de sensibilisation et de prévention ou de gestion d’incidents.

TITEL 3

*Netwerk- en informatiesystemen van digitaledienstverleners*

Artikel 32

Dit artikel vormt slechts de omzetting van de NIS-richtlijn en behoeft geen verdere commentaar.

HOOFDSTUK 1

**De beveiligingseisen**

Artikel 33

Dit artikel verplicht digitaledienstverleners om de risico's voor de beveiliging van netwerk- en informatiesystemen die gebruikt worden voor het verlenen in de Europese Unie van digitale diensten bedoeld in de NIS-richtlijn, te identificeren, alsook om passende en evenredige technische en organisatorische beveiligingsmaatregelen te nemen om deze risico's te beheersen, naar het voorbeeld van wat bepaald is voor de aanbieders van essentiële diensten. Het artikel is grotendeels een omzetting van de richtlijn.

De beveiligingsmaatregelen moeten voldoen aan de uitvoeringsverordeningen van de Europese Commissie, waaronder uitvoeringsverordening (EU) 2018/151 van 30 januari 2018 tot vaststelling van toepassingsbepalingen voor Richtlijn (EU) 2016/1148 wat betreft de nadere specificatie van de 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.

Artikel 34

Het artikel bepaalt dat de digitaledienstverleners een contactpunt moeten aanwijzen, om dezelfde redenen als de aanbieders van essentiële diensten. Zoals hierboven vermeld, mag dit contactpunt niet worden verward met het begrip "functionaris voor gegevensbescherming" krachtens de AVG.

TITRE 3

*Réseaux et systèmes d'information des fournisseurs de service numérique*

Article 32

Cet article constitue une simple transposition de la directive NIS et n'appelle pas de commentaires particuliers.

CHAPITRE 1ER

**Les exigences de sécurité**

Article 33

Cet article impose aux fournisseurs de service numérique d'identifier les risques menaçant la sécurité des réseaux et systèmes d'information utilisés pour fournir dans l'Union européenne de services numériques visés par la directive NIS, et de prendre les mesures techniques et organisationnelles de sécurité nécessaires et proportionnées pour les gérer, de façon similaire à ce qui est prévu pour les opérateurs de services essentiels. L'article constitue largement une transposition de la directive.

Les mesures de sécurité devront être conformes aux règlements d'exécution de la Commission européenne, dont celui du 30 janvier 2018 (UE) 2018/151 portant modalités d'application de la Directive (UE) 2016/1148 précisant les éléments à prendre en considération 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.

Article 34

L'article prévoit que les fournisseurs de service numérique doivent désigner un point de contact, pour les mêmes raisons que les opérateurs de services essentiels. Comme dit plus haut, ce point de contact ne peut être confondu avec la notion de "délégué à la protection des données" en vertu du RGPD.

HOOFDSTUK 2

**Melding van incidenten**

Artikel 35

Dit artikel voorziet in de verplichting om bepaalde incidenten te melden aan de bevoegde autoriteiten en regelt een aantal aspecten in verband met deze meldingen, naar het voorbeeld van wat bepaald is voor de aanbieders van essentiële diensten.

De digitaledienstverleners moeten incidenten melden die een aanzienlijke impact hebben op de verlening van de in de wet bedoelde en in de Europese Unie aangeboden dienst.

De melding gebeurt overeenkomstig de bepalingen van de uitvoeringsverordening (EU) 2018/151 van de Europese Commissie 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.

Overeenkomstig de richtlijn bevestigt de wet bovendien dat de dienstverlener een incident enkel moet melden indien hij toegang heeft tot de informatie die nodig is om de impact ervan te beoordelen.

Artikel 36

Het artikel verduidelijkt dat de melding gebeurt met inachtneming van de door de Koning bepaalde modaliteiten en via het gemeenschappelijke platform bedoeld in artikel 31.

Zoals in artikel 31 is bepaald dat dit platform kan gebruikt worden voor meldingen aan de Gegevensbeschermingsautoriteit.

Artikel 37

Het artikel bepaalt dat het nationale CSIRT de andere betrokken lidstaten van de Europese Unie moet informeren. Het beschermt daarbij de veiligheids- en commerciële belangen van de digitaledienstverlener en de vertrouwelijkheid van de informatie.

CHAPITRE 2

**Notification d'incidents**

Article 35

Cet article consacre l'obligation de notifier certains incidents aux autorités compétentes et règlemente plusieurs questions liées à ces notifications, de façon analogue à ce qui est prévu pour les opérateurs de services essentiels.

Les fournisseurs de services numériques doivent notifier les incidents ayant un impact significatif sur la fourniture du service visé par la loi et offert dans l'Union européenne.

La notification se fait conformément aux dispositions du règlement d'exécution de la Commission européenne du 30 janvier 2018 (UE) 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.

La loi confirme par ailleurs, ce qui résulte de la directive, que le fournisseur ne doit notifier un incident que s'il a accès aux informations nécessaires pour évaluer l'impact.

Article 36

L'article prévoit que la notification est réalisée en respectant les modalités prévues par le Roi et via la plateforme commune visée à l'article 31.

Comme à l'article 31, il est également prévu que ladite plateforme peut servir pour effectuer les notifications à l'Autorité de protection des données.

Article 37

L'article charge le CSIRT national d'informer les autres États de l'Union européenne concernés, tout en veillant à préserver la sécurité et les intérêts commerciaux du fournisseur de service numérique et la confidentialité des informations.

Net zoals voor de aanbieders van essentiële diensten kan het nationale CSIRT, na raadpleging van de digitaledienstverlener, de sectorale overheid en desgevallend de autoriteiten van de andere betrokken lidstaten, algemene informatie meedelen aan het publiek om redenen van incidentpreventie of -beheer of in het algemeen belang.

TITEL 4

*Toezicht en sancties*

HOOFDSTUK 1

**Toezicht op de aanbieders van essentiële diensten**

**Afdeling 1**

*Audits*

Artikel 38

Dit artikel bepaalt dat aanbieders van essentiële diensten jaarlijks een interne audit en minstens om de drie jaar een externe audit moeten uitvoeren.

De interne audit kan worden uitgevoerd door de aanbieder van essentiële diensten zelf, door een andere aanbieder van de sector (collegiale toetsing) of door een externe dienstverlener.

De interne en externe auditverslagen moeten aan de sectorale overheid worden bezorgd.

Gezien de snelle evolutie van de informatie- en communicatietechnologie blijkt het noodzakelijk om aanbieders van essentiële diensten te verplichten minstens om de drie jaar een externe audit van de netwerk- en informatiesystemen te laten uitvoeren. De termijn van drie jaar is een redelijk compromis tussen de kostprijs van een externe audit voor de aanbieder en deze constante evolutie van de technologie.

De wet bepaalt dat een beroep moet worden gedaan op bepaalde instellingen voor de conformiteitsbeoordeling die geaccrediteerd zijn door de accreditatieautoriteit of door een instelling die de wederzijdse erkenningsakkoorden heeft ondertekend.

De inschakeling van geaccrediteerde externe auditors waarborgt een hoog gemeenschappelijk expertiseniveau tussen de verschillende sectoren voor de regelmatige controles van de aanbieders. Dit mechanisme is ook een hulpmiddel voor de inspectiediensten in het

Comme pour les opérateurs de services essentiels, et après consultation du fournisseur de service numérique, de l'autorité sectorielle et le cas échéant des autorités des autres États membres concernés, le CSIRT national peut communiquer au public des informations générales à des fins de prévention ou de gestion d'un incident ou dans l'intérêt général.

TITRE 4

*Contrôle et sanctions*

CHAPITRE 1ER

**Les contrôles des opérateurs de services essentiels**

**Section 1re**

*Audits*

Article 38

Cet article impose aux opérateurs de services essentiels de réaliser annuellement un audit interne, et au moins tous les trois ans un audit externe.

L'audit interne peut être réalisé par l'opérateur de services essentiels lui-même, par un autre opérateur du secteur (évaluation par ses pairs) ou par un prestataire extérieur.

Les rapports d'audit interne et externe doivent être communiqués à l'autorité sectorielle.

Vu l'évolution rapide des technologies de l'information et de la communication, il s'avère nécessaire d'imposer au moins tous les trois ans la réalisation d'un audit externe des réseaux et des systèmes des opérateurs de services essentiels. Le délai de trois ans est un compromis raisonnable entre le coût pour l'opérateur de faire réaliser un audit externe et cette évolution constante des technologies.

La loi impose le recours à certains organismes d'évaluation de la conformité accrédités par l'autorité d'accréditation ou par une institution signataire des accords de reconnaissance mutuelle.

Le recours à des prestataires d'audit externe accrédités assure un niveau commun et élevé d'expertise entre les différents secteurs pour réaliser les contrôles réguliers des opérateurs. Ce mécanisme permet également d'aider les services d'inspection dans leur missions de

kader van hun controleopdrachten en laat toe de noodzakelijke budgettaire kosten voor de goede werking van voormelde diensten te beheersen.

De eerste interne audit moet plaatsvinden binnen drie maanden na de uitwerking van het I.B.B. en de eerste externe audit uiterlijk vierentwintig maanden na de uitvoering van de eerste interne audit.

Hoewel de wet dit niet uitdrukkelijk bepaalt, kunnen verschillende aanbieders, om de kosten voor de tussenkomst van een externe en geaccrediteerde instelling voor de conformiteitsbeoordeling te verdelen, overeenkomen om samen een beroep te doen op dezelfde dienstverlener en voordelige prijsvoorwaarden te bedingen. Ook kunnen verschillende aanbieders van een sector of deelsector de oprichting van een sectorspecifieke instelling voor de conformiteitsbeoordeling aanmoedigen, die zich zal laten accrediteren en voor de aanbieders van deze sector lagere tarieven zal hanteren.

Artikel 39

De Koning moet, na advies van de sectorale overheid en de autoriteit bedoeld in artikel 7, § 1, de accreditatievoorwaarden bepalen. Deze moeten gebaseerd zijn op de normen ISO/IEC 17021 of ISO/IEC 17065. Opgemerkt wordt dat de inhoud van de in deze wet bedoelde technische normen ISO/IEC gratis kan worden geraadpleegd bij het Bureau voor Normalisatie (NBN), bedoeld in artikel VIII.3 van het Wetboek van economisch recht, dat gevestigd is in Brussel.

Tegelijk bepaalt de Koning de eventuele bijkomende eisen waaraan de instellingen voor de conformiteitsbeoordeling moeten voldoen en de regels voor de interne en externe audits.

De Koning kan ook, bij in Ministerraad overlegd besluit, en na advies van de sectorale overheden en van de autoriteit bedoeld in artikel 7, § 1, de voorwaarden bepalen onder dewelke een sectorale overheid zelf een instelling voor de conformiteitsbeoordeling kan erkennen.

De lijst van geaccrediteerde instellingen is beschikbaar bij de sectorale overheid die ze actueel houdt.

Artikel 40

Certificeringsaudits kunnen door de inspectiedienst of de sectorale overheid worden gelijkgesteld met de verplichte interne of zelfs externe audit als bedoeld in

contrôle et de maîtriser les coûts budgétaires nécessaires au bon fonctionnement des services précités.

Le premier audit interne doit être réalisé dans les trois mois de l'élaboration de la P.S.I. et le premier audit externe doit être effectué au plus tard vingt-quatre mois après la réalisation du premier audit interne.

Bien que la loi ne le dise pas explicitement, afin de mutualiser des coûts liés à l'intervention d'un organisme d'évaluation de la conformité externe et accrédité, plusieurs opérateurs peuvent s'entendre pour faire appel ensemble à un même prestataire en négociant avec lui des conditions avantageuses de prix. De même, plusieurs opérateurs d'un secteur ou d'un sous-secteur peuvent encourager la création d'un organisme d'évaluation de la conformité spécifique au secteur qui se fera accréditer et proposera des tarifs réduits pour les opérateurs de ce secteur.

Article 39

Le Roi est chargé de fixer, après avis de l'autorité sectorielle et de l'autorité visée à l'article 7, § 1er, les conditions d'accréditation. Celles-ci doivent être basées sur les normes ISO/IEC 17021 ou ISO/IEC 17065. Il convient de préciser que le contenu des normes techniques ISO/IEC visées dans la présente loi peut être consulté gratuitement sur place au Bureau de Normalisation (NBN), visé à l'article VIII.3 du Code de droit économique et situé à Bruxelles.

En même temps, le Roi fixe les éventuelles exigences supplémentaires imposées aux organismes d'évaluation de la conformité, et les règles applicables aux audits interne et externe.

Le Roi peut également, par arrêté délibéré en Conseil des ministres, et après avis des autorités sectorielles et de l'autorité visée à l'article 7, § 1er, déterminer les conditions pour qu'une autorité sectorielle puisse accorder elle-même un agrément à un organisme d'évaluation de la conformité.

La liste des organismes accrédités est disponible auprès de l'autorité sectorielle et tenue à jour.

Article 40

Les audits de certification peuvent être assimilés à l'audit interne voire à l'audit externe obligatoires visés à l'article 38, §§ 1er et 2, par le service d'inspection ou

artikel 38, §§ 1 en 2. In elk geval worden de verslagen van deze audits aan de sectorale overheid bezorgd.

Artikel 41

Gezien het belang om over nuttige informatie te beschikken om de beveiliging van netwerk- en informatiesystemen te beoordelen, kan de in artikel 7, § 1, van de wet bedoelde autoriteit zich steeds een kopie van de auditverslagen laten bezorgen.

**Afdeling 2**

*Inspectiedienst*

Artikel 42

Het artikel bepaalt dat de inspectiediensten te allen tijde controles mogen uitvoeren om na te gaan of de verplichtingen inzake beveiligingsmaatregelen en het melden van incidenten door de aanbieders worden nageleefd.

De inspectiedienst kan reactief of preventief optreden. Hij kan dit doen op eigen initiatief of op basis van een gemotiveerd verzoek van de in artikel 7, § 1, bedoelde autoriteit of van de sectorale overheid.

De Koning kan de eventuele praktische controlemodaliteiten voor een bepaalde sector bepalen.

De inspectiedienst moet het doel van een verzoek om informatie of bewijzen vermelden, alsook de termijn waarbinnen de informatie of bewijzen moeten worden verstrekt.

Hij kan een beroep doen op experten.

Artikel 43

De inspectiedienst kan buitenlandse bevoegde autoriteiten om samenwerking en bijstand verzoeken wanneer hij netwerk- en informatiesystemen van een aanbieder van essentiële diensten die zich buiten het Belgische grondgebied bevinden wenst te laten controleren.

Artikel 44

De inspectiedienst beschikt over ruime bevoegdheden om grondige controles uit te voeren op de naleving van de beveiligingsmaatregelen en de regels voor het melden van incidenten door de aanbieders van

l'autorité sectorielle. Dans tous les cas, les rapports de ces audits sont transmis à l'autorité sectorielle.

Article 41

Dans l'intérêt de disposer d'informations utiles pour évaluer la sécurité des réseaux et systèmes d'information, l'autorité visée à l'article 7, § 1er, de la loi peut toujours se faire communiquer une copie des rapports d'audits.

**Section 2**

*Service d'inspection*

Article 42

L'article prévoit que les services d'inspection peuvent effectuer des contrôles à tout moment afin de vérifier le respect des obligations des opérateurs en matière de mesures de sécurité et de notification d'incidents.

Le service d'inspection peut intervenir de manière réactive ou préventive. Celui-ci peut agir d'initiative, ou sur base d'une demande motivée de l'autorité visée à l'article 7, § 1er, ou de l'autorité sectorielle.

Le Roi peut fixer les éventuelles modalités pratiques du contrôle dans un secteur déterminé.

Le service d'inspection doit mentionner la finalité de la demande d'informations ou de preuves et préciser le délai pour les lui communiquer.

Il peut faire appel à des experts.

Article 43

Le service d'inspection peut solliciter la coopération et l'assistance des autorités compétentes étrangères lorsqu'il souhaite faire contrôler des réseaux et systèmes d'information d'un opérateur de services essentiels qui sont situés en dehors du territoire belge.

Article 44

Le service d'inspection dispose de larges pouvoirs afin d'effectuer des contrôles approfondis du respect des mesures de sécurité et des règles de notification des incidents par les opérateurs de services essentiels.

essentiële diensten. Zo mogen de leden van de inspectiedienst met name zonder voorafgaande verwittiging alle lokalen betreden die de aanbieder gebruikt, alsook de bewoonde lokalen mits voorafgaande machtiging van de onderzoeksrechter.

Ze moeten een legitimatiekaart bij zich hebben waarvan het model door de Koning wordt bepaald.

De leden van de inspectiedienst en de betrokken experten mogen geen belangenconflict hebben waardoor hun objectiviteit in het gedrang zou kunnen komen.

Vervolgens bepaalt het artikel de bevoegdheden van de beëdigde leden van de inspectiedienst en verduidelijkt het de voorwaarden om een machtiging van de onderzoeksrechter voor het betreden van bewoonde lokalen te bekomen en de na te leven regels tijdens de verhoren. Een “uitbreiding van het onderzoek” is mogelijk voor delen van netwerk- en informatiesystemen die enkel via clouddiensten toegankelijk zijn, steeds onder het toezicht van de Procureur des Konings en met inachtneming van het Wetboek van Strafvordering.

Artikel 45

Het artikel vermeldt dat na elke inspectie een verslag wordt opgesteld dat aan de betrokken aanbieder en de bevoegde sectorale overheid wordt bezorgd.

Net zoals voor interne en externe auditverslagen kan de autoriteit bedoeld in artikel 7, § 1, zich, bij een met redenen omkleed verzoek, de inspectieverslagen laten bezorgen.

Artikel 46

Het artikel bepaalt dat de aanbieder moet meewerken aan de inspecties en de door de inspectiedienst gevraagde informatie moet verstrekken, desgevallend door het nodige materiaal ter beschikking te stellen.

Het artikel maakt het mogelijk om, per sector of deelsector, retributies te heffen voor de inspectieprestaties, die ten laste zijn van de aanbieders van essentiële diensten.

Ainsi, les membres du service d’inspection peuvent notamment pénétrer sans avertissement préalable dans tous les locaux utilisés par l’opérateur, et dans les locaux habités moyennant une autorisation préalable du juge d’instruction.

Ils doivent porter une carte de légitimation dont le modèle sera fixé par le Roi.

Les membres du service d’inspection ainsi que les experts impliqués ne peuvent être en situation de conflit d’intérêts susceptible de compromettre leur objectivité.

L’article détaille ensuite les pouvoirs des membres assermentés du service d’inspection et précise les conditions pour obtenir du juge d’instruction une autorisation de pénétrer dans des locaux habités ainsi que les règles à suivre lors des auditions. Il a été prévu de permettre une “extension de la recherche” pour viser les parties de réseaux et systèmes d’information qui sont accessibles uniquement via des services en nuage (“cloud”), toujours sous le contrôle du Procureur du Roi et dans le respect du Code d’instruction criminelle.

Article 45

L’article prévoit que chaque inspection doit être suivie d’un rapport qui sera transmis à l’opérateur concerné et à l’autorité sectorielle compétente.

Comme pour les rapports d’audit interne et externe, l’autorité visée à l’article 7, § 1er, peut se faire communiquer sur demande motivée les rapports d’inspection.

Article 46

L’article prévoit l’obligation pour l’opérateur de collaborer aux inspections et de fournir les informations demandées par le service d’inspection, y compris si nécessaire en mettant à disposition le matériel nécessaire.

L’article permet l’établissement de rétributions relatives aux prestations d’inspection, par secteur ou par sous-secteur, à charge des opérateurs de services essentiels.

HOOFDSTUK 2

**Toezicht op de digitaledienstverleners**

Artikel 47

Dit artikel machtigt de Koning om het toezicht op de digitaledienstverleners te regelen. Deze moeten geen audits uitvoeren, maar zijn verplicht om de inspectiedienst alle informatie te verstrekken die nodig is om de beveiliging van de netwerk- en informatiesystemen te beoordelen, en elke niet-inachtneming van de beveiligingseisen en de eisen inzake het melden van incidenten recht te zetten.

De wet bepaalt dat de Koning maatregelen kan nemen in geval van niet-naleving van voormelde eisen, alsook op grond van een aangifte door een autoriteit van een andere lidstaat.

HOOFDSTUK 3

**De sancties**

**Afdeling 1**

*Procedure*

Artikel 48

Het artikel beschrijft de procedure voor de vaststelling van inbreuken op de wet, de uitvoeringsbesluiten ervan of individuele administratieve beslissingen hieromtrent. Een eerste remediëringstermijn wordt bepaald door middel van een formele ingebrekestelling. Deze wordt echter voorafgegaan door een gemotiveerde mededeling aan de aanbieder van essentiële diensten of digitaledienstverlener; laatstgenoemde heeft de mogelijkheid om zijn opmerkingen te formuleren en kan vragen om te worden gehoord. Vervolgens stuurt de inspectiedienst de overtreder een ingebrekestelling, met een termijn waarbinnen hij zich in regel moet stellen.

Artikel 49

Bij gebrek aan remediëring na een ingebrekestelling wordt een proces-verbaal opgemaakt door de beëdigde personeelsleden van de inspectiedienst en overgemaakt aan de sectorale overheid.

Elke vrijwillige belemmering van de uitvoering van de controle, weigering om gevraagde informatie te verstrekken en mededeling van onvolledige of onjuiste informatie zal eveneens vastgesteld worden in een

CHAPITRE 2

**Contrôle des fournisseurs de service numérique**

Article 47

Cet article habilite le Roi à régler le contrôle des fournisseurs de service numérique. Ceux-ci ne doivent pas effectuer d'audits, mais ils sont tenus de fournir au service d'inspection toutes les informations nécessaires pour évaluer la sécurité des réseaux et systèmes d'information, et de corriger tout manquement aux exigences de sécurité et de notification d'incidents.

La loi permet au Roi d'adopter des mesures en cas de non-respect des exigences précitées, y compris sur dénonciation d'une autorité d'un autre État membre.

CHAPITRE 3

**Les sanctions**

**Section 1re**

*Procédure*

Article 48

L'article décrit la procédure pour constater des manquements à la loi, ses arrêtés d'exécution ou des décisions administratives individuelles y afférentes. Il est prévu de fixer un premier délai de remédiation, au moyen d'une mise en demeure formelle. Celle-ci sera toutefois précédée d'une information motivée communiquée à l'opérateur de services essentiels ou au fournisseur de service numérique; ce dernier aura la possibilité de formuler ses observations et pourra solliciter d'être entendu. Ensuite, le service d'inspection adressera une mise en demeure au contrevenant avec un délai de mise en conformité.

Article 49

A défaut de remédiation suite à une mise en demeure, un procès-verbal sera dressé par les membres du personnel assermentés du service d'inspection et communiqué à l'autorité sectorielle.

L'entrave volontaire à l'exécution du contrôle, le refus de communiquer les informations demandées et la communication d'informations incomplètes ou inexactes sera également constaté dans un procès-verbal. Il en

proces-verbaal. Hetzelfde geldt voor de potentiële aanbieder van essentiële diensten of de exploitant van een kritieke infrastructuur die de nodige informatie niet meedeelt met het oog op zijn eventuele identificatie als aanbieder die onderworpen is aan de verplichtingen inzake beveiligingsmaatregelen en melding van incidenten, als bedoeld in artikel 14 of artikel 18, § 3.

De wet kent bijzondere bewijskracht toe aan de materiële vaststellingen die het voorwerp uitmaken van dat proces-verbaal (en niet aan de andere constitutieve bestanddelen van de inbreuk). Dit is gerechtvaardigd gezien de hoofdzakelijk technische aard van deze vaststellingen, die het in de praktijk moeilijk maakt om sommige aspecten van de in de wet bedoelde inbreuken vast te stellen op een andere wijze dan door de beëdigde inspecteurs of experten. Bovendien worden de rechten van de beklaagde niet beperkt aangezien het mogelijk blijft om het tegenbewijs te leveren met alle bewijsmiddelen die de rechter zal beoordelen.

Artikel 50

Dit artikel voorziet in de mogelijkheid om administratieve en strafrechtelijke sancties op te leggen.

**Afdeling 2**

*Strafrechtelijke sancties*

Artikel 51

Dit artikel bepaalt de straffen in geval van niet-naleving van de verplichtingen opgelegd door of krachtens de wet.

**Afdeling 3**

*Administratieve sancties*

Artikel 52

Dit artikel vermeldt het principe en het bedrag van de administratieve geldboetes en regelt de tenlasteneming van eventuele expertisekosten.

Artikel 53

Dit artikel verduidelijkt dat het in artikel 49 bedoelde proces-verbaal naar de procureur des Konings en overtreder wordt gestuurd.

va de même de l'opérateur de services essentiels potentiel ou de l'exploitant d'une infrastructure critique qui est en défaut de fournir les informations permettant son identification éventuelle comme opérateur soumis aux obligations de mesures de sécurité et de notification d'incidents, comme visé à l'article 14 ou à l'article 18, § 3.

La loi confère une force probante particulière aux constatations matérielles faisant l'objet de ce procès-verbal (et non aux autres éléments constitutifs de l'infraction). Ceci se justifie eu égard à la nature principalement technique de telles constatations, qui rend difficile en pratique la constatation de certains aspects des infractions prévues par la loi autrement que par les inspecteurs ou experts assermentées. En outre, les droits du prévenu ne sont pas restreints car il demeure possible d'apporter la preuve contraire par tous moyens de preuve que le juge appréciera.

Article 50

Cet article prévoit la possibilité de sanctions administratives comme de sanctions pénales.

**Section 2**

*Sanctions pénales*

Article 51

Cet article prévoit les peines applicables en cas de non-respect des obligations imposées par ou en vertu de la loi.

**Section 3**

*Sanctions administratives*

Article 52

Cet article prévoit le principe et le montant des amendes administratives et règle la prise en charge des frais éventuels d'expertise.

Article 53

Cet article prévoit la communication du procès-verbal visé à l'article 49, au procureur du Roi et à l'auteur de l'infraction.

Artikel 54

Volgens dit artikel beschikt de procureur des Konings over een termijn van twee maanden te rekenen vanaf de ontvangst van het proces-verbaal om strafrechtelijke vervolging in te stellen tegen de aanbieder van essentiële diensten, die hierover binnen dezelfde termijn wordt ingelicht. Er mag geen administratieve geldboete worden opgelegd vóór het verstrijken van deze termijn of vóór de beslissing van de procureur des Konings om niet te vervolgen.

Artikel 55

Dit artikel regelt de principes voor het bepalen van het bedrag van de geldboete, de in aanmerking te nemen omstandigheden, de situaties van herhaling en de situatie van samenloop van inbreuken.

Met het oog op de eerbiediging van de rechten van de verdediging is bepaald dat de overtreder kan worden gehoord of zijn verweermiddelen schriftelijk kan indienen binnen een termijn van 15 dagen.

De leden van de inspectiedienst of van de sectorale overheid die hebben deelgenomen aan de betrokken inspecties of controles mogen, in de mate van het mogelijke, ook niet deelnemen aan beraadslagingen van de sectorale overheid over de sanctie voor de aanbieder van essentiële diensten of digitaledienstverlener.

Artikel 56

Dit artikel bepaalt dat de beslissing ter kennis wordt gebracht van de overtreder.

Artikel 57

Dit artikel maakt het mogelijk om de beslissing te betwisten bij verzoekschrift bij het Marktenhof dat de zaak behandelt zoals in kort geding overeenkomstig de artikelen 1035 tot 1038, 1040 en 1041 van het Gerechtelijk Wetboek en dat de beslissing kan herzien.

Het beroep heeft geen schorsende werking.

Artikel 58

Dit artikel bepaalt de voorwaarden waarin de beslissing uitvoerbaar wordt.

Article 54

Cet article permet au procureur du Roi de mouvoir l'action pénale dans un délai de deux mois à compter de la réception du procès-verbal, à l'encontre de l'opérateur de services essentiels, qui en sera informé dans le même délai. Avant l'expiration de ce délai ou la décision du procureur du Roi de ne pas poursuivre, une amende administrative ne peut être infligée.

Article 55

Cet article règle les principes de détermination du montant de l'amende, des circonstances à prendre en considération, des situations de récidive et la situation du concours.

Pour assurer le respect des droits de la défense, il est prévu de permettre à l'auteur d'être entendu ou de formuler ses moyens de défense par écrit dans un délai de 15 jours.

Les membres du service d'inspection ou de l'autorité sectorielle ayant participé aux inspections ou aux contrôles concernés veilleront également à s'abstenir, dans la mesure du possible, de participer aux délibérations de l'autorité sectorielle relative à la sanction à infliger à l'opérateur de service essentiels ou au fournisseur de service numérique.

Article 56

Cet article prévoit que la décision est notifiée à l'auteur de l'infraction.

Article 57

Cet article permet de contester la décision par voie de requête auprès de la Cour des marchés qui traite l'affaire selon les formes du référé conformément aux articles 1035 à 1038, 1040 et 1041 du Code judiciaire et qui peut réformer la décision.

Le recours n'est pas suspensif.

Article 58

Cet article prévoit les conditions dans lesquelles la décision devient exécutoire.

Artikel 59

Uit dit artikel blijkt dat de verjaringstermijn voor administratieve geldboetes drie jaar bedraagt.

TITEL 5

*CSIRT*

De artikelen 60, 61 en 62, alsook 63 en 64, beschrijven respectievelijk de voorschriften en taken van het nationale CSIRT en van de eventuele sectorale CSIRT's.

Er dient een onderscheid te worden gemaakt tussen het begrip "sectoraal CSIRT", dat eigen is aan het Belgisch recht en het begrip "CSIRT" bedoeld in de Europese NIS-richtlijn. In België zal enkel het nationale CSIRT alle taken uitvoeren van het CSIRT in de zin van de richtlijn. Om evidente, praktische redenen van coördinatie mogen bepaalde taken zoals het monitoren van incidenten op nationaal en internationaal niveau, de regelmatige deelname aan het Europese CSIRT-netwerk en de vaststelling van procedures voor de behandeling van incidenten immers enkel worden toevertrouwd aan het nationale CSIRT. Dat verklaart waarom de opdrachten van een sectoraal CSIRT niet dezelfde zijn als die van het nationale CSIRT.

Artikel 62 verduidelijkt dat het nationale CSIRT alle passende, evenredige en behoedzame maatregelen zal nemen om zijn wettelijke opdrachten te verwezenlijken.

Deze bepaling laat het nationale CSIRT indien nodig toe om af te wijken van sommige bepalingen van het Strafwetboek voor de uitvoering van zijn wettelijke opdrachten, met toepassing van artikel 70 van het Strafwetboek.

TITEL 6

*Verwerking van persoonsgegevens*

HOOFDSTUK 1

**Principes betreffende de verwerking, wettelijke basis en doeleinden**

Dit hoofdstuk bevat bepalingen die, enerzijds, de toepassing van sommige beginselen van de AVG verduidelijken in het kader van het wetsontwerp en, anderzijds, op duidelijke wijze de soorten verwerkingen, categorieën van persoonsgegevens, verwerkingsverantwoordelijken, ontvangers van gegevens, enz. beschrijven.

Article 59

Cet article prévoit que le délai de prescription est de trois ans pour les amendes administratives.

TITRE 5

*CSIRT*

Les articles 60, 61 et 62, ainsi que 63 et 64, respectivement, décrivent les obligations et les tâches du CSIRT national et des éventuels CSIRT sectoriels.

Il convient de distinguer le "CSIRT sectoriel" qui est une notion propre au droit belge et la notion de "CSIRT" visée par la directive européenne NIS. En Belgique, seul le CSIRT national accomplira toutes les tâches dévolues au CSIRT au sens de la directive. En effet, il convient de réserver au seul CSIRT national, pour des raisons pratiques évidentes de coordination, certaines tâches comme le suivi des incidents au niveau national et international, la participation régulière au réseau européen des CSIRT, l'adoption de procédures de gestion des incidents. Cela explique que les missions d'un CSIRT sectoriel ne soient pas identiques à celles du CSIRT national.

L'article 62 précise que le CSIRT national prendra toutes les mesures adéquates, proportionnelles et prudentes afin de réaliser ses missions légales.

Cette disposition permet, si nécessaire, au CSIRT national de déroger à certaines dispositions du Code pénal pour l'exécution de ses missions légales, par application de l'art. 70 du Code pénal.

TITRE 6

*Traitement des données à caractère personnel*

CHAPITRE 1ER

**Principes relatifs au traitement, bases légales et finalités**

Cette section regroupe des dispositions qui visent, d'une part, à clarifier l'application de certains principes du RGPD dans le cadre du projet de loi et, d'autre part, à décrire de façon claire les types de traitements, les catégories de données personnelles, les responsables du traitement, les destinataires des données, etc.

Artikel 65

Het wetsontwerp heeft in essentie tot doel een bepaalde informatie-uitwisseling aan te moedigen, maar met inachtneming van de AVG. Daarom verduidelijkt het artikel in de eerste plaats dat elke gegevensverwerking in uitvoering van de bepalingen van het wetsontwerp het beginsel van minimale gegevensverwerking en het evenredigheidsbeginsel moet naleven. Zo moeten de persoonsgegevens beperkt zijn tot wat noodzakelijk is en in verhouding staan tot de doeleinden waarvoor ze worden verwerkt (beginsel van minimale gegevensverwerking). Dit beginsel impliceert ook dat indien een bepaald doeleinde kan worden gerealiseerd zonder persoonsgegevens te verwerken, voor deze oplossing moet worden gekozen.

Ter illustratie verduidelijkt het artikel ook de gegevenscategorieën die in uitvoering van het wetsontwerp kunnen worden verwerkt, alsook de belangrijkste verwerkingen en gegevensstromen, als leidraad voor de keuzes die de verwerkingsverantwoordelijken zullen moeten maken overeenkomstig het verantwoordingsbeginsel (“accountability”).

Artikel 66

Het artikel bepaalt dat de gegevens indien mogelijk moeten worden gepseudonimiseerd in de zin van de AVG, of geaggregeerd, om het risico op onrechtmatig gebruik te verkleinen.

Voor de duidelijkheid wordt ook vermeld dat de artikelen 9 en 10 van de AVG van toepassing blijven op de verwerking van bijzondere gegevenscategorieën (“gevoelige gegevens”).

Het artikel somt ook de persoonscategorieën op die *a priori* verantwoordelijk kunnen zijn voor de verwerking. Het verduidelijkt dat de gegevens toegankelijk kunnen worden gemaakt voor alle personen die betrokken zijn bij de uitvoering van de wet, voor zover dit noodzakelijk is voor de informatie-uitwisseling waarin het wetsontwerp voorziet.

Artikel 67

Het artikel bepaalt dat de verwerking van persoonsgegevens een wettelijke basis moet hebben en beperkt moet blijven tot wat noodzakelijk is voor deze wettelijke basis, overeenkomstig de artikelen 6.1. c) (bij wet opgelegde verwerking), en 6.1. e) van de AVG (verwerking in het kader van een taak van algemeen belang). Zoals hierboven vermeld, blijft bovendien de regeling voor

Article 65

L’essence du projet de loi est de stimuler certains échanges d’informations, mais dans le respect du RGPD. C’est pourquoi l’article précise tout d’abord que tout traitement de données qui est effectué en exécution des dispositions du projet de loi, doit respecter le principe de minimisation des données et le principe de proportionnalité. Ainsi, les données à caractère personnel doivent être limitées à ce qui est nécessaire et de manière proportionnée au regard des finalités pour lesquelles elles sont traitées (principe de minimisation des données). Ce principe implique aussi que lorsqu’une certaine finalité peut être réalisée sans traiter des données à caractère personnel, il faut choisir cette solution.

L’article précise également, à titre illustratif, les catégories de données qui sont susceptibles d’être traitées en exécution du projet de loi, ainsi que les principaux traitements et flux de données, ceci afin de guider les choix qui devront être arrêtés par les responsables du traitement conformément au principe de responsabilité (“accountability”).

Article 66

L’article dispose que les données devront être, chaque fois que possible, rendues pseudonymes au sens du RGPD, ou agrégées, de façon à diminuer le risque d’une utilisation illicite.

Par souci de clarté, il est aussi précisé que les articles 9 et 10 du RGPD restent applicables au traitement de catégories particulières de données (“données sensibles”).

L’article énumère encore les catégories de personnes qui peuvent être *a priori* responsables du traitement. Il clarifie que les données peuvent être rendues accessibles à toutes les personnes impliquées dans l’exécution de la loi, dans la mesure nécessaire pour les échanges d’informations que le projet de loi prévoit.

Article 67

L’article dispose que les traitements de données à caractère personnel doivent avoir une base légale et rester limité à ce qui est nécessaire par rapport à cette base légale, qui se retrouve en l’occurrence aux articles 6.1. c) (traitement imposé par la loi), et 6.1. e) du RGPD (traitement relevant d’une mission d’intérêt public). Comme indiqué plus haut, le régime des

bijzondere gegevenscategorieën, in de AVG en de nationale wetgevingen die deze aanvullen, van toepassing.

Overeenkomstig artikel 20 van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens moeten de federale autoriteiten protocolakkoorden sluiten tussen de initiële verwerkingsverantwoordelijke en de verwerkingsverantwoordelijke die de gegevens ontvangt, bij de doorgifte van persoonsgegevens op basis van artikel 6.1.c) en e), van de verordening aan een andere overheid of privé-instelling.

Artikel 68

Het artikel legt het finaliteitsbeginsel vast, en somt ter illustratie de voornaamste doeleinden op die in het kader van het wetsontwerp kunnen worden nagestreefd.

Aangezien het wetsontwerp tal van informatie-uitwisselingen wil bevorderen, en er bijgevolg tal van multidirectionele gegevensstromen zullen zijn, lijkt het delicaat of zelfs riskant om alle doeleinden en subdoeleinden volledig vast te leggen in de bepalingen van het wetsontwerp naargelang het soort verwerking.

Het artikel verduidelijkt bovendien dat elke verwerkingsverantwoordelijke, wat hem betreft, de relevante doeleinden en subdoeleinden moet bepalen, alsook alle andere kenmerken van de verwerking. Zo moet elke verwerkingsverantwoordelijke het zogenaamde “accountability-beginsel” van de AVG naleven, rekening houdend met de andere bepalingen van Titel 6 van het wetsontwerp.

HOOFDSTUK 2

**Bewaartermijn**

Artikel 69

Het artikel bepaalt dat de autoriteiten bedoeld in artikel 7 van het wetsontwerp de gegevens niet langer mogen bewaren dan wat strikt nodig is voor de nagestreefde doeleinden. Ook de aanbieders van essentiële diensten en digitaledienstverleners moeten de regels van de AVG toepassen, maar kunnen dezelfde gegevens verwerken voor andere doeleinden die niet vallen onder de toepassing van het wetsontwerp.

Het artikel machtigt de Koning ook om, bij in

catégories particulières de données défini par le RGPD et les législations nationales qui le complètent, reste par ailleurs applicable.

Comme le prévoit l’article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l’égard des traitements de données à caractère personnel, les autorités fédérales devront conclure des protocoles d’accord entre le responsable du traitement initial et le responsable du traitement destinataire des données, lors du transfert de données à caractère personnel sur la base de l’article 6.1.c) et e), du Règlement à toute autre autorité publique ou organisation privée.

Article 68

L’article consacre le principe de finalité, et énumère à titre illustratif les principales finalités qui peuvent être poursuivies dans le cadre du projet de loi.

Vu que le projet de loi tend à promouvoir de nombreux échanges d’informations, et qu’il existera en conséquence de nombreux flux de données multidirectionnels, il apparaît délicat voire hasardeux de fixer de manière exhaustive dans les dispositions du projet de loi l’ensemble des finalités et sous-finalités en fonction de chaque type de traitement.

L’article précise d’ailleurs que chaque responsable du traitement doit définir pour ce qui le concerne les finalités ou sous-finalités pertinentes, ainsi que toutes les autres caractéristiques du traitement. Chaque responsable du traitement doit ainsi se conformer au principe dit de “accountability” selon le RGPD, tout en tenant compte des autres dispositions du Titre 6 du projet de loi.

CHAPITRE 2

**Durée de conservation**

Article 69

L’article impose aux autorités visées à l‘article 7 du projet de loi, de limiter la conservation des données à la période strictement nécessaire au regard des finalités poursuivies. Les opérateurs de services essentiels et les fournisseurs de service numérique devront eux aussi appliquer les règles du RGPD mais sont susceptibles de traiter les mêmes données pour d’autres finalités, étrangères à l’application du projet de loi.

Ministerraad overlegd besluit, maximale bewaartermijnen te bepalen.

HOOFDSTUK 3

**Functionaris voor gegevensbescherming**

Artikel 70

Het artikel voert voor alle aanbieders van essentiële diensten en digitaledienstverleners de verplichting in om een functionaris voor gegevensbescherming aan te wijzen. Zo maakt het gebruik van de mogelijkheid die artikel 37.4. van de AVG biedt.

HOOFDSTUK 4

**Beperking van de rechten van de betrokken personen**

De artikelen 71 en 72 voeren uitzonderingen in op de subjectieve rechten van de betrokkenen krachtens de artikelen 12 tot 22 van de AVG. Deze uitzonderingen zijn gebaseerd op artikel 23 van de AVG en blijven binnen de grenzen van dat artikel. Artikel 71 bepaalt dat ze geen afbreuk mogen doen aan de wezenlijke inhoud van de grondrechten en fundamentele vrijheden en moeten worden toegepast voor zover dit strikt noodzakelijk is voor de door de wet nagestreefde doeleinden, om de juridische bescherming van de fundamentele vrijheden te verbeteren.

Gelet op de verplichtingen in het wetsontwerp moeten tal van persoonsgegevens worden verwerkt. Om de verwezenlijking van de doelstellingen van deze wet niet in het gedrang te brengen, is het nodig om in een aantal afwijkingen te voorzien wat de rechten betreft die de artikelen 12 tot 22 van de AVG toekennen aan de betrokkenen, met als doel de nationale veiligheid, de landsverdediging, de openbare veiligheid, de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten, andere belangrijke doelstellingen van algemeen belang van de Europese Unie of van een lidstaat, of een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt met de uitoefening van het openbaar gezag te waarborgen.

De afwijkingen in deze wet zijn evenwel beperkt tot de verwerking om te voldoen aan de verplichtingen inzake het melden van incidenten bedoeld in hoofdstuk 3 van titel 2 en hoofdstuk 2 van titel 3, en inzake het toezicht bedoeld in titel 4 van deze wet. Deze afwijkingen komen

L'article habilite également le Roi, par arrêté délibéré en conseil des Ministres, à fixer des délais de conservation maximale.

CHAPITRE 3

**Délégué à la protection des données**

Article 70

L'article instaure l'obligation, pour tous les opérateurs de services essentiels et les fournisseurs de service numérique, de désigner un délégué à la protection des données. Il fait ainsi usage de la faculté offerte à l'article 37.4. du RGPD.

CHAPITRE 4

**Limitations des droits des personnes concernées**

Les articles 71 et 72 introduisent des exceptions aux droits subjectifs des personnes concernées en vertu des articles 12 à 22 du RGPD. Ces exceptions sont introduites sur le fondement de et dans les limites permises par l'article 23 du RGPD. L'article 71 précise qu'elles ne peuvent porter préjudice à l'essence des libertés et droits fondamentaux et doivent être appliquées dans la stricte mesure nécessaire aux buts poursuivis par la loi, afin de renforcer la protection juridique des libertés fondamentales.

Les obligations prévues par le projet de loi nécessitent le traitement de nombreuses données à caractère personnel. Afin de ne pas compromettre la réalisation des objectifs de la loi, il apparaît nécessaire de prévoir un certain nombre de dérogations aux droits reconnus aux personnes concernées par les articles 12 à 22 du RGPD, et ce dans le but de préserver la sécurité nationale, la défense nationale, la sécurité publique, la prévention, la détection, la recherche et la poursuite d'infractions, d'autres objectifs importants d'intérêt public général de l'Union européenne ou d'un État membre, ou encore une mission de contrôle, d'inspection ou de réglementation liée à l'exercice de l'autorité publique.

Les dérogations prévues par la présente loi sont toutefois limitées aux traitements effectués pour satisfaire aux obligations en matière de notifications d'incidents visées aux chapitres 3 du titre 2 et 2 du titre 3, et de contrôles visés au titre 4 de la présente

de aanbieders van essentiële diensten en digitaledienstverleners ten goede, alsook de inspectiediensten en autoriteiten bedoeld in artikel 7 van deze wet, voor zover dit noodzakelijk is voor het nagestreefde doel en met inachtneming van het evenredigheidsbeginsel en het beginsel van minimale gegevensverwerking, zoals uitdrukkelijk vermeld in artikel 71. Bijgevolg kan geen vrijstelling worden toegekend wanneer het mogelijk is om de verzoeken van de betrokkene in te willigen op grond van de artikelen 12 tot 22 van de AVG zonder de verwezenlijking van voormelde doeleinden in het gedrang te brengen. Het wetsontwerp past dan ook in het kader van het evenredigheidsbeginsel en het beginsel van minimale gegevensverwerking. Voor zover nodig bepaalt artikel 71 maximale bewaartermijnen ingevolge de vrijstelling.

Het artikel vermeldt nog dat de verwerkingsverantwoordelijke, om de vrijstelling te genieten, aan de bijkomende voorwaarden van artikel 72 moet voldoen, en bovendien de vertrouwelijkheid van de gegevens moet waarborgen. Om redenen van transparantie is hij ook verplicht om jaarlijks de Gegevensbeschermingsautoriteit in te lichten over de weigeringen op grond van de vrijstelling in artikel 71.

Artikel 72

Het artikel regelt de antwoordprocedure voor individuele verzoeken van betrokkenen en waarborgt dat zij duidelijke en transparante informatie krijgen over de uitoefening van hun rechten en de redenen voor de weigering of beperking ervan.

Het artikel bepaalt ook de maximumtermijn tijdens dewelke de weigering of beperking kan worden gehandhaafd.

HOOFDSTUK 5

**Beperkingen inzake de verplichte melding van inbreuken in verband met persoonsgegevens**

Artikel 73

Het artikel voert een andere, beperktere afwijking in wat betreft artikel 34 van de AVG en de verplichting om een inbreuk in verband met persoonsgegevens individueel te melden. Enkel met de toestemming van de autoriteit bedoeld in artikel 7, § 1, van de wet, en voor zover dit noodzakelijk is om de doeleinden bedoeld in artikel 71, § 2, van het wetsontwerp te waarborgen, is deze individuele kennisgeving niet meer verplicht.

loi. Ces dérogations bénéficient aux opérateurs de services essentiels et fournisseurs de service numérique, ainsi qu'aux services d'inspection et autorités visées à l'article 7 de la présente loi, dans la mesure nécessaire au but poursuivi et dans le respect des principes de proportionnalité et de minimisation des données, ce que l'article 71 rappelle explicitement. Une exemption ne pourra donc pas être accordée lorsqu'il est possible d'accéder aux requêtes de la personne concernée sur le fondement des articles 12 à 22 du RGPD sans compromettre la réalisation des finalités susvisées. De cette façon, le projet de loi s'inscrit dans le cadre du principe de proportionnalité et de minimisation des données. En tant que de besoin, l'article 71 définit des durées maximales de conservation des données résultant de l'exemption.

L'article prévoit encore que le responsable du traitement doit, pour bénéficier de l'exemption, respecter les conditions supplémentaires énumérées à l'article 72, et doit en outre assurer la confidentialité des données. En outre il est tenu dans un souci de transparence d'informer l'Autorité de protection des données, annuellement, des refus motivés par l'exemption consacrée à l'article 71.

Article 72

L'article règle la procédure de réponse aux demandes individuelles des personnes concernées et veille à assurer que celles-ci reçoivent une information claire et transparente au sujet de l'exercice de leurs droits et des motifs du refus ou de la limitation de ceux-ci.

L'article fixe également la période maximale durant laquelle le refus ou la limitation peuvent être maintenus.

CHAPITRE 5

**Limitations aux obligations de notification des violations de données à caractère personnel**

Article 73

L'article introduit une autre dérogation, plus limitée, concernant l'article 34 du RGPD et l'obligation de notification individuelle en cas de violation de données personnelles. Ce n'est qu'avec l'autorisation de l'autorité visée à l'article 7, § 1er, de la loi, et que dans la mesure nécessaire pour préserver les finalités visées à l'article 71, § 2, du projet de loi, que cette notification individuelle ne serait plus obligatoire.

TITEL 7

*Slotbepalingen*

HOOFDSTUK 1

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

De artikelen 74 tot 84 passen de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren aan, om er de rol van de autoriteit bedoeld in artikel 7, § 1, van deze wet in te verankeren.

Aangezien de exploitanten van kritieke infrastructuren als aanbieders van essentiële diensten kunnen worden geïdentificeerd, moet ook de autoriteit bedoeld in artikel 7, § 1, van deze wet worden betrokken bij het identificatieproces van de kritieke infrastructuren, wat de beveiliging van netwerk- en informatiesystemen betreft.

De andere artikelen behoeven geen verdere commentaar.

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**

De artikelen 85 en 86 passen de wet van 15 april 1994 aan en behoeven geen verdere commentaar.

HOOFDSTUK 3

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

De artikelen 87 tot 89 passen de wet van 17 januari 2003 aan en behoeven geen verdere commentaar.

TITRE 7

*Disposition finales*

CHAPITRE 1ER

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

Les articles 74 à 84 visent à adapter la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, afin d'y consacrer le rôle de l'autorité visée à l'article 7, § 1er, de la présente loi.

Compte tenu du fait que les exploitants d'infrastructures critiques peuvent être identifiés comme opérateurs de services essentiels, il est utile d'associer également l'autorité visée à l'article 7, § 1er, de la présente loi au processus d'identification des infrastructures critiques, pour ce qui concerne la sécurité des réseaux et systèmes d'information.

Les autres articles n'appellent pas de commentaires particuliers.

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**

Les articles 85 et 86 visent à adapter la loi du 15 avril 1994 et n'appellent pas de commentaire particulier.

CHAPITRE 3

**Modifications de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges**

Les articles 87 à 89 visent à adapter la loi du 17 janvier 2003 et n'appellent pas de commentaire particulier.

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 en van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten**

De artikelen 90 en 91 passen de wetten van 21 november 2017 en 2 augustus 2002 aan en behoeven geen verdere commentaar.

HOOFDSTUK 5

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

De artikelen 92 tot 94 passen de wet van 22 februari 1998 aan en behoeven geen verdere commentaar.

HOOFDSTUK 6

**Inwerkingtreding**

Artikel 95 bepaalt de datum van inwerkingtreding van de wet en behoeft geen verdere commentaar.

*De eerste minister,*

Charles MICHEL

*De minister van Veiligheid en Binnenlandse Zaken,*

Jan JAMBON

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 et de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers**

Les articles 90 et 91 visent à adapter les lois du 21 novembre 2017 et 2 août 2002 et n'appellent pas de commentaire particulier.

CHAPITRE 5

**Modifications de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique**

Les articles 92 à 94 visent à adapter la loi du 22 février 1998 et n'appellent pas de commentaire particulier.

CHAPITRE 6

**Entrée en vigueur**

L'article 95 fixe la date d'entrée en vigueur de la loi et n'appelle pas de commentaire particulier.

*Le premier ministre,*

Charles MICHEL

*Le ministre de la Sécurité et de l'Intérieur,*

Jan JAMBON

**VOORONTWERP VAN WET (I)**

**onderworpen aan het advies van de Raad van State**

**Voorontwerp van wet tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid**

TITEL 1

*Definities en algemene bepalingen*

HOOFDSTUK 1

**Onderwerp en toepassingsgebied**

**Afdeling 1**

*Onderwerp*

Art. 1

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

Art. 2

Deze wet voorziet 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.

§ 2. Deze wet is van toepassing op de digitaledienstverleners, zoals gedefinieerd in artikel 6, 20°, die hun hoofdvestiging in België hebben. Een digitaledienstverlener wordt geacht zijn hoofdvestiging in België te hebben als zijn hoofdkantoor 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 III en hun vertegenwoordiger in België gevestigd is in het kader van de NIS-richtlijn.

**AVANT-PROJET DE LOI (I)**

**soumis à l'avis du Conseil d'État**

**Avant-projet de loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique**

TITRE 1ER

*Définitions et dispositions générales*

CHAPITRE 1ER

**Objet et champ d'application**

**Section 1re**

*Objet*

Art. 1er

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

Art. 2

La présente loi vise 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.

§ 2. La présente loi s'applique aux fournisseurs de service numérique, tels que définis à l'article 6, 20°, dont l'établissement principal est situé en Belgique. Un fournisseur de service numérique est réputé avoir son établissement 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 III et qu'ils établissent en Belgique leur représentant pour les besoins de la directive NIS.

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 elektronische-communicatienetwerken of openbare elektronische-communicatiediensten, 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. Deze wet is niet van toepassing op de aanbieders die behoren tot de sector financiën in de zin van bijlage II van de wet.

Er wordt een uitzondering gemaakt in het vorige lid voor de bepalingen van titel I, van hoofdstuk 1 van titel II, en van artikel 17, §§ 2 en 3, van deze wet.

In afwijking van het eerste lid is artikel 27 van deze wet van toepassing op de aanbieders die behoren tot de sector financiën in de zin van bijlage II van de 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.

§ 3. 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 vorige lid, nader te bepalen.

§ 4. Deze wet is niet van toepassing op de nucleaire installaties bedoeld in 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, met uitzondering van de elementen van een nucleaire installatie bestemd voor de industriële productie van elektriciteit die dienen voor de transmissie van de elektriciteit.

Art. 5

§ 1. Deze wet doet geen afbreuk aan de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de

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. La présente loi n'est pas applicable aux opérateurs relevant du secteur des finances au sens de l'annexe II de la loi.

Il est fait exception à l'alinéa précédent pour les dispositions du titre I, du chapitre 1 du titre II, et de l'article 17, §§ 2 et 3 de la présente loi.

Par dérogation à l'alinéa 1er, l'article 27 de la présente loi est applicable aux opérateurs relevant du secteur des finances au sens de l'annexe II de la 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.

§ 3. 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 précédent.

§ 4. La présente loi n'est pas applicable aux installations nucléaires visées par 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, à l'exception des éléments d'une installation nucléaire destinée à la production industrielle d'électricité qui servent au transport de l'électricité.

Art. 5

§ 1er. La présente loi est sans préjudice de la loi du 1er juillet 2011 relative à la sécurité et à la protection des

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 2011/93/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.

§ 2. Deze wet doet geen afbreuk aan de verplichte beveiligingsmaatregelen voor netwerk- en informatiesystemen die geclassificeerde informatie verwerken, in de zin van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, of 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° “CCB”: het Centrum voor Cybersecurity België opgericht bij het koninklijk besluit van 10 oktober 2014;

2° “sectorale overheid”: de overheid bedoeld in bijlage IV van de wet of aangewezen door de Koning bij in Ministerraad overlegd besluit;

3° “ADCC”: de Algemene Directie Crisiscentrum van de Federale Overheidsdienst Binnenlandse Zaken, opgericht bij het koninklijk besluit van 18 april 1988 tot oprichting van het Coördinatie- en Crisiscentrum van de regering;

4° “nationaal CSIRT “: het Computer Security Incident Response Team, belast met de coördinatie op nationaal en internationaal niveau van het beheer van computerbeveiligingsincidenten voor de in de wet bedoelde aanbieders en diensten;

5° “sectoraal CSIRT”: dienst van de sectorale overheid waarvan de taken bedoeld worden in bijlage I van deze wet;

6° “BELAC”: de accreditatie-instelling opgericht bij het koninklijk besluit van 31 januari 2006 tot oprichting van het BELAC-accreditatiesysteem van instellingen voor de conformiteitsbeoordeling;

7° “instelling voor de conformiteitsbeoordeling”: instelling bedoeld in artikel I.9 van het Wetboek van economisch recht

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 2011/93/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.

§ 2. La présente loi est sans préjudice des mesures de sécurité imposées aux systèmes et réseaux informatiques traitant des informations classifiées, au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, ou des 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° “CCB”: le Centre pour la Cybersécurité Belgique créé par l’arrêté royal du 10 octobre 2014;

2° “autorité sectorielle”: l’autorité publique reprise à l’annexe IV de la loi, ou désignée par le Roi, par arrêté délibéré en Conseil des ministres;

3° “DGCC”: la Direction générale Centre de Crise du Service public fédéral Intérieur, créée par l’arrêté royal du 18 avril 1988 portant création du Centre gouvernemental de Coordination et de Crise;

4° “CSIRT national”: le centre de réponse aux incidents de sécurité informatique, chargé de la coordination, au niveau national et international, de la gestion des incidents de sécurité informatique pour les opérateurs et les services visés par la loi;

5° “CSIRT sectoriel”: service de l’autorité sectorielle dont les tâches sont visées à l’annexe I de la présente loi;

6° “BELAC”: l’organisme d’accréditation créé par l’arrêté royal du 31 janvier 2006 portant création du système BELAC d’accréditation des organismes d’évaluation de la conformité;

7° “organisme d’évaluation de la conformité”: organisme visé à l’article I.9 du Code de droit économique et qui effectue

die conformiteitsbeoordelingsactiviteiten verricht, zoals onder meer kalibratie, proeven, certificatie en keuring;

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 punten 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 en 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 voldoet aan de criteria bedoeld in artikel 11, § 2;

12° “incident”: elke gebeurtenis met een reële negatieve impact op de beveiliging van netwerk- en informatiesystemen;

13° “incidentenbehandeling”: alle procedures ter ondersteuning van de opsporing, analyse en beheersing van en reactie op een incident;

14° “risico”: elke redelijkerwijs vast te stellen omstandigheid of gebeurtenis met een mogelijke negatieve impact op de beveiliging van netwerk- en informatiesystemen;

15° “intersectoraal criterium”: factor die gemeenschappelijk is voor alle sectoren bedoeld in bijlage II van deze wet en die het belang van een verstorend effect voor de verlening van een essentiële dienst in de zin van artikel 11, § 2, c bepaalt;

16° “sectoraal criterium”: factor die eigen is aan een sector of deelsector bedoeld in bijlage II van deze wet en die het belang van een verstorend effect voor de verlening van een essentiële dienst in de zin van artikel 11, § 2, c bepaalt;

des opérations d’évaluation de la conformité, comme l’étalonnage, les essais, la certification et l’inspection;

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 qui répond aux critères visés à l’article 11, § 2;

12° “incident”: tout événement ayant un impact négatif réel sur la sécurité des réseaux et des systèmes d’information;

13° “gestion d’incident”: toutes les procédures utiles à la détection, à l’analyse et au confinement d’un incident et toutes les procédures utiles à l’intervention en cas d’incident;

14° “risque”: toute circonstance ou tout événement raisonnablement identifiable ayant un impact négatif potentiel sur la sécurité des réseaux et des systèmes d’information;

15° “critère intersectoriel”: facteur commun à tous les secteurs visés à l’annexe II de la présente loi et déterminant l’importance d’un effet perturbateur sur la fourniture d’un service essentiel au sens de l’article 11, § 2, c;

16° “critère sectoriel”: facteur propre à un secteur ou sous-secteur visé à l’annexe II de la présente loi et déterminant l’importance d’un effet perturbateur sur la fourniture d’un service essentiel au sens de l’article 11, § 2, c;

17° “beveiligingsbeleid voor de netwerk- en informatiesystemen” (I.B.B.): een document als bedoeld in artikel 14, § 2, van deze wet met de maatregelen voor de beveiliging van de netwerk- en informatiesystemen die de aanbieders van essentiële diensten of de digitaledienstverleners hebben genomen;

18° “contactpunt voor de beveiliging van de netwerk- en informatiesystemen”: is het contactpunt aangewezen door de aanbieders van essentiële diensten of de digitaledienstverleners dat de functie van contactpunt uitoefent ten aanzien van de sectorale overheid, het CCB en de ADCC, voor elke vraag in verband met de beveiliging van de netwerk- en informatiesystemen waarvan de verleende essentiële diensten afhankelijk zijn.

19° “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 III;

20° “digitaledienstverlener”: elke rechtspersoon die een digitale dienst aanbiedt als bedoeld in bijlage III van deze wet;

21° “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 het CCB of de bevoegde sectorale overheid kan worden gecontacteerd in plaats van de digitaledienstverlener, wat de uit deze wet voortvloeiende verplichtingen betreft;

22° “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;

23° “domeinnaamsysteem” of “DNS”: een hiërarchisch opgebouwd adresseringssysteem in een netwerk dat een zoekvraag naar een domeinnaam beantwoordt;

24° “DNS-dienstverlener”: een entiteit die DNS-diensten op het internet verleent;

25° “register voor topleveldomeinnamen”: een entiteit die de internetdomeinnamen van een specifiek topleveldomein registreert en beheert;

26° “onlinemarktplaats”: een digitale dienst die het consumenten, zoals gedefinieerd in artikel I.1., 2°, van het Wetboek van economisch recht, en/of ondernemers, zoals gedefinieerd in artikel I.8, 39°, van hetzelfde Wetboek, mogelijk maakt online verkoop- of dienstenovereenkomsten met ondernemers

17° “politique de sécurité des systèmes et réseaux d’information” (P.S.I.): un document visé à l’article 14, § 2 de la présente loi, reprenant les mesures de sécurité des réseaux et des systèmes d’information adoptées par un opérateur de services essentiels ou par un fournisseur de service numérique;

18° “point de contact pour la sécurité des systèmes et réseaux d’information”: est 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 de l’autorité sectorielle, du CCB, et de la DGCC pour toute question liée à la sécurité des réseaux et des systèmes d’information dont sont tributaires les services essentiels fournis.

19° “service numérique”: un service au sens de l’article 1er, paragraphe 1, 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 III;

20° “fournisseur de service numérique”: une personne morale qui fournit un service numérique visé à l’annexe III de la présente loi;

21° “représentant d’un fournisseur de service numérique”: une personne physique ou morale établie en Belgique qui est expressément désignée pour agir pour le compte d’un fournisseur de service numérique non établi dans l’Union, qui peut être contactée par le CCB ou l’autorité sectorielle compétente à la place du fournisseur de service numérique concernant ses obligations découlant de la présente loi;

22° “point d’échange internet (IXP)”: une structure de réseau qui permet l’interconnexion de plus de deux systèmes autonomes indépendants, essentiellement aux fins de faciliter l’échange de trafic internet; un IXP n’assure l’interconnexion que pour des systèmes autonomes; un IXP n’exige pas que le trafic internet passant entre une paire quelconque de systèmes autonomes participants transite par un système autonome tiers, pas plus qu’il ne modifie ou n’altère par ailleurs un tel trafic;

23° “système de noms de domaine (DNS)”: un système hiérarchique et distribué d’affectation de noms dans un réseau qui résout les questions liées aux noms de domaines;

24° “fournisseur de services DNS”: une entité qui fournit des services DNS sur l’internet;

25° “registre de noms de domaine de haut niveau”: une entité qui administre et gère l’enregistrement de noms de domaine internet dans un domaine de haut niveau donné;

26° “place de marché en ligne”: un service numérique qui permet à des consommateurs au sens de l’article I.1., 2° du Code de droit économique et/ou à des professionnels, au sens de l’article I.8, 39° du même Code, de conclure des contrats de vente ou de service en ligne avec des professionnels,

te sluiten op de website van de onlinemarktplaats of op de website van een ondernemer die gebruikmaakt van door de onlinemarktplaats aangeboden informaticadiensten;

27° "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;

28° "cloudcomputerdienst": een digitale dienst die toegang mogelijk maakt tot een schaalbare en elastische pool van deelbare computercapaciteit;

29° "certificeringsaudit": een audit uitgevoerd door een instelling voor de conformiteitsbeoordeling bedoeld in artikel 6, 7°, die, overeenkomstig artikel 21, § 3, van deze wet, geaccrediteerd is door BELAC of door een instelling die de erkenningsakkoorden van de "European Cooperation for Accreditation" medeondertekend heeft.

HOOFDSTUK 3

**Bevoegde autoriteiten en samenwerking op nationaal niveau**

**Afdeling 1**

*Bevoegde autoriteiten*

Art. 7

§ 1. Het CCB is, als nationale autoriteit, belast met de opvolging en de coördinatie van de uitvoering van deze wet.

§ 2. De sectorale overheden zijn, voor hun respectievelijke sector, belast met het toezicht op de uitvoering van de bepalingen van deze wet.

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

§ 3. Het CCB wordt aangewezen als centraal nationaal contactpunt inzake de beveiliging van de netwerk- en informatiesystemen, hierna "NIS-contactpunt" genoemd, voor het geheel van de aanbieders van essentiële diensten en digitaledienstverleners, voor België in zijn relatie met de Europese Commissie, de lidstaten van de Europese Unie, de Samenwerkingsgroep en het CSIRT-netwerk. Daartoe vertegenwoordigt het België binnen de Samenwerkingsgroep bedoeld in artikel 11 van de NIS-richtlijn.

§ 4. Het CCB oefent de functie van nationaal CSIRT uit om meldingen van incidenten door aanbieders van essentiële

soit sur le site internet de la place de marché en ligne, soit sur le site internet d'un professionnel qui utilise les services informatiques fournis par la place de marché en ligne;

27° "moteur de recherche en ligne": un service numérique qui permet aux utilisateurs d'effectuer des recherches sur, en principe, tous les sites internet ou sur les sites internet dans une langue donnée, sur la base d'une requête lancée sur n'importe quel sujet sous la forme d'un mot clé, d'une phrase ou d'une autre entrée, et qui renvoie des liens à partir desquels il est possible de trouver des informations en rapport avec le contenu demandé;

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

29° "audit de certification": un audit réalisé par un organisme d'évaluation de la conformité visé à l'article 6, 7° et accrédité, conformément à l'article 21, § 3 de la présente loi, par BELAC ou par une institution qui est co-signataire des accords de reconnaissance du "European Cooperation for Accreditation".

CHAPITRE 3

**Autorités compétentes et coopération au niveau national**

**Section 1re**

*Autorités compétentes*

Art. 7

§ 1er. Le CCB est chargé, au titre d'autorité nationale, du suivi et de la coordination de la mise en œuvre de la présente loi.

§ 2. Les autorités sectorielles sont chargées, pour leur secteur respectif, de veiller à la mise en œuvre des dispositions de la présente loi.

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.

§ 3. Le CCB est désigné comme point de contact national unique en matière de sécurité des réseaux et des systèmes d'information, ci-après dénommé "point de contact NIS" 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 et le réseau des CSIRT. A cette fin, il représente la Belgique au sein du Groupe de coopération visé à l'article 11 de la directive NIS.

§ 4. Le CCB exerce la fonction de CSIRT national afin de recevoir les notifications d'incidents des opérateurs de

diensten en digitaledienstverleners te ontvangen. Het ontvangt ook de meldingen van incidenten in andere landen.

§ 5. Ter ondersteuning van het nationale CSIRT kan elke sectorale overheid ervoor kiezen om een sectoraal CSIRT uit te bouwen, mits naleving van de verplichtingen bedoeld in bijlage I van deze wet.

§ 6. Het CCB 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.

**Afdeling 2**

*Samenwerking op nationaal niveau*

Art. 8

§ 1. Het CCB, de ADCC en de sectorale overheden werken nauw samen om de in deze wet vastgestelde verplichtingen te vervullen.

§ 2. Naargelang de behoeften en overeenkomstig de toepasselijke wettelijke bepalingen werken de overheden bedoeld in het eerste lid ook samen met, onder meer, de diensten van het Openbaar Ministerie, de politie en de Gegevensbeschermingsautoriteit.

HOOFDSTUK 4

**Informatie-uitwisseling**

Art. 9

§ 1. Onverminderd de wettelijke bepalingen die de vertrouwelijkheid van de informatie m.b.t. de wezenlijke belangen van de openbare veiligheid waarborgen, mag de informatie uitgewisseld in het kader van deze wet met de autoriteiten van de Europese Unie en buitenlandse of nationale autoriteiten worden uitgewisseld wanneer die uitwisseling noodzakelijk is voor de toepassing van deze wet.

De uitgewisselde informatie wordt beperkt tot hetgeen relevant is voor en evenredig is met het doel van die uitwisseling. Bij die uitwisseling van informatie wordt de vertrouwelijkheid van de informatie gewaarborgd en worden de veiligheids- en commerciële belangen van aanbieders van essentiële diensten en digitaledienstverleners beschermd.

Met inachtneming van het eerste en tweede lid wordt, voor de toepassing van deze wet, afgeweken van de door andere wetgeving opgelegde verplichtingen inzake het beroepsgeheim.

§ 2. De sectorale overheid, de inspectiedienst, het CCB en de ADCC beperken de toegang tot de informatie bedoeld in de titels 2 en 3 en tot de informatie die hun wordt toevertrouwd door de aanbieders van essentiële diensten of de digitaledienstverleners, tot de personen die er de kennis van nodig

services essentiels et des fournisseurs de service numérique. Il reçoit également les notifications d'incidents d'autres États.

§ 5. En appui du CSIRT national, chaque autorité sectorielle peut choisir de développer un CSIRT sectoriel, moyennant le respect des obligations visées à l'annexe I de la présente loi.

§ 6. Le CCB 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.

**Section 2**

*Coopération au niveau national*

Art. 8

§ 1er. Le CCB, la DGCC et les autorités sectorielles coopèrent étroitement aux fins du respect des obligations énoncées dans la présente loi.

§ 2. En fonction des besoins et conformément aux dispositions légales applicables, les autorités visées à l'alinéa 1 coopèrent également, entre autres, avec les services du Ministère public, de la police et de l'Autorité de protection des données.

CHAPITRE 4

**Echanges d'information**

Art. 9

§ 1er. Sous réserve des dispositions légales garantissant la confidentialité des informations liées aux intérêts essentiels de la sécurité publique, les informations échangées dans le cadre de la présente loi peuvent faire l'objet d'un échange avec des autorités de l'Union européenne, avec des autorités étrangères ou nationales, lorsque cet échange est nécessaire à l'application de la présente loi.

Les informations échangées se limitent au minimum nécessaire et sont proportionnées à l'objectif de cet échange. 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.

Dans le respect des alinéas 1er et 2, il est dérogé, pour l'exécution de la présente loi, aux obligations de secret professionnel imposés par d'autres législations.

§ 2. L'autorité sectorielle, le service d'inspection, le CCB et la DGCC limitent l'accès aux informations visées aux titres 2 et 3 et aux informations qui leur sont confiées par l'opérateur de services essentiels ou le fournisseur de service numérique, aux personnes ayant besoin d'en connaître et d'y avoir accès

hebben en er toegang toe moeten hebben voor de uitoefening van hun functie of opdracht die verband houdt met deze wet.

§ 3. Onverminderd andere strengere wettelijke bepalingen moeten de aanbieder van essentiële diensten, zijn medewerkers en onderaannemers de toegang tot de inhoud van de maatregelen in het I.B.B. beperken tot de personen die er de kennis van nodig hebben en er toegang toe moeten hebben voor de uitoefening van hun functie in het kader van hun activiteit voor de aanbieder van essentiële diensten of opdracht die verband houdt met deze wet. Ze zijn gebonden aan het beroepsgeheim wat deze informatie betreft.

§ 4. De aanbieder van essentiële diensten, de digitaledienstverlener, het CCB, de sectorale overheid, de inspectiedienst en de ADCC werken te allen tijde samen door een adequate informatie-uitwisseling betreffende de beveiliging van de netwerk- en informatiesystemen.

HOOFDSTUK 5

**Nationale strategie voor de beveiliging van netwerk- en informatiesystemen**

Art. 10

§ 1. Na raadpleging van het CCB, de ADCC, de sectorale overheden en de Gegevensbeschermingsautoriteit keurt de Koning, bij in Ministerraad overlegd besluit, de nationale strategie voor de beveiliging van netwerk- en informatiesystemen goed. In deze strategie worden passende strategische en regelgevingsdoelstellingen bepaald om een hoog beveiligingsniveau van de netwerk- en informatiesystemen tot stand te brengen en te handhaven. Ze moet minstens betrekking hebben op de in bijlage II van deze wet bedoelde sectoren en de in bijlage III van deze wet bedoelde diensten.

§ 2. 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;

pour l'exercice de leurs fonctions ou de leur mission en lien avec la présente loi.

§ 3. Sans préjudice d'autres dispositions légales plus contraignantes, l'opérateur de services essentiels, ses agents et ses sous-traitants ne peuvent donner accès au contenu des mesures figurant dans la P.S.I. qu'aux personnes qui ont besoin d'en connaître et d'y avoir accès pour l'exercice de leurs fonctions dans le cadre de leur activité pour l'opérateur de services essentiels ou de leur mission en lien avec la présente la loi. Ils sont tenus au secret professionnel en ce qui concerne ces informations.

§ 4. L'opérateur de services essentiels, le fournisseur de service numérique, le CCB, l'autorité sectorielle, le service d'inspection et la DGCC collaborent en tout temps, par un échange adéquat d'informations concernant la sécurité des systèmes et réseaux d'informations.

CHAPITRE 5

**Stratégie nationale en matière de sécurité des réseaux et des systèmes d'information**

Art. 10

§ 1er. Après consultation du CCB, de la DGCC, des autorités sectorielles et de l'Autorité de protection des données, le Roi adopte, par arrêté délibéré en Conseil des ministres, la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information qui 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 et de couvrir au moins les secteurs visés à l'annexe II et les services visés à l'annexe III de la présente loi.

§ 2. 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 rôles et les responsabilités des organismes publics et des autres acteurs pertinents;

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

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

e) 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 potentiële aanbieders van essentiële diensten van haar sector en houdt hierbij minstens rekening met de soorten aanbieders in bijlage II van deze wet en met de door hen verleende essentiële diensten.

Binnen de grenzen van hun respectievelijke bevoegdheden overleggen het CCB en de ADCC met e sectorale overheid om over te gaan tot deze identificatie.

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

§ 2. Om de in paragraaf 1 bedoelde aanbieders te identificeren, moet de sectorale overheid de volgende criteria toepassen:

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 zou aanzienlijke verstorende effecten hebben voor de verlening van die dienst;

d) de in § 4 bedoelde criteria en weerslagniveaus of drempelwaarden.

Voor een identificatie volstaat het dat de potentiële aanbieder van essentiële diensten minstens aan een van de vastgestelde criteria, drempelwaarden of weerslagniveaus voldoet.

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

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 potentiels de son secteur, en prenant au minimum en compte les types d'opérateurs qui figurent à l'annexe II de la présente loi, et les services essentiels qu'ils fournissent.

Dans les limites de leurs compétences respectives, le CCB et la DGCC se concertent avec l'autorité sectorielle pour procéder à cette identification.

L'autorité sectorielle consulte, le cas échéant, les régions et/ou les communautés concernées et les représentants des entités visées à l'annexe II.

§ 2. Pour identifier les opérateurs visés au paragraphe 1er, l'autorité sectorielle doit appliquer 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 aurait un effet perturbateur important sur la fourniture dudit service;

d) les critères et les niveaux d'incidence ou les seuils visés au § 4.

Pour ce faire, il suffit que l'opérateur de services essentiels potentiel réponde au moins soit à un critère, soit un seuil et soit un niveau d'incidence fixé pour être identifié.

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

§ 4. Om het belang van het in artikel 11, § 2, c), bedoelde verstorende effect te bepalen, stelt de sectorale overheid sectorale of intersectorale criteria, weerslagniveaus of drempelwaarden vast.

Binnen de grenzen van hun respectievelijke bevoegdheden overleggen het CCB en de ADCC met de sectorale overheid om over te gaan tot deze vaststelling, na raadpleging, in voorkomend geval, van de betrokken gewesten en/of gemeenschappen en van de vertegenwoordigers van de in bijlage II bedoelde entiteiten.

§ 5. De sectorale overheid houdt minstens rekening met de volgende intersectorale criteria:

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

b) de afhankelijkheid van de andere in bijlage II 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.

Na raadpleging van het CCB en de ADCC kan de Koning deze intersectorale criteria aanvullen na raadpleging van de sectorale overheden, de gewesten en gemeenschappen.

§ 6. De potentiële aanbieder van essentiële diensten bezorgt de sectorale overheid, op haar verzoek of op verzoek van het CCB of de ADCC, 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 sectorale overheid maakt de door de potentiële aanbieder meegedeelde relevante informatie over aan het CCB en de ADCC.

§ 7. De sectorale overheid bezorgt het CCB en de ADCC een gemotiveerd voorstel van lijst van potentiële aanbieders van essentiële diensten in haar sector, samen met een of meer toegepaste identificatiecriteria.

Wanneer geen enkele potentiële aanbieder van essentiële diensten is geïdentificeerd binnen een sector of deelsector, licht de sectorale overheid de redenen hiervoor schriftelijk toe.

Het CCB en de ADCC brengen, binnen de grenzen van hun respectievelijke bevoegdheden, advies uit over het

§ 4. Afin de déterminer l'importance de l'effet perturbateur visé à l'article 11, § 2, c), l'autorité sectorielle établit des critères sectoriels ou intersectoriels, des niveaux d'incidence ou des seuils.

Dans les limites de leurs compétences respectives, le CCB et la DGCC se concertent avec l'autorité sectorielle pour procéder à cette détermination après consultation, le cas échéant, des régions et/ou des communautés concernées et des représentants des entités visés à l'annexe II.

§ 5. L'autorité sectorielle prend en compte, au moins les critères intersectoriels suivants:

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

b) la dépendance des autres secteurs visés à l'annexe II 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) la portée géographique eu égard à la zone 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.

Après consultation du CCB et de la DGCC, le Roi peut compléter ces critères intersectoriels, après consultation des autorités sectorielles, des régions et des communautés.

§ 6. L'opérateur de services essentiels potentiel transmet à l'autorité sectorielle, à la demande de celle-ci, du CCB ou de la DGCC, 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 communiquées par l'autorité sectorielle au CCB et à la DGCC.

§ 7. L'autorité sectorielle communique au CCB et à la DGCC une proposition motivée de liste des opérateurs de services essentiels potentiels dans son secteur avec le ou les critères d'identification retenus.

Lorsqu'aucun opérateur de services essentiels potentiel n'a été identifiée au sein d'un secteur ou d'un sous-secteur, l'autorité sectorielle en expose par écrit les raisons.

Le CCB et la DGCC, dans les limites de leurs compétences respectives, rendent un avis sur la proposition motivée de

gemotiveerde voorstel van lijst, in voorkomend geval na raadpleging van de gewesten en gemeenschappen.

§ 8. Wanneer de sectorale overheid vaststelt dat de aanbieder van essentiële diensten een of meer essentiële diensten in minstens één andere lidstaat van de Europese Unie verleent, brengt ze het CCB en de ADCC 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.

§ 9. De sectorale overheid brengt de aanbieder op de hoogte van haar gemotiveerde beslissing betreffende zijn aanwijzing als aanbieder van essentiële diensten. Deze kennisgeving gebeurt op beveiligde wijze. De Koning kan de hierbij toe te passen beveiligingsmaatregelen bepalen.

Ze bezorgt ook een kopie van deze beslissing aan het CCB en de ADCC.

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

§ 10. Binnen de 3 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 het CCB.

§ 11. 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.

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 bijwerkingen worden naar het CCB en de ADCC gestuurd.

§ 12. Onverminderd de toepassing van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen worden de bestuursdocumenten betreffende de toepassing van dit artikel 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.

liste, le cas échéant après consultation des régions et des communautés.

§ 8. Lorsque l'autorité sectorielle constate que l'opérateur de services essentiels fournit un ou des services essentiels dans au moins un autre État membre de l'Union européenne, elle en informe le CCB et la DGCC. 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.

§ 9. 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. Le Roi peut préciser les mesures de sécurité à appliquer à cette notification.

Elle communique également copie de cette décision au CCB et à la DGCC.

L'autorité sectorielle en informe, le cas échéant, les régions et/ou les communautés concernées.

§ 10. Dans les 3 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 au CCB.

§ 11. 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.

Au minimum, l'autorité sectorielle réexamine et, le cas échéant, met à jour l'identification des opérateurs de services essentiels et de leurs services essentiels tous les deux ans.

Les actualisations sont adressées au CCB et à la DGCC.

§ 12. Sans préjudice de l'application de la loi du 11 décembre 1998 relative à la classification, aux habilitations, attestations et avis de sécurité, les documents administratifs liés à l'application du présent article, 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 communiqué sous forme d'une copie pour le public.

Art. 12

§ 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 betreffende de beveiliging en de bescherming van de kritieke infrastructuren 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 II van deze wet en de verlening van hun essentiële diensten afhankelijk is van netwerk- en informatiesystemen.

Deze aanwijzing gebeurt in overleg met het CCB en de ADCC 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 het CCB of de ADCC, 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 maakt de door de exploitant meegedeelde relevante informatie over aan het CCB en de ADCC.

§ 4. Artikel 11, § 9, is van toepassing op de gemotiveerde beslissing tot aanwijzing van een exploitant van kritieke infrastructuur als aanbieder van essentiële diensten.

Art 13

De Koning kan, bij in Ministerraad overlegd besluit, andere sectoren of soorten aanbieders toevoegen aan bijlage II van deze wet.

HOOFDSTUK 2

**Beveiligingsmaatregelen**

Artikel 14

§ 1. 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, gezien de stand van de techniek, voor een niveau van fysieke en logische beveiliging van netwerk- en informatiesystemen dat is afgestemd op de risico's die zich voordoen.

Art. 12

§ 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 relative à la sécurité et à la protection des infrastructures critiques 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 II 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 le CCB et la DGCC 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, du CCB ou de la DGCC, 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 au CCB et à la DGCC.

§ 4. L'article 11, § 9 est applicable à la décision motivée de désignation d'un exploitant d'une infrastructure critique en qualité d'opérateur de services essentiels.

Art. 13

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

CHAPITRE 2

**Mesures de sécurité**

Art. 14

§ 1er. 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.

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.

§ 2. De aanbieder van essentiële diensten werkt een beveiligingsbeleid uit voor zijn netwerk- en informatiesystemen (hierna "I.B.B." genoemd) dat minstens de in de paragrafen 1 en 4 bedoelde concrete beveiligingsdoelstellingen en -maatregelen bevat.

§ 3. 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 in het I.B.B.

§ 4. Op voorstel van de Eerste minister en van de bevoegde ministers kan de Koning beveiligingsmaatregelen opleggen aan de aanbieders van essentiële diensten van verschillende sectoren.

Het voorstel wordt geformuleerd na advies van het CCB, de ADCC, de sectorale overheden en, in voorkomend geval, van de gewesten of gemeenschappen.

De sectorale overheid kan, in overleg met het CCB en, in voorkomend geval, na raadpleging van de gewesten of gemeenschappen, eisen dat de aanbieders van essentiële diensten die tot haar sector of deelsectoren behoren bijkomende beveiligingsmaatregelen naleven.

§ 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 betreffende de beveiliging en de bescherming van de kritieke infrastructuren en in artikel 11 van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer, worden gelijkgesteld met het I.B.B. indien alle in paragraaf 2 bedoelde informatie erin opgenomen is.

Art. 15

Behoudens tegenbewijs geniet de aanbieder van essentiele diensten het vermoeden dat de inhoud van het I.B.B. bedoeld in artikel 14, § 2, conform is, wanneer zijn beveiligingsmaatregelen 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, na advies van BELAC, de sectorale overheid en het CCB.

Het in het vorige lid bedoelde conformiteitsbewijs wordt geleverd aan de hand van een certificaat uitgereikt door een instelling voor de conformiteitsbeoordeling, bedoeld in artikel

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.

§ 2. 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 aux paragraphes 1er et 4.

§ 3. 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.

§ 4. Sur proposition du Premier ministre et des Ministres compétents, le Roi peut imposer certaines mesures de sécurité applicables aux opérateurs de services essentiels de plusieurs secteurs.

La proposition est formulée après avis du CCB, de la DGCC, des autorités sectorielles et, le cas échéant, des régions ou des communautés.

L'autorité sectorielle, en concertation avec le CCB et, le cas échéant, après consultation des régions ou des communautés, peut exiger certaines mesures complémentaires de sécurité aux opérateurs de services essentiels relevant de son secteur ou de ses sous-secteurs.

§ 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 relative à la sécurité et la protection des infrastructures critiques et à l'article 11 de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien sont assimilées à la P.S.I. lorsque toutes les informations visées au paragraphe 2 y sont reprises.

Art. 15

Sauf preuve contraire, l'opérateur de services essentiels bénéficie d'une présomption de conformité du contenu de la PSI visée à l'article 14, § 2, lorsque ses mesures de sécurité répondent aux exigences de la norme ISO/IEC 27001 ou à une norme nationale, étrangère ou internationale reconnue équivalente par le Roi, après avis de BELAC, de l'autorité sectorielle et du CCB.

La preuve de la conformité visée à l'alinéa précédent est fournie par un certificat délivré par un organisme d'évaluation de la conformité, visé à l'article 6, 7° de la présente loi et

6, 7°, van deze wet, die volgens de norm ISO/IEC 17021 of ISO/IEC 17065 geaccrediteerd is door BELAC 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 geaccrediteerd is.

Art. 16

§ 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, alsook na elke bijwerking van deze gegevens.

De sectorale overheid bezorgt deze gegevens aan het CCB en de ADCC.

§ 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 in paragraaf 1 bedoelde sectorale overheid.

§ 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. 17

§ 1. De aanbieder van essentiële diensten meldt het nationale CSIRT, de sectorale overheid of haar sectorale CSIRT, en de ADCC onverwijld alle incidenten die een aanzienlijke impact hebben op de beschikbaarheid, vertrouwelijkheid, integriteit of authenticiteit van de informatiesystemen waarvan de door hem verleende essentiële dienst of diensten afhankelijk zijn.

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.

§ 2. Dit artikel 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.

§ 3. Aanbieders die behoren tot de sector financiën in de zin van bijlage II van de wet, met uitzondering van de exploitanten van een handelsplatform, melden beveiligingsincidenten onverwijld aan de Nationale Bank van België. Deze laatste

accrédité selon la norme ISO/IEC 17021 ou ISO/IEC 17065 par BELAC ou par une institution qui est co-signataire des accords de reconnaissance du "*European Cooperation for Accreditation*".

Le certificat délivré doit être dans le domaine de certification pour lequel l'organisme est accrédité.

Art. 16

§ 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, ainsi qu'après chaque mise à jour de ces données.

L'autorité sectorielle transmet ces données au CCB et à la DGCC.

§ 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 visée 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. 17

§ 1er. L'opérateur de services essentiels notifie au CSIRT national, à l'autorité sectorielle ou à son CSIRT sectoriel, et à la DGCC, sans retard injustifié, tous les incidents ayant un impact significatif sur la disponibilité, la confidentialité, l'intégrité ou l'authenticité des systèmes d'information dont sont tributaires le ou les services essentiels qu'il fournit.

L'obligation de notifier 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.

§ 2. Le présent article 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.

§ 3. Les opérateurs relevant des secteur des finances au sens de l'annexe II de la loi, à l'exception des opérateurs de plate-forme de négociation, notifient, sans retard injustifié, les incidents de sécurité à la Banque nationale de Belgique. Cette

bezorgt de melding vervolgens onverwijld aan het nationale CSIRT en de ADCC.

§ 4. Wanneer een aanbieder van essentiële diensten afhankelijk is van een derde digitaledienstverlener, meldt de aanbieder van essentiële diensten alle gevallen waarin een incident bij zijn digitaledienstverlener aanzienlijke gevolgen heeft voor de beschikbaarheid, vertrouwelijkheid, integriteit of authenticiteit van de informatiesystemen waarvan de door hem verleende essentiële dienst of diensten afhankelijk zijn, en dit volgens de in dit artikel beschreven procedures.

§ 5. De Koning is belast met de oprichting van een gemeenschappelijk en beveiligd meldingsplatform om de uitvoering en verwerking van de meldingen te vergemakkelijken die deze wet oplegt aan de aanbieders van essentiële diensten en digitaledienstverleners.

Op voorstel van de Eerste minister, de bevoegde ministers en na advies van de Gegevensbeschermingsautoriteit kan de Koning in dit platform ook de meldingen opnemen van aanbieders van essentiële diensten en digitaledienstverleners, opgelegd door 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.

§ 6. De Koning kan specifieke modaliteiten voor de melding en rapportering van incidenten bepalen.

§ 7. Op voorstel van de bevoegde minister kan de Koning, per sector of deelsector, de weerslagniveaus of de drempelwaarden bepalen die noodzakelijkerwijs een aanzienlijke impact hebben in de zin van paragraaf 1.

Het voorstel van koninklijk besluit wordt geformuleerd na advies van het nationale CSIRT, de ADCC, de sectorale overheid en, in voorkomend geval, van de betrokken gewesten of gemeenschappen.

TITEL 3

*Netwerk- en informatiesystemen van digitaledienstverleners*

Art. 18

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).

dernière transmet alors la notification, sans retard injustifié, au CSIRT national et à la DGCC.

§ 4. Lorsqu'un opérateur de services essentiels s'appuie sur un tiers fournisseur de service numérique, l'opérateur de services essentiels notifie tout incident ayant un impact significatif sur la disponibilité, la confidentialité, l'intégrité ou l'authenticité des systèmes d'information dont sont tributaires le ou les services essentiels qu'il fournit, en raison d'un incident touchant son fournisseur de service numérique, selon les procédures décrites au présent article.

§ 5. Le Roi est chargé de créer une plate-forme commune et sécurisée de notification afin de faciliter la mise en œuvre et le traitement des notifications imposées aux opérateurs de services essentiels et aux fournisseurs de service numérique par la présente loi.

Sur proposition du Premier ministre, des Ministres compétents, et après avis de l'Autorité de protection des données, le Roi peut inclure dans cette plate-forme les notifications faites par les opérateurs de services essentiels et les fournisseurs de service numérique, imposés par le 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.

§ 6. Le Roi peut déterminer des modalités particulières de notification et de rapportage des incidents.

§ 7. Sur proposition du ministre compétent, le Roi peut établir des niveaux d'incidence ou des seuils, par secteur ou sous-secteur, constituant nécessairement un impact significatif au sens du paragraphe 1er.

La proposition d'arrêté royal est formulée après avis du CSIRT national, de la DGCC, de l'autorité sectorielle et, le cas échéant, des régions ou des communautés concernées.

TITRE 3

*Réseaux et systèmes d'information des fournisseurs de service numérique*

Art. 18

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).

HOOFDSTUK 1

**De beveiligingseisen**

Art. 19

§ 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 III bedoelde diensten en nemen passende en evenredige technische en organisatorische maatregelen om die risico's te beheersen.

Deze maatregelen zorgen, gezien de stand van de techniek, 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 III 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.

§ 3. De digitaledienstverleners duiden een contactpunt aan voor de informatiebeveiliging en delen de gegevens ervan mee aan de sectorale overheid die bevoegd is voor de digitaledienstverleners, alsook na elke bijwerking van deze gegevens. De sectorale overheid bezorgt deze informatie aan het CCB.

HOOFDSTUK 2

**Melding van incidenten**

Art. 20

§ 1. De digitaledienstverleners melden ieder incident dat aanzienlijke gevolgen heeft voor de verlening van een door hen in de Europese Unie aangeboden dienst als bedoeld in bijlage III, onverwijld aan het nationale CSIRT, de sectorale overheid of haar sectorale CSIRT. 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.

§ 2. De melding gebeurt overeenkomstig de uitvoeringsverordeningen van de Europese Commissie, waaronder de

CHAPITRE 1ER

**Les exigences de sécurité**

Art. 19

§ 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 III et prennent les mesures techniques et organisationnelles nécessaires et proportionnées pour les gérer.

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

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 III de la présente loi qui sont offerts dans l'Union européenne, de manière à garantir la continuité de ces services.

§ 3. 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 au CCB.

CHAPITRE 2

**Notification d'incidents**

Art. 20

§ 1er. Les fournisseurs de service numérique notifient au CSIRT national, à l'autorité sectorielle ou à son CSIRT sectoriel, sans retard injustifié, tout incident ayant un impact significatif sur la fourniture d'un service visé à l'annexe III qu'ils offrent, dans l'Union européenne. Les notifications contiennent des 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.

§ 2. La notification se fait conformément aux règlements d'exécution de la Commission européenne, dont celui du

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.

§ 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.

§ 4. Deze melding gebeurt overeenkomstig de door de Koning bepaalde modaliteiten en via het platform bedoeld in artikel 17, § 5, van deze wet.

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

§ 6. Wanneer publieke bewustwording nodig is om een incident te voorkomen of een lopend incident te beheersen, of wanneer de openbaarmaking van het incident anderszins in het algemeen belang is, kunnen het CCB en, in voorkomend geval, de autoriteiten of CSIRT's van andere betrokken lidstaten van de Europese Unie na overleg met de betrokken digitaledienstverlener het publiek informeren over afzonderlijke incidenten of verlangen dat de digitaledienstverlener dit doet.

TITEL 4

*Toezicht en sancties*

HOOFDSTUK 1

**Toezicht op de aanbieders van essentiële diensten**

**Afdeling 1**

*Audits*

Art. 21

§ 1. De aanbieder van essentiële diensten realiseert, jaarlijks en op zijn kosten, een interne audit 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.

30 janvier 2018 (UE) 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.

§ 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.

§ 4. Cette notification est réalisée conformément aux modalités prévues par le Roi et via la plate-forme visée à l'article 17, § 5 de la présente loi.

§ 5. Lorsque c'est approprié, et notamment si l'incident visé au paragraphe 1 concerne au moins un autre État membre de l'Union européenne, le CCB informe le ou les autres États membres touchés. Ce faisant, le CCB 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.

§ 6. Après avoir consulté le fournisseur de service numérique concerné, le CCB et, lorsque c'est approprié, les autorités ou les CSIRT des autres États membres de l'Union européenne concernés peuvent informer le public d'incidents particuliers ou imposer au fournisseur de service numérique de le faire, dans le cas où la sensibilisation du public est nécessaire pour prévenir un incident ou pour gérer un incident en cours, ou lorsque la divulgation de l'incident est dans l'intérêt public à d'autres égards.

TITRE 4

*Contrôle et sanctions*

CHAPITRE 1ER

**Les contrôles des opérateurs de services essentiels**

**Section 1re**

*Audits*

Art. 21

§ 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.

De sectorale overheid kan, in overleg met het CCB, de inhoud en de overige regels die van toepassing zijn op deze interne audit bepalen.

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

§ 2. Certificeringsaudits of interne audits uitgevoerd bij aanbieders van essentiële diensten die het in artikel 15 van de wet bedoelde vermoeden genieten, kunnen door de inspectiedienst of de sectorale overheid worden gelijkgesteld met de verplichte jaarlijkse interne audit bedoeld in paragraaf 1. De verslagen van deze audits worden binnen de dertig dagen door de aanbieder van essentiële diensten aan de sectorale overheid bezorgd.

§ 3. De aanbieder van essentiële diensten laat, minstens om de drie jaar en op zijn kosten, een externe audit uitvoeren door een geaccrediteerde of door de sectorale overheid erkende instelling voor de conformiteitsbeoordeling als bedoeld in artikel 6, 7°.

De in het vorige lid bedoelde accreditatie is een accreditatie van de in artikel 6, 7°, bedoelde instelling voor de conformiteitsbeoordeling die wordt uitgereikt door BELAC of door een instelling die de erkenningsakkoorden van de "*European Cooperation for Accreditation*" medeondertekend heeft en die aan de minimumeisen van de ISO/IEC 17021 of ISO/IEC 17065 en aan eventuele bijkomende sectorale eisen voldoet.

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

De sectorale overheid bepaalt, in overleg met het CCB, de bijkomende sectorale eisen waaraan de in artikel 6, 7°, bedoelde instelling voor de conformiteitsbeoordeling onderworpen kan zijn en de regels die van toepassing zijn op de externe audit.

De Koning bepaalt, bij in Ministerraad overlegd besluit, de voorwaarden en modaliteiten van de eventuele erkenning bedoeld in het eerste lid die door de sectorale overheid aan de instelling voor de conformiteitsbeoordeling wordt verleend.

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

§ 4. Certificeringsaudits uitgevoerd bij aanbieders van essentiële diensten die het in artikel 15 van de wet bedoelde vermoeden genieten, kunnen door de inspectiedienst of de sectorale overheid worden gelijkgesteld met de verplichte externe audit bedoeld in paragraaf 3. De verslagen van deze audits worden binnen de dertig dagen door de aanbieder van essentiële diensten aan de sectorale overheid bezorgd.

§ 5. Het CCB kan de sectorale overheid, mits motivering, vragen hem de certificerings- of auditverslagen van een aanbieder van essentiële diensten te bezorgen.

L'autorité sectorielle peut déterminer, en concertation avec le CCB, le contenu et les autres règles applicables à l'audit interne.

L'opérateur de services essentiels transmet les rapports d'audit interne, dans les trente jours, à l'autorité sectorielle.

§ 2. Les audits de certification ou les audits internes réalisés auprès des opérateurs de services essentiels bénéficiant de la présomption visée à l'article 15 de la loi peuvent être assimilés, par le service d'inspection ou l'autorité sectorielle, à l'audit interne annuel obligatoire visé au paragraphe 1. Les rapports de ces audits sont transmis, par l'opérateur de services essentiels, dans les trente jours, à l'autorité sectorielle.

§ 3. 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 visé à l'article 6, 7°, accrédité ou agréé par l'autorité sectorielle.

L'accréditation visée à l'alinéa précédent est une accréditation de l'organisme d'évaluation de la conformité visé à l'article 6, 7° délivrée par BELAC, ou par une institution qui est co-signataire des accords de reconnaissance du "*European Cooperation for Accreditation*", répondant aux exigences minimales de l'ISO/IEC 17021 ou ISO/IEC 17065 et aux éventuelles exigences supplémentaires sectorielles.

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

L'autorité sectorielle détermine, en concertation le CCB, les exigences supplémentaires sectorielles auxquels peut être soumis l'organisme d'évaluation de la conformité visé à l'article 6, 7° et les règles applicables à l'audit externe.

Le Roi détermine, par arrêté délibéré en Conseil des ministres, les conditions et les modalités de l'éventuel agrément visé à l'alinéa 1er et accordé par l'autorité sectorielle à l'organisme d'évaluation de la conformité.

L'opérateur de services essentiels transmet les rapports d'audit externe, dans les trente jours, à l'autorité sectorielle.

§ 4. Les audits de certification réalisés auprès des opérateurs de services essentiels bénéficiant de la présomption visée à l'article 15 de la loi peuvent être assimilés, par le service d'inspection ou l'autorité sectorielle, à l'audit externe obligatoire visé au paragraphe 3. Les rapports de ces audits sont transmis, dans les trente jours, par l'opérateur de services essentiels, à l'autorité sectorielle.

§ 5. Le CCB peut solliciter, de manière motivée, de l'autorité sectorielle la transmission des rapports de certification ou d'audits d'un opérateur de services essentiels.

§ 6. 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.

**Afdeling 2**

*Inspectiedienst*

Art. 22

§ 1. Voor de aanbieders van essentiële diensten wordt per sector of, in voorkomend geval, per deelsector een inspectiedienst opgericht die belast is met het toezicht op de naleving van de bepalingen van deze wet en van de uitvoeringsbesluiten ervan door de aanbieders van essentiële diensten van die sector of deelsector.

De Koning wijst voor een welbepaalde sector of, in voorkomend geval, per deelsector de inspectiedienst aan die bevoegd is voor het toezicht. Hij kan de eventuele sectorale praktische controlemodaliteiten bepalen.

Voor de sector van de digitale infrastructuren wordt het Belgisch Instituut voor postdiensten en telecommunicatie aangewezen als inspectiedienst. De Koning kan de praktische controlemodaliteiten voor deze sector bepalen, na advies van het Instituut.

§ 2. 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.

§ 3. Onverminderd artikel 21 kunnen de inspectiediensten en de sectorale overheden op elk ogenblik grondige controles uitvoeren op de naleving door de aanbieder van essentiële diensten van de beveiligingsmaatregelen en van de regels voor het melden van incidenten.

Het CCB kan de inspectiedienst of de sectorale overheid, mits motivering, aanbevelen om deze controles uit te voeren.

§ 4. De aanbieder van essentiële diensten verleent zijn volledige medewerking aan de leden van de inspectiedienst of de sectorale overheid 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.

§ 5. 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 of van de sectorale overheid op elk ogenblik over de volgende toezichtbevoegdheden bij de uitoefening van

§ 6. 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.

**Section 2**

*Service d'inspection*

Art. 22

§ 1er. Pour les opérateurs de services essentiels, 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 dudit secteur ou sous-secteur.

Le Roi désigne, pour un secteur déterminé ou, le cas échéant, par sous-secteur, le service d'inspection compétent pour effectuer le contrôle. Il peut fixer les éventuelles modalités sectorielles pratiques du contrôle.

Pour le secteur des infrastructures numériques, l'Institut belge pour les services postaux et les télécommunications est désigné en tant que service d'inspection. Le Roi peut fixer les modalités pratiques du contrôle pour ce secteur, après avis de l'Institut.

§ 2. 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.

§ 3. Sans préjudice de l'article 21, les services d'inspection et les autorités sectorielles peuvent à tout moment réaliser des contrôles approfondis du respect par l'opérateur de services essentiels des mesures de sécurité et des règles de notification des incidents.

Le CCB peut recommander, de manière motivée, au service d'inspection ou à l'autorité sectorielle de réaliser des contrôles.

§ 4. L'opérateur de services essentiels apporte son entière collaboration aux membres du service d'inspection ou de l'autorité sectorielle 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.

§ 5. 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 ou de l'autorité sectorielle disposent, à tout moment, des compétences de contrôle suivantes dans l'exercice de leur mission,

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;

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.

Bij het formuleren van een eis tot informatie of bewijs vermeldt de inspectiedienst of de sectorale overheid het doel van de eis en specificeert ze welke informatie moet worden verstrekt.

§ 6. Voor het bekomen van een machtiging tot betreding van bewoonde ruimten richten de leden van de inspectiedienst of de sectorale overheid een met redenen omkleed verzoek aan de onderzoeksrechter. Dit verzoek bevat minstens de volgende gegevens:

— de identificatie van de bewoonde ruimten waartoe de leden van de inspectiedienst of de sectorale overheid toegang wensen te hebben;

— de eventuele inbreuken die het voorwerp zijn van het toezicht;

— alle bescheiden en inlichtingen waaruit blijkt dat het gebruik van dit middel nodig is.

De onderzoeksrechter beslist binnen een termijn van maximum 48 uur na de ontvangst van het verzoek. De beslissing van de onderzoeksrechter is met redenen omkleed.

De bezoeken aan de bewoonde lokalen zonder machtiging van de bewoner gebeuren tussen vijf en eenentwintig uur door minstens twee leden van de inspectiedienst of de sectorale overheid die samen optreden.

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

1° dat zijn verklaringen gebruikt kunnen worden als bewijs in rechte;

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 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.

Au moment de formuler une demande d'informations ou de preuves, le service d'inspection ou l'autorité sectorielle mentionne la finalité de la demande et précise quelles sont les informations exigées.

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

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

— les infractions éventuelles qui font l 'objet du contrôle

— 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.

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 ou de l'autorité sectorielle agissant conjointement.

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

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

2° dat hij mag vragen dat alle vragen die gesteld worden, en zijn antwoorden genoteerd worden met de gebruikte woorden.

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

Het verhoor vermeldt nauwkeurig het tijdstip waarop het begint, eventueel onderbroken en hernomen wordt, en eindigt. Het vermeldt de identiteit van de personen die in het verhoor of in een deel ervan tussenkomen.

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 leden van de inspectiedienst of de sectorale overheid die een persoon ondervragen, informeren hem erover dat hij een kopie mag vragen van de tekst van het verhoor. Deze kopie wordt gratis geleverd.

§ 8. De leden van de inspectiedienst of de sectorale overheid mogen elk informaticasysteem 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 of de sectorale overheid, tegen een ontvangstbewijs dat een inventaris bevat, het informaticasysteem en de erin opgenomen gegevens in beslag nemen.

§ 9. De leden van de inspectiedienst of de sectorale overheid kunnen een beroep doen op experten.

§ 10. Na elke inspectie stelt de inspectiedienst een verslag op en bezorgt een kopie daarvan aan de geïnspecteerde aanbieder van essentiële diensten en aan de bevoegde sectorale overheid.

Als het toezicht wordt verhinderd, kunnen de beëdigde leden van de inspectiedienst de bijstand vorderen van de federale of lokale politiediensten.

§ 11. Wanneer de netwerk- en informatiesystemen van een aanbieder van essentiële diensten zich buiten het Belgische grondgebied bevinden, kan de inspectiedienst of de sectorale overheid, in overleg met het CCB, de bevoegde toezichthouders van deze andere landen om samenwerking en bijstand verzoeken. Deze bijstand en samenwerking kunnen betrekking hebben op informatie-uitwisseling en verzoeken om toezichtmaatregelen.

§ 12. De leden van de inspectiedienst of sectorale overheid waarborgen het vertrouwelijke karakter van de gegevens van

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.

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 ou de l'autorité sectorielle qui interrogent une personne l'informent qu'elle peut demander une copie du texte de son audition. Cette copie lui est délivrée gratuitement.

§ 8. Les membres du service d'inspection ou l'autorité sectorielle 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 ou l'autorité sectorielle peuvent saisir, contre récépissé contenant un inventaire, le système informatique et les données qu'il contient.

§ 9. Les membres du service d'inspection ou de l'autorité sectorielle peuvent faire appel à des experts.

§ 10. Après chaque inspection, le service d'inspection rédige un rapport et en transmet une copie à l'opérateur de services essentiels inspecté et à l'autorité sectorielle compétente.

En cas d'obstacle au contrôle, les membres assermentés du service d'inspection peuvent requérir l'assistance des services de police, fédérale ou locale.

§ 11. 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 ou l'autorité sectorielle, en concertation avec le CCB, 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.

§ 12. Les membres du service d'inspection ou de l'autorité sectorielle garantissent le caractère confidentiel des données

vertrouwelijke aard of bedrijfsgeheimen waarvan ze kennis nemen bij de uitoefening van hun opdracht en zien erop toe dat deze gegevens uitsluitend worden aangewend voor de uitoefening van hun toezichtsopdracht krachtens deze wet.

§ 13. 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.

§ 14. Het CCB kan de inspectiedienst, mits motivering, vragen om zijn inspectieverslagen te bezorgen.

§ 15. Voor iedere sector of deelsector kan de Koning, bij in Ministerraad overlegd besluit 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 berekenings- en betalingsmodaliteiten.

HOOFDSTUK 2

**Toezicht op de digitaledienstverleners**

Art. 23

§ 1. De Koning kan de praktische controlemodaliteiten van de digitaledienstverleners bepalen.

§ 2. De sectorale overheid kan een digitaledienstverlener verplichten:

a) haar, binnen de door haar vastgestelde termijn, de informatie te 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 recht te zetten binnen de door haar vastgestelde termijn.

§ 3. De sectorale overheid kan, 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 sectorale overheid over dezelfde bevoegdheden als deze bedoeld in artikel 22.

§ 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 sectorale overheid, in overleg met het CCB, de bevoegde toezichthouders van deze andere landen om samenwerking en

confidentielles ou des secrets d'entreprise dont ils prennent connaissance dans l'exercice de leur mission et s'assurent que ces données ne seront utilisées que dans l'exercice de leur mission de contrôle en vertu de la présente loi.

§ 13. 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.

§ 14. Le CCB peut solliciter, de manière motivée, du service d'inspection la transmission de ses rapports d'inspection.

§ 15. 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. 23

§ 1er Le Roi peut fixer les modalités pratiques du contrôle des fournisseurs de service numérique

§ 2. L'autorité sectorielle peut imposer à un fournisseur de service numérique:

a) de lui communiquer, dans le délai qu'elle lui fixe, 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 qu'elle lui fixe.

§ 3. L'autorité sectorielle 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, l'autorité sectorielle dispose des mêmes pouvoirs que ceux prévues à l'article 22.

§ 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, l'autorité sectorielle, en concertation avec le CCB, peut solliciter la coopération et l'assistance

bijstand verzoeken. Deze bijstand en samenwerking kunnen betrekking hebben op informatie-uitwisseling en verzoeken om toezichtmaatregelen.

§ 6. De sectorale overheid kan de in dit artikel bedoelde bevoegdheden ook uitoefenen op verzoek van bevoegde overheden van een andere lidstaat van de Europese Unie.

§ 7. Het CCB kan de sectorale overheid vragen hem de controleverslagen van een digitaledienstverlener te bezorgen.

§ 8. De Koning kan, bij in Ministerraad overlegd besluit 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 berekenings- en betalingsmodaliteiten.

HOOFDSTUK 3

**De sancties**

**Afdeling 1**

*Procedure*

Art. 24

§ 1. Wanneer in een inspectieverslag of een externe auditverslag wordt vastgesteld dat een inbreuk is begaan op deze wet of op de uitvoeringsbesluiten ervan, kan de inspectiedienst of de sectorale overheid de betrokken aanbieder van essentiële diensten of digitaledienstverlener in gebreke stellen om zijn verplichtingen na te komen binnen een door deze dienst of overheid 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.

Het CCB kan, mits motivering, de inspectiedienst of de sectorale overheid ook aanbevelen om de aanbieder van essentiële diensten of digitaledienstverlener in gebreke te stellen.

§ 2. Als de inspectiedienst vaststelt dat de aanbieder van essentiële diensten of digitaledienstverlener geen gevolg geeft aan de ingebrekestelling binnen de gestelde termijn, worden de feiten vastgesteld in een proces-verbaal door de beëdigde leden van de inspectiedienst of de sectorale overheid.

§ 3. 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 of de sectorale overheid.

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. L'autorité sectorielle 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. Le CCB peut solliciter de l'autorité sectorielle la transmission des rapports de contrôle 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. 24

§ 1er. Lorsqu'un rapport d'inspection ou un rapport d'audit externe démontre qu'une infraction a été commise à l'encontre de la présente loi ou de ses actes d'exécution, le service d'inspection ou l'autorité sectorielle peuvent mettre en demeure l'opérateur de services essentiels ou le fournisseur de service numérique concerné de se conformer, dans un délai qu'il ou elle 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.

Le CCB peut également, de manière motivée, recommander au service d'inspection ou à l'autorité sectorielle de mettre en demeure l'opérateur de services essentiels ou le fournisseur de service numérique.

§ 2. 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 ou de l'autorité sectorielle.

§ 3. 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 ou de l'autorité sectorielle dans un procès-verbal.

§ 4. De paragrafen 1 en 2 zijn ook van toepassing op de potentiële aanbieder van essentiële diensten die de in de artikelen 11 en 12 bedoelde informatieverplichtingen niet nakomt.

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

Art. 25

De inbreuken op de bepalingen van deze wet of de uitvoeringsbesluiten ervan kunnen het voorwerp uitmaken hetzij van strafrechtelijke sancties, hetzij van administratieve sancties.

**Afdeling 2**

*Strafrechtelijke sancties*

Art. 26

§ 1. Wordt gestraft met een gevangenisstraf van acht dagen tot een jaar en een geldboete van 26 euro tot 50 000 euro of een van die straffen alleen, de overtreder die de verplichtingen opgelegd door of krachtens deze wet of de uitvoeringsbesluiten ervan niet naleeft.

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

§ 2. Wordt gestraft met een gevangenisstraf van acht dagen tot een maand en een geldboete van 26 euro tot 10 000 euro of een van die straffen alleen, hij die de uitvoering van de controle door de leden van de inspectiedienst vrijwillig verhindert of belemmert, de informatie die hem gevraagd is naar aanleiding van deze controle weigert mee te delen, of opzettelijk foutieve of onvolledige informatie meedeelt.

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

§ 3. De bepalingen van Boek 1 van het Strafwetboek, met inbegrip van hoofdstuk VII en artikel 85, zijn van toepassing op voornoemde inbreuken.

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.

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

§ 4. Les paragraphes 1 et 2 sont également applicables à l'opérateur de services essentiels potentiel qui ne se conforme pas aux obligations d'information visées aux articles 11 et 12.

§ 5. Les procès-verbaux rédigés par les membres assermentés du service d'inspection ou de l'autorité sectorielle font foi jusqu'à preuve du contraire.

Art. 25

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. 26

§ 1er. 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 l'auteur qui ne respecte pas les obligations imposées par ou en vertu de la présente loi ou de ses actes d'exécution.

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.

§ 2. Est puni d'une peine d'emprisonnement de huit jours à un mois et d'une amende de 26 euros à 10 000 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.

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 un an.

§ 3. Les dispositions du Livre 1er du Code pénal, en ce compris le chapitre VII et l'article 85, sont applicables auxdites infractions.

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.

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

**Afdeling 3**

*Administratieve sancties*

Art. 27

§ 1. Bij het vaststellen van inbreuken op deze wet of op de uitvoeringsbesluiten ervan kan de overtreder bestraft worden met een administratieve geldboete.

§ 2. Wordt gestraft met een geldboete van 500 tot 75 000 €, de overtreder die de in de artikelen 16 en 19 bedoelde verplichtingen inzake het melden van incidenten niet nakomt.

§ 3. Wordt gestraft met een geldboete van 500 tot 100 000 €, de overtreder die de in de artikelen 13 en 18 bedoelde beveiligingsverplichtingen niet nakomt.

§ 4. Wordt gestraft met een geldboete van 500 tot 125 000 €, de overtreder die de controleverplichtingen bedoeld in de hoofdstukken 1 en 2 van titel 4 niet nakomt.

§ 5. Wordt gestraft met een geldboete van 500 tot 125 000 €, de overtreder die de in artikel 11 bedoelde informatieverplichtingen niet nakomt.

Art. 28

Het origineel van het proces-verbaal wordt naar de procureur des Konings gestuurd.

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

Art. 29

De procureur des Konings beschikt over een termijn van twee maanden, te rekenen vanaf de dag van ontvangst van het proces-verbaal, om de overtreder 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 indien de procureur des Konings vooraf meedeelt dat hij geen gevolg aan het feit wenst te geven.

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

Art. 30

§ 1. De beslissing om een administratieve geldboete op te leggen wordt gemotiveerd. Ze vermeldt ook het bedrag van de administratieve geldboete en de bedoelde inbreuken.

**Section 3**

*Sanctions administratives*

Art. 27

§ 1er. Lors de la constatation d'infractions à la présente loi ou à ses arrêtés d'exécution, une amende administrative peut être infligée à l'auteur de l'infraction.

§ 2. Est puni d'une amende de 500 à 75 000 € l'auteur de l'infraction qui ne se conforme pas aux obligations de notification d'incidents visées aux articles 16 et 19.

§ 3. Est puni d'une amende de 500 à 100 000 € l'auteur qui ne se conforme pas aux obligations de sécurité visées aux articles 13 et 18.

§ 4. Est puni d'une amende de 500 à 125 000 € l'auteur qui ne se conforme pas aux obligations de contrôle visées au chapitre 1er et 2 du titre 4.

§ 5. Est puni d'une amende de 500 à 125 000 € l'auteur qui ne se conforme pas aux obligations d'information visées à l'article 11.

Art. 28

L'original du procès-verbal est envoyé au procureur du Roi.

Une copie du procès-verbal est dans le même temps envoyée à l'auteur.

Art. 29

Le procureur du Roi dispose d'un délai de deux mois à compter du jour de la réception du procès-verbal pour informer l'auteur 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. 30

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

§ 2. De sectorale overheid bezorgt de overtreder op voorhand haar gemotiveerd voorstel van administratieve sanctie en laat hem weten dat hij het recht heeft om, binnen de 15 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 vierde werkdag na de verzending ervan door de sectorale overheid.

§ 3. Rekening houdend met de aangevoerde verweermiddelen binnen de in paragraaf 2 bedoelde termijn en bij gebrek aan een antwoord van de overtreder binnen diezelfde termijn, kan de sectorale overheid een in artikel 25 bedoelde administratieve sanctie opleggen.

§ 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. 31

De beslissing wordt bij een ter post aangetekend schrijven ter kennis gebracht van de overtreder.

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

Art. 32

De overtreder die de beslissing van de sectorale overheid betwist, kan, op straffe van nietigheid die ambtshalve wordt uitgesproken en op straffe van verval, binnen een termijn van zestig dagen vanaf de ontvangst van de kennisgeving van de beslissing, beroep instellen bij ondertekend verzoekschrift dat bij de griffie van het Marktenhof, bedoeld in artikel 101 van het Gerechtelijk Wetboek, wordt ingediend.

Het Marktenhof behandelt de zaak zoals in kort geding overeenkomstig de artikelen 1035 tot 1038, 1040 en 1041 van het Gerechtelijk Wetboek en kan de beslissing herzien.

Dit beroep schorst de uitvoering van de beslissing niet.

Art. 33

Als de overtreder de administratieve geldboete niet betaalt binnen de gestelde termijn en de in artikel 30 bepaalde beroepsmogelijkheid is uitgeput, is de beslissing om een administratieve geldboete op te leggen rechtstreeks uitvoerbaar en kan de sectorale overheid een dwangbevel uitvaardigen.

§ 2. L'autorité sectorielle informe au préalable l'auteur de sa proposition motivée de sanction administrative et lui fait part de son droit, dans les 15 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 l'auteur le quatrième jour ouvrable 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 de l'auteur dans ce même délai, l'autorité sectorielle peut adopter une sanction administrative visée à l'article 25.

§ 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. 31

La décision est notifiée par lettre recommandée à la poste à l'auteur de l'infraction.

Une invitation à acquitter l'amende dans un délai d'un mois est jointe.

Art. 32

L'auteur de l'infraction qui conteste la décision de l'autorité sectorielle peut interjeter appel, à peine de nullité prononcée d'office, par voie de requête signée et déposée au greffe auprès de la Cour des marchés, visée à l'article 101 du Code judiciaire, dans un délai de soixante jours à partir de la réception de la notification de la décision, à peine de déchéance.

La Cour des marchés traite l'affaire selon les formes du référé conformément aux articles 1035 à 1038, 1040 et 1041 du Code judiciaire et peut réformer la décision.

Ce recours ne suspend pas l'exécution de la décision.

Art. 33

Lorsque l'auteur de l'infraction reste en défaut de payer l'amende administrative dans le délai imparti et que la possibilité de recours fixée à l'article 30 est épuisée, la décision d'infliger une amende administrative a force exécutoire et l'autorité sectorielle peut décerner une contrainte.

Art. 34

De sectorale overheid kan geen administratieve geldboete opleggen als een termijn van drie jaar, te rekenen vanaf de dag waarop de feiten vastgesteld worden, verstreken is.

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

TITEL 5

*Slotbepalingen*

Art. 35

De personen die optreden voor rekening van een aanbieder van essentiële diensten of digitaledienstverlener mogen geen nadelige gevolgen ondervinden vanwege de aanbieder van essentiële diensten of digitaledienstverlener ingevolge de uitvoering, te goeder trouw en in het kader van hun functie, van de verplichtingen die voortvloeien uit deze wet

HOOFDSTUK 1

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

Art. 36

In artikel 3 van de wet wordt een 13° ingevoegd, luidende:

““CCB”: het Centrum voor Cybersecurity België als bedoeld in artikel 6, 1°, van de wet van xx xx 2018 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid”.

In artikel 3 van de wet wordt een 14° ingevoegd, luidende:

““beveiliging van netwerk- en informatiesystemen”: de beveiliging van netwerk- en informatiesystemen als bedoeld in artikel 6, 8° en 9°, van de wet van xx xx 2018 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid”.

Art. 37

In artikel 5 van de wet wordt een paragraaf 3 toegevoegd, luidende:

“§ 3. Tijdens het hele identificatieproces, als bedoeld in deze afdeling, wordt het CCB 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. 34

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 est constaté.

Le paiement selon la procédure administrative éteint également la possibilité d’engager des poursuites pénales pour les faits visés.

TITRE 5

*Disposition finales*

Art. 35

Les personnes qui agissent pour le compte d’un opérateur de services essentiels ou d’un fournisseur de service numérique ne peuvent subir de conséquences négatives de la part de l’opérateur de services essentiels ou du fournisseur de service numérique en raison de l’exécution, de bonne foi et dans le cadre de leurs fonctions, des obligations découlant de la présente loi.

CHAPITRE 1ER

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

Art. 36

A l’article 3 de la loi, est inséré un 13°, rédigé comme suit:

““CCB”: Centre pour la Cybersécurité Belgique, tel que visé à l’article 6, 1°, de la loi du xx xx 2018 établissant un cadre pour la sécurité des réseaux et des systèmes d’information d’intérêt général pour la sécurité publique”.

A l’article 3 de la loi, est inséré un 14°, rédigé comme suit:

““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 xx xx 2018 établissant un cadre pour la sécurité des réseaux et des systèmes d’information d’intérêt général pour la sécurité publique”.

Art. 37

A l’article 5 de la loi, un paragraphe 3 est ajouté et rédigé comme suit:

“§ 3. Tout au long du processus d’identification visé à la présente section, le CCB est associé 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. 38

Op het einde van paragraaf 2 van artikel 14 van de wet worden de volgende woorden toegevoegd: “en, in voorkomend geval, het CCB wat de beveiliging van netwerk- en informatiesystemen betreft.”.

Art. 39

In artikel 18 van de wet worden de woorden “De ADCC, de politiediensten en het OCAD” vervangen door de woorden “De ADCC, de politiediensten, het OCAD en, in voorkomend geval, het CCB, wat de beveiliging van netwerk- en informatiesystemen betreft,”.

Art. 40

In artikel 19 van de 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, het CCB, wat de beveiliging van netwerk- en informatiesystemen betreft,”.

Art. 41

In artikel 22 van de wet 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 het CCB”.

Art. 42

In artikel 3 van de wet worden de volgende wijzigingen aangebracht:

3°, c) wordt gewijzigd als volgt: “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); 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);”;

een 3°, e) wordt ingevoegd, luidende: “voor de sector van de digitale infrastructuren: het Belgisch Instituut voor postdiensten en telecommunicatie (B.I.P.T.);”;

een 3°, f) wordt ingevoegd, luidende: “voor de gezondheidssector: de minister bevoegd voor Volksgezondheid of, bij delegatie van deze laatste, een leidend personeelslid van zijn administratie;”;

Art. 38

A la fin du paragraphe 2 de l’article 14 de la loi, il est ajouté les mots “et, le cas échéant, le CCB pour ce qui concerne la sécurité des réseaux et systèmes d’information.”.

Art. 39

A l’article 18 de la loi, les mots “La DGCC, les services de police et l’OCAM” sont remplacés par “La DGCC, les services de police, l’OCAM et, le cas échéant le CCB pour ce qui concerne la sécurité des réseaux et systèmes d’information,”.

Art. 40

A l’article 19 de la 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 “L’exploitant, le point de contact pour la sécurité, l’autorité sectorielle, la DGCC, l’OCAM, les services de police et, le cas échéant, le CCB pour ce qui concerne la sécurité des réseaux et systèmes d’information”.

Art. 41

A l’article 22 de la loi, 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 le CCB”.

Art. 42

A l’article 3 de la loi, les modifications suivantes sont apportées:

le 3°, c) est modifié comme suit: “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); 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);”;

un 3°, e) est inséré, rédigé comme suit: “pour le secteur des infrastructures numériques: l’Institut belge des services postaux et des télécommunications (I.B.P.T.);”;

un 3°, f) est inséré, rédigé comme suit: “pour le secteur de la santé: le ministre ayant la Santé publique dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration;”;

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. 43

In hoofdstuk III 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 wordt een artikel 15*ter* ingevoegd, dat als volgt luidt:

"Art. 15*ter*. Het Agentschap wordt aangewezen als inspectiedienst, als bedoeld in artikel 22 van de wet van xx 2018 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang en is het 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 controlemodaliteiten".

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. 44

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 een 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. 45

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° de woorden ", met betrekking tot de sector van de digitale infrastructuur en" worden ingevoegd tussen de woorden "radioapparatuur" en de woorden "met betrekking tot";

2° in de bepaling onder 3° worden de woorden ", van de wet van 1 juli 2011 betreffende de veiligheid en de bescherming

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. 43

Dans le chapitre III 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, 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 22 de la loi du xx 2018 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique 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 de contrôle".

CHAPITRE 3

**Modifications de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges**

Art. 44

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. 45

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° les mots ", en ce qui concerne le secteur des infrastructures numériques," sont insérés entre les mots "équipement hertzien" et les mots "et en ce qui concerne";

2° au 3°, les mots ", de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, pour ce

van de kritieke infrastructuren, wat de sector van de elektronische communicatie betreft, van de wet [omzetting NIS-wet], wat de sector van de digitale infrastructuur betreft" ingevoegd tussen de woorden "in het tweetalig gebied Brussel-Hoofdstad" en de woorden "en hun uitvoeringsbesluiten".

Art. 46

In artikel 24, eerste lid, van dezelfde wet, gewijzigd door de wet van 27 maart 2014 worden de woorden ", de wet van 1 juli 2011 betreffende de veiligheid en de bescherming van de kritieke infrastructuren, wat de elektronische-communicatiesector betreft, de wet [wet tot omzetting van de NIS-richtlijn], wat de sector van de digitale infrastructuur 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 en van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten**

Art. 47

§ 1. 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 de artikelen 11 en 14, §§ 2 en 3 van de wet van […] 2018 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid".

§ 2. Artikel 79 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 een paragraaf 4, luidend als volgt: "§ 4. De in dit artikel bedoelde maatregelen mogen ook genomen worden in geval van overtreding van de artikelen 11 en 14, §§ 2 en 3 van de wet van […] 2018 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid".

Art. 48

Punt 15° van artikel 75, § 1, van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector, 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 het Centrum voor Cybersecurity België en de Algemene Directie Crisiscentrum van de Federale Overheidsdienst Binnenlandse Zaken voor de uitvoering van de bepalingen van de wet van … 2018 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang

qui concerne le secteur des communications électroniques, de la loi [transposition loi NIS], pour ce qui concerne le secteur des infrastructures numériques" sont insérés entre les mots "en région bilingue de Bruxelles-Capitale" et les mots "et de leurs arrêtés d'exécution".

Art. 46

Dans l'article 24, alinéa 1er, de la même loi, modifié par la loi du 27 mars 2014, 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 à la loi [loi de transposition de la directive NIS], 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 et de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers**

Art. 47

§ 1er. 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 des articles 11 et 14, §§ 2 et 3 de la loi du […] 2018 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique".

§ 2. L'article 79 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 un paragraphe 4, rédigé comme suit: "§ 4. Les mesures visées au présent article peuvent également être prises en cas de violation des articles 11 et 14, §§ 2 et 3 de la loi du […] 2018 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique".

Art. 48

Le point 15° de l'article 75, § 1 de la loi du 2 août 2002 relative à la surveillance du secteur financier, 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, au Centre pour la Cybersécurité Belgique et à la Direction générale Centre de Crise du Service public fédéral Intérieur pour les besoins de l'exécution des dispositions de la loi du … 2018 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique et de

voor de openbare veiligheid en van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren".

HOOFDSTUK 5

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

Art. 49

Artikel 36/14, § 1, van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België wordt aangevuld als volgt:

20° de woorden "aan het Centrum voor Cybersecurity België" worden ingevoegd tussen de woorden "de analyse van de dreiging," en "en aan de politiediensten";

24°: "24° binnen de grenzen van het recht van de Europese Unie, aan het Centrum voor Cybersecurity België en de Algemene Directie Crisiscentrum van de Federale Overheidsdienst Binnenlandse Zaken voor de uitvoering van de bepalingen van de wet van … 2018 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.".

Art. 50

In dezelfde wet wordt een hoofdstuk IV/4 ingevoegd, bestaande uit één enkel artikel 36/47, luidende:

"Hoofdstuk IV/4 Toezicht door de Bank in het kader van de wet van … 2018 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.

Art. 36/47. De Bank ziet als bevoegde sectorale overheid toe op de naleving door de aanbieders van de sector financiën van de bepalingen van de wet van xx 2018, 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 27 van de wet van … 2018 [de datum en titel van de NIS-wet invullen]. De artikelen 36/8 tot 36/12/3 en artikel 36/21 zijn van toepassing.".

la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques".

CHAPITRE 5

**Modifications de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique**

Art. 49

L'article 36/14, § 1er de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique est complété comme suit:

20° entre les mots "l'analyse de la menace" et "et aux services de police" sont ajoutés les mots "au Centre pour la Cybersécurité Belgique";

24°: "24° dans les limites du droit de l'Union européenne, au Centre pour la Cybersécurité Belgique et à la Direction générale Centre de Crise du Service public fédéral Intérieur pour les besoins de l'exécution des dispositions de la loi du … 2018.".

Art. 50

Dans la même loi, il est inséré un chapitre IV/4, comportant un seul article 36/47 rédigé comme suit:

"Chapitre IV/4 Surveillance par la Banque dans le cadre de la loi du … 2018 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.

Art. 36/47. En tant qu'autorité sectorielle compétente, la Banque contrôle le respect par les opérateurs du secteur des finances, des dispositions de la loi du xx 2018, 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 27 de la loi du ... 2018 [compléter par la date et l'intitulé de la loi NIS]. Les articles 36/8 à 36/12/3 et l'article 36/21 sont applicables.".

HOOFDSTUK 6

**Inwerkingtreding**

Art 51

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

CHAPITRE 6

**Entrée en vigueur**

Art. 51

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

**ADVIES VAN DE RAAD VAN STATE (I)**
**NR. 63.296/4**
**VAN 2 MEI 2018**

Op 5 april 2018 is de Raad van State, afdeling Wetgeving, door de Eerste minister verzocht binnen een termijn van dertig dagen een advies te verstrekken over een voorontwerp van wet "tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid".

Het voorontwerp is door de vierde kamer onderzocht op 2 mei 2018. De kamer was samengesteld uit Martine Baguet, kamervoorzitter, Bernard Blero en Wanda Vogel, staatsraden, Sébastien Van Drooghenbroeck en Jacques Englebert, assessoren, en Anne-Catherine Van Geersdaele, griffier.

Het verslag is uitgebracht door Patrick Ronvaux, eerste auditeur.

De overeenstemming tussen de Franse en de Nederlandse tekst van het advies is nagezien onder toezicht van Martine Baguet.

Het advies, waarvan de tekst hierna volgt, is gegeven op 2 mei 2018.

*

Aangezien de adviesaanvraag ingediend is op basis van artikel 84, § 1, eerste·lid, 2°, van de wetten "op de Raad van State", gecoördineerd op 12 januari 1973, beperkt de afdeling Wetgeving overeenkomstig artikel 84, § 3, van de voornoemde gecoördineerde wetten haar onderzoek tot de rechtsgrond van het voorontwerp,‡ de bevoegdheid van de steller van de handeling en de te vervullen voorafgaande vormvereisten.

Wat die drie punten betreft, geeft het voorontwerp aanleiding tot de volgende opmerkingen.

Bevoegdheid van de steller van de handeling

Het is niet voor het eerst dat de afdeling Wetgeving advies moet uitbrengen over een voorontwerp van wet dat, met toepassing van een om te zetten Europese richtlijn, aanbieders van essentiële diensten beoogt te inventariseren teneinde sommige van hun infrastructuren die noodzakelijk worden geacht voor het behoud van verschillende centrale functies voor het bestaan van de Natie, preventief te beschermen.

Die onderneming kan op zichzelf bevoegdheidsproblemen doen rijzen, wanneer de te beschermen infrastructuren afhangen van operatoren die hun activiteiten uitoefenen op gebieden waarvoor de deelstaten of sommige deelstaten bevoegd zijn gemaakt, en wanneer de federale wet die deelstaten eenzijdig wil betrekken bij de identificatie van de te beschermen infrastructuren, een identificatie die de Federale

‡ Aangezien het om een voorontwerp van wet gaat, wordt onder "rechtsgrond" de overeenstemming met de hogere normen verstaan.

**AVIS DU CONSEIL D'ÉTAT (I)**
**N° 63.296/4**
**DU 2 MAI 2018**

Le 5 avril 2018, le Conseil d'État, section de législation, a été invité par le Premier ministre à communiquer un avis, dans un délai de trente jours, sur un avant-projet de loi "établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique".

L'avant-projet a été examiné par la quatrième chambre le 2 mai 2018. La chambre était composée de Martine Baguet, président de chambre, Bernard Blero et Wanda Vogel, conseillers d'État, Sébastien Van Drooghenbroeck et Jacques Englebert, assesseurs, et Anne-Catherine Van Geersdaele, greffier.

Le rapport a été présenté par Patrick Ronvaux, premier auditeur.

La concordance entre la version française et la version néerlandaise a été vérifiée sous le contrôle de Martine Baguet.

L'avis, dont le texte suit, a été donné le 2 mai 2018.

*

Comme la demande d'avis est introduite sur la base de l'article 84, § 1er, alinéa 1er, 2°, des lois "sur le Conseil d'État", coordonnées le 12 janvier 1973, la section de législation limite son examen au fondement juridique de l'avant-projet‡, à la compétence de l'auteur de l'acte ainsi qu'à l'accomplissement des formalités préalables, conformément à l'article 84, § 3, des lois coordonnées précitées.

Sur ces trois points, l'avant-projet appelle les observations suivantes.

Compétence de l'auteur de l'acte

Ce n'est pas la première fois que la section de législation est saisie d'un avant-projet de loi visant, en exécution d'une directive européenne à transposer, à recenser des opérateurs de services essentiels en vue d'assurer de manière préventive la protection de certaines de leurs infrastructures jugées nécessaires au maintien de diverses fonctions centrales pour la vie de la Nation.

Cette opération peut soulever en soi des questions de compétence lorsque les infrastructures à protéger dépendent d'opérateurs qui exercent leurs activités dans l'orbite de compétences qui ont été attribuées aux entités fédérées ou à certaines d'entre-elles et que la loi fédérale entend associer de manière unilatérale ces entités à l'identification des infrastructures à protéger, identification que l'État fédé-

‡ S'agissant d'un avant-projet de loi, on entend par "fondement juridique" la conformité aux normes supérieures.

Staat, wat hem betreft, doet krachtens de restbevoegdheden die hij op het gebied van de openbare veiligheid uitoefent.

Die bevoegdheidskwestie is als volgt geanalyseerd in advies 48.989/VR,[1] op 9 december 2010 gegeven over een voorontwerp dat heeft geleid tot de wet van 1 juli 2001 "betreffende de beveiliging en de bescherming van de kritieke infrastructuren":

"1. Het voorliggende voorontwerp voorziet, zoals te lezen staat in artikel 2, eerste lid, ervan, inzonderheid in de omzetting van Richtlijn 2008/114/EG van de Raad van 8 december 2008 inzake de identificatie van Europese kritieke infrastructuren, de aanmerking van infrastructuren als Europese kritieke infrastructuren en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuren te verbeteren (hierna "de richtlijn" genoemd).

Artikel 1 van de richtlijn geeft aan dat bij deze richtlijn een procedure wordt ingesteld voor de identificatie en de aanmerking van Europese kritieke infrastructuren, om de bescherming van de mensen te bevorderen

De kritieke infrastructuur wordt in artikel 2, a), van de richtlijn in wezen gedefinieerd als "een voorziening (…, die) van essentieel belang is voor het behoud van vitale maatschappelijke functies, de gezondheid, de veiligheid, de beveiliging, de economische welvaart of het maatschappelijk welzijn, waarvan de verstoring of vernietiging (…) aanzienlijke gevolgen zou hebben doordat die functies ontregeld zouden raken". Artikel 3, lid 3, van de richtlijn bepaalt dat deze op dit ogenblik uitsluitend van toepassing is in de sectoren energie en vervoer. Volgens de eerste overweging van de richtlijn hebben de stellers ervan in de eerste plaats het aannemen van "voorstellen (beoogd) over de wijze waarop de preventie van, de paraatheid bij en de reactie op terreuraanslagen op kritieke infrastructuur in Europa kunnen worden verbeterd". In dat verband is besloten dat het Europese programma voor de bescherming van kritieke infrastructuren, waarvan de richtlijn een beleidsmiddel is, "gebaseerd moet zijn op een alle risico's omvattende aanpak, waarbij de bestrijding van terroristische dreigingen als prioriteit zou gelden", een aanpak waarbij "in het proces ter bescherming van kritieke infrastructuur rekening (dient) te worden gehouden met door mensen veroorzaakte dreigingen, technologische dreigingen en natuurrampen" (derde overweging).

[1] *Parl.St*. Kamer 2010-11, nr. 1357/001, 53-64, *http://www.raadvst-consetat.be/dbx/adviezen/48989.pdf.*

ral entreprend pour ce qui le concerne sous le couvert des compétences résiduelles qu'il exerce dans le domaine de la sécurité publique.

Cette question de compétence a été analysée dans les termes suivants à l'occasion de l'avis n° 48.989/VR [1] donné le 9 décembre 2010 sur un avant-projet devenu la loi du 1er juillet 2011 "relative à la sécurité et la protection des infrastructures critiques":

"1. Ainsi que l'exprime son article 2, alinéa 1er, l'avant-projet à l'examen a notamment pour objet de transposer la Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection (ci-après, la directive).

Comme l'énonce l'article 1er de la directive, il s'agit d'établir une procédure de recensement et de désignation des infrastructures critiques européennes en vue d'éventuellement améliorer leur protection afin de contribuer à la protection des personnes.

L'infrastructure critique est en substance définie par l'article 2, a), de la directive comme "le point (…) qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, et dont l'arrêt ou la destruction aurait un impact significatif (…) du fait de la défaillance de ces fonctions". L'article 3, paragraphe 3, de la directive mentionne qu'elle s'applique pour l'instant uniquement dans les secteurs de l'énergie et des transports. Selon le premier considérant de la directive, ses auteurs ont d'abord eu en vue l'adoption de "mesures en vue de renforcer la prévention, la préparation et la réponse de l'Union européenne face aux attaques terroristes contre des infrastructures critiques". Par la suite, tout en maintenant "une priorité donnée à la lutte contre la menace terroriste", le programme européen de protection des infrastructures critiques, dont la directive est un instrument, s'est fondé sur "une approche tous risques (qui) tient compte des risques d'origine humaine, des menaces technologiques et des catastrophes naturelles dans le processus de protection des infrastructures critiques" (troisième considérant).

[1] *Doc. parl*., Chambre, 2010-2011, n° 1357/001, pp. 53-64, *http://www.raadvst-consetat.be/dbx/avis/48989.pdf.*

Gelet op hetgeen voorafgaat, moet worden beschouwd dat de omzetting van deze richtlijn hoofdzakelijk leidt tot de tenuitvoerlegging van de aangelegenheid van de preventieve bescherming op het gebied van de openbare veiligheid, die tot de exclusieve restbevoegdheid van de federale wetgever behoort[2].

Hetzelfde geldt voor de overige bepalingen van het voorontwerp die weliswaar niet voorzien in de omzetting van de richtlijn, maar strekken tot het aannemen van analoge maatregelen met betrekking tot de nationale kritieke infrastructuren, de andere punten van federaal belang en de punten van lokaal belang.

2. De maatregelen die op basis van het voorontwerp zullen worden getroffen, kunnen evenwel een weerslag hebben op operatoren die een infrastructuur exploiteren welke, uit een ander oogpunt beschouwd, tot de bevoegdheid *ratione materiae* van de gewesten kan behoren, meer in het bijzonder wat betreft de sectoren energie en vervoer, waarop de richtlijn toepassing vindt (artikel 6, § 1, VII en X, van de bijzondere wet van 8 augustus 1980 tot hervorming der instellingen).

De steller van het voorontwerp heeft overigens oog gehad voor dit aspect, daar hij de gewesten wenst te "betrekken" bij het uitwerken van de toepasselijke regelgeving en bij de uitvoering ervan, zoals blijkt uit de volgende bepalingen van het voorontwerp:

— artikel 5, § 1, tweede lid, naar luid waarvan de sectorale overheid [3] de Europese kritieke infrastructuren identificeert "na eensluidend advies van de gewesten voor de potentiële kritieke infrastructuren die onder hun bevoegdheden vallen";

— artikel 6, § 2, naar luid waarvan de sectorale overheid "de sectorale criteria (bepaalt) waaraan de Europese kritieke infrastructuren moeten beantwoorden, rekening houdend met de bijzondere karakteristieken van de betrokken sector, (…), in voorkomend geval, na eensluidend advies van de betrokken gewesten";

— artikel 6, § 5, naar luid waarvan de sectorale overheid "geval per geval de drempelwaarden (bepaalt) die van toepassing zijn op de intersectorale criteria waaraan de Euro-

[2] *Voetnoot 1 van het geciteerde advies:* Raad van State, Belgische Staat, nr. 175 462, 8 oktober 2007. Andere voorbeelden van wetten die de Federale Staat heeft aangenomen met het oog op de preventieve bescherming van de "vitale maatschappelijke functies": de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, die onder meer de bescherming van het "economisch potentieel van het land" beoogt, of de wet van 10 juli 2006 betreffende de analyse van de dreiging, die onder meer 's lands "fundamentele belangen" beoogt.

[3] *Voetnoot 2 van het geciteerde advies:* Voor de Europese kritieke infrastructuren is de federale minister bevoegd voor het Vervoer of diens gemachtigde (artikel 3, 3°, a), van het voorontwerp), dan wel de federale minister bevoegd voor de Energie of diens gemachtigde (artikel 3, 3°, b), van het voorontwerp) de sectorale overheid.

Eu égard à ce qui précède, il y a lieu de considérer que la transposition de cette directive met principalement en œuvre la matière de la protection préventive exercée dans le domaine de la sécurité publique, qui relève des compétences résiduelles exclusives du législateur fédéral [2].

Il en va de même pour ce qui concerne les autres dispositions de l'avant-projet qui, tout en n'ayant pas pour objet de transposer la directive, tendent à l'adoption de mesures analogues pour ce qui concerne les infrastructures critiques nationales ainsi que les autres points d'intérêt fédéral et les points d'intérêt local.

2. Toutefois, les mesures qui seront prises sur la base de l'avant-projet seront susceptibles de concerner des opérateurs exploitant des infrastructures qui, envisagées d'un autre point de vue, pourraient relever de la compétence matérielle des régions, s'agissant spécialement des secteurs de l'énergie et du transport, auxquels la directive s'applique (article 6, § 1er, VII et X, de la loi spéciale du 8 août 1980 de réformes institutionnelles).

L'auteur de l'avant-projet est d'ailleurs sensible à cet aspect des choses puisqu'il a le souci d'"associer" les régions à la réglementation applicable et à sa mise en œuvre, comme en témoignent les dispositions suivantes de l'avant-projet:

— l'article 5, § 1er, alinéa 2, selon lequel l'autorité sectorielle [3] procède à l'identification des infrastructures critiques européennes "après avis conforme des régions pour les infrastructures critiques potentielles relevant de leurs compétences";

— l'article 6, § 2, selon lequel l'autorité sectorielle "établit des critères sectoriels auxquels doivent répondre les infrastructures critiques européennes eu égard aux caractéristiques particulières du secteur concerné, (...), le cas échéant, après avis conforme des régions concernées";

— l'article 6, § 5, selon lequel "l'autorité sectorielle établit au cas par cas les seuils applicables aux critères intersectoriels auxquels doivent répondre les infrastructures critiques

[2] *Note de bas de page n° 1 de l'avis cité:* C.E., État belge, n° 175 462, 8 octobre 2007. Pour d'autres exemples de lois adoptées par l'État fédéral en vue d'assurer la protection préventive des "fonctions vitales de la société", voir la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité qui vise notamment à protéger "le potentiel économique du pays" ou la loi du 10 juillet 2006 relative à l'analyse de la menace qui a notamment en vue les "intérêts fondamentaux" du pays.

[3] *Note de bas de page n° 2 de l'avis cité:* Pour les infrastructures critiques européennes, l'autorité sectorielle est le ministre fédéral ayant les Transports dans ses attributions ou son délégué (article 3, 3°, a, de l'avant-projet) ou le ministre fédéral ayant l'Énergie dans ses attributions ou son délégué (article 3, 3°, b), de l'avant-projet.

pese kritieke infrastructuren dienen te beantwoorden, (…), in voorkomend geval, na eensluidend advies van de betrokken gewesten";

— artikel 7, § 2, tweede lid, naar luid waarvan de Algemene Directie Crisiscentrum van de Federale Overheidsdienst Binnenlandse Zaken (hierna "ADCC" genoemd) "in samenwerking met (…), in voorkomend geval (…) de betrokken gewesten, belast (is) met het voeren van bilaterale of multilaterale besprekingen met de betrokken lidstaten van de Europese Unie, (…) inzake de potentiële Europese kritieke infrastructuren geïdentificeerd op Belgisch grondgebied (…)";

— artikel 13, § 6, tweede lid, naar luid waarvan "de Koning bepaalt, in voorkomend geval, met instemming van de betrokken gewesten, voor een bepaalde sector of een deelsector, de frequentie van de oefeningen en van de bijwerkingen" van het beveiligingsplan van de exploitant van een Europese kritieke infrastructuur;

— artikel 24, § 2, tweede lid, naar luid waarvan de Koning "de nadere regels van [de controle van de inachtneming van de bepalingen van de ontworpen wet door de exploitanten van de bij deze wet bedoelde infrastructuren] kan vastleggen, in voorkomend geval met instemming van de betrokken gewesten".

3. Aangezien de gewesten bevoegdheden bezitten op het gebied van energie en vervoer, aangezien dit eveneens zou kunnen gelden voor andere sectoren waarop de ontworpen wet toepassing zou vinden en volgens de steller zelf van het voorontwerp bij de uitvoering van de wet de weerslag van sommige van de voorgenomen maatregelen voelbaar zou kunnen zijn in het beheer van infrastructuren die tot de bevoegdheid van de gewesten behoren, kan worden aanvaard dat de gewesten worden betrokken bij het aannemen van de uitvoeringsmaatregelen omschreven in de ontworpen tekst.

De steller van het voorontwerp moet evenwel aldus te werk gaan dat de autonomie van de verschillende beleidsniveaus in acht wordt genomen. De federale wetgever kan niet eenzijdig – bij wege van een gewone wet – een gedwongen medewerking van de gewesten aan het bij het voorontwerp uitgestippelde systeem opleggen. De medewerking van de gewesten kan dus indien nodig alleen facultatief zijn, en op een zodanige wijze dat, indien ze dat verzuimen, zulks niet verhindert dat de bevoegde federale overheid de voorgenomen maatregelen kan nemen.

4. Indien in de toekomst mocht blijken dat het aannemen van maatregelen ter uitvoering van de wet inhoudt dat bevoegdheden eigen aan de federale overheid en aan de gewesten gezamenlijk worden uitgeoefend, en niet meer dat uitsluitend de enkele federale bevoegdheid op het gebied van de openbare veiligheid wordt uitgeoefend, moet daaromtrent met de gewesten een samenwerkingsakkoord worden gesloten."

In het kader van het voorliggende voorontwerp worden de gewesten en/of de gemeenschappen bij de gang van zaken betrokken ingevolge de artikelen 7, § 2, tweede lid, 11, § 1, derde lid, § 4, § 5, tweede lid, § 7, derde lid, § 8 en § 9,

européennes, (...), le cas échéant après avis conforme des régions concernées";

— l'article 7, § 2, alinéa 2, selon lequel la Direction générale Centre de Crise du service public fédéral Intérieur (ci-après, DGCC) "est chargée en collaboration (...), le cas échéant, avec les régions concernées (...) de mener des discussions bilatérales ou multilatérales avec les États membres de l'Union européenne concernés (...) en ce qui concerne les infrastructures critiques européennes potentielles identifiées sur le territoire belge (...)";

— l'article 13, § 6, alinéa 2, selon lequel "le Roi, le cas échéant, en accord avec les régions concernées, détermine pour un secteur ou un sous-secteur déterminé la fréquence des exercices et des mises à jour" du plan de sécurité de l'exploitant d'une infrastructure critique européenne;

— l'article 24, § 2, alinéa 2, selon lequel le Roi "peut fixer les modalités du contrôle, le cas échéant en accord avec les régions concernées", du respect des dispositions de la loi en projet par les exploitants d'infrastructures concernées par celle-ci.

3. Comme les régions détiennent des compétences dans les domaines de l'énergie et du transport, qu'il pourrait en être de même pour d'autres secteurs auxquels la loi en projet s'appliquerait et que, selon l'auteur de l'avant-projet lui-même, dans l'exécution de la loi, l'incidence de certaines des mesures envisagées pourrait affecter la gestion d'infrastructures relevant des compétences régionales, il est admissible d'associer les régions à l'adoption des mesures d'exécution du texte en projet.

Toutefois, ce faisant, il doit le faire d'une manière qui respecte l'autonomie des différents niveaux de pouvoir. Le législateur fédéral ne peut imposer unilatéralement – par le biais d'une loi ordinaire – une collaboration forcée des régions au système mis en place par l'avant-projet. L'intervention des régions ne peut être prévue, si nécessaire, que de façon facultative et en manière telle que leur éventuelle abstention n'empêche pas l'adoption des mesures envisagées par l'autorité fédérale compétente.

4. Si, dans l'avenir, il devait s'avérer que l'adoption des mesures d'exécution de la loi devait impliquer l'exercice conjoint de compétences propres à l'autorité fédérale et aux régions, et non plus uniquement la mise en œuvre de la seule compétence fédérale en matière de sécurité publique, il conviendrait de conclure un accord de coopération avec les régions sur ces questions".

Dans le cadre de l'avant-projet à l'examen, les Régions et/ou les Communautés sont associées au processus opératoire par l'effet des articles 7, § 2, alinéa 2, 11, § 1er, alinéa 3, § 4, § 5, alinéa 2, § 7, alinéa 3, § 8 et § 9, alinéa 3, 14, § 4, et 17,

derde lid, 14, § 4, en 17, § 7, van het voorontwerp, telkens op een wijze die verenigbaar is met de hierboven naar voren gebrachte principes.

Ten aanzien van die principes doet het voorontwerp dan ook geen enkel bevoegdheidsprobleem rijzen.

VOORAFGAAND VORMVEREISTE

Uit de bespreking van artikel 9 blijkt dat het voorontwerp in het bijzonder de uitwisseling van "persoonsgegevens" beoogt te organiseren.

Uit het dossier blijkt niet dat het voorontwerp van wet om advies is voorgelegd aan de Commissie voor de bescherming van de persoonlijke levenssfeer.

De adviesaanvrager wordt erop gewezen dat het advies van de toezichthoudende autoriteit die "verantwoordelijk is voor het toezicht op de toepassing van de algemene verordening gegevensbescherming" vanaf 25 mei 2018, de datum waarop de algemene verordening[4] gegevensbescherming toepasselijk wordt, een verplicht vormvereiste is.[5-6]

ALGEMENE OPMERKINGEN

Doordat de wetgevende macht rechtstreeks de diensten van de uitvoerende macht aanwijst die door de Koning zijn opgericht en op hem aangewezen zijn om de opdrachten uit te voeren die betrekking hebben op de uitvoering van het voorontwerp, zoals bijvoorbeeld het geval is in artikel 6, 1° en 3°, mengt ze zich in de interne organisatie van de uitvoerende macht.

In principe staat het echter aan de Koning te bepalen welke van zijn diensten bij de toepassing en de tenuitvoerlegging van de wet een rol dienen te spelen.

Het staat tevens aan de Koning de lijst met de dienstopdrachten waarmee de NIS-richtlijn correct kan worden omgezet, aan te vullen.

Zo volstaat het bijvoorbeeld niet dat in artikel 6, 1°, van het voorontwerp het "CCB" wordt aangewezen als "het Centrum voor Cybersecurity België opgericht bij het koninklijk besluit van 10 oktober 2014", noch dat in artikel 7, §§ 1 en 3 tot 6, van het voorontwerp de opdrachten worden vermeld waarmee het CCB wordt belast om te voldoen aan de vereisten van Richtlijn (EU) 2016/1148 van het Europees Parlement en de

4 Verordening (EU) 2016/679 van het Europees Parlement en de Raad 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 Zie de artikelen 36, lid 4, en 57, lid 1, alsook overweging 96 van de algemene verordening gegevensbescherming.

6 Vanaf 25 mei 2018 wordt de Commissie voor de bescherming van de persoonlijke levenssfeer opgevolgd door de Gegevensbeschermingsautoriteit (zie wet van 3 december 2017 "tot oprichting van de Gegevensbeschermingsautoriteit").

§ 7, de l'avant-projet, chaque fois d'une manière compatible avec les principes dégagés ci-dessus.

L'avant-projet ne soulève dès lors aucun problème de compétence au regard de ces principes.

FORMALITÉ PRÉALABLE

Il ressort du commentaire de l'article 9 que l'avant-projet entend notamment organiser l'échange de "données à caractère personnel".

Il n'apparait pas du dossier que l'avant-projet de loi ait été soumis à l'avis de la Commission de la protection de la vie privée.

À dater du 25 mai 2018, date à laquelle le règlement général sur la protection des données [4] sera d'application, l'attention du demandeur d'avis est attirée sur le fait que l'avis de l'autorité de contrôle "responsable pour le contrôle de l'application du règlement général sur la protection des données" constituera une formalité obligatoire [5-6].

OBSERVATIONS GÉNÉRALES

En désignant directement des services du pouvoir exécutif qui ont été créés par le Roi et qui dépendent de Lui pour exercer des missions liées à l'exécution de l'avant-projet, comme c'est le cas par exemple à l'article 6, 1° et 3°, le pouvoir législatif s'immisce dans l'organisation interne du pouvoir exécutif.

Or, c'est en principe au Roi qu'il revient de désigner ceux de Ses services qui seront chargés d'intervenir dans le processus d'application et de mise en œuvre de la loi.

C'est également à Lui qu'il appartient de compléter la liste des missions de service qui permettront d'assurer la transposition correcte de la directive NIS.

Ainsi, pour ne citer qu'un exemple, il ne suffit pas de désigner, à l'article 6, 1°, de l'avant-projet le "CCB" comme étant "le Centre pour la Cybersécurité Belgique créé par l'arrêté royal du 10 octobre 2014", pas plus qu'à l'article 7, § 1er et 3 à 6, de l'avant-projet d'énoncer les missions dont il est investi pour satisfaire aux exigences de la Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 "concer-

4 Règlement (UE) n° 2016/679 du Parlement et du Conseil du 27 avril 2016 "relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la Directive 95/46/CE (règlement général sur la protection des données)".

5 Voir les articles 36, paragraphe 4, et 57, paragraphe 1, ainsi que le considérant 96 du règlement général sur la protection des donnes.

6 À dater du 25 mai 2018, l'Autorité de protection des données succèdera à la Commission de la protection de la vie privée (voir la loi du 3 décembre 2017 "portant création de l'Autorité de protection des données").

Raad van 6 juli 2016 “houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie” (NIS-richtlijn). De opdrachten waarmee het CCB momenteel belast is, lijken in artikel 3 van het koninklijk besluit van 10 oktober 2014 “tot oprichting van het Centrum voor Cybersecurity België” weliswaar voldoende ruim geformuleerd zodat ze ook de opdrachten omvatten die de steller van het voorontwerp in het licht van de NIS-richtlijn aan het CCB wil verlenen. Dat neemt niet weg dat het, met naleving van de Belgische internrechtelijke regels voor de bevoegdheidsverdeling tussen de wetgevende en de uitvoerende macht, aan de Koning en enkel aan de Koning staat om het CCB de precieze opdrachten te verlenen die het met toepassing van de NIS-richtlijn zal uitvoeren. Alhoewel artikel 4 van het koninklijk besluit van 10 oktober 2014 stelt dat “[h]et CCB (…) voor de vervulling van zijn opdrachten over een eigen personeelsenveloppe en -plan [beschikt]”, staat het niettemin evenzo aan de uitvoerende macht, in het kader van de middelen die haar ter beschikking zijn gesteld, ervoor te zorgen dat het CCB, zoals vereist bij artikel 8, lid 5, van de NIS-richtlijn, beschikt over “de nodige middelen (…) om de taken die [het] zijn toegewezen op doeltreffende en efficiënte wijze uit te voeren en aldus de doelstellingen (…) te verwezenlijken” die bij die richtlijn zijn vastgesteld.

Iedere bepaling van het voorontwerp die strekt tot aanwijzing van een (intersectorale of sectorale nationale[7]) administratieve overheid en tot vaststelling van de opdrachten daarvan alsook van de wijze waarop die opdrachten moeten worden uitgevoerd (procedure, criteria …), moet dienovereenkomstig herzien worden, aangezien die overheid al door de Koning opgericht is, of door de Koning opgericht zou moeten worden, volgens de beginselen die de verdeling regelen van de bevoegdheden tussen de wetgevende en de uitvoerende macht.

In het licht van die beginselen is het bijgevolg niet aanvaardbaar dat in ieder geval de artikelen 7, 8, 9, § 2 en § 4, 11, 14, § 3, tweede lid, 17, § 3, tweede zin, 20, § 5 en § 6, 21, § 1, tweede lid, 22, § 3, tweede lid 2, § 9 (*partim*) en 14, 23, § 2 tot § 7, 24, § 1, tweede lid, alsook 36 tot 41 van het voorontwerp worden aangenomen zoals ze thans zijn gesteld; zij zullen dan ook niet verder onderzocht worden door de afdeling Wetgeving.

Ten slotte moeten de concordantietabellen aldus aangepast worden dat daarin de koninklijke besluiten worden vermeld die vastgesteld zijn, gewijzigd moeten worden of vastgesteld moeten worden om de NIS-richtlijn correct en volledig om te zetten.

2. De concordantietabellen, in voorkomend geval gelezen in samenhang met de memorie van toelichting en de bespre-

[7] Uit artikel 7, § 2, van het voorontwerp blijkt immers dat het de bedoeling is van de steller dat de sectorale overheden opgericht worden bij koninklijk besluit, hetgeen veronderstelt dat de reeds bestaande eveneens bij koninklijk besluit opgericht zijn. In dat opzicht moeten de bepalingen tot vaststelling van de opdrachten van die sectorale overheden die eventueel aangepast zullen moeten worden rekening houdend met de NIS-richtlijn, ook bij koninklijk besluit worden vastgesteld (zie aangaande dat punt inzonderheid de artikelen 11, § 1 tot § 11, en 12, § 1, van het voorontwerp).

nant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d’information dans l’Union (Directive “NIS”)”. Certes, les missions dont le CCB est actuellement en charge semblent assez largement énoncées à l’article 3 de l’arrêté royal du 10 octobre 2014 “portant création du Centre pour la Cybersécurité Belgique” que pour absorber celles que l’auteur de l’avant-projet se propose de lui confier au regard de la directive NIS. Il n’en demeure pas moins que dans le respect des règles de droit interne belge qui président à la répartition des compétences entre les pouvoirs législatif et exécutif, c’est au Roi et à Lui seul qu’il appartient d’attribuer au CCB les missions précises qu’il va exercer en application de la directive NIS. De même, si l’article 4 de l’arrêté royal du 10 octobre 2014 précise que “[p]our l’exécution de ses missions, le CCB dispose d’une enveloppe et d’un plan de personnel propre”, il n’en revient pas moins que c’est au pouvoir exécutif qu’il revient dans le cadre des moyens mis à sa disposition de s’assurer que le CCB disposera des “ressources suffisantes pour pouvoir s’acquitter de [ses] tâches de manière effective et efficace et atteindre ainsi les objectifs” fixés par la directive NIS, comme le requiert l’article 8, paragraphe 5, de cette directive.

L’avant-projet doit en conséquence être revu dans chacune des dispositions qui impliquent la désignation d’une autorité administrative (nationale intersectorielle ou sectorielle [7]) et la détermination de ses missions et de la manière de l’exercer (procédure, critères, …) dès lors que cette autorité a déjà été créée par le Roi ou devrait l’être au titre des principes régissant la répartition des compétences entre les pouvoirs législatif et exécutif.

Au regard de ces principes, il n’est dès lors pas admissible qu’en tout cas, les articles 7, 8, 9, §§ 2 et 4, 11, 14, § 3, alinéa 2, 17, § 3, deuxième phrase, 20, §§ 5 et 6, 21, § 1er, alinéa 2, 22, §§ 3, alinéa 2, 9 *partim* et 14, 23, §§ 2 à 7, 24, § 1er, alinéa 2, ainsi que 36 à 41 de l’avant-projet soient adoptés en l’état; ils ne seront dès lors pas examinés plus avant par la section de législation.

Enfin, les tableaux de correspondance seront adaptés afin d’y mentionner les arrêtés royaux pris, à modifier ou à prendre pour transposer correctement et complètement la directive NIS.

2. Les tableaux de correspondance, le cas échéant, lus en combinaison avec l’exposé des motifs et le commentaire

[7] En effet, à lire l’article 7, § 2, de l’avant-projet, l’intention de l’auteur est que les autorités sectorielles soient créées par arrêté royal, ce qui suppose que pour celles qui existent c’est également par arrêté royal qu’elles ont été créées. Dans cette mesure, les dispositions déterminant les missions de ces autorités sectorielles qui devront éventuellement être adaptées compte tenu de la directive NIS, doivent aussi faire l’objet d’un arrêté royal (Voir sur ce point plus spécialement, les articles 11, §§ 1er à 11, et 12, § 1er, de l’avant-projet).

king van de artikelen, moeten het mogelijk maken na te gaan in welke mate de NIS-richtlijn correct omgezet is.

Uit een dergelijke oefening die de afdeling Wetgeving heeft uitgevoerd binnen de perken van de omvang van het voorontwerp van wet, het aantal adviesaanvragen die ze momenteel moet onderzoeken en de termijnen waarover ze daartoe beschikt, blijkt evenwel dat de tabellen die haar bezorgd zijn, met betrekking tot verscheidene bepalingen van het voorontwerp, niet beantwoorden aan de nauwkeurigheidsvereisten waaraan ze moeten voldoen.

Gelet op algemene opmerking 1 en louter bij wijze van voorbeeld bevat de tabel die de overeenstemming weergeeft tussen het voorontwerp en de NIS-richtlijn de volgende vergissingen:

— artikel 2 van het voorontwerp is niet de omzetting van artikel 1, lid 1, van de NIS-richtlijn: hier moet artikel 25, lid 1, derde alinea, van de richtlijn vermeld worden;

— artikel 4, § 2, van het voorontwerp zou de omzetting zijn van artikel 1, lid 7, van de NIS-richtlijn: als het zo is dat daartoe uit een en ander afgeleid moet worden dat de juridische instrumenten tot regeling van de financiële sector de tenuitvoerlegging vormen van sectorspecifieke rechtshandelingen in de zin van dat artikel 1, lid 7, van de NIS-richtlijn, verdient het aanbeveling de bespreking van het artikel op dat punt aan te vullen, en indien zulks niet het geval is, zou in de bespreking van het artikel duidelijk vermeld moeten worden in welk opzicht de uitzondering waarin voorzien wordt voor de financiële sector, haar oorsprong vindt in datzelfde artikel 1, lid 7, of in een andere relevante bepaling van de NIS-richtlijn; een vergelijkbare opmerking geldt voor artikel 4, § 4, van het voorontwerp: wat dat artikel betreft volstaat het niet in de concordantietabel te preciseren dat het “louter nationaal” is zonder meer uitleg te geven in de bespreking van het artikel, waarin overigens niks gezegd wordt dienaangaande; een vergelijkbare opmerking geldt voor artikel 17, § 3, van het voorontwerp;

— het is de afdeling Wetgeving niet duidelijk in welk opzicht artikel 6, 15° en 16°, de omzetting zou zijn van artikel 6, lid 1 en 2, van de NIS-richtlijn, dat geen definitie bevat van de intersectorale en sectorale criteria maar in werkelijkheid de procedure betreft voor het vaststellen van een aanzienlijk verstorend effect op de levering van een essentiële dienst;

— met betrekking tot verscheidene bepalingen van de NIS-richtlijn wordt aangegeven dat ze omgezet zijn in een artikel of in één van de onderverdelingen daarvan; *in casu* wordt de richtlijn evenwel niet omgezet bij de bepaling zelf, maar bij een regeling die bijvoorbeeld vastgesteld wordt door de Koning die daartoe in die gevallen gemachtigd is: die precisering moet

des articles doivent permettre d’appréhender la mesure dans laquelle la directive NIS est correctement transposée.

Or, il apparait d’un tel exercice opéré par la section de législation dans les limites de l’ampleur de l’avant-projet de loi, du nombre de demandes d’avis qu’elle doit actuellement examiner et des délais impartis pour ce faire, que les tableaux qui lui ont été transmis sont, pour plusieurs dispositions de l’avant-projet, en défaut de satisfaire aux exigences de précision auxquelles il s’impose qu’ils satisfassent.

Compte tenu de l’observation générale n° 1 et à titre de simples exemples, dans le tableau établissant la correspondance entre l’avant-projet et la directive NIS,

— l’article 2 de l’avant-projet n’est pas la transposition de l’article premier, paragraphe 1 de la directive NIS: c’est l’article 25, paragraphe 1er, alinéa 3, de la directive qui doit être mentionné;

— l’article 4, § 2, de l’avant-projet constituerait une transposition de l’article premier, paragraphe 7, de la directive NIS: si tant est qu’il faille pour ce faire en déduire que les instruments juridiques régissant le secteur des finances constituent la mise en œuvre d’actes juridiques sectoriels au sens de cet article premier, paragraphe 7, de la directive NIS, le commentaire de l’article serait judicieusement complété sur ce point et si tel n’est pas le cas, il y aurait lieu d’indiquer clairement dans le commentaire de l’article en quoi l’exception prévue pour le secteur des finances trouve sa source dans ce même article premier, paragraphe 7 ou une autre disposition pertinente de la directive NIS; une observation similaire vaut pour l’article 4, § 4, de l’avant-projet dont il ne suffit pas de préciser dans le tableau de correspondance qu’il est “strictement national” sans donner de plus amples précisions dans le commentaire de l’article par ailleurs muet à cet égard; une observation similaire vaut pour l’article 17, § 3, de l’avant-projet;

— la section de législation n’aperçoit pas en quoi l’article 6, 15° et 16°, serait la transposition de l’article 6, paragraphes 1 et 2, de la directive NIS qui ne porte aucune définition des critères intersectoriels et sectoriels mais concerne en réalité la procédure de détermination d’un effet disruptif important sur la fourniture d’un service essentiel;

— plusieurs dispositions de la directive NIS sont renseignées comme transposées dans un article ou l’une de ses subdivisions; or, en l’occurrence, ce n’est pas la disposition elle-même qui transpose mais un dispositif que par exemple le Roi est habilité à prendre pour ce faire: cette précision doit apparaitre clairement dans le tableau de concordance afin

duidelijk naar voren komen in de concordantietabel zodat geen misverstanden ontstaan met betrekking tot de correcte en volledige omzetting die bij het voorontwerp zelf tot stand wordt gebracht;[8]

— artikel 19, § 3, van het voorontwerp zou de omzetting zijn van artikel 17 van de NIS-richtlijn; dat lijkt evenwel niet het geval te zijn, al was het maar gezien de respectieve inhoud ervan, aangezien bij de eerste bepaling de digitaledienstverleners verplicht worden een contactpunt voor de informatiebeveiliging aan te duiden, terwijl de tweede bepaling betrekking heeft op de bevoegde autoriteiten, hun verplichtingen inzake toezicht en de middelen die nodig zijn om ze uit te voeren.

Die tabel en de tabel in omgekeerde richting moeten dienovereenkomstig herzien worden en de bespreking van de artikelen moet, in voorkomend geval, aangevuld worden met de informatie die noodzakelijk is voor de adressaten van de regel om de strekking ervan te begrijpen.

3. De hiernavolgende bijzondere opmerkingen worden gemaakt onder voorbehoud van die algemene opmerkingen, die verband houden met de correcte en volledige omzetting van de NIS-richtlijn, rekening houdend met de vereisten van de richtlijn zelf en met de regels van intern recht.

Het voorontwerp moet herzien worden rekening houdend daarmee.

BIJZONDERE OPMERKINGEN

Dispositief

Artikel 9

Artikel 9, § 1, derde lid, van het voorontwerp bepaalt:

“Met inachtneming van het eerste en tweede lid wordt, voor de toepassing van deze wet, afgeweken van de door andere wetgeving opgelegde verplichtingen inzake het beroepsgeheim.”.

Die bepaling kan niet volstaan om de rechtszekerheid te waarborgen en de bescherming van de personen die aan het beroepsgeheim gebonden zijn, die aangeklaagd zouden kunnen worden voor de niet-inachtneming ervan en daardoor strafrechtelijk gestraft zouden kunnen worden.

In de bepaling moet duidelijk aangegeven worden om welke wetgevingen het hier gaat.

[8] Zie bijvoorbeeld de artikelen 17, § 5 tot § 7, eerste lid, en 20, § 2, van het voorontwerp, die in feite niet de omzetting vormen van – volgens de concordantietabel – respectievelijk de artikelen 15, lid 4, en 14, lid 4 tot 6, van de NIS-richtlijn, en artikel 16, lid 4 en 8 van de NIS-richtlijn.

de ne pas induire en erreur quant à la correcte et complète transposition opérée par l’avant-projet lui-même [8];

— l’article 19, § 3, de l’avant-projet serait la transposition de l’article 17 de la directive NIS; or, ne fut-ce qu’aux termes de leurs contenus respectifs il ne semble pas que tel soit le cas, la première disposition imposant des obligations aux fournisseurs de service numérique quant à renseigner un point de contact pour la sécurité informatique tandis que la seconde concerne les autorités compétentes, leurs obligations en termes de contrôle et de moyens nécessaires à les exercer.

Ce tableau et le tableau en sens inverse seront en conséquence revus et, le cas échéant, le commentaire des articles complété des informations indispensables au destinataire de la règle pour en comprendre la portée.

3. C’est sous réserve de ces observations générales qui tiennent à la correcte et complète transposition de la directive NIS compte tenu des exigences de la directive elle-même et des règles de droit interne que les observations particulières suivantes sont formulées.

L’avant-projet sera revu pour en tenir compte.

OBSERVATIONS PARTICULIÈRES

Dispositif

Article 9

L’article 9, § 1er, alinéa 3, de l’avant-projet dispose

“[d]ans le respect des alinéas 1 et 2, il est dérogé, pour l’exécution de la présente loi, aux obligations de secret professionnel imposés par d’autres législations”.

Cette disposition ne peut suffire à garantir la sécurité juridique et la protection des personnes investies d’une obligation de secret professionnel qui pourraient être incriminées pour ne pas avoir respecté celui-ci et encourir de ce fait d’être sanctionnées pénalement.

La disposition doit indiquer précisément les législations qui sont ainsi concernées.

[8] Voir, par exemple, les articles 17, §§ 5 à 7, alinéa 1er, et 20, § 2, de l’avant-projet qui ne transposent pas à proprement parler respectivement, selon le tableau de concordance, les articles 15, paragraphe 4, et 14, paragraphes 4 à 6, de la directive NIS, et l’article 16, paragraphes 4 et 8 de la directive NIS.

Artikel 14

Het ontworpen artikel 14, § 4, eerste lid, bepaalt dat de daarin beoogde koninklijke besluiten vastgesteld zullen worden "[o]p voorstel van de Eerste minister en van de bevoegde ministers".

Zoals de afdeling Wetgeving daar evenwel in haar advies 60.490/1 van 10 januari 2017[9] aan heeft herinnerd,

"[worden,] [o]nder voorbehoud van de machtigingen die hij verleent, de beslissingen van de uitvoerende macht genomen door de Koning (artikel 37 van de Grondwet). Het komt de Koning toe, en niet de wetgevende macht, om met inachtneming van de desbetreffende grondwettelijke bepalingen, de organisatie en de werking van de uitvoerende macht te regelen, inzonderheid door de respectieve rol te bepalen die de Ministerraad, de eventuele ministeriële comités, de ministers, de diverse besturen en bestuursorganen vervullen bij de voorbereiding en de uitvoering van de beslissingen van de uitvoerende macht."

Het ontworpen artikel 14, § 4, eerste lid, moet dienovereenkomstig herzien worden.

Dezelfde opmerking geldt voor de ontworpen artikelen 17, § 5, tweede lid, en 7, eerste lid.

Artikel 17

Paragraaf 1, tweede lid, luidt:

"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.".

In de bespreking van het artikel staat het volgende:

"De aanbieder van essentiële diensten moet niet wachten tot hij over alle relevante informatie over een incident beschikt om het te melden. Wanneer hij uit de hem ter beschikking staande informatie reeds kan afleiden dat het incident een aanzienlijke impact heeft, moet hij het melden.

In eerste instantie is ervoor gekozen om de aanbieders te laten beoordelen of een incident een aanzienlijke impact kan hebben op de beschikbaarheid, vertrouwelijkheid, integriteit of authenticiteit van de door hen verleende essentiële diensten. De wet bepaalt dus geen criteria maar machtigt de Koning, na advies van het CCB, de ADCC en de sectorale overheden, alsook, in voorkomend geval, van de deelgebieden, om, per

[9] Advies 60.490/1, op 10 januari 2017 verstrekt over een voorontwerp dat ontstaan heeft gegeven aan de wet van 21 juli 2017 "tot instelling van een programma voor duurzame samenwerking op onderzoeksvlak tussen de federale wetenschappelijke instellingen en de universiteiten", *Parl.St.* Kamer 2016-17, nr. 2479/001, 41-45, *http://www.raadvst-consetat.be/dbx/adviezen/60490.pdf.*

Article 14

L'article 14, § 4, alinéa 1er, en projet prévoit que les arrêtés royaux qu'il vise seront adoptés "[s]ur proposition du Premier ministre et des Ministres compétents".

Cependant, et ainsi que l'a rappelé la section de législation dans son avis n° 60.490/1 donné le 10 janvier 2017 [9],

"Les décisions du pouvoir exécutif sont prises par le Roi sous réserve des habilitations qu'Il confère (article 37 de la Constitution). C'est au Roi, et non au pouvoir législatif, qu'il revient de régler, dans le respect des dispositions constitutionnelles en la matière, l'organisation et le fonctionnement du pouvoir exécutif, notamment en définissant le rôle respectif qu'assurent le Conseil des ministres, les comités ministériels éventuels, les ministres ainsi que les diverses administrations et organes de gestion dans la préparation et l'exécution des décisions du pouvoir exécutif".

L'article 14, § 4, alinéa 1er, en projet sera revu en conséquence.

La même observation vaut pour l'article 17, § 5, alinéa 2, et 7, alinéa 1er, en projet.

Article 17

Le paragraphe 1er, alinéa 2, précise

"[l]'obligation de notifier 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".

Le commentaire de l'article indique

"L'opérateur de services essentiels ne doit pas attendre de disposer de toutes les informations pertinentes sur un incident pour procéder à la notification. Lorsque les informations à sa disposition lui permette[nt] déjà de savoir qu'il s'agit d'un incident ayant un impact significatif, il convient qu'il le notifie.

Le choix a été fait, dans un premier temps, de laisser les opérateurs apprécier si l'incident est de nature à avoir un impact significatif sur la disponibilité, la confidentialité, l'intégrité ou l'authenticité des services essentiels qu'ils fournissent. La loi ne fixe donc pas de critères mais habilite le Roi, après avis du CCB, de la DGCC et des autorités sectorielles ainsi que, le cas échéant, des entités fédérées, à établir des niveaux

[9] Avis n° 60.490/1 donné le 10 janvier 2017 sur un avant-projet devenu la loi du 21 juillet 2017 "instaurant un programme de coopération durable sur le plan de la recherche entre les établissements scientifiques fédéraux et les universités", *Doc. parl.*, Chambre, 2016-2017, n° 2479/001, pp. 41-45, *http://www.raadvst-consetat.be/dbx/avis/60490.pdf.*

sector of deelsector, de weerslagniveaus of drempelwaarden te bepalen die noodzakelijkerwijs een aanzienlijke impact hebben.

Deze in paragraaf 7 vermelde mogelijkheid waarover de Koning beschikt, heeft tot doel om de aanbieders van essentiële diensten, indien nodig, meer rechtszekerheid te bieden wat de gevallen betreft waarin wordt aangenomen dat een incident noodzakelijkerwijs een aanzienlijke impact heeft. In afwachting van deze weerslagniveaus of drempelwaarden worden de aanbieders verzocht rekening te houden met alle gebeurtenissen die een impact hebben op de beschikbaarheid, vertrouwelijkheid, integriteit of authenticiteit van de informatiesystemen voor het verlenen van een essentiële dienst."

Artikel 17, § 1, tweede lid, van het voorontwerp, gelezen in het licht van de bespreking van het artikel, schept niet op afdoende wijze de rechtszekerheid en voorzienbaarheid van een norm die vereist is voor een bepaling waarvan de niet-naleving luidens artikel 26 van het voorontwerp van wet een strafrechtelijke wordt bestraft.

Het artikel moet dienovereenkomstig herzien worden.

Artikel 21

Het ontworpen artikel 21, § 1, tweede lid, bepaalt dat de sectorale overheid de inhoud en de overige regels die van toepassing zijn op de interne audit bedoeld in het eerste lid van dezelfde bepaling, kan vaststellen.

Zodoende delegeert de ontworpen bepaling een verordeningsbevoegdheid aan die overheid.

Uit bijlage IV van de ontworpen wet blijkt dat de aldus bedoelde "sectorale overheid" niet noodzakelijkerwijs noch in alle gevallen een politiek verantwoordelijke overheidsinstantie is, zoals dat het geval is voor een minister.

Volgens de vaste adviespraktijk van de afdeling Wetgeving is de delegatie van een verordeningsbevoegdheid aan een overheidsinstantie die niet politiek verantwoordelijk is, slechts

d'incidence ou des seuils, par secteur ou sous-secteur, constituant nécessairement un impact significatif.

Cette faculté laissée au Roi au paragraphe 7 vise à offrir si besoin une plus grande sécurité juridique aux opérateurs de services essentiels quant aux hypothèses dans lesquelles un incident doit nécessairement être "considéré comme ayant un impact significatif". Dans l'attente de tels niveaux d'incidence ou de seuils, les opérateurs seront invités à prendre en compte tous les événements ayant un effet sur la disponibilité, la confidentialité, l'intégrité ou l'authenticité des systèmes d'information liés à la fourniture d'un service essentiel".

L'article 17, § 1er, alinéa 2, de l'avant-projet, lu à la lumière du commentaire de l'article n'est pas suffisamment créateur de la sécurité juridique et de la prévisibilité de la norme requises pour une disposition dont le non-respect est assorti d'une sanction pénale aux termes de l'article 26 de l'avant-projet de loi.

Il sera en conséquence revu.

Article 21

L'article 21, § 1er, alinéa 2, en projet prévoit que l'autorité sectorielle peut déterminer le contenu et les autres règles applicables à l'audit interne visé à l'alinéa 1er de la même disposition.

Ce faisant, la disposition en projet délègue à cette autorité un pouvoir réglementaire.

Il ressort de l'annexe IV à la loi en projet que l' "autorité sectorielle" ainsi visée n'est pas nécessairement et dans tous les cas une autorité politiquement responsable, à l'instar d'un ministre.

Selon la légisprudence constante de la section de législation, la délégation d'un pouvoir réglementaire à une autorité qui n'est pas politiquement responsable, ne peut se concevoir

onder beperkende voorwaarden denkbaar.[10] Onder meer is vereist dat de verordeningen die op basis van die delegatie zijn vastgesteld, bekrachtigd worden door een overheidsinstantie die zelf politiek verantwoordelijk is.

De ontworpen bepaling voldoet niet aan die voorwaarde. Ze moet dus worden herzien.

Dezelfde opmerking geldt voor het ontworpen artikel 21, § 3, vierde lid.

Artikel 24

In paragraaf 5 staat dat de beëdigde leden van de inspectiedienst of van de sectorale overheid processen-verbaal kunnen opstellen die bewijskracht hebben tot het tegendeel is bewezen.

Het Grondwettelijk Hof heeft erop gewezen dat een dergelijke regel een uitzondering vormt op de algemene regel dat een proces-verbaal als een loutere inlichting geldt en derhalve ook op de regel van de vrije bewijslevering in strafzaken, waarbij de rechter, naar eigen overtuiging, de bewijswaarde van een bepaald element beoordeelt, zodat het verschil in behandeling dat eruit voortvloeit op een redelijke verantwoording dient te berusten en het de rechten van de beklaagde niet op een onevenredige wijze mag beperken.[11]

Het verdient bijgevolg aanbeveling in de bespreking van het voorontwerp te rechtvaardigen dat de processen-verbaal bedoeld in artikel 24, § 5, van het voorontwerp een bijzondere bewijskracht krijgen.

[10] Advies 42.387/VR, op 27 maart 2007 gegeven over een voorontwerp dat ontstaan heeft gegeven aan de wet van 15 mei 2007 "houdende instemming met het samenwerkingsakkoord tussen de Federale Overheid, het Vlaamse Gewest, het Waalse Gewest en het Brussels Hoofdstedelijk Gewest inzake de uitvoering van sommige bepalingen van het Protocol van Kyoto, afgesloten te Brussel, op 19 februari 2007", *Parl.St.* Senaat 2006-07, nr. 2411/1, 30-35, *http://www.raadvst-consetat.be/dbx/adviezen/42387.pdf;* advies 44.607/1, op 12 juni 2008 gegeven over een voorontwerp dat ontstaan heeft gegeven aan het decreet van 10 juli 2008 "betreffende het stelsel van leren en werken in de Vlaamse Gemeenschap", *Parl.St.* Vl.Parl. 2007-08, nr. 1760/1, 241-265, *http://www.raadvst-consetat.be/dbx/adviezen/44607.pdf*; advies 50.217/4, op 21 september 2011 gegeven over een ontwerp dat heeft geleid tot het koninklijk besluit van 2 december 2011 "betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer", *http://www.raadvst-consetat.be/dbx/avis/50217.pdf*. Zie ook J. Vande Lanotte, G. Goedertier, Y. Haeck, J. Goossens en T. De Pelsmaeker, *Belgisch Publiekrecht*, vol. 1, Brugge, Die Keure, 2015, 148-149. De afdeling Wetgeving heeft zich in dezelfde zin uitgesproken in advies 63.202/2, op 26 april 2018 gegeven over een voorontwerp van wet "tot oprichting van het informatieveiligheidscomité en tot wijziging van diverse wetten betreffende de uitvoering van Verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad 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".

[11] Zie bijvoorbeeld GwH 6 april 2000, nr. 40/2000, B.14.1, en GwH 14 februari 2001, nr. 16/2001, B.12.1.

qu'à des conditions restrictives [10]. Il est notamment requis que les règlements adoptés sur base de cette délégation fassent l'objet d'une ratification par une autorité qui, quant à elle, est politiquement responsable.

La disposition en projet ne satisfait pas à cette condition. Elle sera donc revue.

La même observation vaut pour l'article 21, § 3, alinéa 4, en projet.

Article 24

Au paragraphe 5, les membres assermentés du service d'inspection ou de l'autorité sectorielle peuvent rédiger des procès-verbaux faisant foi jusqu'à preuve du contraire.

La Cour constitutionnelle a souligné qu'une telle règle constitue une exception à la règle générale selon laquelle un procès-verbal vaut en tant que simple renseignement et dès lors également au régime de la libre administration de la preuve en matière répressive, selon lequel le juge apprécie, en fonction de sa propre conviction, la valeur probante d'un élément déterminé, de sorte que la différence de traitement qui en résulte doit être raisonnablement justifiée et ne peut restreindre les droits du prévenu de manière disproportionnée [11].

Il est par conséquent recommandé de justifier, dans le commentaire de l'avant-projet, l'attribution d'une force probante particulière aux procès-verbaux visés à l'article 24, § 5, de l'avant-projet.

[10] Avis n° 42.387/VR donné le 27 mars 2007 sur un avant-projet devenu la loi du 15 mai 2007 "portant assentiment à l'accord de coopération entre l'Autorité fédérale, la Région flamande, la Région wallonne et la Région de Bruxelles-Capitale relatif à la mise en œuvre de certaines dispositions du Protocole de Kyoto, conclu à Bruxelles, le 19 février 2007", *Doc. parl.,* Sénat, 2006-2007, n° 2411/1, pp 30-35, *http://www.raadvst-consetat.be/dbx/avis/42387.pdf;* avis n° 44.607/1 donné le 12 juin 2008 sur un avant-projet devenu le decret du 10 juillet 2008 "betreffende het stelsel van leren en werken in de Vlaamse Gemeenschap", *Doc. parl.*, Parl. fl., 2007-2008, n° 1760/1, pp. 241-265, *http://www.raadvst-consetat.be/dbx/avis/44607.pdf*; avis n° 50.217/4 donné le 21 septembre 2011 sur un projet devenu l'arrêté royal du 2 décembre 2011 "concernant les infrastructures critiques dans le sous-secteur du transport aérien", *http://www.raadvst-consetat.be/dbx/avis/50217.pdf*. Voir également J. Vande Lanotte, G. Goedertier, Y. Haeck, J. Goossens et T. De Pelsmaeker, *Belgisch Publiekrecht,* vol. 1, Bruges, Die Keure, 2015, pp. 148-149. La section de législation s'est prononcée dans le même sens dans l'avis n° 63.202/2 donné le 26 avril 2018 sur un avant-projet de loi "instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circ

[11] Voir, par exemple, C.C., 6 avril 2000, n° 40/2000, B.14.1, et C.C., 14 février 2001, n° 16/2001, B.12.1.

Artikel 26

Paragraaf 2 voorziet in een strafrechtelijke bestraffing van eenieder

"die de uitvoering van de controle door de leden van de inspectiedienst vrijwillig verhindert of belemmert, de informatie die hem gevraagd is naar aanleiding van deze controle weigert mee te delen, of opzettelijk foutieve of onvolledige informatie meedeelt."

Er wordt echter opgemerkt dat het recht om zichzelf niet te beschuldigen, dat gewaarborgd is door artikel 6 van het Europees Verdrag voor de rechten van de mens, verhindert dat een persoon, "tegen wie een vervolging is ingesteld" in de zin van die bepaling, kan worden bestraft omdat hij geweigerd heeft zijn medewerking te verlenen aan het bewijzen van zijn eigen schuld.[12]

Artikel 30

1. In paragraaf 2 is sprake van "werkdag". Aangezien dat begrip in juridisch opzicht nergens duidelijk omschreven wordt en het besluit normaal gezien zal worden toegepast in contexten waarin het begrip werkdag kan verschillen, zou het begrip moeten worden gedefinieerd, ofwel zou moeten worden voorzien in een termijn berekend in "dagen".

2. In paragraaf 3, *in fine*, dienen de woorden "artikel 25" te worden vervangen door de woorden "artikel 27".

Artikel 31

Men schrijve "aangetekende zending" in plaats van "ter post aangetekend schrijven", want door de liberalisering van de sector heeft Bpost het monopolie van dergelijke zendingen verloren.

Artikel 32

1. In de Franse tekst van het eerste lid schrijve men "introduire un recours" in plaats van "interjeter appel".

2. De steller wordt gewezen op de incoherentie dat wordt voorzien in procedurevormvereisten die gelden op straffe van ambtshalve uitgesproken nietigheid, terwijl de regeling inzake nietigheid sinds de inwerkingtreding op 1 november 2015 van de wet van 19 oktober 2015 "houdende wijziging van het burgerlijk procesrecht en houdende diverse bepalingen inzake justitie" herzien is zodat de rechter geen enkele mogelijkheid meer heeft om een exceptie van nietigheid op te werpen.

[12] Zie onder meer advies 60.619/2, op 25 januari 2017 gegeven over een voorontwerp dat heeft geleid tot de wet van 2 oktober 2017 "tot regeling van de private en bijzondere veiligheid", *Parl.St.* Kamer 2016-17, nr. 54-2388/001, 194 en referenties aangehaald in noot 44, *http://www.raadvst-consetat.be/dbx/adviezen/60619.pdf.*

Article 26

Le paragraphe 2, réprime pénalement

"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".

Il est toutefois rappelé que le droit de ne pas s'auto-incriminer, garanti par l'article 6 de la Convention européenne des droits de l'homme, fait obstacle à ce qu'une personne, "pénalement accusée" au sens de cette disposition, puisse être sanctionnée pour avoir refusé de prêter son concours à l'établissement de sa propre culpabilité [12].

Article 30

1. Au paragraphe 2, il est question de "jour ouvrable". Cette dernière notion ne recevant aucune qualification juridique précise et l'arrêté ayant vocation à s'appliquer dans des contextes dans lesquels la notion de jour ouvrable peut varier, il conviendrait soit de la définir, soit, de prévoir un délai calculé en "jours".

2. Au paragraphe 3, *in fine,* il y a lieu de remplacer les mots "l'article 25" par les mots "l'article 27".

Article 31

Il convient d'écrire "envoi recommandé" plutôt que "lettre recommandée à la poste" car, par l'effet d'un mouvement de libéralisation du secteur, Bpost a perdu le monopole de ce type d'envoi.

Article 32

1. À l'alinéa 1er, dans la version française, il y a convient d'écrire "introduire un recours" au lieu de "interjeter appel".

2. L'attention de l'auteur est attirée sur l'incohérence de prévoir des formalités de procédures sanctionnées par une nullité prononcée d'office alors que depuis l'entrée en vigueur, le 1er novembre 2015, de la loi du 19 octobre 2015 "modifiant le droit de la procédure civile et portant des dispositions diverses en matière de justice", le régime des nullités a été revu en supprimant toute possibilité pour le juge d'encore soulever une exception de nullité.

[12] Voir entre autres l'avis n° 60.619/2 donné le 25 janvier 2017 sur un avant-projet devenu la loi du 2 octobre 2017 "réglementant la sécurité privée et particulière", *Doc. parl.,* Chambre, 2016-2017, n° 54-2388/1, p. 194 et références citées à la note 44, *http://www.raadvst-consetat.be/dbx/avis/60619.pdf.*

Artikel 33

Er dient verwezen te worden naar artikel 32 in plaats van naar artikel 30.

Artikel 34

Het druist in tegen de rechtszekerheid om de verjaringstermijn te doen ingaan “te rekenen vanaf de dag waarop de feiten vastgesteld worden”. Die termijn moet ingaan vanaf de dag waarop de feiten zijn begaan.

Artikel 42[13]

Het ziet ernaar uit dat de ontworpen wijziging in de bepaling onder a) veeleer strekt tot vervanging dan tot wijziging van artikel 3, c), van de wet van 1 juli 2011.

Artikel 44

De afdeling Wetgeving begrijpt niet waarom niet in elke wet die met het oog op de omzetting van de richtlijn in kwestie door het voorontwerp wordt gewijzigd, een soortgelijk artikel wordt ingevoegd.

Artikel 47

De ontworpen paragraaf 4, in paragraaf 2, heeft als gevolg dat de sancties waarin is voorzien in geval van schending van de Europese richtlijn die door het voorontwerp wordt omgezet, zullen verschillen naargelang van de sector waarin die wet toepasselijk zal zijn, aangezien de “maatregelen”, bepaald bij artikel 79 van de wet van 21 november 2017 dat bij artikel 47 van het voorontwerp wordt gewijzigd, verschillen van de sancties waarin de artikelen 24 tot 34 van het voorontwerp voorzien.

De steller van het voorontwerp moet een dergelijk verschil kunnen rechtvaardigen.

De opmerking geldt *mutatis mutandis* voor artikel 50 van het voorontwerp, in zoverre het de artikelen 36/8 tot 36/12/3 en artikel 36/21 van de wet van 22 februari 1998 toepasselijk maakt op de Nationale Bank van België, die in het kader van de richtlijn die bij het voorontwerp wordt omgezet, optreedt als sectorale overheid.

*

*De griffier,* *De voorzitter,*

Anne-Catherine VAN GEERSDAELE — Martine BAGUET

[13] Dat artikel zou moeten worden samengevoegd met artikel 36 van het voorontwerp, aangezien beide artikelen wijzigingen aanbrengen in hetzelfde artikel.

Article 33

Il y a lieu de viser l’article 32 et non l’article 30.

Article 34

Il est contraire à la sécurité juridique de faire débuter le délai de prescription “à compter du jour où le fait est constaté”, ce délai doit courir à partir du jour où le fait est commis.

Article 42 [13]

Au a), la modification en projet paraît être appelée à devoir remplacer l’article 3, c), de la loi du 1er juillet 2011 plutôt qu’à le modifier.

Article 44

La section de législation n’aperçoit pas pourquoi un article similaire n’est pas introduit dans chacune des lois que l’avant-projet modifie pour transposer la directive concernée.

Article 47

Au paragraphe 2, le paragraphe 4 en projet a pour effet que les sanctions prévues pour la violation de la directive européenne transposée par l’avant-projet diffèreront selon le secteur dans lequel cette loi trouve à s’appliquer puisque les “mesures” prévues à l’article 79 de la loi du 21 novembre 2017 qui est modifiée par l’article 47 de l’avant-projet diffèrent des sanctions prévues par les articles 24 à 34 de l’avant-projet.

L’auteur de l’avant-projet doit être en mesure de justifier pareille différence.

L’observation vaut *mutatis mutandis* pour l’article 50 de l’avant-projet en tant que celui-ci rend applicable les articles 36/8 à 36/12/3 et l’article 36/21 de la loi du 22 février 1998 à la Banque Nationale de Belgique agissant comme autorité sectorielle dans le cadre de la directive transposée par l’avant-projet.

*

*Le greffier,* *Le président,*

Anne-Catherine VAN GEERSDAELE — Martine BAGUET

[13] Cet article devrait être fusionné avec l’article 36 de l’avant-projet puisqu’il apporte des modifications au même article que celui que l’article 36 de l’avant-projet modifie.

**VOORONTWERP VAN WET (II)**

**onderworpen aan het advies van de Raad van State**

**Voorontwerp van wet tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid**

TITEL 1

*Definities en algemene bepalingen*

HOOFDSTUK 1

**Onderwerp en toepassingsgebied**

**Afdeling 1**

*Onderwerp*

Art. 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 14, 15 en 30, alsook hoofdstuk 3 van titel 3 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 hoofdvestiging in België hebben. Een digitaledienstverlener wordt geacht zijn hoofdvestiging in België te hebben als zijn hoofdkantoor 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

**AVANT-PROJET DE LOI (II)**

**soumis à l'avis du Conseil d'État**

**Avant-projet de loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique**

TITRE 1ER

*Définitions et dispositions générales*

CHAPITRE 1ER

**Objet et champ d'application**

**Section 1re**

*Objet*

Art. 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 14, 15 et 30, ainsi que du chapitre 3 du titre 3 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 l'établissement principal est situé en Belgique. Un fournisseur de service numérique est réputé avoir son établissement 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

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 elektronische-communicatienetwerken of openbare elektronische-communicatiediensten, 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 vorige 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 van de wet, met uitzondering van de bepalingen van titel I, hoofdstuk 1 van titel II en van artikel 26.

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 van de 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 operatoren die behoren tot de sector financiën in de zin van bijlage I van de wet zijn onderworpen aan de artikelen 65 tot 67.

In afwijking op wat voorafgaat zijn de artikelen 65 tot 67 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.

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 précédent.

§ 3. La présente loi n'est pas applicable aux opérateurs relevant du secteur des finances au sens de l'annexe I de la loi, à l'exception des dispositions du titre I, du chapitre 1er du titre II et de l'article 26.

Par dérogation à l'alinéa premier, l'article 52 est applicable aux 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 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 loi sont soumis aux articles 65 à 67.

Par dérogation à ce qui précède, les articles 65 à 67 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. 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 vorige 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. 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 2011/93/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.

§ 2. 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.

§ 3. 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 in Ministerraad overlegd besluit;

§ 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 précédent, 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. 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 2011/93/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.

§ 2. 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.

§ 3. 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° “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;

5° “instelling voor de conformiteitsbeoordeling”: instelling bedoeld in artikel I.9 van het Wetboek van economisch recht die conformiteitsbeoordelingsactiviteiten verricht, zoals onder meer kalibratie, proeven, certificatie en keuring;

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

7° “accreditatieautoriteit”: instelling die door de Koning is opgericht in uitvoering van artikel VIII.30 van het wetboek van economisch recht;

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 punten 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 en 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 van de wet, die aan de criteria bedoeld in artikel 12, § 1, voldoet en die als dusdanig is aangewezen door de sectorale overheid;

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;

5° “organisme d’évaluation de la conformité”: organisme visé à l’article I.9 du Code de droit économique et qui effectue des opérations d’évaluation de la conformité, comme l’étalonnage, les essais, la certification et l’inspection;

6° “audit de certification”: un audit réalisé dans le cadre d’une certification visée à l’article 22, § 2;

7° “autorité d’accréditation”: organisme créé par le Roi en exécution de l’article VIII.30 du Code de droit économique;

8° “réseau et système d’information”:

a) un réseau de communications électroniques au sens de l’article 2, 3°, de la loi du 13 juin 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 loi, qui répond aux critères visés à l’article 12, § 1er, et qui est désignée comme telle par l’autorité sectorielle;

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 van de wet;

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 van 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 van 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 de aanbieders van essentiële diensten hebben 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 van 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, of de bevoegde sectorale overheid kan worden gecontacteerd in plaats van de digitaledienstverlener, wat de uit deze wet voortvloeiende verplichtingen betreft;

23° “internetknooppunt (IXP)”: een netwerkinfrastructuur die de onderlinge verbinding van meer dan twee onafhankelijke

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 loi;

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, ou l’autorité sectorielle compétente à la place du fournisseur de 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

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., 2°, van het Wetboek van economisch recht, en/of ondernemers, zoals gedefinieerd in artikel I.8, 39°, van hetzelfde Wetboek, mogelijk maakt online verkoop- of dienstenovereenkomsten met ondernemers te sluiten op de website van de onlinemarktplaats of op de website van een ondernemer 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.

autonomes indépendants, essentiellement aux fins de faciliter l'échange de trafic internet; un IXP n'assure l'interconnexion que pour des systèmes autonomes; un IXP n'exige pas que le trafic internet passant entre une paire quelconque de systèmes autonomes participants transite par un système autonome tiers, pas plus qu'il ne modifie ou n'altère par ailleurs un tel trafic;

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 administre et gère l'enregistrement de 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., 2°, du Code de droit économique et/ou à des professionnels, au sens de l'article I.8, 39°, du même Code, de conclure des contrats de vente ou de service en ligne avec des professionnels, soit sur le site internet de la place de marché en ligne, soit sur le site internet d'un professionnel qui utilise les services informatiques fournis par la place de marché en ligne;

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.

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 Samenwerkingsgroep en het CSIRT-netwerk. Daartoe vertegenwoordigt het contactpunt België binnen de Samenwerkingsgroep bedoeld in artikel 11 van de NIS-richtlijn.

§ 2. De Koning wijst de autoriteit aan die de rol van nationaal CSIRT vervult, namelijk het nationale computer security incident response team.

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 in Ministerraad overlegd besluit, de sectorale overheden aan die, voor hun respectievelijke sector, belast zijn met het toezicht op de uitvoering van de bepalingen van deze wet.

De Koning kan sectorale overheden oprichten, bestaande uit vertegenwoordigers van de Federale Staat, de Gemeenschappen en de Gewesten, overeenkomstig de modaliteiten 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 § 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.

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 et le réseau des CSIRT. A cette fin, le point de contact représente la Belgique au sein du Groupe de coopération visé à l'article 11 de la directive NIS.

§ 2. Le Roi désigne l'autorité chargée d'assurer le rôle de CSIRT national, qui est le centre national de réponse aux incidents de sécurité informatique.

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.

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 § 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.

**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 § 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 7de 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

**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 § 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, 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 en rapport 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

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. Bij die uitwisseling van informatie wordt de vertrouwelijkheid van de informatie gewaarborgd en worden de veiligheids- en 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 in Ministerraad overlegd besluit, de autoriteit aan die belast is met de actualisering van de nationale strategie voor de beveiliging van netwerk- en informatiesystemen.

§ 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;

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 au minimum nécessaire et sont proportionnées à l'objectif de cet échange. 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 en matière de sécurité des réseaux et des systèmes d'information.

§ 2. La stratégie visée au paragraphe 1er est mise à jour, après avis des autorités visées à l'article 7 et, le cas échéant, des autorités de contrôle des données à caractère personnel. Elle couvre au moins les secteurs visés à l'annexe I et les services visés à l'annexe II.

Cette stratégie définit les objectifs stratégiques et réglementaires appropriées en vue de parvenir à un niveau élevé de sécurité des réseaux et des systèmes d'information et de le maintenir.

§ 3. La stratégie nationale en matière de sécurité des réseaux et des systèmes d'information porte, entre autres, sur les points suivants:

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

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

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

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

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

f) 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 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. In samenwerking met de aangewezen 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;

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. En collaboration avec l'opérateur de services essentiels désigné, 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.

Au minimum, l'autorité sectorielle réexamine et, le cas échéant, met à jour l'identification des opérateurs de services essentiels et de leurs services essentiels 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) 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

§ 1. Om het belang van het in artikel 12, § 2, c), bedoelde verstorende effect vast te stellen, bepaalt de sectorale overheid sectorale en/of intersectorale criteria, weerslagniveaus en 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.

b) la fourniture de ce service est tributaire des réseaux et des systèmes d'information; et

c) un incident serait susceptible d'avoir un effet perturbateur important sur la fourniture dudit service, en tenant compte des critères et des niveaux d'incidence ou seuils visés à l'article 13.

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

Art. 13

§ 1er. Afin de déterminer l'importance de l'effet perturbateur visé à l'article 12, § 2, c), l'autorité sectorielle établit, pour son secteur, des critères sectoriels et/ou intersectoriels, des niveaux d'incidence et 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, 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) la portée géographique eu égard à la zone 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

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 meegedeelde relevante informatie wordt overgemaakt 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 gemotiveerd voorstel van lijst van potentiële aanbieders van essentiële diensten in haar sector, samen met een of meer toegepaste identificatiecriteria.

Wanneer geen enkele potentiële aanbieder van essentiële diensten is geïdentificeerd binnen een sector of deelsector, licht de sectorale overheid 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 gemotiveerde voorstel van lijst, in voorkomend geval na raadpleging van de gewesten en gemeenschappen.

§ 2. Wanneer de sectorale overheid vaststelt dat de potentiële 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 gemotiveerde 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 de 3 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.

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 potentiels dans son secteur avec le ou les critères d'identification retenus.

Lorsqu'aucun opérateur de services essentiels potentiel n'a été identifiée 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'opérateur de services essentiels potentiels 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 3 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.

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

Art. 17

Onverminderd de eventuele toepassing van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen worden de bestuursdocumenten betreffende de toepassing van dit artikel 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 betreffende de beveiliging en de bescherming van de kritieke infrastructuren 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 11, § 9, is van toepassing op de gemotiveerde beslissing tot aanwijzing van een exploitant van een kritieke infrastructuur als aanbieder van essentiële diensten.

Art 19

De Koning kan, bij in Ministerraad overlegd besluit, andere sectoren of soorten aanbieders toevoegen aan bijlage I van deze wet.

L'autorité sectorielle communique ce descriptif à l'autorité visée à l'article 7, § 1er.

Art. 17

Sans préjudice de l'application éventuelle de la loi du 11 décembre 1998 relative à la classification, aux habilitations, attestations et avis de sécurité, les documents administratifs liés à l'application du présent article, 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 communiqué sous forme d'une 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 relative à la sécurité et à la protection des infrastructures critiques 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 11, § 9, 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.

HOOFDSTUK 2

**Beveiligingsmaatregelen**

Art. 20

§ 1. 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, gezien de stand van de techniek, 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 in het I.B.B.

§ 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 betreffende de beveiliging en de bescherming van de kritieke infrastructuren en in artikel 11 van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van

CHAPITRE 2

**Mesures de sécurité**

Art. 20

§ 1. 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.

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 relative à la sécurité et la protection des infrastructures critiques et à l'article 11 de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien sont assimilées à la

het 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 in Ministerraad overlegd besluit.

Het in het eerste lid bedoelde besluit wordt genomen na advies van de 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 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 in paragraaf 1 bedoelde sectorale overheid.

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

P.S.I. lorsque toutes les informations visées au paragraphe 2 y sont reprises.

Art. 22

§ 1er. La PSI 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 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 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 PSI.

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 aux 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 visée 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.

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.

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, 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.

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 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.

La Banque nationale de Belgique 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 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 sont portés à son attention 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 doit, dans le respect du droit de l'Union ou de la législation nationale conforme au droit de l'Union, préserver la sécurité et les intérêts commerciaux de l'opérateur de services essentiels ainsi que la confidentialité des informations communiquées dans sa notification.

Le CSIRT national transmet les notifications visées au premier alinéa 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. 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 belast met de modaliteiten voor de melding en rapportering van incidenten bepalen, met inbegrip van de oprichting van een beveiligd meldingsplatform.

Via dit platform kunnen aanbieders van essentiële diensten ook inbreuken in verband met persoonsgegevens melden aan de Gegevensbeschermingsautoriteit, 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.

§ 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*

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 1

**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.

§ 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, en ce compris, 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, premier alinéa, 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.

§ 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*

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 1ER

**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.

Deze maatregelen zorgen, gezien de stand van de techniek, 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.

§ 3. De beveiligingsmaatregelen voldoen aan de uitvoeringsverordeningen van de Europese Commissie, waaronder Uitvoeringsverordening (EU) 2018/151 van 30 januari 2018 tot vaststelling van toepassingsbepalingen voor Richtlijn (EU) 2016/1148 wat betreft de nadere specificatie van de 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.

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 2

**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.

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

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.

§ 3. Les mesures de sécurité sont conformes aux Règlements d'exécution de la Commission européenne, dont celui du 30 janvier 2018 (UE) 2018/151 portant modalités d'application de la Directive (UE) 2016/1148 précisant les éléments à prendre en considération 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.

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 2

**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. 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 modaliteiten en via het platform bedoeld in artikel 31

§ 2. Indien geen meldingsplatform bestaat of indien dit niet beschikbaar is, bezorgt de digitaledienstverlener zijn melding via beveiligde communicatiemiddelen die door de Koning worden bepaald.

§ 3. Via het platform bedoeld in artikel 31 van deze wet kunnen digitaledienstverleners ook inbreuken in verband met persoonsgegevens melden aan de Gegevensbeschermingsautoriteit, 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 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

§ 2. La notification se fait conformément aux Règlements d'exécution de la Commission européenne, dont celui du 30 janvier 2018 (UE) 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. En cas d'absence ou en cas d'indisponibilité de la plate-forme de notification, le fournisseur de service numérique adresse sa notification par les moyens sécurisés de communication définis par le Roi.

§ 3. La plate-forme visée à l'article 31 de la présente loi 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, premier alinéa, 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. Lorsque c'est approprié, et notamment si l'incident visé au 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, lorsque c'est approprié, les autorités ou les CSIRTs 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

beheersen, of wanneer de openbaarmaking van het incident anderszins in het algemeen belang is.

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 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.

incident en cours ou lorsque la divulgation de l’incident est dans l’intérêt public à d’autres égards.

TITRE 4

*Contrôle et sanctions*

CHAPITRE 1ER

**Les contrôles des opérateurs de services essentiels**

**Section 1re**

*Audits*

Art. 38

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

L’opérateur de services essentiels transmet les rapports d’audit interne, dans les trente jours, à l’autorité sectorielle.

§ 2. L’opérateur de services essentiels fait réaliser, au moins tous les trois ans et à ses frais, un audit externe réalisé par un organisme d’évaluation de la conformité accrédité par l’autorité 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. Bij in Ministerraad overlegd besluit 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.

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

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

Art. 40

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

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

Art. 41

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

**Section 2**

*Service d'inspection*

Art. 42

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

§ 2. L'autorité visée à l'article 7, § 1er, ou l'autorité sectorielle peut recommander, de manière motivée, au service d'inspection de réaliser des contrôles.

Après avis de l'autorité sectorielle et de l'autorité visée à l'article 7, § 1er, le Roi peut fixer les éventuelles modalités sectorielles pratiques du contrôle.

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

Le service d'inspection peut faire appel à des experts.

Art. 43

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.

§ 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.

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.

§ 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. Om een machtiging tot betreding van bewoonde lokalen te bekomen, richten de personeelsleden van de inspectiedienst of van de sectorale overheid 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.

Bezoeken aan bewoonde lokalen zonder toestemming van de bewoner gebeuren tussen vijf en eenentwintig uur door minstens twee leden van de inspectiedienst of van de sectorale overheid 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.

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 informatica systeem en de erin opgenomen gegevens die zij nodig hebben voor hun

§ 4. Pour obtenir l'autorisation de pénétrer dans des locaux habités, les membres du personnel du service d'inspection ou de l'autorité sectorielle 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.

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 ou de l'autorité sectorielle agissant conjointement.

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

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

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

3° qu'elle a le droit de garder le silence et de ne pas contribuer à sa propre incrimination.

Toute personne interrogée peut utiliser les documents en sa possession, sans que cela puisse entraîner le report de l'audition. Elle peut, lors de l'audition ou ultérieurement, exiger que ces documents soient joints à l'audition.

L'audition mentionne avec précision l'heure à laquelle elle a pris cours, est éventuellement interrompue et reprise, et prend fin. Elle mentionne l'identité des personnes qui 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

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 of van de sectorale overheid, tegen een ontvangstbewijs dat een inventaris bevat, het informatica systeem en de erin opgenomen gegevens in beslag nemen.

Art. 45

§ 1. Na elke inspectie stelt de inspectiedienst een verslag op en bezorgt 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 of van de sectorale overheid 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 in Ministerraad overlegd besluit 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 berekenings- en betalingsmodaliteiten.

HOOFDSTUK 2

**Toezicht op de digitaledienstverleners**

Art. 47

§ 1. De Koning bepaalt de praktische modaliteiten van het toezicht op de digitaledienstverleners.

§ 2. De digitaledienstverlener moet met name:

a) 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;

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 ou de l'autorité sectorielle peuvent saisir, contre récépissé contenant un inventaire, le système informatique et les données qu'il contient.

Art. 45

§ 1er. Après chaque inspection, le service d'inspection rédige un rapport et en transmet 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 ou de l'autorité sectorielle 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, 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) 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 lidstatenlanden, 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.

§ 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 controleverslagen van een digitaledienstverlener te bezorgen.

§ 8. De Koning kan, bij in Ministerraad overlegd besluit 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 berekenings- en betalingsmodaliteiten.

HOOFDSTUK 3

**De sancties**

**Afdeling 1**

*Procedure*

Art. 48

§ 1. Wanneer een of meer inbreuken op de eisen van de wet, de koninklijke besluiten 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.

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, § 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 de contrôle 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 royaux 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.

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

§ 2. De inspectiedienst deelt de overtreder vooraf, op gemotiveerde 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 proces-verbaal door de beëdigde leden van de inspectiedienst. 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 die de in de artikel 14 bedoelde informatieverplichtingen 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 36 wordt bestraft met een gevangenisstraf

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 qui ne se conforme pas aux obligations d'information visées à l'article 14.

§ 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

van acht dagen tot een jaar en een geldboete van 26 euro tot 20 000 euro of met een van beide straffen.

§ 2. Niet-naleving van een van de beveiligingsverplichtingen opgelegd door de Koning of de sectorale overheid krachtens artikel 21 of 34 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 beide straffen.

§ 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 beide straffen.

§ 4. Niet-naleving van een van de informatieverplichtingen bedoeld in artikel 14 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 beide straffen.

§ 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 beide straffen.

§ . 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 voornoemde inbreuken.

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, paragrafen 2 en 3, van deze wet geven aanleiding tot 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 36 wordt bestraft met een geldboete van 500 tot 75 000 €.

l'une de ces peines seulement quiconque ne se conforme pas à une des obligations de notification d'incidents visées aux articles 24 ou 36.

§ 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 34.

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

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

§ 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 auxdites infractions.

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, paragraphes 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 € quiconque ne se conforme pas aux obligations de notification d'incidents visées aux articles 24 ou 36.

§ 3. Niet-naleving van de beveiligingsverplichtingen opgelegd door de Koning of de sectorale overheid krachtens artikel 21 of 34 wordt bestraft met een geldboete van 500 tot 100 000 €.

§ 4. Niet-naleving van de informatieverplichtingen bedoeld in artikel 14 wordt bestraft met een geldboete van 500 tot 125 000 €.

§ 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 €.

§ 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 €.

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 gemotiveerd. Ze vermeldt ook het bedrag van de administratieve geldboete en de bedoelde inbreuken.

§ 2. De sectorale overheid bezorgt de overtreder op voorhand haar gemotiveerd 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. Est puni d'une amende de 500 à 100 000 € quiconque ne se conforme pas aux obligations de sécurité imposées par le Roi ou l'autorité sectorielle en vertu des articles 21 ou 34.

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

§ 5. Est puni d'une amende de 500 à 200 000 € 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 € 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 manquements 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. Rekening houdend met de aangevoerde verweermiddelen binnen de in paragraaf 2 bedoelde termijn en bij gebrek aan een antwoord van de overtreder binnen diezelfde termijn, kan de sectorale overheid een in artikel 25 bedoelde administratieve sanctie opleggen.

§ 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 ingeleid bij verzoekschrift op tegenspraak dat, op straffe van verval, binnen de 60 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 de 24 uur op straffe van tenuitvoerlegging door beslag, alsook een boekhoudkundige verantwoording van de gevorderde bedragen en een afschrift van de uitvoerbaarverklaring.

§ 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 25.

§ 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.

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 60 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 délégué 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 24 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. 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 de vijftien dagen te rekenen vanaf de betekening van het dwangbevel.

De bepalingen van hoofdstuk VIII, 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 deel V 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.

§ 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, 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 partie V 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 est commis.

Le paiement selon la procédure administrative éteint également la possibilité d'engager des poursuites pénales pour les faits visés.

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 de 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 extra 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*

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, diffusion de messages d'alerte, annonces et 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 normalisées pour les procédures de gestion des risques et incidents, ainsi que les 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

*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.

Zijn communicatiekanalen moeten voorts duidelijk worden gespecificeerd en bekend zijn bij de gebruikersgroep en de samenwerkingspartners.

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 continuiteit gewaarborgd is. Hiertoe wordt voorzien in redundante systemen en reservewerkruimten.

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 gebruiken van te maken, zelfs die gegevens voortkomend 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.

et disposer de plusieurs moyens pour être contactés et contacter autrui à tout moment.

De plus, ses canaux de communication doivent être clairement précisés et bien connus des partenaires et collaborateurs.

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.

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, révéler, divulguer à une autre personne, ou 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.

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 risico- en analyse van sectorale 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 extra 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 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.

Zijn communicatiekanalen moeten voorts duidelijk worden gespecificeerd en bekend zijn bij de gebruikersgroep en de samenwerkingspartners.

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.

CHAPITRE 2

**Le CSIRT sectoriel**

**Section 1re**

*Tâches du CSIRT sectoriel*

Art. 63

Les tâches d'un CSIRT sectoriel sont, en coordination avec le CSIRT national, au moins les suivantes:

a) le suivi des incidents sectoriels;

b) l'activation du mécanisme d'alerte précoce, diffusion de messages d'alerte, annonces et diffusion d'informations sur les risques et 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 concernant 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 services de communication en évitant les points uniques de défaillance et disposer de plusieurs moyens pour être contactés et contacter autrui à tout moment.

De plus, ses canaux de communication doivent être clairement précisés et bien connus des partenaires et collaborateurs.

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

TITEL 6

*Verwerking van persoonsgegevens*

Art. 65

§ 1. Overeenkomstig artikel 23.1, a), b), c), d), e), h), van Art. 20 Verordening (EU) nr. 2016/679 van het Europees Parlement en de Raad 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), worden bepaalde verplichtingen en rechten van deze verordening beperkt of uitgesloten, zonder afbreuk te doen aan de wezenlijke inhoud van de grondrechten en fundamentele vrijheden en 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, in het kader van het melden van incidenten, als bedoeld in hoofdstuk 3 van titel 2 en hoofdstuk 2 van titel 3. Deze artikelen zijn evenmin van toepassing op het toezicht bedoeld in titel 4.

§ 3. De betrokken verwerkingsverantwoordelijke is de aanbieder van essentiële diensten, de digitaledienstverlener, de inspectiedienst of de autoriteit bedoeld in artikel 7, elk voor de gegevens die hij of zij bezit in het kader van voormelde opdrachten.

§ 4. De vrijstelling geldt voor alle categorieën van persoonsgegevens die door de verwerkingsverantwoordelijke(n) worden verwerkt voor de doeleinden bedoeld in paragraaf 2, alsook voor de daarmee verband houdende voorbereidende werkzaamheden of de procedures voor de eventuele toepassing van een administratieve sanctie. Elke verwerkingsverantwoordelijke moet passende maatregelen nemen om elke vorm van misbruik of onrechtmatige toegang of overdracht van voormelde persoonsgegevens te voorkomen.

§ 5. De persoonsgegevens waarvoor de vrijstelling bedoeld in paragraaf 2 geldt, worden niet langer bewaard dan noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt, met een maximale bewaartermijn die de duur van de verjaringstermijn van de eventuele inbreuken bedoeld in de artikelen 51 en 52 niet mag overschrijden.

Art. 66

In uitvoering van artikel 37.4 van de verordening wijst een aanbieder van essentiële diensten, een digitaledienstverlener of een autoriteit bedoeld in artikel 7 van de wet die persoonsgegevens verwerken een functionaris voor

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.

TITRE 6

*Traitement des données à caractère personnel*

Art. 65

§ 1er. En application de l'article 23.1, a), b), c), d), e), h), du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la Directive 95/46/CE (règlement général sur la protection des données), certaines obligations et droits prévus par ledit règlement sont limités ou exclus, sans porter préjudice à l'essence des libertés et droits fondamentaux et dans la stricte mesure nécessaire au but poursuivi.

§ 2. Les articles 12 à 22 dudit règlement ne sont pas applicables aux traitements de données à caractère personnel effectués par un opérateur de services essentiels, un fournisseur de service numérique ou une autorité visée à l'article 7, dans le cadre des notifications d'incidents visées aux chapitres 3 du titre 2 et 2 du titre 3, et aux contrôles visés au titre 4.

§ 3. Le responsable du traitement concerné est soit l'opérateur de services essentiels, soit le fournisseur de service numérique, soit le service d'inspection, soit l'autorité visée à l'article 7, chacun pour les données qu'il détient dans le cadre des missions précitées.

§ 4. L'exemption vaut pour toutes les catégories de données à caractère personnel traitées par le ou les responsables du traitement en lien avec les finalités visées au paragraphe 2, ainsi qu'aux actes préparatoires y relatifs ou aux procédures visant à l'application éventuelle d'une sanction administrative. Chaque responsable du traitement est tenu de prendre des mesures appropriées pour éviter toute forme d'abus, d'accès ou de transfert illicites desdites données à caractère personnel.

§ 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 aux articles 51 et 52.

Art. 66

En exécution de l'article 37.4 du règlement, un opérateur de service essentiel, un fournisseur de service numérique ou une autorité visée à l'article 7 de la loi qui traitent des données à caractère personnel désigne un délégué à la

gegevensbescherming aan. Dit is noodzakelijk wanneer de verwerking van die gegevens waarschijnlijk een hoog risico inhoudt als bedoeld in artikel 35 van de verordening.

Art. 67

§ 1. De betrokkenen kunnen een verzoek in verband met hun rechten 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 recht op rectificatie, 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 65 zou ondermijnen. Afhankelijk van de complexiteit van de verzoeken en van het aantal ervan kan die termijn indien nodig worden 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. De betrokken verwerkingsverantwoordelijke wordt vrijgesteld van het meedelen van een inbreuk in verband met persoonsgegevens aan een of meer welbepaalde betrokkenen, in de zin van artikel 34 van de voormelde Europese verordening, wanneer en voor zover deze individuele kennisgeving de verwezenlijking van de doelstellingen van deze wet, of de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of van inbreuken op deze wet, in het gedrang zou brengen.

protection des données, nécessairement lorsque le traitement de ces données peut engendrer un risque élevé tel que visé à l'article 35 du règlement.

Art. 67

§ 1er. Les personnes concernées peuvent adresser une demande concernant leur droits 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 à son droit de rectification, 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 65. 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 aux informations limitées concernant le traitement de ses données à caractère personnel, dans la mesure où cette communication ne compromet pas la réalisation des objectifs de la présente loi, de manière telle que la personne concernée se trouve dans l'impossibilité de savoir si elle fait l'objet d'une enquête ou pas, et sans pouvoir en aucun cas rectifier, effacer, limiter, notifier, transmettre à un tiers des données personnelles, ni cesser toute forme de traitement desdites données qui soit nécessaire dans le cadre défini ci-avant.

§ 5. 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 européen précité, lorsque et dans la mesure où une telle notification individuelle risque de compromettre la réalisation des objectifs de la présente loi ou la prévention, la détection, la recherche et la poursuite d'infractions pénales ou de manquements à la présente loi.

TITEL 7

*Slotbepalingen*

HOOFDSTUK 1

**Bescherming van de uitvoerende personeelsleden**

Art. 68

§ 1. De personen die optreden voor rekening van een aanbieder van essentiële diensten of digitaledienstverlener mogen geen nadelige gevolgen ondervinden vanwege de aanbieder van essentiële diensten of digitaledienstverlener ingevolge de uitvoering, te goeder trouw en in het kader van hun functie, van de verplichtingen die voortvloeien uit deze wet.

§ 2. De beslissingen genomen in strijd met paragraaf 1 zullen worden beschouwd als nietig en zonder rechtsgevolgen.

HOOFDSTUK 2

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

Art. 69

Artikel 2 van de wet van 1 juli 2011 wordt aangevuld met een derde lid, als volgt:

"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. 70

Artikel 3 van de wet van 1 juli 2011 wordt gewijzigd als volgt:

— in punt 3°:

"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);

TITRE 7

*Dispositions finales*

CHAPITRE 1ER

**Protection des agents d'exécution**

Art. 68

§ 1er. Les personnes qui agissent pour le compte d'un opérateur de services essentiels ou d'un fournisseur de service numérique ne peuvent subir de conséquences négatives de la part de l'opérateur de services essentiels ou du fournisseur de service numérique en raison de l'exécution, de bonne foi et dans le cadre de leurs fonctions, des obligations découlant de la présente loi.

§ 2. Les décisions prises en contradiction avec le paragraphe 1er seront considérées comme nulles et sans effet juridique.

CHAPITRE 2

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

Art. 69

L'article 2 de la loi du 1er juillet 2011 est complété par un troisième 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. 70

L'article 3 de la loi du 1er juillet 2011 est modifié comme suit:

— au point 3°:

"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);

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 wet of door de Koning bij in Ministerraad overlegd besluit;

g) voor de sector water: de overheid aangewezen door de wet of door de Koning bij in Ministerraad overlegd besluit;";

— een nieuw punt 13°: "13° "de wet van xx xx 2018": de wet van xx xx 2018 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;";

— een nieuw punt 14°: "14° "beveiliging van netwerk- en informatiesystemen": de beveiliging van netwerk- en informatiesystemen als bedoeld in artikel 6, 8° en 9°, van de wet van xx xx 2018;";

— een nieuw punt 15°: "15° "digitale infrastructuren": de aanbieders bedoeld in punt 6 van bijlage 1 van de wet van xx xx 2018;";

— een nieuw punt 16°: "16° "water": de aanbieders bedoeld in punt 5 van bijlage 1 van de wet van xx xx 2018;";

— een nieuw punt 17°: "17° "gezondheidszorg": de aanbieders bedoeld in punt 4 van bijlage 1 van de wet van xx xx 2018.".

Art. 71

Artikel 4, § 4, van de wet van 1 juli 2011 wordt gewijzigd als volgt:

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

Art. 72

In artikel 5 van de wet van 1 juli 2011 wordt een paragraaf 3 toegevoegd, luidende:

"§ 3. Tijdens het hele identificatieproces als bedoeld in deze afdeling wordt de autoriteit bedoeld in artikel 7, § 1, van de wet van xx 2018 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.".

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 la loi ou par le Roi, par arrêté délibéré en Conseil des ministres;

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

— un nouveau point 13°: "13° "la loi du xx xx 2018": la loi du xx xx 2018 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique;";

— un nouveau point 14°: "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 xx xx 2018;";

— un nouveau point 15°: "15° "infrastructures numériques": opérateurs visés au point 6 de l'annexe 1 de la loi du xx xx 2018;";

— un nouveau point 16°: "16° "eau": opérateurs visés au point 5 de l'annexe 1 de la loi du xx xx 2018;";

— un nouveau point 17°: "17° "santé": opérateurs visés au point 4 de l'annexe 1 de la loi du xx xx 2018.".

Art. 71

L'article 4, § 4, de la loi du 1er juillet 2011 est modifié comme suit:

"Le présent chapitre s'applique au secteur des finances, aux opérateurs de plate-forme de négociation visés à l'article 3, 3°, d) de la loi, au secteur des communications électroniques, au secteur des infrastructures numériques, au secteur de la santé et au secteur de l'eau, en ce qui concerne la sécurité et la protection des infrastructures critiques nationales.".

Art. 72

A l'article 5 de la loi du 1er juillet 2011, un paragraphe 3 est ajouté et 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 xx xx 2018 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. 73

Op het einde van paragraaf 2 van artikel 14 van de wet van 1 juli 2011 worden de volgende woorden toegevoegd:

"en, in voorkomend geval, de autoriteit bedoeld in artikel 7, § 1, van de wet van xx 2018 wat de beveiliging van netwerk- en informatiesystemen betreft.".

Art. 74

In artikel 18 van de wet van 1 juli 2011 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 xx 2018, wat de beveiliging van netwerk- en informatiesystemen betreft,".

Art. 75

In artikel 19 van de wet van 1 juli 2011 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 xx 2018, wat de beveiliging van netwerk- en informatiesystemen betreft,".

Art. 76

In artikel 22 van de wet van 1 juli 2011 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 xx 2018,".

Art. 77

Op het einde van paragraaf 2 van artikel 24 van de wet van 1 juli 2011 wordt de volgende zin toegevoegd:

"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. Niettemin kan de Autoriteit voor Financiële Diensten en Markten haar inspectieopdrachten delegeren, mits akkoord van de opdrachtnemer.".

Art. 73

A la fin du paragraphe 2 de l'article 14 de la loi du 1er juillet 2011, il est ajouté les mots:

"et, le cas échéant, l'autorité visée à l'article 7, § 1er, de la loi du xx xx 2018, pour ce qui concerne la sécurité des réseaux et systèmes d'information.".

Art. 74

A l'article 18 de la loi du 1er juillet 2011, les mots "La DGCC, les services de police et l'OCAM" sont remplacés par "La DGCC, les services de police, l'OCAM et, le cas échéant, l'autorité visée à l'article 7, § 1er, de la loi du xx xx 2018 pour ce qui concerne la sécurité des réseaux et systèmes d'information,".

Art. 75

A l'article 19 de la loi du 1er juillet 2011, 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 "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 xx xx 2018 pour ce qui concerne la sécurité des réseaux et systèmes d'information,".

Art. 76

A l'article 22 de la loi du 1er juillet 2011, 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 xx xx 2018,".

Art. 77

A la fin du paragraphe 2 de l'article 24 de la loi du 1er juillet 2011, il est ajouté la phrase suivante:

"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. L'Autorité des services et marchés financiers peut néanmoins déléguer ses missions d'inspection, moyennant l'accord du délégataire.".

HOOFDSTUK 3

**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. 78

Artikel 1 wordt aangevuld als volgt:

— "de wet van xx xx 2018": de wet van xx xx 2018 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;".

Art. 79

In de wet van 15 april 1994 wordt een artikel 15*ter* ingevoegd, dat als volgt luidt:

"Art. 15*ter*. Het Agentschap wordt aangewezen als inspectiedienst, in de zin van artikel 42 van de wet van xx 2018, 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 4

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

Art. 80

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 tweede 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. 81

In artikel 14, § 1, eerste lid, van dezelfde wet, gewijzigd bij de wetten van 13 december 2010, 10 juli 2012, 27 maart 2014,

CHAPITRE 3

**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. 78

L'article 1er est complété comme suit:

— "la loi du xx xx 2018": la loi du xx xx 2018 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique;".

Art. 79

Il est inséré un article 15*ter* dans la loi du 15 avril 1994, rédigé comme suit:

"Art. 15*ter*. L'Agence est désignée comme service d'inspection, au sens de l'article 42 de la loi du xx 2018 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 4

**Modifications de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges**

Art. 80

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 second 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. 81

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 april 2017, 5 mei 2017 en 31 juli 2017, worden de volgende wijzigingen aangebracht:

— in het eerste lid worden de woorden ", met betrekking tot de sector digitale infrastructuren in de zin van de wet van xx 2018 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";

— in de bepaling onder 3° worden de woorden ", van 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, van de wet van xx 2018 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".

— in de bepaling onder 3° wordt een tweede lid toegevoegd, luidende:

"Voor de toepassing van de wet van xx 2018 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 aanbieders van essentiële diensten van de sector digitale infrastructuren. De Koning kan de praktische inspectiemodaliteiten voor deze sector bepalen, na advies van het Instituut.".

Art. 82

In artikel 24, eerste lid, van de wet van 17 januari 2003 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 xx 2018, wat de sector digitale infrastructuren betreft" ingevoegd tussen de woorden "in het tweetalig gebied Brussel-Hoofdstad" en de woorden "en hun uitvoeringsbesluiten".

18 avril 2017, 5 mai 2017 et 31 juillet 2017, les modifications suivantes sont apportées:

— à l'alinéa 1er, les mots ", en ce qui concerne le secteur des infrastructures numériques au sens de la loi du xx 2018 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";

— au 3°, les mots ", de 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, de la loi du xx 2018 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 "en région bilingue de Bruxelles-Capitale" et les mots "et de leurs arrêtés d'exécution".

— au 3°, il est ajouté un second alinéa, rédigé comme suit:

"Pour l'application de la loi du xx 2018 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 les opérateurs de services essentiels du secteur des infrastructures numériques. Le Roi peut fixer les modalités pratiques des inspections pour ce secteur, après avis de l'Institut.".

Art. 82

Dans l'article 24, alinéa 1er, de la loi du 17 janvier 2003, 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 2018, 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".

HOOFDSTUK 5

**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 en van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten**

Art. 83

§ 1. Het eerste lid van artikel 71 van de wet van 21 november 2017 wordt aangevuld met de woorden "en van titel 2 van de wet van […] 2018 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.".

§ 2. Een tweede lid wordt toegevoegd aan artikel 71 van de wet van 21 november 2017, luidende:

"Voor de toepassing van de wet van xx 2018 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid wordt de FSMA aangewezen als sectorale overheid en inspectiedienst voor de exploitanten van een handelsplatform in de zin van deze wet. Niettemin kan de Autoriteit voor Financiële Diensten en Markten haar inspectieopdrachten delegeren, mits akkoord van de opdrachtnemer.".

§ 3. Artikel 79 van de wet van 21 november 2017 wordt aangevuld met een paragraaf 4, luidend als volgt:

"§ 4. In geval van schending van de toepasselijke bepalingen van de wet van […] 2018 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.".

Art. 84

Punt 15° van artikel 75, § 1, van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector, 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 xx 2018 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 5

**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 et de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers**

Art. 83

§ 1er. La fin du premier alinéa de l'article 71 de la loi du 21 novembre 2017 est complété par les mots "et du titre 2 de la loi du […] 2018 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.".

§ 2. Un second alinéa est ajouté à l'article 71 de la loi du 21 novembre 2017, rédigé comme suit:

"Pour l'application de la loi du xx 2018 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, la FSMA est désigné comme autorité sectorielle et service d'inspection pour les opérateurs de plate-forme de négociation au sens de la présente loi. L'Autorité des services et marchés financiers peut néanmoins déléguer ses missions d'inspection, moyennant l'accord du délégataire.".

§ 3. L'article 79 de la loi du 21 novembre 2017 est complété par un paragraphe 4, rédigé comme suit:

"§ 4. En cas de violation des dispositions applicables de la loi du […] 2018 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.".

Art. 84

Le point 15° de l'article 75, § 1er, de la loi du 2 août 2002 relative à la surveillance du secteur financier, 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 xx 2018 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".

HOOFDSTUK 6

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

Art. 85

Artikel 36/1 van de wet van 22 februari 1998 wordt aangevuld als volgt:

— “25° “de wet van xx xx 2018”: de wet van xx xx 2018 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.”.

Art. 86

Artikel 36/14, § 1, van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België wordt aangevuld als volgt:

20° de woorden “aan de autoriteit bedoeld in artikel 7, § 1, van de wet van xx 2018” worden ingevoegd tussen de woorden “de analyse van de dreiging,” en “en aan de politiediensten”;

24°: “24° binnen de grenzen van het recht van de Europese Unie, aan de autoriteiten bedoeld in artikel 7 van de wet van xx 2018 voor de uitvoering van de bepalingen van de wet van xx 2018 en van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren.”.

Art. 87

In dezelfde wet wordt een hoofdstuk IV/4 ingevoegd, bestaande uit één enkel artikel 36/47, luidende:

“Hoofdstuk IV/4 Toezicht door de Bank in het kader van de wet van … 2018 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 xx 2018 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 de wet van … 2018. De artikelen 36/8 tot 36/12/3 en artikel 36/21 zijn van toepassing.

CHAPITRE 6

**Modifications de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique**

Art. 85

L’article 36/1 de la loi du 22 février 1998 est complété comme suit:

“25° “la loi du xx xx 2018”: la loi du xx xx 2018 établissant un cadre pour la sécurité des réseaux et des systèmes d’information d’intérêt général pour la sécurité publique.”.

Art. 86

L’article 36/14, § 1er, de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique est complété comme suit:

20° entre les mots “l’analyse de la menace” et “et aux services de police” sont ajoutés les mots “à l’autorité visée à l’article 7, § 1er, de la loi du xx xx 2018”;

24°: “24° dans les limites du droit de l’Union européenne, aux autorités visées à l’article 7 de la loi du xx 2018 pour les besoins de l’exécution des dispositions de la loi du xx 2018 et de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.”.

Art. 87

Dans la même loi, il est inséré un chapitre IV/4, comportant un seul article 36/47 rédigé comme suit:

“Chapitre IV/4 Surveillance par la Banque dans le cadre de la loi du … 2018 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 xx 2018, 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 du ... 2018. Les articles 36/8 à 36/12/3 et l’article 36/21 sont applicables.

De Bank deelt relevante informatie over incidentmeldingen die zij ontvangt krachtens de wet van … 2018 zo snel mogelijk met de ECB.”.

HOOFDSTUK 7

**Inwerkingtreding**

Art. 88

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

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 … 2018.”.

CHAPITRE 7

**Entrée en vigueur**

Art. 88

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

## ADVIES VAN DE RAAD VAN STATE (II) NR. 63.972/4 VAN 17 SEPTEMBER 2018

Op 19 juli 2018 is de Raad van State, afdeling Wetgeving, door de Eerste minister verzocht binnen een termijn van dertig dagen van rechtswege[1*] verlengd tot 4 september 2018 een advies te verstrekken over een voorontwerp van wet "tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid".

Het voorontwerp is door de vierde kamer onderzocht op 17 september 2018. De kamer was samengesteld uit Martine Baguet, kamervoorzitter, Bernard Blero en Wanda Vogel, staatsraden, Christian Behrendt en Marianne Dony, assessoren, en Charles-Henri Van Hove, toegevoegd griffier.

Het verslag is uitgebracht door Laurence Vancrayebeck, eerste auditeur.

De overeenstemming tussen de Franse en de Nederlandse tekst van het advies is nagezien onder toezicht van Wanda Vogel.

Het advies, waarvan de tekst hierna volgt, is gegeven op 17 september 2018.

*

Aangezien de adviesaanvraag ingediend is op basis van artikel 84, § 1, eerste lid, 2°, van de wetten "op de Raad van State", gecoördineerd op 12 januari 1973, beperkt de afdeling Wetgeving overeenkomstig artikel 84, § 3, van de voornoemde gecoördineerde wetten haar onderzoek tot de rechtsgrond van het voorontwerp,[2‡] de bevoegdheid van de steller van de handeling en de te vervullen voorafgaande vormvereisten.

Wat die drie punten betreft, geeft het voorontwerp aanleiding tot de volgende opmerkingen.

### ONTVANKELIJKHEID

De afdeling Wetgeving is verzocht om binnen een termijn van dertig dagen advies uit te brengen over een voorontwerp van wet dat reeds aan haar voorgelegd is en waarover ze op 2 mei 2018 advies 63.296/4 gegeven heeft.

Zoals in de brief met de adviesaanvraag vermeld staat, is een nieuwe adviesaanvraag ingediend omdat de ontworpen

1 * Deze verlenging vloeit voort uit artikel 84, § 1, eerste lid, 2°, *in fine*, van de wetten op de Raad van State, gecoördineerd op 12 januari 1973, waarin wordt bepaald dat deze termijn van rechtswege verlengd wordt met vijftien dagen wanneer hij begint te lopen tussen 15 juli en 31 juli of wanneer hij verstrijkt tussen 15 juli en 15 augustus.

2 ‡ Aangezien het om een voorontwerp van wet gaat, wordt onder "rechtsgrond" de overeenstemming met de hogere normen verstaan.

## AVIS DU CONSEIL D'ÉTAT (II) N° 63.972/4 DU 17 SEPTEMBRE 2018

Le 19 juillet 2018, le Conseil d'État, section de législation, a été invité par le Premier ministre à communiquer un avis, dans un délai de trente jours prorogé de plein droit[1*] jusqu'au 4 septembre 2018, sur un avant-projet de loi "établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique".

L'avant-projet a été examiné par la quatrième chambre le 17 septembre 2018. La chambre était composée de Martine Baguet, président de chambre, Bernard Blero et Wanda Vogel, conseillers d'État, Christian Behrendt et Marianne Dony, assesseurs, et Charles-Henri Van Hove, greffier assumé.

Le rapport a été présenté par Laurence Vancrayebeck, première auditrice.

La concordance entre la version française et la version néerlandaise a été vérifiée sous le contrôle de Wanda Vogel.

L'avis, dont le texte suit, a été donné le 17 septembre 2018.

*

Comme la demande d'avis est introduite sur la base de l'article 84, § 1er, alinéa 1er, 2°, des lois "sur le Conseil d'État", coordonnées le 12 janvier 1973, la section de législation limite son examen au fondement juridique de l'avant-projet[2‡], à la compétence de l'auteur de l'acte ainsi qu'à l'accomplissement des formalités préalables, conformément à l'article 84, § 3, des lois coordonnées précitées.

Sur ces trois points, l'avant-projet appelle les observations suivantes.

### RECEVABILITÉ

La section de législation est saisie d'une demande d'avis dans les trente jours sur un avant-projet de loi qui lui a déjà été soumis et qui a donné lieu, le 2 mai 2018, à l'avis n° 63.296/4.

Comme l'indique la lettre de demande d'avis, une nouvelle demande est adressée compte tenu de ce que le texte

1 * Ce délai résulte de l'article 84, § 1er, alinéa 1er, 2°, *in fine*, des lois "sur le Conseil d'État", coordonnées le 12 janvier 1973 qui précise que ce délai est prolongé de plein droit de quinze jours lorsqu'il prend cours du 15 juillet au 31 juillet ou lorsqu'il expire entre le 15 juillet et le 15 aout.

2 ‡ S'agissant d'un avant-projet de loi, on entend par "fondement juridique" la conformité aux normes supérieures.

tekst gewijzigd is om met dat advies rekening te houden terwijl daarin eveneens nieuwe bepalingen opgenomen zijn.

Wanneer de afdeling Wetgeving een advies heeft gegeven, heeft ze de bevoegdheid opgebruikt die ze krachtens de wet heeft; het komt haar derhalve niet toe om zich opnieuw uit te spreken over reeds onderzochte bepalingen, ongeacht of ze herzien zijn om rekening te houden met de opmerkingen die in het eerste advies gemaakt zijn, dan wel ongewijzigd blijven.

Dat geldt niet wanneer overwogen wordt in de tekst volledig nieuwe bepalingen in te voegen waarvan de inhoud losstaat van de opmerkingen of voorstellen die door de afdeling Wetgeving in het eerste advies geformuleerd zijn: in zo'n geval moet de afdeling Wetgeving nogmaals geraadpleegd worden, met betrekking tot de nieuwe bepalingen.

Dat geldt evenmin wanneer na het eerste advies nieuwe juridische gegevens opduiken die kunnen rechtvaardigen dat de tekst nogmaals door de afdeling Wetgeving onderzocht wordt: in zo'n geval moeten de bepalingen van de tekst waarvoor die nieuwe gegevens consequenties hebben, aan de afdeling Wetgeving voorgelegd worden.

Gelet op wat voorafgaat, is in de aangegeven mate onderzoek gewijd aan de volgende bepalingen: de artikelen 2 en 3, § 1, tweede lid, artikel 4, § 3, derde en vierde lid, en § 4, artikel 5, §§ 2 en 3, artikel 6, 1° tot 4°, 6°, 7°, 11°, 12°, 30° tot 32°, de artikelen 7, 8 en 9, § 1 en § 3, eerste lid, artikel 10, §§ 1 en 2, de artikelen 11 tot 18, artikel 21, § 2, tweede lid, en § 5, artikel 22, § 2, tweede lid, artikel 23, § 1, artikel 25, eerste lid, de artikelen 26 tot 31, 33, § 3, 35, § 1, 36, §§ 2 en 3, 37 en 42, artikel 44, § 3, 5° en 6°, en de artikelen 47, §§ 1 tot 7, 48, §§ 2 en 3, 49, §§ 1 en 3, 51, §§ 1 tot 5, 52, §§ 1, 5 en 6, 55, § 2, 57, eerste lid, 58, 60, 61, 63, 64 tot 68, § 2, 70 tot 79, 81, 3e streepje, 83, 85 en 87.

ONDERZOEK VAN HET VOORONTWERP

Artikel 3

In paragraaf 1, tweede lid, dient naar hoofdstuk 3 van titel 4 verwezen te worden (en niet naar hoofdstuk 3 van titel 3).

Artikel 10

Bij paragraaf 1 wordt de Koning ertoe gemachtigd de autoriteit aan te wijzen "die belast is met de actualisering van de nationale strategie voor de beveiliging van netwerk- en informatiesystemen". Die taak op het stuk van "actualisering" kan alleen begrepen worden als er reeds een nationale strategie bestaat, wat niet duidelijk blijkt uit de tekst van het ontwerp.

Deze bepaling moet in dat opzicht herzien worden.

Artikel 13

In paragraaf 1, eerste lid, dient de verwijzing naar "§ 2" vervangen te worden door een verwijzing naar "§ 1".

en projet a été modifié pour tenir compte de cet avis, "mais intègre également de nouvelles dispositions".

Lorsque la section de législation a donné un avis, elle a épuisé la compétence que lui confère la loi, et il ne lui appartient dès lors pas de se prononcer à nouveau sur les dispositions déjà examinées, qu'elles aient été revues pour tenir compte des observations faites dans le premier avis ou qu'elles demeurent inchangées.

Il en va différemment lorsqu'il est envisagé d'insérer dans le texte des dispositions entièrement nouvelles, dont le contenu est indépendant des observations ou suggestions formulées dans le premier avis de la section de législation: en pareil cas, une nouvelle consultation de la section de législation est requise, portant sur les dispositions nouvelles.

Il en va aussi différemment quand interviennent, après le premier avis, des éléments juridiques nouveaux, de nature à justifier un nouvel examen du texte par la section de législation: en pareil cas, la section de législation doit être saisie des dispositions du texte affectées par ces éléments nouveaux.

Eu égard à ce qui précède, et dans la mesure indiquée, seront examinées les dispositions suivantes: les articles 2 et 3, § 1er, alinéa 2, l'article 4, § 3, alinéas 3 et 4, et § 4, l'article 5, §§ 2 et 3, l'article 6, 1° à 4°, 6°, 7°, 11°, 12°, 30° à 32°, les articles 7, 8 et 9, § 1er et § 3, alinéa 1er, l'article 10, §§ 1er et 2, les articles 11 à 18, l'article 21, § 2, alinéa 2, et § 5, l'article 22, § 2, alinéa 2, l'article 23, § 1er, l'article 25, alinéa 1er, les articles 26 à 31, 33, § 3, 35, § 1er, 36, §§ 2 et 3, 37 et 42, l'article 44, § 3, 5° et 6°, et les articles 47, §§ 1er à 7, 48, §§ 2 et 3, 49, §§ 1er et 3, 51, §§ 1er à 5, 52, §§ 1er, 5 et 6, 55, § 2, 57, alinéa 1er, 58, 60, 61, 63, 64 à 68, § 2, 70 à 79, 81, 3e tiret, 83, 85 et 87.

EXAMEN DE L'AVANT-PROJET

Article 3

Au paragraphe 1er, alinéa 2, il convient de viser le chapitre 3 du titre 4 (et non du titre 3).

Article 10

Le paragraphe 1er habilite le Roi à désigner l'autorité "chargée de maintenir à jour la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information". Cette mission de "maintien à jour" ne peut se comprendre que si une stratégie nationale existe déjà, ce qui ne ressort pas clairement du texte du projet.

La disposition sera revue à cet égard.

Article 13

Au paragraphe 1er, alinéa 1er, il y a lieu de remplacer la mention du "§ 2" par celle du "§ 1er".

Artikel 17

1. De afdeling Wetgeving begrijpt niet wat bedoeld wordt met de verwijzing naar de “bestuursdocumenten betreffende de toepassing van dit artikel”. Wellicht dienen de woorden “van dit artikel” vervangen te worden door de woorden “van dit hoofdstuk”.[3]

2. Doordat de wet van 11 december 1998 reeds in artikel 6, 31°, gedefinieerd wordt als de wet van 11 december 1998 “betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen”, dient het volledige opschrift van die wet niet overgenomen te worden in de ontworpen bepaling.

Een soortgelijke opmerking dient gemaakt te worden bij artikel 18, § 1, en artikel 21, § 5, voor zover daarin het volledige opschrift opgenomen is van de wet van 1 juli 2011, terwijl die wet gedefinieerd wordt in artikel 6, 30°.

Artikel 33

Paragraaf 3, waarin bepaald wordt dat de beveiligingsmaatregelen moeten “voldoen aan de uitvoeringsverordeningen van de Europese Commissie, waaronder [de] Uitvoeringsverordening (…) van 30 januari 2018 (…)” is overbodig en moet weggelaten worden.

Artikel 47

In paragraaf 2, a), dient vermeld te worden aan wie de digitaledienstverlener de informatie moet verstrekken die nodig is om de beveiliging van zijn netwerk- en informatiesystemen te beoordelen.

Artikelen 65 tot 67

1. De artikelen 65 tot 67 strekken ertoe uitvoering te geven aan artikel 23 van Verordening (EU) 2016/679 van het Europees Parlement en de Raad 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)” (hierna de “AVG” genoemd), waarbij de lidstaten gemachtigd worden de reikwijdte te beperken van de rechten en verplichtingen van de betrokkenen als bedoeld in de AVG.

Hoewel de reikwijdte van de rechten bepaald bij de artikelen 5, 12 tot 22 en 34 van de AVG krachtens artikel 23, lid 1, van de AVG beperkt kan worden, is volgens die bepaling tevens vereist dat de lidstaat daartoe het bewijs levert van een gerechtvaardigd doel en dat “die beperking de wezenlijke inhoud van de grondrechten en fundamentele vrijheden onverlet laat en in een democratische samenleving een noodzakelijke en

[3] Zie in die zin de bespreking van dit artikel.

Article 17

1. La section de législation n’aperçoit pas la portée de la référence aux “documents administratifs liés à l’application du présent article”. Sans doute convient-il de remplacer les termes “du présent article” par les termes “du présent chapitre”[3].

2. Dès lors que l’article 6, 31°, définit la loi du 11 décembre 1998 comme étant la loi du 11 décembre 1998 “relative à la classification et aux habilitations, attestations et avis de sécurité”, il n’y a pas lieu de reprendre, dans la disposition en projet, l’intitulé complet de cette loi.

Une observation similaire vaut pour l’article 18, § 1er, et l’article 21, § 5, en ce qu’ils visent l’intitulé complet de la loi du 1er juillet 2011, qui fait l’objet de l’article 6, 30°.

Article 33

Le paragraphe 3, qui prévoit que les mesures de sécurité doivent être “conformes aux règlements d’exécution de la Commission européenne, dont celui du 30 janvier 2018 […]”, est inutile et sera dès lors omis.

Article 47

Au paragraphe 2, a), il convient d’indiquer à qui le fournisseur de service numérique doit communiquer les informations nécessaires pour évaluer la sécurité de ses réseaux et systèmes d’information.

Articles 65 à 67

1. Les articles 65 à 67 entendent mettre en œuvre l’article 23 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 “relatif à la protection des personnes physiques à l’égard de traitement de données à caractère personnel et à la libre circulation de ces données, et abrogeant la Direction 95/46/CE (règlement général sur la protection des données)” (ci-après: le RGPD), qui autorise les États membres à limiter la portée des droits et obligations des personnes concernées, tels que prévus par le RGPD.

Si l’article 23, paragraphe 1er, du RGPD permet la limitation de la portée des droits prévus par les articles 5, 12 à 22 et 34 du RGPD, il exige également que l’État membre justifie pour ce faire d’un objectif légitime et qu’“une telle limitation respecte l’essence des libertés et droits fondamentaux et qu’elle constitue une mesure nécessaire et proportionnée dans une société démocratique”. Compte tenu de son caractère

[3] Voir en ce sens le commentaire de l’article.

evenredige maatregel is". Aangezien die bepaling van de verordening een afwijkende bepaling is, moet ze overigens strikt geïnterpreteerd worden.

Een overheidsinmenging in het recht op eerbiediging van het privéleven dient niet alleen op een voldoende precieze wettelijke bepaling, maar ook op een redelijke verantwoording te steunen, en moet daarenboven evenredig zijn met de doelstellingen die door de wetgever nagestreefd worden. De wetgever beschikt ter zake over een beoordelingsvrijheid die evenwel niet onbeperkt is: opdat een wettelijke regeling verenigbaar is met het recht op eerbiediging van het privéleven, is vereist dat de wetgever een billijk evenwicht heeft gevonden tussen alle rechten en belangen die in het geding zijn. De uitoefening van de rechten waarin de artikelen 5, 12 tot 22 en 34 van de AVG voorzien, draagt bij tot een dergelijk evenwicht.[4]

In dit verband dient opgemerkt te worden dat het feit dat in artikel 65, § 1, van het ontwerp voorgeschreven wordt dat bepaalde verplichtingen en rechten van de AVG beperkt of uitgesloten worden "zonder afbreuk te doen aan de wezenlijke inhoud van de grondrechten en fundamentele vrijheden en voor zover dit strikt noodzakelijk is voor het nagestreefde doel", waarbij aldus een verplichting herhaald wordt die in de AVG aan de lidstaten opgelegd wordt, niet de garantie biedt dat zulks *in casu* wel degelijk het geval is.[5]

Wat de nagestreefde doelstellingen betreft, worden zowel in artikel 65, § 1, als in de artikelsgewijze bespreking[6] de redenen aangevoerd die vermeld staan in artikel 23.1, a), b), c), d), e) en h), van de AVG.

Wat de proportionaliteit betreft, dient opgemerkt te worden dat van de artikelen 12 tot en met 22 van de AVG slechts afgeweken wordt voor de verwerking van persoonsgegevens die in het kader van het melden van incidenten en in het kader van het toezicht plaatsvindt (artikel 65, § 2, van het ontwerp) en dat die afwijking beperkt is, aangezien voor bepaalde gevallen toch in een recht van toegang of in een recht op rectificatie voorzien wordt (artikel 67).

4 Zie inzonderheid advies 63.470/2-4, dat op 7 juni 2018 gegeven is over een voorontwerp dat geleid heeft tot de wet van 30 juli 2018 "houdende diverse financiële bepalingen" en de daarin vervatte verwijzingen, *Parl.St.* Kamer 2017-18, nr. 54-3172/001, 356 tot 366, *http://www.raadvst-consetat.be/dbx/adviezen/63470.pdf.*

5 Een dergelijke louter declaratieve bepaling is trouwens niet op haar plaats in een regelgevende tekst.

6 "Om de verwezenlijking van de doelstellingen van deze wet niet in het gedrang te brengen, is het nodig om in een aantal afwijkingen te voorzien, voornamelijk vanuit het oogpunt van de rechten die door de artikelen 12 tot 22 van de AVG aan de betrokkenen worden toegekend, en dit met als doel de nationale veiligheid, de landsverdediging, de openbare veiligheid, de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten, andere belangrijke doelstellingen van algemeen belang van de Europese Unie of van een lidstaat, of een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt met de uitoefening van het openbaar gezag te waarborgen.".

dérogatoire, cette disposition doit, du reste, faire l'objet d'une interprétation stricte.

Une ingérence des pouvoirs publics dans l'exercice du droit au respect de la vie privée doit reposer non seulement sur une disposition législative suffisamment précise mais aussi sur une justification raisonnable et être proportionnée aux buts poursuivis par le législateur. Le législateur dispose en la matière d'une marge d'appréciation. Cette marge n'est toutefois pas illimitée: pour qu'une norme soit compatible avec le droit au respect de la vie privée, il faut que le législateur ait établi un juste équilibre entre tous les droits et intérêts en cause. L'exercice des droits prévus par les articles 5, 12 à 22 et 34 du RGPD participe à l'existence d'un tel équilibre[4].

Il y a lieu de relever à cet égard que le fait d'énoncer, à l'article 65, § 1er, du projet que "certaines obligations et droits" prévus par le RGPD sont limités ou exclus, "sans porter préjudice à l'essence des libertés et droits fondamentaux et dans la stricte mesure nécessaire au but poursuivi", répétant ainsi une obligation que le RGPD impose aux États membres, ne permet pas de garantir que tel est bien le cas en l'espèce[5].

En ce qui concerne les objectifs poursuivis, tant l'article 65, § 1er, que le commentaire des articles[6] invoquent les motifs prévus à l'article 23.1, a), b), c), d), e) et h), du RGPD.

Quant à la proportionnalité, on relèvera, d'une part, que la dérogation aux articles 12 à 22 du RGPD concerne les seuls traitements de données à caractère personnel qui sont effectués dans le cadre des notifications d'incidents et des contrôles (article 65, § 2, du projet) et que cette dérogation est limitée, puisque dans certaines hypothèses, un droit d'accès ou de rectification est tout de même prévu (article 67).

4 Voir notamment l'avis n° 63.470/2-4 donné le 7 juin 2018 sur un avant-projet devenu la loi du 30 juillet 2018 "portant des dispositions financières diverses" et les références qui y sont citées, *Doc. parl.*, Chambre, 2017-2018, n° 54-3172/001, pp. 356 à 366, *http://www.raadvst-consetat.be/dbx/avis/63470.pdf.*

5 Une telle disposition purement déclarative n'a d'ailleurs pas sa place dans un texte normatif.

6 "Afin de ne pas compromettre la réalisation des objectifs de la loi, il apparait nécessaire de prévoir un certain nombre de dérogations, principalement sous l'angle des droits reconnus aux personnes concernées par les articles 12 à 22 du RGPD, et ce dans le but de préserver la sécurité nationale, la défense nationale, la sécurité publique, la prévention, la détection, la recherche et la poursuite d'infractions, d'autres objectifs importants d'intérêt public général de l'Union européenne ou d'un État membre, ou encore une mission de contrôle, d'inspection ou de règlementation liée à l'exercice de l'autorité publique".

Gelet op deze gegevens en doordat deze bepalingen door de Gegevensbeschermingsautoriteit niet grondiger onderzocht zijn, kunnen de aldus vastgestelde beperkingen blijkbaar aanvaard worden.

2. Luidens artikel 23, lid 2, van de AVG bevatten de wettelijke maatregelen bedoeld in lid 1 van datzelfde artikel

"specifieke bepalingen met betrekking tot, in voorkomend geval, ten minste:

(…)

d) de waarborgen ter voorkoming van misbruik of onrechtmatige toegang of doorgifte;

(…);

f) de opslagperiodes en de toepasselijke waarborgen, rekening houdend met de aard, de omvang en de doeleinden van de verwerking of van de categorieën van verwerking;

g) de risico's voor de rechten en vrijheden van de betrokkenen, (…)".

Voor zover in artikel 65, § 4, van het ontwerp louter bepaald wordt dat "[e]lke verwerkingsverantwoordelijke (…) passende maatregelen [moet] nemen om elke vorm van misbruik of onrechtmatige toegang of overdracht van voormelde persoonsgegevens te voorkomen", gaat die bepaling niet alleen voorbij aan artikel 23, lid 2, van de AVG, doordat die eerstgenoemde bepaling geen "specifieke wettelijke bepalingen" vormt, aangezien daarin alleen een algemeen geldende bepaling van de AVG overgenomen wordt, maar ook aan artikel 22 van de Grondwet, doordat bij die bepaling aan de operatoren in kwestie de taak toevertrouwd wordt om maatregelen uit te werken ter waarborging van de bescherming van de rechten van de betrokkenen tegen ongeoorloofde inmengingen in hun recht op eerbiediging van hun privéleven zonder dat de essentiële elementen daarvan bepaald worden, terwijl bij artikel 22 van de Grondwet de bevoegdheid om vast te stellen in welke gevallen en onder welke voorwaarden aan het recht op eerbiediging van het privéleven afbreuk gedaan kan worden, uitsluitend in handen van de wetgever gelegd wordt.[7-8]

3. In artikel 66 wordt bepaald dat de dienstenaanbieders, de dienstverleners en de autoriteiten bedoeld in artikel 7, ter uitvoering van artikel 37, lid 4, van de AVG, een functionaris voor gegevensbescherming moeten aanwijzen. In dat artikel wordt daaraan toegevoegd dat die verplichting "noodzakelijk [geldt] wanneer de verwerking van die gegevens waarschijnlijk een hoog risico inhoudt als bedoeld in artikel 35 van de verordening". De afdeling Wetgeving begrijpt niet wat er juist met die precisering bedoeld wordt. Het is immers van tweeën één: ofwel is de verplichting om een functionaris voor gegevensbescherming aan te wijzen een algemene verplichting en is er geen grond om te preciseren dat die verplichting

Eu égard à ces éléments et en l'absence d'un examen plus approfondi de ces dispositions par l'Autorité de protection des données, les limitations ainsi prévues semblent admissibles.

2. L'article 23, paragraphe 2, du RGPD prévoit que toute mesure législative visée au paragraphe 1er du même article

"contient des dispositions spécifiques relatives, au moins, le cas échéant:

[…]

d) aux garanties destinées à prévenir les abus ou l'accès ou le transfert illicites;

[…];

f) aux durées de conservation et aux garanties applicables, en tenant compte de la nature, de la portée et des finalités du traitement ou des catégories de traitement;

g) aux risques pour les droit et libertés des personnes concernées; […]".

L'article 65, § 4, du projet, en ce qu'il se borne à prévoir que "[c]haque responsable du traitement est tenu de prendre des mesures appropriées pour éviter toute forme d'abus, d'accès ou de transfert illicites desdites données à caractère personnel", méconnait non seulement l'article 23, paragraphe 2, du RGPD, en ce qu'il ne constitue pas des "dispositions législatives spécifiques", puisqu'il se limite à reproduire une disposition d'application générale du RGPD, mais également l'article 22 de la Constitution dès lors qu'il confie aux opérateurs en cause l'élaboration des mesures tendant à garantir la protection des droits des personnes concernées contre les ingérences injustifiées dans leur droit au respect de la vie privée, sans en fixer les éléments essentiels, alors que l'article 22 de la Constitution réserve au législateur le pouvoir de fixer dans quels cas et dans quelles conditions il peut être porté atteinte au droit au respect de la vie privée[7-8].

3. L'article 66 prévoit qu'en exécution de l'article 37, paragraphe 4, du RGPD, les opérateurs, fournisseurs de services et autorités visées à l'article 7 doivent désigner un délégué à la protection des données. Il ajoute que c'est le cas "nécessairement lorsque le traitement de ces données peut engendrer un risque élevé tel que visé à l'article 35 du règlement". La section de législation n'aperçoit pas la portée exacte de cette précision. De deux choses l'une: soit l'obligation de désigner un délégué à la protection est une obligation générale et il n'y a pas lieu de préciser que cette obligation concerne "nécessairement" l'hypothèse d'un risque élevé, soit l'obligation de désigner un délégué à la protection des données

7 Zie wat de formele en materiële strekking betreft van dat wettelijkheidsbeginsel in verband met de bescherming van het privéleven bij de verwerking van persoonsgegevens: GwH 15 maart 2018, nr. 29/2018, B.13.1 en B.13.3.

8 Zie voormeld advies 63.470/2-4.

7 Voir sur la portée formelle et matérielle de ce principe de légalité en ce qui concerne la protection de la vie privée lors de traitement de données à caractère personnel, C.C., 15 mars 2018, n° 29/2018, B.13.1 et B.13.3.

8 Voir l'avis n° 63.470/2-4, précité.

"noodzakelijk" geldt ingeval zich een hoog risico voordoet, ofwel wordt de verplichting om een functionaris voor gegevensbescherming aan te wijzen alleen opgelegd in dat geval van een hoog risico en mag in die bepaling bijgevolg alleen naar dat geval verwezen worden.

Artikel 66 moet dienovereenkomstig gewijzigd worden.

4. Artikel 67, § 5, voorziet in een vrijstelling, voor de betrokken verwerkingsverantwoordelijke, van het meedelen van een inbreuk in verband met persoonsgegevens aan de betrokkenen wanneer aan bepaalde criteria voldaan is. Volgens de bespreking van dat artikel is voor die vrijstelling de toestemming van de autoriteit bedoeld in artikel 7, § 1, vereist. Die precisering komt niet voor in het dispositief.

Het dispositief en de bespreking ervan moeten op elkaar afgestemd worden.

Artikel 68

De bedoeling van paragraaf 2 komt niet duidelijk tot uiting. In verband daarmee dienen op zijn minst in de bespreking van dit artikel verduidelijkingen gegeven te worden.

Artikelen 77 en 83

Bij deze bepalingen worden aan de autoriteit voor financiële diensten en markten (FSMA) inspectieopdrachten toevertrouwd, terwijl het aan die autoriteit toegestaan wordt "haar inspectieopdrachten [te] delegeren, mits akkoord van de opdrachtnemer". De wetgever dient op zijn minst de criteria te vermelden waarmee een dergelijke delegatie afgebakend kan worden (in welk geval, aan welk type instantie, enz.).

*De griffier,* *De voorzitter,*

Charles-Henri VAN HOVE Martine BAGUET

n'est imposée que dans cette hypothèse de risque élevé et la disposition ne doit dès lors viser que cette hypothèse.

L'article 66 sera modifié en conséquence.

4. L'article 67, § 5, prévoit une dispense, pour le responsable du traitement concerné, de communiquer une violation de données à caractère personnel aux personnes concernées lorsque certains critères sont remplis. Selon le commentaire de l'article, cette dispense est soumise à l'autorisation de l'autorité visée à l'article 7, § 1er. Cette précision n'apparait pas dans le dispositif.

Le dispositif et son commentaire seront harmonisés.

Article 68

La portée du paragraphe 2 n'apparait pas clairement. Il convient à tout le moins d'apporter des précisions dans le commentaire de l'article.

Articles 77 et 83

Ces dispositions confient des missions d'inspection à l'autorité des services et marchés financiers (FSMA), tout en lui permettant de "déléguer ses missions d'inspection, moyennant l'accord du délégataire". Il convient que le législateur indique à tout le moins les critères permettant d'encadrer une telle délégation (dans quelle hypothèse, à quel type d'organisme, etc.).

*Le greffier,* *Le président,*

Charles-Henri VAN HOVE Martine BAGUET

**WETSONTWERP**

FILIP,

KONING DER BELGEN,

*Aan allen die nu zijn en hierna wezen zullen,*
ONZE GROET.

Op de voordracht van de eerste minister en van de minister van Veiligheid en Binnenlandse Zaken,

HEBBEN WIJ BESLOTEN EN BESLUITEN WIJ:

De eerste minister en de minister van Veiligheid en Binnenlandse Zaken zijn ermee belast in onze naam bij de Kamer van volksvertegenwoordigers het ontwerp van wet in te dienen waarvan de tekst hierna 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°,

**PROJET DE LOI**

PHILIPPE,

ROI DES BELGES,

*À tous, présents et à venir,*
SALUT.

Sur la proposition du premier ministre et du ministre de la Sécurité et de l'Intérieur,

NOUS AVONS ARRÊTÉ ET ARRÊTONS:

Le premier ministre et le ministre de la Sécurité et de l'Intérieur sont chargés de présenter, en notre nom, à la Chambre des représentants, le projet de loi dont la teneur suit:

TITRE 1ER

*Définitions et dispositions générales*

CHAPITRE 1ER

**Objet et champ d'application**

**Section 1er**

*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°,

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 hoofdvestiging in België hebben. Een digitaledienstverlener wordt geacht zijn hoofdvestiging in België te hebben als zijn hoofdkantoor 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 elektronische-communicatienetwerken of openbare elektronische-communicatiediensten, 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.

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 l'établissement principal est situé en Belgique. Un fournisseur de service numérique est réputé avoir son établissement 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.

De Koning is ermee belast de eventuele gelijkwaardige sectorspecifieke handelingen, als bedoeld in het vorige 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 van de wet, met uitzondering van de bepalingen van titel I, hoofdstuk 1 van titel II en van artikel 26.

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 van de 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 financiele instrumenten en houdende omzetting van Richtlijn 2014/65/EU.

De sectorale overheden en de operatoren die behoren tot de sector financiën in de zin van bijlage I van de 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 vorige 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

Le Roi est chargé de préciser les éventuels actes sectoriels équivalents visés à l'alinéa précédent.

§ 3. La présente loi n'est pas applicable aux opérateurs relevant du secteur des finances au sens de l'annexe I de la loi, à l'exception des dispositions du titre I, du chapitre 1er du titre II et de l'article 26.

Par dérogation à l'alinéa premier, l'article 52 est applicable aux 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 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 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 précédent, 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

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 2011/93/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 in Ministerraad overlegd besluit;

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;

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 2011/93/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;

5° “instelling voor de conformiteitsbeoordeling”: instelling bedoeld in artikel I.9 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° “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 punten 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 en 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 van de 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

5° “organisme d’évaluation de la conformité”: organisme visé à l’article I.9 du Code de droit économique;

6° “audit de certification”: un audit réalisé dans le cadre d’une certification visée à l’article 22, § 2;

7° “autorité nationale d’accréditation”: organisme créé par le Roi en exécution de l’article VIII.30 du Code de droit économique;

8° “réseau et système d’information”:

a) un réseau de communications électroniques au sens de l’article 2, 3°, de la loi du 13 juin 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 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

een van de sectoren opgenomen in bijlage I van de 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 van 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 van 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 de aanbieders van essentiële diensten hebben 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;

des secteurs repris à l'annexe I de la 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° “digitaledienstverlener”: elke rechtspersoon die een digitale dienst aanbiedt als bedoeld in bijlage II van 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 de digitaledienstverlener, wat de uit deze wet voortvloeiende verplichtingen 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., 2°, van het Wetboek van economisch recht, en/of ondernemers, zoals gedefinieerd in artikel I.8, 39°, van hetzelfde Wetboek, mogelijk maakt online verkoop- of dienstenovereenkomsten met ondernemers te sluiten op de website van de onlinemarktplaats of op de website van een ondernemer 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

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 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 IXP n’assure l’interconnexion que pour des systèmes autonomes; un IXP n’exige pas que le trafic internet passant entre une paire quelconque de systèmes autonomes participants transite par un système autonome tiers, pas plus qu’il ne modifie ou n’altère par ailleurs un tel trafic;

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 administre et gère l’enregistrement de 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., 2°, du Code de droit économique et/ou à des professionnels, au sens de l’article I.8, 39°, du même Code, de conclure des contrats de vente ou de service en ligne avec des professionnels, soit sur le site internet de la place de marché en ligne, soit sur le site internet d’un professionnel qui utilise les services informatiques fournis par la place de marché en ligne;

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

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 Samenwerkingsgroep en het CSIRT-netwerk. Daartoe vertegenwoordigt het

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

contactpunt België binnen de Samenwerkingsgroep bedoeld in artikel 11 van de NIS-richtlijn.

§ 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 in Ministerraad overlegd besluit, de sectorale overheden aan die, voor hun respectievelijke sector, belast zijn met het toezicht op de uitvoering van de bepalingen van deze wet.

De Koning kan sectorale overheden oprichten, bestaande uit vertegenwoordigers van de Federale Staat, de Gemeenschappen en de Gewesten, overeenkomstig de modaliteiten 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 § 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 vorige 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.

coopération et le réseau des CSIRT. A cette fin, le point de contact représente la Belgique au sein du Groupe de coopération visé à l'article 11 de la directive NIS.

§ 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.

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 § 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 précédent, 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. Naargelang de behoeften die nodig zijn voor de uitvoering van de wet en overeenkomstig de toepasselijke wettelijke bepalingen werken de in § 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

§ 2. En fonction des besoins nécessaires à l'exécution de la loi et conformément aux dispositions légales applicables, les autorités visées au § 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, 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 en rapport 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

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 veiligheids- en 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 in Ministerraad overlegd besluit, de autoriteit aan die belast is met de actualisering van de bestaande nationale strategie voor de beveiliging van netwerk- en informatiesystemen.

§ 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;

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 au minimum nécessaire et sont proportionnées à l'objectif de cet échange, notamment dans le respect du Règlement UE 2016/679. Cet échange d'informations préserve la confidentialité des informations concernées et protège la sécurité et les intérêts commerciaux des opérateurs de services essentiels et des fournisseurs de service numérique.

CHAPITRE 5

**Stratégie nationale en matière de sécurité des réseaux et des systèmes d'information**

Art. 10

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

§ 2. La stratégie visée au paragraphe 1er est mise à jour, après avis des autorités visées à l'article 7 et, le cas échéant, des autorités de contrôle des données à caractère personnel. Elle couvre au moins les secteurs visés à l'annexe I et les services visés à l'annexe II.

Cette stratégie définit les objectifs stratégiques et réglementaires appropriées en vue de parvenir à un niveau élevé de sécurité des réseaux et des systèmes d'information et de le maintenir.

§ 3. La stratégie nationale en matière de sécurité des réseaux et des systèmes d'information porte, entre autres, sur les points suivants:

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

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

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 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

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

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

§ 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.

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.

Au minimum, l'autorité sectorielle réexamine et, le cas échéant, met à jour l'identification des opérateurs de services essentiels et de leurs services essentiels tous les deux ans.

Les actualisations sont adressées aux autorités visées à l'article 7, §§ 1er et 4.

Art. 12

§ 1er. Pour identifier les opérateurs visés à l'article 11, l'autorité sectorielle applique les critères suivants:

a) l'entité fournit un service qui est essentiel au maintien d'activités sociétales et/ou économiques critiques;

b) la fourniture de ce service est tributaire des réseaux et des systèmes d'information; et

c) un incident serait susceptible d'avoir un effet perturbateur important sur la fourniture dudit service, en tenant compte des critères et des niveaux d'incidence ou seuils visés à l'article 13.

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

Art. 13

§ 1er. Afin de déterminer l'importance de l'effet perturbateur visé à l'article 12, § 1er, c), l'autorité sectorielle établit, pour son secteur, des critères sectoriels et/ou intersectoriels, des niveaux d'incidence ou des seuils.

L'effet perturbateur important est établi dès que l'opérateur de services essentiels potentiel répond soit à un seuil soit à un niveau d'incidence.

Dans les limites de leurs compétences respectives, les autorités visées à l'article 7, §§ 1er et 4, se concertent avec l'autorité sectorielle pour déterminer les critères, les niveaux d'incidence et les seuils, le cas échéant, après consultation des régions, des communautés concernées et des représentants des entités visées à l'annexe I.

§ 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 meegedeelde relevante informatie wordt overgemaakt 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 gemotiveerd voorstel van lijst van aanbieders van essentiële diensten van haar sector, samen met een of meer toegepaste identificatiecriteria.

§ 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) la portée géographique eu égard à la zone 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.

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 gemotiveerde 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 gemotiveerde 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 de 3 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

Onverminderd de eventuele toepassing van de wet van 11 december 1998 worden de bestuursdocumenten betreffende de toepassing van hoofdstuk 1 van titel 2 van de wet 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

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 3 mois de sa désignation, l'opérateur de services essentiels transmet à l'autorité sectorielle un descriptif des réseaux et des systèmes d'information dont la fourniture du ou des services essentiels concernés est tributaire.

L'autorité sectorielle communique ce descriptif à l'autorité visée à l'article 7, § 1er.

Art. 17

Sans préjudice de l'application éventuelle de la loi du 11 décembre 1998, les documents administratifs liés à l'application du chapitre 1er du titre 2 de la loi, 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

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 gemotiveerde beslissing tot aanwijzing van een exploitant van een kritieke infrastructuur als aanbieder van essentiële diensten.

Art 19

De Koning kan, bij in Ministerraad overlegd besluit, andere sectoren of soorten aanbieders toevoegen aan bijlage I van deze wet.

relative à la publicité de l'administration, qui ne peuvent être consultés, faire l'objet d'explications ou être communiqué sous forme d'une 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.

HOOFDSTUK 2

**Beveiligingsmaatregelen**

Artikel 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, gezien de stand van de techniek, 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 in het I.B.B.

§ 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.

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.

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. 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 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 in Ministerraad overlegd besluit.

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.

§ 5. Les mesures de sécurité physique et logique des réseaux et systèmes d'information contenues dans le plan de sécurité de l'exploitant (P.S.E.) visé à l'article 13 de la loi du 1er juillet 2011 et à l'article 11 de l'arrêté royal du 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien sont assimilées à la P.S.I. lorsque toutes les informations visées au paragraphe 2 y sont reprises.

Art. 22

§ 1er. La PSI 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 PSI.

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 aux autorités visées à l'article 7, §§ 1er, et 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.

§ 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

§ 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.

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. 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, sans retard, tous les incidents ayant un impact significatif sur la disponibilité, la confidentialité, l'intégrité ou l'authenticité des réseaux et des systèmes d'information dont sont tributaires le ou les services essentiels qu'ils fournissent. La Banque nationale de Belgique détermine l'impact significatif visé par cet alinéa.

La Banque nationale de Belgique 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 sont portés à son attention par le CSIRT national, l'autorité sectorielle ou l'autorité visée à l'article 7, § 4.

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 belast met de modaliteiten voor de melding en rapportering van incidenten bepalen, met inbegrip van de oprichting van een beveiligd meldingsplatform.

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

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 doit, dans le respect du droit de l'Union ou de la législation nationale conforme au droit de l'Union, préserver la sécurité et les intérêts commerciaux de l'opérateur de services essentiels ainsi que la confidentialité des informations communiquées dans sa notification.

Le CSIRT national transmet les notifications visées au premier alinéa 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, en ce compris, 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, premier alinéa, du Règlement UE 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*

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 microondernemingen (2003/361/EG).

HOOFDSTUK 1

**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.

Deze maatregelen zorgen, gezien de stand van de techniek, 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

§ 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*

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 1ER

**Les exigences de sécurité**

Art. 33

§ 1er. Les fournisseurs de service numérique identifient les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'ils utilisent pour offrir, dans l'Union, les services visés à l'annexe II et prennent les mesures techniques et organisationnelles nécessaires et proportionnées pour les gérer.

Ces mesures garantissent, compte tenu de l'état des connaissances, 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

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 2

**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.

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 2

**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 (UE) 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

§ 1. Deze melding gebeurt overeenkomstig de door de Koning bepaalde modaliteiten en via het platform bedoeld in artikel 31.

§ 2. Via het platform bedoeld in artikel 31 van deze wet 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 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.

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 de la présente loi 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, premier alinéa, 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. Lorsque c'est approprié, et notamment si l'incident visé au 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, lorsque c'est approprié, 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.

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;

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° 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 in Ministerraad overlegd besluit 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

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

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

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:

de services essentiels des mesures de sécurité et des règles de notification des incidents.

§ 2. L'autorité visée à l'article 7, § 1er, ou l'autorité sectorielle peut recommander, de manière motivée, au service d'inspection de réaliser des contrôles.

Après avis de l'autorité sectorielle et de l'autorité visée à l'article 7, § 1er, le Roi peut fixer les éventuelles modalités sectorielles pratiques du contrôle.

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

Le service d'inspection peut faire appel à des experts.

Art 43

Lorsque les réseaux et les systèmes d'information d'un opérateur de services essentiels sont situés en dehors du territoire belge, le service d'inspection, en concertation avec l'autorité visée à l'article 7, § 1er, peut solliciter la coopération et l'assistance des autorités de contrôle compétentes de ces autres 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° 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 bij de kamer van inbeschuldigingstelling binnen de vijftien dagen na de kennisgeving van de beslissing.

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 devant la chambre des mises en accusation dans les quinze jours de la notification de la décision.

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.

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 informatica systeem en de erin opgenomen gegevens in beslag nemen.

Les visites sans autorisation de l'occupant dans des locaux habités se font entre cinq et vingt-et-une heures par au moins deux membres du service d'inspection agissant conjointement.

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

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

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

3° qu'elle a le droit de garder le silence et de ne pas contribuer à sa propre incrimination.

Toute personne interrogée peut utiliser les documents en sa possession, sans que cela puisse entraîner le report de l'audition. Elle peut, lors de l'audition ou ultérieurement, exiger que ces documents soient joints à l'audition.

L'audition mentionne avec précision l'heure à laquelle elle a pris cours, est éventuellement interrompue et reprise, et prend fin. Elle mentionne l'identité des personnes qui 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. 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 de Procureur des Konings verzoeken op te treden, onder de voorwaarden bedoeld in artikel 39*bis*, § 3, van het Wetboek van Strafvordering.

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 in Ministerraad overlegd besluit 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 berekenings- en betalingsmodaliteiten.

HOOFDSTUK 2

**Toezicht op de digitaledienstverleners**

Art. 47

§ 1. De Koning bepaalt de praktische modaliteiten van het toezicht op de digitaledienstverleners.

§ 2. De digitaledienstverlener moet met name:

§ 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 du Procureur du Roi, lequel pourra intervenir dans les conditions visées à l'article 39*bis*, § 3, du Code d'instruction criminelle.

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 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 lidstatenlanden, 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.

§ 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 in Ministerraad overlegd besluit 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 berekenings- en betalingsmodaliteiten.

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, § 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.

HOOFDSTUK 3

**De sancties**

**Afdeling 1**

*Procedure*

Art. 48

§ 1. Wanneer een of meer inbreuken op de eisen van de wet, de koninklijke besluiten 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 gemotiveerde 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 proces-verbaal door de beëdigde leden van de inspectiedienst. 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

CHAPITRE 3

**Les sanctions**

**Section 1re**

*Procédure*

Art. 48

§ 1er. Lorsqu'un ou plusieurs manquements aux exigences imposées par la loi, ses arrêtés royaux 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

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 36 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 beide straffen.

§ 2. Niet-naleving van een van de beveiligingsverplichtingen opgelegd door de Koning of de sectorale overheid krachtens artikel 21 of 34 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 beide straffen.

§ 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 beide straffen.

§ 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 beide straffen.

§ 5. Iedere vrijwillige verhindering of belemmering van de uitvoering van de controle door de leden van de inspectiedienst, weigering om de informatie mee te

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 36.

§ 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 34.

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

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

§ 5. Est puni d'une peine d'emprisonnement de huit jours à deux ans et d'une amende de 26 euros à 75 000 euros ou de l'une de ces peines seulement,

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 beide straffen.

§ . 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 voornoemde inbreuken.

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, paragrafen 2 en 3, van deze wet geven aanleiding tot 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 36 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 34 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

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 auxdites infractions.

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, paragraphes 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 36.

§ 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 34.

§ 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

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 gemotiveerd. Ze vermeldt ook het bedrag van de administratieve geldboete en de bedoelde inbreuken.

§ 2. De sectorale overheid bezorgt de overtreder op voorhand haar gemotiveerd 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 en bij gebrek aan een antwoord van de overtreder binnen diezelfde termijn, kan de sectorale overheid een in artikel 25 bedoelde administratieve sanctie opleggen.

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 manquements 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 25.

§ 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 ingeleid bij verzoekschrift op tegenspraak dat, op straffe van verval, binnen de 60 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

§ 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.

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 60 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 délégué à cette fin.

§ 2. La contrainte est signifiée au contrevenant par exploit d'huissier de justice. La signification contient

bevat een bevel om te betalen binnen de 24 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 de vijftien dagen te rekenen vanaf de betekening van het dwangbevel.

De bepalingen van hoofdstuk VIII, 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 deel V 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.

un commandement de payer dans les 24 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, 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 partie V 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 est commis.

Le paiement selon la procédure administrative éteint également la possibilité d'engager des poursuites pénales pour les faits visés.

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 de 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 extra taken toevertrouwen.

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, diffusion de messages d'alerte, annonces et 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 normalisées pour les procédures de gestion des risques et incidents, ainsi que les 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.

**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.

Zijn communicatiekanalen moeten voorts duidelijk worden gespecificeerd en bekend zijn bij de gebruikersgroep en de samenwerkingspartners.

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.

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 gebruiken van te maken, zelfs die gegevens voortkomend 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

**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 contactés et contacter autrui à tout moment.

De plus, ses canaux de communication doivent être clairement précisés et bien connus des partenaires et collaborateurs.

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.

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, révéler, divulguer à une autre personne, ou 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

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.

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 risico- en analyse van sectorale 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 extra 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

système informatique et en prenant toutes précautions raisonnables afin qu'aucun dommage matériel ne soit causé au système informatique.

Les fonctionnaires dirigeants du CSIRT national veillent, par l'adoption de procédures internes, au respect des conditions visées au présent article.

CHAPITRE 2

**Le CSIRT sectoriel**

**Section 1re**

*Tâches du CSIRT sectoriel*

Art. 63

Les tâches d'un CSIRT sectoriel sont, en coordination avec le CSIRT national, au moins les suivantes:

a) le suivi des incidents sectoriels;

b) l'activation du mécanisme d'alerte précoce, diffusion de messages d'alerte, annonces et diffusion d'informations sur les risques et 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

(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.

Zijn communicatiekanalen moeten voorts duidelijk worden gespecificeerd en bekend zijn bij de gebruikersgroep en de samenwerkingspartners.

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.

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 moet de verwerkingsverantwoordelijke, bij de verwerking van persoonsgegevens in het kader van de uitvoering van deze wet, ervoor zorgen 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,

de défaillance et disposer de plusieurs moyens pour être contactés et contacter autrui à tout moment.

De plus, ses canaux de communication doivent être clairement précisés et bien connus des partenaires et collaborateurs.

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.

TITRE 6

*Traitement des données à caractère personnel*

CHAPITRE 1ER

**Principes relatifs au traitement, bases légales 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

enerzijds, en de overheden bedoeld in artikel 7, anderzijds,

— de verwerking van specifieke informatie tussen de entiteiten bedoeld in het vorige lid 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 overtredingen,

— 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

§ 1. Indien mogelijk moeten de verwerkte gegevens worden 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 moeten 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, of nog 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

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 à l'alinéa précédent 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.

Art. 66

§ 1er. Chaque fois que possible, les données traitées doivent être 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 doivent être traitées dans le respect dudit règlement et des lois et règlements qui complètent ou précisent celui-ci.

§ 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 encore 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

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 overheden.

§ 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 vorige paragraaf kan de Koning de maximale bewaartermijn van dezelfde gegevens bepalen bij in Ministerraad overlegd besluit.

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 différents 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 des traitements 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 précédent, le Roi peut fixer la durée maximale de conservation des mêmes données par arrêté délibéré en conseil des Ministres.

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, moet een functionaris voor gegevensbescherming aanwijzen.

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 2 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 verwerkingen noodzakelijk zijn voor de hierboven bepaalde doeleinden, met name voor zover de toepassing van de rechten bepaald in de Europese 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 § 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.

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

**Limitations 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 aux opérations de traitements de données à caractère personnel effectués par un opérateur de services essentiels, un fournisseur de service numérique ou une autorité visée à l'article 7, qui sont effectuées dans le respect de la présente loi et pour satisfaire aux obligations que celle-ci impose en matière de notifications d'incidents visées aux chapitres 3 du titre 2 et 2 du titre 3 , ainsi que de contrôles visés au titre 4. L'exemption ne vaut que si et dans la mesure où ces opérations sont nécessaires pour les finalités définies ci-avant, notamment dans la mesure où l'application des droits prévus par le règlement européen 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 § 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. De vrijstelling geldt, onder voorbehoud van het evenredigheidsbeginsel en in voorkomend geval van het beginsel van minimale gegevensverwerking, voor alle categorieën van persoonsgegevens waarvan de entiteiten bedoeld in paragraaf 3 de verwerkingsverantwoordelijken zijn, voor zover de verwerking van deze gegevens in overeenstemming is met de doeleinden bedoeld in paragraaf 2, alsook 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 op de 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 het artikel 72 hierna 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

§ 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 dont les entités visées au paragraphe 3 sont les responsables du traitement, dans la mesure où le traitement de ces données n'est pas étranger aux finalités visées au paragraphe 2, ainsi que 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 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 ci-après, 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 aux 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

binnen een maand na ontvangst van het verzoek, over iedere weigering of beperking van hun 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 worden 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. 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 overheden 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 documenten verwerkt die afkomstig zijn van de inspectiedienst met het oog op de vervolging;

cause dans un délai d'un mois à compter de la réception de la demande, de tout refus ou de toute limitation de leurs 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 aux informations concernant le traitement de ses données à caractère personnel, dans la mesure où cette communication ne compromet pas la réalisation des objectifs de la présente loi de manière telle que la personne concernée se trouve dans l'impossibilité de savoir si elle fait l'objet d'une enquête ou pas, et sans pouvoir en aucun cas rectifier, effacer, limiter, notifier, transmettre à un tiers des données personnelles, ni cesser toute forme de traitement desdites données qui soit nécessaire dans le cadre défini ci-avant.

§ 5. La mesure de refus ou de limitation des droits prévus aux articles 12 à 22 du Règlement UE 2016/679, doit être levée:

— pour les mesures justifiées par les obligations en matière de notification d'incidents, lors de la clôture du traitement d'un incident par les autorités visées à l'article 24 ou 34;

— pour les mesures justifiées par les obligations en vertu du titre 4, lors de la clôture du contrôle ou de l'enquête ou des actes préparatoires à ceux-ci effectués par le service d'inspection, ainsi que pendant la période durant laquelle l'autorité sectorielle traite les pièces provenant du service d'inspection en vue d'exercer des poursuites;

— 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 moet ook de maatregel van weigering of beperking van de rechten bepaald in de artikelen 12 tot 22 van Verordening EU 2016/679 opheffen zodra deze maatregel niet meer nodig is overeenkomstig artikel 68, § 2.

§ 7. In alle toepassingsgevallen van de §§ 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

§ 1. 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, van deze wet, voor zover deze individuele kennisgeving de verwezenlijking van de doeleinden bedoeld in artikel 71, § 2, van deze wet 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 wordt aangevuld met een derde lid, als volgt:

“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.”.

— 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 conformément à l’article 68, § 2.

§ 7. Dans tous les cas d’application des §§ 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

§ 1er. 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, de la présente loi, 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, de la présente loi.

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 est complété par un troisième 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

Artikel 3 van de wet van 1 juli 2011 wordt gewijzigd als volgt:

— in punt 3°:

–“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 financiele instrumenten en houdende omzetting van Richtlijn 2014/65/EU: de Autoriteit voor Financiële Diensten en Markten (FSMA);

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 wet of door de Koning bij in Ministerraad overlegd besluit;

g) voor de sector water: de overheid aangewezen door de wet of door de Koning bij in Ministerraad overlegd besluit;”;

— een nieuw punt 13°: “13° “de wet van xx xx 2018”: de wet van xx xx 2018 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;”;

— een nieuw punt 14°: “14° “beveiliging van netwerk- en informatiesystemen”: de beveiliging van netwerk- en informatiesystemen als bedoeld in artikel 6, 8° en 9°, van de wet van xx xx 2018;”;

— een nieuw punt 15°: “15° “digitale infrastructuren”: de aanbieders bedoeld in punt 6 van bijlage 1 van de wet van xx xx 2018;”;

— een nieuw punt 16°: “16° “water”: de aanbieders bedoeld in punt 5 van bijlage 1 van de wet van xx xx 2018;”;

— een nieuw punt 17°: “17° “gezondheidszorg”: de aanbieders bedoeld in punt 4 van bijlage 1 van de wet van xx xx 2018.”.

Art. 75

L’article 3 de la loi du 1er juillet 2011 est modifié comme suit:

— au point 3°:

“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);

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 la loi ou par le Roi, par arrêté délibéré en Conseil des ministres;

g) pour le secteur de l’eau: l’autorité publique désignée par la loi ou par le Roi, par arrêté délibéré en Conseil des ministres;”;

— un nouveau point 13°: “13° “la loi du xx xx 2018”: la loi du xx xx 2018 établissant un cadre pour la sécurité des réseaux et des systèmes d’information d’intérêt général pour la sécurité publique;”;

— un nouveau point 14°: “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 xx xx 2018;”;

— un nouveau point 15°: “15° “infrastructures numériques”: opérateurs visés au point 6 de l’annexe 1 de la loi du xx xx 2018;”;

— un nouveau point 16°: “16° “eau”: opérateurs visés au point 5 de l’annexe 1 de la loi du xx xx 2018;”;

— un nouveau point 17°: “17° “santé”: opérateurs visés au point 4 de l’annexe 1 de la loi du xx xx 2018.”.

Art. 76

Artikel 4, § 4, van de wet van 1 juli 2011 wordt gewijzigd als volgt:

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

Art. 77

In artikel 5 van de wet van 1 juli 2011 wordt een paragraaf 3 toegevoegd, luidende:

"§ 3. Tijdens het hele identificatieproces als bedoeld in deze afdeling wordt de autoriteit bedoeld in artikel 7, § 1, van de wet van xx 2018 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, paragraaf 5*bis*, van de wet van 1 juli 2011 worden de woorden "met uitzondering van die welke worden uitgebaat door een exploitant van een handelsplatform," toegevoegd tussen de woorden "vallen," en "worden".

In artikel 13, paragraaf 6, tweede lid, van de wet van 1 juli 2011 worden de woorden ", met uitzondering van de kritieke infrastructuren die worden uitgebaat door een exploitant van een handelsplatform," toegevoegd tussen de woorden "de sector financiën" en "worden".

Art. 79

Op het einde van paragraaf 2 van artikel 14 van de wet van 1 juli 2011 worden de volgende woorden toegevoegd: "en, in voorkomend geval, de autoriteit bedoeld in artikel 7, § 1, van de wet van xx 2018 wat de beveiliging van netwerk- en informatiesystemen betreft.".

Art. 80

In artikel 18 van de wet van 1 juli 2011 worden de woorden "De ADCC, de politiediensten en het OCAD"

Art. 76

L'article 4, § 4, de la loi du 1er juillet 2011 est modifié comme suit:

"Le présent chapitre s'applique au secteur des finances, aux opérateurs de plate-forme de négociation visés à l'article 3, 3°, d) de la loi, au secteur des communications électroniques, au secteur des infrastructures numériques, au secteur de la santé et au secteur de l'eau, en ce qui concerne la sécurité et la protection des infrastructures critiques nationales.".

Art. 77

A l'article 5 de la loi du 1er juillet 2011, un paragraphe 3 est ajouté et 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 xx xx 2018 est associée aux concertations nationales et internationales menées par les autorités sectorielles et la DGCC, pour les aspects de l'identification des infrastructures critiques liés à la sécurité des réseaux et systèmes d'information.".

Art. 78

A l'article 13, paragraphe 5*bis* de la loi du 1er juillet 2011, les mots "à l'exception de celles exploitées par un opérateur de plate-forme de négociation" sont ajoutés entre les mots "du secteur des finances" et ", les mesures de sécurité".

A l'article 13, paragraphe 6, alinéa 2, de la loi du 1er juillet 2011, les mots "à l'exception des infrastructures critiques exploitées par un opérateur de plate-forme de négociation" sont ajoutés entre les mots "le secteur des finances" et ", les exercices".

Art. 79

A la fin du paragraphe 2 de l'article 14 de la loi du 1er juillet 2011, il est ajouté les mots "et, le cas échéant, l'autorité visée à l'article 7, § 1er, de la loi du xx xx 2018, pour ce qui concerne la sécurité des réseaux et systèmes d'information.".

Art. 80

A l'article 18 de la loi du 1er juillet 2011, les mots "La DGCC, les services de police et l'OCAM" sont

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 xx 2018, wat de beveiliging van netwerk- en informatiesystemen betreft,”.

Art. 81

In artikel 19 van de wet van 1 juli 2011 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 xx 2018, wat de beveiliging van netwerk- en informatiesystemen betreft,”.

Art. 82

In artikel 22 van de wet van 1 juli 2011 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 xx 2018,”.

Art. 83

In artikel 22*bis* van de wet van 1 juli 2011 worden de woorden “, met uitzondering van de deelsector van de exploitanten van een handelsplatform,” toegevoegd tussen de woorden “de sector financiën” en “maakt”.

In hetzelfde artikel wordt tevens een tweede lid toegevoegd, dat als volgt luidt:

“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 sector valt.”.

Art. 84

In het derde lid van paragraaf 2 van artikel 24 worden de woorden “, met uitzondering van de deelsector van

remplacés par “La DGCC, les services de police, l’OCAM et, le cas échéant, l’autorité visée à l’article 7, § 1er, de la loi du xx xx 2018 pour ce qui concerne la sécurité des réseaux et systèmes d’information,”.

Art. 81

A l’article 19 de la loi du 1er juillet 2011, 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 “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 xx xx 2018 pour ce qui concerne la sécurité des réseaux et systèmes d’information,”.

Art. 82

A l’article 22 de la loi du 1er juillet 2011, 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 xx xx 2018,”.

Art. 83

A l’article 22*bis* de la loi du 1er juillet 2011, les mots “à l’exception du sous-secteur des opérateurs de plate-forme de négociation” sont ajoutés entre les mots “le secteur des finances” et “, la Banque nationale de Belgique”.

Un second alinéa est également ajouté au même article, rédigé comme suit:

“Pour les opérateurs de plate-forme de négociation, la FSMA communique au ministre des Finances un rapport relatif aux tâches qu’elle accomplit en vertu de la présente loi selon une périodicité appropriée n’excédant toutefois pas trois ans. La FSMA l’informe toutefois sans délai de toute menace concrète et imminente pesant sur une infrastructure critique relevant de son secteur.”.

Art. 84

A l’alinéa 3 du paragraphe 2 de l’article 24, les mots “à l’exception du sous-secteur des opérateurs de

de exploitanten van een handelsplatform," toegevoegd tussen de woorden "de sector financiën" en "wordt".

Op het einde van paragraaf 2 van artikel 24 van de wet van 1 juli 2011 wordt de volgende zin toegevoegd:

"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 wordt aangevuld als volgt:

— "de wet van xx xx 2018": de wet van xx xx 2018 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;".

Art. 86

In de wet van 15 april 1994 wordt een artikel 15*ter* ingevoegd, dat als volgt luidt:

"Art. 15*ter*. Het Agentschap wordt aangewezen als inspectiedienst, in de zin van artikel 42 van de wet van xx 2018, 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.

plate-forme de négociation" sont ajoutés entre les mots "le secteur des finances" et ", la Banque nationale de Belgique".

A la fin du paragraphe 2 de l'article 24 de la loi du 1er juillet 2011, il est ajouté la phrase suivante:

"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 est sans préjudice de la possibilité pour la FSMA de, pour l'exécution des missions qui lui sont confiées par la présente loi, 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 est complété comme suit:

— "la loi du xx xx 2018": la loi du xx xx 2018 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique;".

Art. 86

Il est inséré un article 15*ter* dans la loi du 15 avril 1994, rédigé comme suit:

"Art. 15*ter*. L'Agence est désignée comme service d'inspection, au sens de l'article 42 de la loi du xx 2018 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.

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

Le Roi fixe les modalités pratiques des inspections, après avis de l’Agence.”.

HOOFDSTUK 3

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

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

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 tweede 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. 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 second 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

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 xx 2018 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”;

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 xx 2018 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° de bepaling onder 3° wordt vervangen als volgt:

“3° het toezicht op de naleving van de volgende normen en van hun uitvoeringsbesluiten:

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;

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;

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

d) 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 Belgische post- en telecommunicatiesector;

e) 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 xx 2018 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 xx 2018 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 de wet van 17 januari 2003 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 xx 2018, wat de sector digitale infrastructuren betreft" ingevoegd tussen de woorden "in het tweetalig gebied Brussel-Hoofdstad" en de woorden "en hun uitvoeringsbesluiten".

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 xx 2018 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 xx 2018 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 loi du 17 janvier 2003, 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 2018, 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".

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 en van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten**

Art. 90

§ 1. Het eerste lid van artikel 71 van de wet van 21 november 2017 wordt aangevuld met de woorden "en van titel 2 van de wet van […] 2018 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 […] 2018 kan de FSMA niettemin een gespecialiseerde externe dienstverlener belasten met de uitvoering van welbepaalde toezichttaken of de bijstand van een dergelijke dienstverlener verkrijgen.".

§ 2. Artikel 79 van de wet van 21 november 2017 wordt aangevuld met een paragraaf 4, luidend als volgt:

"§ 4. In geval van schending van de toepasselijke bepalingen van de wet van […] 2018 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.".

Art. 91

Punt 15° van artikel 75, § 1, van de wet van 2 augustus 2002 betreffende het toezicht op de financiele sector, 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 xx 2018 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 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 et de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers**

Art. 90

§ 1er. La fin du premier alinéa de l'article 71 de la loi du 21 novembre 2017 est complété par les mots "et du titre 2 de la loi du […] 2018 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 […] 2018, 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. ".

§ 2. L'article 79 de la loi du 21 novembre 2017 est complété par un paragraphe 4, rédigé comme suit:

"§ 4. En cas de violation des dispositions applicables de la loi du […] 2018 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.".

Art. 91

Le point 15° de l'article 75, § 1er, de la loi du 2 août 2002 relative à la surveillance du secteur financier, 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 xx 2018 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".

HOOFDSTUK 5

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

Art. 92

Artikel 36/1 van de wet van 22 februari 1998 wordt aangevuld als volgt:

"28° "de wet van xx xx 2018": de wet van xx xx 2018 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.".

Art. 93

Artikel 36/14, § 1, van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België wordt aangevuld als volgt:

20° de woorden "aan de autoriteit bedoeld in artikel 7, § 1, van de wet van xx 2018" worden ingevoegd tussen de woorden "de analyse van de dreiging," en "en aan de politiediensten";

24°: "24° binnen de grenzen van het recht van de Europese Unie, aan de autoriteiten bedoeld in artikel 7 van de wet van xx 2018 voor de uitvoering van de bepalingen van de wet van xx 2018 en van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren.".

Art. 94

In dezelfde wet wordt een hoofdstuk IV/4 ingevoegd, bestaande uit één enkel artikel 36/47, luidende:

"Hoofdstuk IV/4 Toezicht door de Bank in het kader van de wet van … 2018 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 xx 2018 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

CHAPITRE 5

**Modifications de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique**

Art. 92

L'article 36/1 de la loi du 22 février 1998 est complété comme suit:

"28° "la loi du xx xx 2018": la loi du xx xx 2018 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.".

Art. 93

L'article 36/14, § 1er, de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique est complété comme suit:

20° entre les mots "l'analyse de la menace" et "et aux services de police" sont ajoutés les mots "à l'autorité visée à l'article 7, § 1er, de la loi du xx xx 2018";

24°: "24° dans les limites du droit de l'Union européenne, aux autorités visées à l'article 7 de la loi du xx 2018 pour les besoins de l'exécution des dispositions de la loi du xx 2018 et de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.".

Art. 94

Dans la même loi, il est inséré un chapitre IV/4, comportant un seul article 36/47 rédigé comme suit:

"Chapitre IV/4 Surveillance par la Banque dans le cadre de la loi du … 2018 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 xx 2018, 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

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 de wet van … 2018. 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 … 2018 zo snel mogelijk met de ECB.".

HOOFDSTUK 6

**Inwerkingtreding**

Art. 95

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

Gegeven te Ciergnon, 30 oktober 2018

**FILIP**

VAN KONINGSWEGE :

*De eerste minister,*

Charles MICHEL

*De minister van Veiligheid en Binnenlandse Zaken,*

Jan JAMBON

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 du ... 2018. 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 … 2018.".

CHAPITRE 6

**Entrée en vigueur**

Art. 95

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

Donné à Ciergnon, le 30 octobre 2018

**PHILIPPE**

PAR LE ROI :

*Le premier ministre,*

Charles MICHEL

*Le ministre de la Sécurité et de l'Intérieur,*

Jan JAMBON

## Bijlage I bij het wetsontwerp

**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"). |
| | | 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 12bis 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. |
| **6.Digitale infrastructuren** | | IXP. |
| | | Leveranciers van DNS-diensten. |
| | | Registers van topleveldomeinnamen. |

## Annexe I au projet de loi

**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. |
| | 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 12bis de la loi du 22 février 1998 fixant le statut organique de la Banque nationale de Belgique. |

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

## Bijlage II bij het wetsontwerp

**Soorten digitale diensten**

1. Onlinemarktplaats
2. Onlinezoekmachines
3. Cloudcomputerdiensten

## Annexe II au projet de loi

**Types de services numériques**

1. Place de marché en ligne
2. Moteurs de recherche en ligne
3. Service d'informatique en nuage

## Concordantietabel richtlijn - wetsontwerp
## Tableau de correspondance directive - projet de loi

**Directive (UE) 2016/1148 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 (NIS)**

**Richtlijn (EU) 2016/1148 van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (NIS)**

| | Directive / Richtlijn 2016/1148 | Projet de loi / Wetsontwerp |
|---|---|---|
| **CHAPITRE I : DISPOSITIONS GENERALES**<br>**HOOFDSTUK I : ALGEMENE BEPALINGEN** | | |
| **Objet et champ d'application**<br>**Onderwerp en toepassingsgebied** | | |
| | Art. 1.1 | (exposé des motifs / memorie van toelichting) |
| | Art. 1.2 | (ne doit pas être transposé / dient niet te worden omgezet) |
| | Art. 1.3 | Art. 4, §1 |
| | Art. 1.4 | Art. 5, §2 |
| | Art. 1.5 | Art. 9, §1, al. 2 ; art. 9, §3 |
| | Art. 1.6 | Art. 4, § 4 ; art. 5, §§3 - 4 |
| | Art. 1.7 | Art. 4, §§2 - 3 |
| **Traitement des données à caractère personnel**<br>**Bescherming en verwerking van persoonsgegevens** | Art. 2 | Art. 65 - 73 |
| **Harmonisation minimale**<br>**Minimumharmonisatie** | Art. 3 | (ne doit pas être transposé / dient niet te worden omgezet) |
| **Définitions**<br>**Definities** | Art. 4.1 | Art. 6, 8° |
| | Art. 4.2 | Art. 6, 9° |

| | | |
|---|---|---|
| | Art. 4.3 | Art. 6, 10° |
| | Art. 4.4 | Art. 6, 11° |
| | Art. 4.5 | Art. 6, 20° |
| | Art. 4.6 | Art. 6, 21° |
| | Art. 4.7 | Art. 6, 13° |
| | Art. 4.8 | Art. 6, 14° |
| | Art. 4.9 | Art. 6, 15° |
| | Art. 4.10 | Art. 6, 22° |
| | Art. 4.11 | (ne doit pas être transposé (Règlement UE 1025/2012) / dient niet te worden omgezet (Verordening EU 1025/2012)) |
| | Art. 4.12 | (ne doit pas être transposé (Règlement UE 1025/2012) / dient niet te worden omgezet (Verordening EU 1025/2012)) |
| | Art. 4.13 | Art. 6, 23° |
| | Art. 4.14 | Art. 6, 24° |
| | Art. 4.15 | Art. 6, 25° |
| | Art. 4.16 | Art. 6, 26° |
| | Art. 4.17 | Art. 6, 27° |
| | Art. 4.18 | Art. 6, 28° |
| | Art. 4.19 | Art. 6, 29° |
| **Identification des opérateurs de services essentiels**<br>**Identificatie van aanbieders van essentiële diensten** | Art. 5.1 | Art. 3, §1 ; art. 7, §4 ; art. 11, § 1 |
| | Art. 5.2 | Art. 12, § 1 |
| | Art. 5.3 | (ne doit pas être transposé / dient niet te worden omgezet) |
| | Art. 5.4 | Art. 15, §2 |

| | | |
|---|---|---|
| | Art. 5.5 | Art. 11, §3 |
| | Art. 5.6 | (ne doit pas être transposé / dient niet te worden omgezet) |
| | Art. 5.7 | (ne doit pas être transposé / dient niet te worden omgezet) |
| **Effet disruptif important**<br>**Aanzienlijk verstorend effect** | Art. 6.1 | Art. 13, §2 |
| | Art. 6.2 | Art. 13, § 1 |
| **CHAPITRE II : CADRES NATIONAUX SUR LA SECURITE DES RESEAUX ET DES SYSTEMES D'INFORMATION**<br>**HOOFDSTUK II NATIONALE KADERS VOOR DE BEVEILIGING VAN NETWERK- EN INFORMATIESYSTEMEN** | | |
| **Stratégie nationale en matière de sécurité des réseaux et des systèmes d'information**<br>**Nationale strategie voor de beveiliging van netwerk- en informatiesystemen** | Art. 7.1 | Art. 10 |
| | Art. 7.2 | (ne doit pas être transposé / dient niet te worden omgezet) |
| | Art. 7.3 | (ne doit pas être transposé / dient niet te worden omgezet) |
| **Autorités nationales compétentes et point de contact unique**<br>**Nationale bevoegde autoriteiten en centraal contactpunt** | Art. 8.1 | Art. 7, §1 par délégation au Roi / bij machtiging aan de Koning |
| | Art. 8.2 | Art. 7, §1 par délégation au Roi / bij machtiging aan de Koning |
| | Art. 8.3 | Art. 7, § 1 par délégation au Roi / bij machtiging aan de Koning |
| | Art. 8.4 | Art. 7, §2, 2ème al. / 2de lid |

| | | |
|---|---|---|
| | Art. 8.5 | (ne doit pas être transposé / dient niet te worden omgezet) |
| | Art. 8.6 | Art. 8, § 2 |
| | Art. 8.7 | (ne doit pas être transposé / dient niet te worden omgezet) |
| **Centre de réponse aux incidents de sécurité informatique (CSIRT)**<br>**Computer security incident response teams („CSIRT's")** | Art. 9.1 | Art. 7, § 2 par délégation au Roi / bij machtiging aan de Koning |
| | Art. 9.2 | (ne doit pas être transposé / dient niet te worden omgezet) |
| | Art. 9.3 | (ne doit pas être transposé / dient niet te worden omgezet) |
| | Art. 9.4 | (ne doit pas être transposé / dient niet te worden omgezet) |
| | Art. 9.5 | (ne doit pas être transposé / dient niet te worden omgezet) |
| **Coopération au niveau national**<br>**Samenwerking op nationaal niveau** | Art. 10.1 | Art. 8, § 1 |
| | Art. 10.2 | Art. 25 ; art. 31, § 1 ; art. 35, § 1, al. 2 / lid 2 |
| | Art. 10.3 | Art. 29, al. 1 et 2 / art. 29, lid 1 en 2; art. 37, § 1 |
| **CHAPITRE III : COOPERATION**<br>**HOOFDSTUK III : SAMENWERKING** | | |

| | | |
|---|---|---|
| **Groupe de coopération**<br>**Samenwerkingsgroep** | Art. 11 | (ne doit pas être transposé / dient niet te worden omgezet) |
| **Réseau des CSIRT**<br>**Het CSIRT-netwerk** | Art. 12 | (ne doit pas être transposé / dient niet te worden omgezet) |
| **Coopération internationale**<br>**Internationale samenwerking** | Art. 13 | (ne doit pas être transposé / dient niet te worden omgezet) |
| **CHAPITRE IV : SECURITE DES RESEAUX ET DES SYSTEMES D'INFORMATION DES OPERATEURS DE SERVICES ESSENTIELS**<br>**HOOFDSTUK IV BEVEILIGING VAN DE NETWERK- EN INFORMATIESYSTEMEN VAN AANBIEDERS VAN ESSENTIELE DIENSTEN** | | |
| **Exigences de sécurité et notification d'incidents**<br>**Beveiligingseisen en melding van incidenten** | Art. 14.1 | Art. 20 à 22 / art. 20 tot en met 22 |
| | Art. 14.2 | Art. 20 à 22 / art. 20 tot en met 22 ; art. 28, § 1 |
| | Art. 14.3 | Art. 24, §1 |
| | Art. 14.4 | (ne doit pas être transposé / dient niet te worden omgezet) |
| | Art. 14.5 | Art. 29 |
| | Art. 14.6 | Art. 31, §2 |
| | Art. 14.7 | (ne doit pas être transposé / dient niet te worden omgezet) |
| **Mise en œuvre et exécution**<br>**Uitvoering en handhaving** | Art. 15.1 | Art. 7, §5 ; Art. 21 ; art. 38 ; art. 41 |
| | Art. 15.2 | Art. 38 ; art. 41 ; art. 42 à 46 / art. 42 t.e.m. 46 |
| | Art. 15.3 | Art. 21, §§ 3 et 4 / art. 21, §§ 3 en 4 |
| | Art. 15.4 | Art. 8, § 2 |
| **CHAPITRE V : SECURITE DES RESEAUX ET DES SYSTEMES D'INFORMATION DES FOURNISSEURS DE SERVICE NUMERIQUE**<br>**HOOFDSTUK V: BEVEILIGING VAN DE NETWERK- EN INFORMATIESYSTEMEN VAN DIGITALEDIENSTVERLENERS** | | |

| | | |
|---|---|---|
| **Exigences de sécurité et notification d'incidents**<br><br>**Beveiligingseisen en melding van incidenten** | Art. 16.1 | Art. 33, §1 |
| | Art. 16.2 | Art. 33, §2 |
| | Art. 16.3 | Art. 35 |
| | Art. 16.4 | Art. 35, §§ 2 et 3 / §§ 2 en 3 |
| | Art. 16.5 | Art. 27 |
| | Art. 16.6 | Art. 37, §1 |
| | Art. 16.7 | Art. 37, §2 |
| | Art. 16.8 + (EU) 2018/151 | (ne doit pas être transposé / dient niet te worden omgezet) |
| | Art. 16.9 | (ne doit pas être transposé / dient niet te worden omgezet) |
| | Art. 16.10 | (ne doit pas être transposé / dient niet te worden omgezet) |
| | Art. 16.11 | Art. 32 |
| **Mise en œuvre et exécution**<br>**Uitvoering en handhaving** | Art. 17.1 | Art. 47 |
| | Art. 17.2 | Art. 47, §§ 2 et 3 / §§ 2 en 3 |
| | Art. 17.3 | Art. 47, § 5 |
| **Compétence et territorialité**<br>**Jurisdictie en territorialiteit** | Art. 18.1 | Art. 3, §2, al.1 |
| | Art. 18.2 | Art. 3, §2, al.2 |
| | Art. 18.3 | (ne doit pas être transposé / dient niet te worden omgezet) |
| **CHAPITRE VI : NORMALISATION ET NOTIFICATION VOLONTAIRE**<br>**HOOFDSTUK VI NORMALISATIE EN VRIJWILLIGE MELDING** | | |

| | | |
|---|---|---|
| **Normalisation**<br>**Normalisatie** | Art. 19.1 | Art. 22 |
| | Art. 19.2 | (ne doit pas être transposé / dient niet te worden omgezet) |
| **Notification volontaire**<br>**Vrijwillige melding** | Art. 20.1 | Art. 30, § 1 |
| | Art. 20.2 | Art. 30, § 2 |
| **CHAPITRE VII : DISPOSITIONS FINALES**<br>**HOOFDSTUK VII SLOTBEPALINGEN** | | |
| **Sanctions**<br>**Sancties** | Art. 21 | Art. 48 à 59 / Art. 48 t.e.m. 59 |
| **Comité**<br>**Comitéprocedure** | Art. 22 | (ne doit pas être transposé / dient niet te worden omgezet) |
| **Réexamen**<br>**Evaluatie** | Art. 23 | (ne doit pas être transposé / dient niet te worden omgezet) |
| **Mesures transitoires**<br>**Overgangsmaatregelen** | Art. 24 | (ne doit pas être transposé / dient niet te worden omgezet) |
| **Transposition**<br>**Omzetting** | Art. 25 | Art. 2 |
| **Entrée en vigueur**<br>**Inwerkingtreding** | Art. 26 | (ne doit pas être transposé / dient niet te worden omgezet) |
| **Destinataires**<br>**Adressaten** | Art. 27 | (ne doit pas être transposé / dient niet te worden omgezet) |
| **ANNEXE I : OBLIGATIONS ET TACHES DES CENTRES DE REPONSE AUX INCIDENTS DE SECURITE INFORMATIQUE (CSIRT)** | Annexe I / Bijlage I | Art. 60 à 64 / art. 60 t.e.m. 64 |

| | | |
|---|---|---|
| **BIJLAGE I**<br>**VOORSCHRIFTEN EN TAKEN VOOR COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRT's)** | | |
| **ANNEXE II : TYPES D'ENTITES AUX FINS DE L'ART. 4, POINT 4)**<br>**BIJLAGE II SOORT ENTITEITEN VOOR DE TOEPASSINGEN VAN ARTIKEL 4, PUNT 4** | Annexe II / Bijlage II | Annexe / Bijlage I ; art. 19 |
| **ANNEXE III : TYPE DE SERVICES NUMERIQUES AUX FINS DE L'ART. 4, POINT 5)**<br>**BIJLAGE III : SOORTEN DIGITALE DIENSTEN VOOR DE TOEPASSING VAN ARTIKEL 4, PUNT 5** | Annexe III / Bijlage III | Annexe II |

## Concordantietabel wetsontwerp - richtlijn
## Tableau de correspondance projet de loi - directive

**Directive (UE) 2016/1148 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 (NIS)**

**Richtlijn (EU) 2016/1148 van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (NIS)**

| | Projet de loi / Wetsontwerp | Directive / Richtlijn 2016/1148 |
|---|---|---|
| **TITRE 1ER – DEFINITIONS ET DISPOSITIONS GENERALES**<br>**TITEL 1 – DEFINITIES EN ALGEMENE BEPALINGEN** | | |
| **Chapitre I : Objet et champ d'application**<br>**Hoofdstuk I : Onderwerp en toepassingsgebied** | | |
| **Section 1. Objet**<br>**Afdeling 1. Onderwerp** | | |
| | Art. 1 | (disposition strictement nationale précisant le fondement constitutionnel de la loi / louter nationale wetsbepaling om de grondwettelijke grondslag van de wet te preciseren) |
| | Art. 2 | art. 25.1, al. 3 / lid 3 |
| **Section 2. Champ d'application**<br>**Afdeling 2. Toepassingsgebied** | | |
| | Art. 3, § 1 | Art. 5.1 |
| | Art. 3, §2, al.1 | Art. 18.1 |
| | Art. 3, §2, al.2 | Art. 18.2 |
| | Art. 4, §1 | Art. 1.3 |
| | Art. 4, §2 | Art. 1.7 |

| | | |
|---|---|---|
| | Art. 4, §3 | Art. 1.7 ; cf. exposé des motifs / memorie van toelichting (l'article précise que la loi n'est pas applicable aux opérateurs relevant du secteur des finances, sous réserve de certaines dispositions / het artikel bepaalt dat de wet niet van toepassing is op operatoren die behoren tot de sector financiën, onder voorbehoud van bepaalde wetsbepalingen) |
| | Art. 4, §4 | Art. 1.6 ; cf. exposé des motifs / memorie van toelichting |
| | Art. 5, §1 | (Cette disposition précise l'application du RGPD / Deze bepaling specifieert de toepassing van de AVG) |
| | Art. 5, §2 | Art. 1.4 |
| | Art. 5, §3 | Art. 1. 6 |
| | Art. 5, §4 | Art. 1.6 |
| **Chapitre I : Définitions**<br><br>**Hoofdstuk 2: Definities** | | |
| | Art. 6, 1° | (définition strictement nationale / louter nationale definitie) |
| | Art. 6, 2° | (définition strictement nationale / louter nationale definitie) |
| | Art. 6, 3° | (définition strictement nationale / louter nationale definitie) |

| | | |
|---|---|---|
| Art. 6, 4° | (définition strictement nationale / louter nationale definitie) | |
| Art. 6, 5° | (définition strictement nationale / louter nationale definitie) | |
| Art. 6, 6° | (définition strictement nationale / louter nationale definitie) | |
| Art. 6, 7° | (définition strictement nationale / louter nationale definitie) | |
| Art. 6, 8° | Art. 4.1 | |
| Art. 6, 9° | Art. 4.2 | |
| Art. 6, 10° | Art. 4.3 | |
| Art. 6, 11° | Art. 4.4 | |
| Art. 6, 12° | (définition strictement nationale / louter nationale definitie) | |
| Art. 6, 13° | Art. 4.7 | |
| Art. 6, 14° | Art. 4.8 | |
| Art. 6, 15° | Art. 4.9 | |
| Art. 6, 16° | (définition strictement nationale / louter nationale definitie) | |
| Art. 6, 17° | (définition strictement nationale / louter nationale definitie) | |
| Art. 6, 18° | (définition strictement nationale / louter nationale definitie) | |
| Art. 6, 19° | (définition strictement nationale / louter nationale definitie) | |
| Art. 6, 20° | Art. 4.5 | |
| Art. 6, 21° | Art. 4.6 | |

| | | |
|---|---|---|
| | Art. 6, 22° | Art. 4.10 |
| | Art. 6, 23° | Art. 4.13 |
| | Art. 6, 24° | Art. 4.14 |
| | Art. 6, 25° | Art. 4.15 |
| | Art. 6, 26° | Art. 4.16 |
| | Art. 6, 27° | Art. 4.17 |
| | Art. 6, 28° | Art. 4.18 |
| | Art. 6, 29° | Art. 4.19 |
| | Art. 6,30° | (définition strictement nationale / louter nationale definitie) |
| | Art. 6,31° | (définition strictement nationale / louter nationale definitie) |
| | Art. 6,32° | (définition strictement nationale / louter nationale definitie) |
| | Art. 6, 33° | (disposition en vue du RGPD / bepaling met het oog op de AVG) |
| **Chapitre 3. Autorités compétentes et coopération au niveau national**<br>**Hoofdstuk 3. Bevoegde autoriteiten en samenwerking op nationaal niveau** | | |
| **Section 1. Autorités compétentes**<br>**Afdeling 1. Bevoegde autoriteiten** | | |
| | Art. 7, §1 (Cet article charge le Roi de désigner l'autorité nationale chargée du suivi et de la coordination de la mise en œuvre de la loi et de jouer le rôle de point de contact national unique / Dit artikel bepaalt dat de koning de nationale autoriteit aanwijst die belast is met de opvolging en coördinatie van de uitvoering van deze wet en de rol speelt van centraal nationaal contactpunt) | Art. 8.1, art. 8.2, art. 8.3 par délégation au Roi / bij machtiging aan de Koning |
| | Art. 7, §2 (L'article prévoit que le Roi désigne l'autorité chargée d'assurer le rôle de CSIRT national / Dit artikel verduidelijkt | Art. 9.1 par délégation au Roi / bij machtiging aan de Koning ; art. 8.4 |

| | | |
|---|---|---|
| | dat de Koning de autoriteit aanwijst die de rol van nationaal CSIRT vervult) | |
| | Art. 7, §3 (Cet article charge le Roi de désigner les autorités sectorielles / Dit artikel machtigt de Koning om sectorale overheden aan te stellen) | (disposition strictement nationale / louter nationale bepaling) |
| | Art. 7, §4 (Cet article habilite le Roi à désigner l'autorité chargée de coordonner l'identification des opérateurs essentiels / Dit artikel bepaalt dat de Koning de autoriteit moet aanwijzen die bevoegd is voor de coördinatie van de identificatie van aanbieders van essentiële diensten) | Art. 5.1 par délégation au Roi / bij machtiging aan de Koning |
| | Art. 7, §5 (compétence de contrôle du service d'inspection / toezichtsbevoegdheid van de inspectiedienst) | Art. 15.1 |
| **Section 2. Coopération au niveau national**<br>**Afdeling 2. Samenwerking op nationaal niveau** | | |
| | Art. 8, § 1 | Art. 10.1 |
| | Art. 8, § 2 | Art. 8.6 ; art. 15.4 |
| | Art. 8, § 3 | (disposition strictement nationale / louter nationale bepaling) |
| **Chapitre 4. Echanges d'information**<br>**Hoofdstuk 4. Informatie-uitwisseling** | | |
| | Art. 9, § 1, al. 1 | (disposition strictement nationale / louter nationale bepaling) |
| | Art. 9, §1, al. 2 | Art. 1.5 |

| | | |
|---|---|---|
| | Art. 9, § 2 | (disposition strictement nationale / louter nationale bepaling) |
| | Art. 9, § 3 | Art. 1.5, art. 14.5 |
| **Chapitre 5. Stratégie nationale en matière de sécurité des réseaux et des systèmes d'information**<br>**Hoofdstuk 5. Nationale strategie voor de beveiliging van netwerk- en informatiesystemen** | | |
| | Art. 10 | Art. 7.1 par délégation au Roi / bij machtiging aan de Koning |
| **Titre 2. - Réseaux et systèmes d'information des opérateurs de services essentiels**<br>**Titel 2. - Netwerk- en informatiesystemen van de aanbieders van essentiële diensten** | | |
| **Chapitre 1. Identification des opérateurs de services essentiels**<br>**Hoofdstuk 1. Identificatie van de aanbieders van essentiële diensten** | | |
| | Art. 11, §1 | Art. 5.1 |
| | Art. 11, §2 | (strictement national/louter nationaal) |
| | Art. 11, §3 | Art. 5.5 |
| | Art. 12, § 1 | Art. 5.2 |
| | Art. 12, § 2 | (disposition strictement nationale / louter nationale bepaling) |
| | Art. 13, §1 | Art. 6.2 |
| | Art. 13, §2 | Art. 6.1 |
| | Art. 13, §3 | (disposition strictement nationale / louter nationale bepaling) |
| | Art. 14 | (disposition strictement nationale / louter nationale bepaling) |
| | Art. 15, §1 | (disposition strictement nationale / louter nationale bepaling) |
| | Art. 15, §2 | Art. 5.4 |

| | | |
|---|---|---|
| | Art. 15, §3 | (disposition strictement nationale / louter nationale bepaling) |
| | Art. 16 | (disposition strictement nationale / louter nationale bepaling) |
| | Art. 17 | (disposition strictement nationale en matière de publicité de l'administration / louter nationale bepaling inzake openbaarheid van bestuur) |
| | Art. 18 | (disposition strictement nationale et lien avec la loi belge transposant la directive 2008/114 / louter nationale bepaling en verband met de Belgische houdende omzetting van de richtlijn 2008/114) |
| | Art. 19 | (disposition strictement nationale permettant au Roi de compléter la liste visée à l'annexe I / louter nationale bepaling die de Koning machtigt om de lijst in bijlage I bij te vullen) |
| **Chapitre 2. Mesures de sécurité**<br><br>**Hoofdstuk 2. Beveiligingsmaatregelen** | | |
| | Art. 20 | Art. 14.1 ; art. 14.2 |
| | Art. 21, §§ 1 et 2 / §§ 1 en 2 | Art. 15.1 ; art. 15.2 |
| | Art. 21, §§ 3 et 4 / §§ 3 en 4 | Art. 15.3 |
| | Art. 21, § 5 | (disposition strictement nationale et lien avec la loi belge transposant la directive 2008/114 / louter nationale bepaling en verband met de Belgische |

| | | |
|---|---|---|
| | | houdende omzetting van de richtlijn 2008/114) |
| | Art. 22 | (disposition strictement nationale / louter nationale bepaling, cf. art. 19.1) |
| | Art. 23 | (disposition strictement nationale / louter nationale bepaling) |
| | | |
| **Chapitre 3. Notification d'incidents**<br>**Hoofdstuk 3. Melding van incidenten** | | |
| | Art. 24, §1 | Art. 14.3 |
| | Art. 24, §§2 - 4 | (disposition strictement nationale / louter nationale bepaling) |
| | Art. 25 | (disposition strictement nationale / louter nationale bepaling, cf. art. 10.2) |
| | Art. 26 | (disposition strictement nationale rendant applicables ou adaptant certaines obligations de notification prévues par la loi, dans le secteur des finances / louter nationale bepaling die bepaalde vermeldingsplichten uit deze wet in de sector financiën toepasselijk maken of aanpassen) |
| | Art. 27 | Art. 16.5 |
| | Art. 28 | Art. 14.2 |
| | Art. 29 | Art. 14.5 ; art. 10.3 |
| | Art. 30, §1 | Art. 20.1 |
| | Art. 30, §2 | Art. 20.2 |

| | | |
|---|---|---|
| | Art. 31, §1 | (disposition strictement nationale permettant au Roi de fixer les modalités de notification des incidents / louter nationale bepaling die de Koning machtigt om de modaliteiten voor de melding en rapportering van incidenten vast te leggen, cf. art. 10.2) |
| | Art. 31, §2 | Art. 14.6 |
| **Titre 3. - Réseaux et systèmes d'information des fournisseurs de service numérique**<br>**Titel 3. - Netwerk- en informatiesystemen van digitaledienstverleners** | | |
| | Art. 32 | Art. 16.11 |
| **Chapitre 1. Les exigences de sécurité**<br>**Hoofdstuk 1. De beveiligingseisen** | | |
| | Art. 33, §1 | Art. 16.1 |
| | Art. 33, §2 | Art. 16.2 |
| | Art. 34 | (disposition strictement nationale / louter nationale bepaling) |
| **Chapitre 2. Notification d'incidents**<br>**Hoofdstuk 2. Melding van incidenten** | | |
| | Art. 35, §1 | Art. 16.3 ; art. 10.2 |
| | Art. 35, §2 | renvoi au règlement d'exécution CE 2018/151 / verwijzing naar de uitvoeringsverordening EC 2018/151 ; art. 16.4 |
| | Art. 35, §3 | Art. 16.4, *in fine* |
| | Art. 36 | (disposition strictement nationale / louter nationale bepaling) |
| | Art. 37,§1 | Art. 16.6 ; art. 10.3 |
| | Art. 37,§2 | Art. 16.7 |
| **Titre 4. - Contrôle et sanctions**<br>**Titel 4. - Toezicht en sancties** | | |

| | | |
|---|---|---|
| **Chapitre 1er. Les contrôles des opérateurs de services essentiels**<br>**Hoofdstuk 1. Toezicht op de aanbieders van essentiële diensten** | | |
| **Section 1. Audits**<br>**Afdeling 1. Audits** | | |
| | Art. 38 | Art. 15.1 ; art. 15.2 (b) |
| | Art. 39 | (disposition strictement nationale / louter nationale bepaling) |
| | Art. 40 | (disposition strictement nationale / louter nationale bepaling) |
| | Art. 41 | (disposition strictement nationale / louter nationale bepaling) |
| **Section 2. Service d'inspection**<br>**Afdeling 2. Inspectiedienst** | | |
| | Art. 42 | Art. 15 |
| | Art. 43 | (disposition strictement nationale / louter nationale bepaling, cf. art. 15) |
| | Art. 44 - 46 | Art. 15 |
| **Chapitre 2. Contrôle des fournisseurs de service numérique**<br>**Hoofdstuk 2. Toezicht op de digitaledienstverleners** | | |
| | Art. 47 | Art. 17 par délégation au Roi / bij machtiging aan de Koning |
| **Chapitre 3. Les sanctions**<br>**Hoofdstuk 3. De sancties** | | |
| **Section 1. Procédure**<br>**Afdeling 1. Procedure** | | |
| | Art. 48 - 50 | Art. 21 |
| **Section 2. Sanctions pénales**<br>**Afdeling 2. Strafrechtelijke sancties** | | |
| | Art. 51 | Art. 21 |

| | | |
|---|---|---|
| **Section 3. Sanctions administratives**<br>**Afdeling 3. Administratieve sancties** | | |
| | Art. 52-59 | Art. 21 |
| **Titre 5. - CSIRT**<br>**Titel 5. - CSIRT** | | |
| **Chapitre 1er. Le CSIRT national**<br><br>**Hoofdstuk 1. Het nationale CSIRT** | | |
| Section 1re. Tâches du CSIRT national<br>Afdeling 1. Taken van het nationale CSIRT | | |
| | Art. 60 | Annexe / Bijlage I (2) |
| Section 2. Obligations du CSIRT national<br>Afdeling 2. Voorschriften voor het nationale CSIRT | | |
| | Art. 61 | Annexe / Bijlage I (1) |
| | Art. 62 | (disposition strictement nationale / louter nationale bepaling) |
| **Chapitre 2. Le CSIRT sectoriel**<br>**Hoofdstuk 2. Het sectoraal CSIRT** | | |
| Section 1re. Tâches du CSIRT sectoriel<br>Afdeling 1. Taken van het sectoraal CSIRT | | |
| | Art. 63 | Annexe / Bijlage I (2) |
| Section 2. Obligations d'un CSIRT sectoriel<br>Afdeling 2. Voorschriften voor een sectoraal CSIRT | | |
| | Art. 64 | Annexe / Bijlage I (1) |
| **Titre 6. – Traitement des données à caractère personnel**<br>**Titel 6. – Verwerking van persoonsgegevens** | | |
| Section 1. Principes relatifs au traitement, bases légales et finalités<br>Afdeling 1. Beginselen inzake verwerking, wettelijke basis en doeleinden | | |

| | | |
|---|---|---|
| | Art. 65 - 68 | Cette disposition donne effet à l'article 2 adapté au sens de principes du RGPD / Deze bepaling geeft uitvoering aan artikel 2 dat is aangepast aan de beginselen van de AVG |
| Section 2. Durée de conservation<br>Afdeling 2. Bewaartermijn | | |
| | Art. 69 | Cette disposition donne effet à l'article 2 adapté au sens de principes du RGPD / Deze bepaling geeft uitvoering aan artikel 2 dat is aangepast aan de beginselen van de AVG |
| Section 3. Délégué à la protection des données<br>Afdeling 3. Functionaris voor gegevensbescherming | | |
| | Art. 70 | Cette disposition donne effet à l'article 2 adapté au sens de principes du RGPD / Deze bepaling geeft uitvoering aan artikel 2 dat is aangepast aan de beginselen van de AVG |
| Section 4. Limitations des droits des personnes concernées<br>Afdeling 4. Beperking van de rechten van de betrokken personen | | |
| | Art. 71 - 72 | Cette disposition donne effet à l'article 2 adapté au sens de principes du RGPD / Deze bepaling geeft uitvoering aan artikel 2 dat is aangepast aan de beginselen van de AVG |
| Section 5. Limitations aux obligations de notification des violations de données à caractère personnel<br>Afdeling 5. Beperkingen inzake de verplichte melding van inbreuken in verband met persoonsgegevens | | |
| | Art. 73 | Cette disposition donne effet à l'article 2 adapté au sens de principes du RGPD / Deze bepaling geeft uitvoering aan artikel 2 dat is aangepast aan de beginselen van de AVG |

| | | |
|---|---|---|
| **Titre 7. - Disposition finales**<br>**Titel 7. - Slotbepalingen** | | |
| **Chapitre 1. Modifications de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques**<br>**Hoofdstuk 1. Wijzigingen van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren** | | |
| | Art. 74 - 84 | (dispositions strictement nationales / louter nationale bepalingen) |
| **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.**<br>**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 - 86 | (dispositions strictement nationales / louter nationale bepalingen) |
| **Chapitre 3. Modifications de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges**<br>**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 - 89 | (dispositions strictement nationales / louter nationale bepalingen) |
| **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 et de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers**<br>**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 en van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten** | | |
| | Art. 90 - 91 | (dispositions strictement nationales / louter nationale bepalingen) |
| **Chapitre 5. Modifications de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique**<br>**Hoofdstuk 5. Wijzigingen van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België** | | |
| | Art. 92 – 94 | (dispositions strictement nationales / louter nationale bepalingen) |
| **Chapitre 6. Entrée en vigueur**<br>**Hoofdstuk 6. Inwerkingtreding** | | |
| | Art. 95 | / |
| **ANNEXE I. TYPES D'OPÉRATEURS DE SERVICES ESSENTIELS VISÉS À L'ARTICLE 11, § 1ER** | Annexe I / Bijlage I | Annexe II / Bijlage II |

| | | |
|---|---|---|
| **BIJLAGE I. SOORTEN AANBIEDERS VAN ESSENTIËLE DIENSTEN BEDOELD IN ARTIKEL 11, § 1** | | |
| **ANNEXE II. TYPE DE SERVICES NUMERIQUES**<br>**BIJLAGE II. SOORTEN DIGITALE DIENSTEN** | Annexe II / Bijlage II | Annexe III / Bijlage III |

## COÖRDINATIE VAN DE ARTIKELEN

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| **Wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren** | **Wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren** |
| **Art. 2.** Deze wet voorziet in de gedeeltelijke omzetting van de Richtlijn 2008/114/EG van de Raad van 8 december 2008 inzake de identificatie van Europese kritieke infrastructuren, de aanmerking van infrastructuren als Europese kritieke infrastructuren en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuren te verbeteren. | **Art. 2.** Deze wet voorziet in de gedeeltelijke omzetting van de Richtlijn 2008/114/EG van de Raad van 8 december 2008 inzake de identificatie van Europese kritieke infrastructuren, de aanmerking van infrastructuren als Europese kritieke infrastructuren en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuren te verbeteren. |
| De ADCC, zoals gedefinieerd in artikel 3, 1°, wordt aangeduid als nationaal contactpunt voor de bescherming van Europese kritieke infrastructuren, hierna « EPCIP-contactpunt » genoemd, voor het geheel van de sectoren en deelsectoren, voor België in haar relatie met de Europese Commissie en de Lidstaten van de Europese Unie. | De ADCC, zoals gedefinieerd in artikel 3, 1°, wordt aangeduid als nationaal contactpunt voor de bescherming van Europese kritieke infrastructuren, hierna « EPCIP-contactpunt » genoemd, voor het geheel van de sectoren en deelsectoren, voor België in haar relatie met de Europese Commissie en de Lidstaten van de Europese Unie. |
| | **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. 3.** Voor de toepassing van deze wet en de uitvoeringsbesluiten ervan wordt verstaan onder: | **Art. 3.** Voor de toepassing van deze wet en de uitvoeringsbesluiten ervan wordt verstaan onder: |
| 1° "ADCC": Algemene Directie Crisiscentrum van de Federale Overheidsdienst Binnenlandse Zaken, belast met de bijzondere bescherming van goederen en personen en met de nationale coördinatie op het vlak van openbare orde ; | 1° "ADCC": Algemene Directie Crisiscentrum van de Federale Overheidsdienst Binnenlandse Zaken, belast met de bijzondere bescherming van goederen en personen en met de nationale coördinatie op het vlak van openbare orde ; |
| 2° "OCAD": Coördinatieorgaan voor de dreigingsanalyse ingesteld door de wet van 10 juli 2006 betreffende de analyse van de dreiging ; | 2° "OCAD": Coördinatieorgaan voor de dreigingsanalyse ingesteld door de wet van 10 juli 2006 betreffende de analyse van de dreiging ; |
| 3° "sectorale overheid": | 3° "sectorale overheid": |
| a) voor de sector vervoer: de Minister bevoegd voor Vervoer of, bij delegatie door deze, een leidend personeelslid van zijn administratie ; | a) voor de sector vervoer: de Minister bevoegd voor Vervoer of, bij delegatie door deze, een leidend personeelslid van zijn administratie ; |
| b) voor de sector energie: de Minister bevoegd voor Energie of, bij delegatie door deze, een leidend personeelslid van zijn administratie ; | b) voor de sector energie: de Minister bevoegd voor Energie of, bij delegatie door deze, een leidend personeelslid van zijn administratie ; |

## COÖRDINATIE VAN DE ARTIKELEN

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| c) voor de sector financiën : de Nationale Bank van België; | **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;** |
| | 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);** |
| d) voor de sector elektronische communicatie: de minister bevoegd voor Elektronische Communicatie of, bij delegatie door deze, een leidend personeelslid van zijn administratie of een lid van het Belgisch Instituut voor postdiensten en telecommunicatie; | **e) voor de sector elektronische communicatie en digitale infrastructuren: het Belgisch Instituut voor postdiensten en telecommunicatie;** |
| | **f) voor de sector gezondheidszorg: de overheid aangewezen door de wet of door de Koning bij in Ministerraad overlegd besluit;** |
| | **g) voor de sector water: de overheid aangewezen door de wet of door de Koning bij in Ministerraad overlegd besluit;** |
| 4° "kritieke infrastructuur": installatie, systeem of een deel daarvan, van federaal belang, dat van essentieel belang is voor het behoud van vitale maatschappelijke functies, de gezondheid, de veiligheid, de beveiliging, de economische welvaart of het maatschappelijk welzijn, en waarvan de verstoring van de werking of de vernietiging een aanzienlijke weerslag zou hebben doordat die functies ontregeld zouden raken; | 4° "kritieke infrastructuur": installatie, systeem of een deel daarvan, van federaal belang, dat van essentieel belang is voor het behoud van vitale maatschappelijke functies, de gezondheid, de veiligheid, de beveiliging, de economische welvaart of het maatschappelijk welzijn, en waarvan de verstoring van de werking of de vernietiging een aanzienlijke weerslag zou hebben doordat die functies ontregeld zouden raken; |
| 5° "nationale kritieke infrastructuur": kritieke infrastructuur op het Belgisch grondgebied waarvan de verstoring van de werking of de vernietiging een aanzienlijke weerslag in het land zou hebben; | 5° "nationale kritieke infrastructuur": kritieke infrastructuur op het Belgisch grondgebied waarvan de verstoring van de werking of de vernietiging een aanzienlijke weerslag in het land zou hebben; |
| 6° "Europese kritieke infrastructuur": de nationale kritieke infrastructuur waarvan de verstoring van de werking of de vernietiging een aanzienlijke weerslag in ten minste twee lidstaten van de Europese Unie zou hebben of de kritieke infrastructuur die niet | 6° "Europese kritieke infrastructuur": de nationale kritieke infrastructuur waarvan de verstoring van de werking of de vernietiging een aanzienlijke weerslag in ten minste twee lidstaten van de Europese Unie zou hebben of de kritieke infrastructuur die niet |

## COÖRDINATIE VAN DE ARTIKELEN

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| gelegen is op het Belgische grondgebied, maar op het grondgebied van een andere Lidstaat van de Europese Unie, waarvan de verstoring van de werking of de vernietiging een aanzienlijke weerslag zou hebben in ten minste twee Lidstaten van de Europese Unie, waaronder België; | gelegen is op het Belgische grondgebied, maar op het grondgebied van een andere Lidstaat van de Europese Unie, waarvan de verstoring van de werking of de vernietiging een aanzienlijke weerslag zou hebben in ten minste twee Lidstaten van de Europese Unie, waaronder België; |
| 7° "andere punten van federaal belang": de plaatsen die niet zijn aangeduid als kritieke infrastructuur, maar die van bijzonder belang zijn voor de openbare orde, voor de bijzondere bescherming van personen en goederen, voor het beheer van noodsituaties of voor de militaire belangen en die het voorwerp uitmaken van beschermingsmaatregelen genomen door de ADCC; | 7° "andere punten van federaal belang": de plaatsen die niet zijn aangeduid als kritieke infrastructuur, maar die van bijzonder belang zijn voor de openbare orde, voor de bijzondere bescherming van personen en goederen, voor het beheer van noodsituaties of voor de militaire belangen en die het voorwerp uitmaken van beschermingsmaatregelen genomen door de ADCC; |
| 8° "punten van lokaal belang": de plaatsen die geen kritieke infrastructuren noch andere punten van federaal belang zijn, maar die van bijzonder belang zijn voor de uitvoering van de opdrachten van bestuurlijke politie op lokaal niveau en die het voorwerp uitmaken van beschermingsmaatregelen genomen door de burgemeester; | 8° "punten van lokaal belang": de plaatsen die geen kritieke infrastructuren noch andere punten van federaal belang zijn, maar die van bijzonder belang zijn voor de uitvoering van de opdrachten van bestuurlijke politie op lokaal niveau en die het voorwerp uitmaken van beschermingsmaatregelen genomen door de burgemeester; |
| 9° "elektronische communicatie": de elektronische communicatie bedoeld bij de wet van 13 juni 2005 betreffende de elektronische communicatie; | 9° "elektronische communicatie": de elektronische communicatie bedoeld bij de wet van 13 juni 2005 betreffende de elektronische communicatie; |
| 10° "exploitant": iedere natuurlijke persoon of rechtspersoon die verantwoordelijk is voor de investeringen in of voor de dagelijkse werking van een nationale of Europese kritieke infrastructuur; | 10° "exploitant": iedere natuurlijke persoon of rechtspersoon die verantwoordelijk is voor de investeringen in of voor de dagelijkse werking van een nationale of Europese kritieke infrastructuur; |
| 11° "politiediensten": de politiediensten bedoeld bij de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus; | 11° "politiediensten": de politiediensten bedoeld bij de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus; |
| 12° « SICAD » : communicatie- en informatiedienst van het arrondissement, zoals bedoeld bij de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus. | 12° « SICAD » : communicatie- en informatiedienst van het arrondissement, zoals bedoeld bij de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus. |
| | **13° "de wet van xx xx 2018": de wet van xx xx 2018 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;** |

## COÖRDINATIE VAN DE ARTIKELEN

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| | **14° "beveiliging van netwerk- en informatiesystemen": de beveiliging van netwerk- en informatiesystemen als bedoeld in artikel 6, 8° en 9°, van de wet van xx xx 2018;** |
| | **15° "digitale infrastructuren": de aanbieders bedoeld in punt 6 van bijlage 1 van de wet van xx xx 2018;** |
| | **16° "water": de aanbieders bedoeld in punt 5 van bijlage 1 van de wet van xx xx 2018;"** |
| | **"17° "gezondheidszorg": de aanbieders bedoeld in punt 4 van bijlage 1 van de wet van xx xx 2018.** |
| **Art. 4.** § 1. Dit hoofdstuk is van toepassing op de vervoersector en de energiesector wat de beveiliging en de bescherming van de nationale en de Europese kritieke infrastructuren betreft. | **Art. 4.** § 1. Dit hoofdstuk is van toepassing op de vervoersector en de energiesector wat de beveiliging en de bescherming van de nationale en de Europese kritieke infrastructuren betreft. |
| Het is echter niet van toepassing op de nucleaire installaties bedoeld bij 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, met uitzondering van de elementen van een nucleaire installatie bestemd voor de industriële productie van elektriciteit die dienen voor de transmissie van de elektriciteit. | Het is echter niet van toepassing op de nucleaire installaties bedoeld bij 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, met uitzondering van de elementen van een nucleaire installatie bestemd voor de industriële productie van elektriciteit die dienen voor de transmissie van de elektriciteit. |
| Artikel 8 en de artikelen 12 tot 26 zijn enkel van toepassing op de kritieke infrastructuren die gelegen zijn op het Belgisch grondgebied. | Artikel 8 en de artikelen 12 tot 26 zijn enkel van toepassing op de kritieke infrastructuren die gelegen zijn op het Belgisch grondgebied. |
| § 2. De sector Energie bestaat uit de volgende deelsectoren : | § 2. De sector Energie bestaat uit de volgende deelsectoren : |
| 1° elektriciteit, samengesteld uit infrastructuren en voorzieningen voor elektriciteitsproductie en -transmissie, met het oog op elektriciteitsvoorziening; | 1° elektriciteit, samengesteld uit infrastructuren en voorzieningen voor elektriciteitsproductie en -transmissie, met het oog op elektriciteitsvoorziening; |
| 2° olie, samengesteld uit aardolieproductie, -raffinage, -behandeling, -opslag en -transmissie van pijpleidingen; | 2° olie, samengesteld uit aardolieproductie, -raffinage, -behandeling, -opslag en -transmissie van pijpleidingen; |
| 3° gas, samengesteld uit gasproductie, -raffinage, -behandeling, -opslag en -transmissie van pijpleidingen en terminals voor vloeibaar aardgas. | 3° gas, samengesteld uit gasproductie, -raffinage, -behandeling, -opslag en -transmissie van pijpleidingen en terminals voor vloeibaar aardgas. |

## COÖRDINATIE VAN DE ARTIKELEN

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| De sector Vervoer bestaat uit de volgende deelsectoren : | De sector Vervoer bestaat uit de volgende deelsectoren : |
| 1° wegvervoer;<br>2° spoorvervoer;<br>3° luchtvervoer;<br>4° vervoer over de binnenwateren;<br>5° lange omvaart en short sea shipping en havens. | 1° wegvervoer;<br>2° spoorvervoer;<br>3° luchtvervoer;<br>4° vervoer over de binnenwateren;<br>5° lange omvaart en short sea shipping en havens. |
| § 3. In afwijking van §1, eerste lid, is dit hoofdstuk niet van toepassing op de deelsector van het luchtvervoer. | § 3. In afwijking van §1, eerste lid, is dit hoofdstuk niet van toepassing op de deelsector van het luchtvervoer. |
| Onverminderd artikel 2, tweede lid, neemt de Koning, bij een in Ministerraad overlegd besluit, de nodige maatregelen, met inbegrip van de opheffing, de aanvulling, de wijziging of de vervanging van wetsbepalingen, om de omzetting te verzekeren van de Richtlijn 2008/114/EG van de Raad van 8 december 2008 inzake de identificatie van Europese kritieke infrastructuren, de aanmerking van infrastructuren als Europese kritieke infrastructuren en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuren te verbeteren wat het luchtvervoer betreft. | Onverminderd artikel 2, tweede lid, neemt de Koning, bij een in Ministerraad overlegd besluit, de nodige maatregelen, met inbegrip van de opheffing, de aanvulling, de wijziging of de vervanging van wetsbepalingen, om de omzetting te verzekeren van de Richtlijn 2008/114/EG van de Raad van 8 december 2008 inzake de identificatie van Europese kritieke infrastructuren, de aanmerking van infrastructuren als Europese kritieke infrastructuren en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuren te verbeteren wat het luchtvervoer betreft. |
| § 4. Dit hoofdstuk is van toepassing op de financiële sector en op de sector elektronische communicatie wat de beveiliging en de bescherming van de nationale kritieke infrastructuren betreft. | **§ 4. Dit hoofdstuk is van toepassing op de sector financiën, de exploitanten van een handelsplatform bedoeld in artikel 3, 3°, d) van de wet de sector elektronische communicatie, de sector digitale infrastructuren, de sector gezondheidszorgen en de sector water wat de beveiliging en de bescherming van de nationale kritieke infrastructuren betreft.** |
| **Art. 5.** § 1. Teneinde de kritieke infrastructuren die onder haar bevoegdheid vallen te identificeren, overlegt de sectorale overheid vooraf met de ADCC, en raadpleegt, indien ze dit nuttig acht, de vertegenwoordigers van de sector en de exploitanten van potentiële kritieke infrastructuren. | **Art. 5.** § 1. Teneinde de kritieke infrastructuren die onder haar bevoegdheid vallen te identificeren, overlegt de sectorale overheid vooraf met de ADCC, en raadpleegt, indien ze dit nuttig acht, de vertegenwoordigers van de sector en de exploitanten van potentiële kritieke infrastructuren. |
| Met hetzelfde doel gaat de sectorale overheid over tot de voorafgaande raadpleging van de gewesten, voor de potentiële kritieke infrastructuren die onder hun bevoegdheden vallen. | Met hetzelfde doel gaat de sectorale overheid over tot de voorafgaande raadpleging van de gewesten, voor de potentiële kritieke infrastructuren die onder hun bevoegdheden vallen. |
| § 2. De te volgen procedure voor de identificatie van de nationale en de Europese kritieke infrastructuren wordt vastgesteld in bijlage. | § 2. De te volgen procedure voor de identificatie van de nationale en de Europese kritieke infrastructuren wordt vastgesteld in bijlage. |

## COÖRDINATIE VAN DE ARTIKELEN

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| | **§ 3. Tijdens het hele identificatieproces als bedoeld in deze afdeling wordt de autoriteit bedoeld in artikel 7, § 1, van de wet van xx 2018 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. 13.** § 1. De exploitant van een kritieke infrastructuur werkt een beveiligingsplan van de exploitant, hierna B.P.E. genaamd, met het oog op het voorkomen, beperken en neutraliseren van de risico's op verstoring van de werking of van de vernietiging van de kritieke infrastructuur door het op punt stellen van interne materiële en organisatorische maatregelen. | **Art. 13.** § 1. De exploitant van een kritieke infrastructuur werkt een beveiligingsplan van de exploitant, hierna B.P.E. genaamd, met het oog op het voorkomen, beperken en neutraliseren van de risico's op verstoring van de werking of van de vernietiging van de kritieke infrastructuur door het op punt stellen van interne materiële en organisatorische maatregelen. |
| § 2. Het B.P.E. bevat minstens : | § 2. Het B.P.E. bevat minstens : |
| 1° permanente interne beveiligingsmaatregelen, die toegepast moeten worden in alle omstandigheden; | 1° permanente interne beveiligingsmaatregelen, die toegepast moeten worden in alle omstandigheden; |
| 2° graduele interne beveiligingsmaatregelen toe te passen in functie van de dreiging. | 2° graduele interne beveiligingsmaatregelen toe te passen in functie van de dreiging. |
| Voor een bepaalde sector of in voorkomend geval per deelsector, kan de Koning deze maatregelen specificeren en opleggen om bepaalde informatie op te nemen in het B.P.E. | Voor een bepaalde sector of in voorkomend geval per deelsector, kan de Koning deze maatregelen specificeren en opleggen om bepaalde informatie op te nemen in het B.P.E. |
| § 3. De procedure van uitwerking van het B.P.E. bevat minstens de volgende stappen: | § 3. De procedure van uitwerking van het B.P.E. bevat minstens de volgende stappen: |
| 1° de inventaris en de ligging van de punten van de infrastructuur die, indien ze geraakt zouden worden, de verstoring van haar werking of haar vernietiging zouden kunnen veroorzaken; | 1° de inventaris en de ligging van de punten van de infrastructuur die, indien ze geraakt zouden worden, de verstoring van haar werking of haar vernietiging zouden kunnen veroorzaken; |
| 2° een risicoanalyse, bestaande uit een identificatie van de voornaamste scenario's van pertinente potentiële dreigingen van opzettelijke handelingen met het oog op de verstoring van de werking of de vernietiging van de kritieke infrastructuur ; | 2° een risicoanalyse, bestaande uit een identificatie van de voornaamste scenario's van pertinente potentiële dreigingen van opzettelijke handelingen met het oog op de verstoring van de werking of de vernietiging van de kritieke infrastructuur ; |
| 3° een analyse van de kwetsbaarheden van de kritieke infrastructuur en de potentiële weerslag van de verstoring van haar werking of van haar vernietiging in functie van de verschillende in aanmerking genomen scenario's; | 3° een analyse van de kwetsbaarheden van de kritieke infrastructuur en de potentiële weerslag van de verstoring van haar werking of van haar vernietiging in functie van de verschillende in aanmerking genomen scenario's; |

## COÖRDINATIE VAN DE ARTIKELEN

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| 4° voor elk scenario uit de risicoanalyse, de identificatie, de selectie en de aanwijzing in volgorde van prioriteit van de interne beveiligingsmaatregelen. | 4° voor elk scenario uit de risicoanalyse, de identificatie, de selectie en de aanwijzing in volgorde van prioriteit van de interne beveiligingsmaatregelen. |
| § 4. De exploitant werkt het B.P.E. uit binnen een termijn van één jaar na de betekening aan de exploitant van de aanduiding van zijn infrastructuur als kritieke infrastructuur. | § 4. De exploitant werkt het B.P.E. uit binnen een termijn van één jaar na de betekening aan de exploitant van de aanduiding van zijn infrastructuur als kritieke infrastructuur. |
| Binnen een termijn van uiterlijk vierentwintig maanden, te rekenen vanaf de betekening van de aanduiding van zijn infrastructuur als kritieke infrastructuur, implementeert hij de interne beveiligingsmaatregelen voorzien in het B.P.E. | Binnen een termijn van uiterlijk vierentwintig maanden, te rekenen vanaf de betekening van de aanduiding van zijn infrastructuur als kritieke infrastructuur, implementeert hij de interne beveiligingsmaatregelen voorzien in het B.P.E. |
| Voor een welbepaalde sector of, in voorkomend geval, per deelsector, kan de bevoegde sectorale overheid deze termijn aanpassen in functie van het type van maatregelen die zijn voorzien in het B.P.E. § 5. Wat betreft de havens die vallen onder het toepassingsgebied van de wet van 5 februari 2007 betreffende de maritieme beveiliging, wordt het havenbeveiligingsplan opgelegd door die wet, gelijkgesteld met het B.P.E. | Voor een welbepaalde sector of, in voorkomend geval, per deelsector, kan de bevoegde sectorale overheid deze termijn aanpassen in functie van het type van maatregelen die zijn voorzien in het B.P.E. § 5. Wat betreft de havens die vallen onder het toepassingsgebied van de wet van 5 februari 2007 betreffende de maritieme beveiliging, wordt het havenbeveiligingsplan opgelegd door die wet, gelijkgesteld met het B.P.E. |
| § 5bis. Voor de kritieke infrastructuren die onder de bevoegdheid van de sector financiën vallen, worden de beveiligingsmaatregelen, zoals het continuïteitsbeleid, de continuïteitsplannen en de plannen voor fysieke en logische beveiliging, die de ondernemingen dienen in te voeren in het kader van het prudentieel toezichtsstatuut dat op hen van toepassing is en/of in het kader van het toezicht (oversight) dat de Nationale Bank van België op hen uitoefent, gelijkgesteld met het B.P.E. | § 5bis. Voor de kritieke infrastructuren die onder de bevoegdheid van de sector financiën vallen, **met uitzondering van die welke worden uitgebaat door een exploitant van een handelsplatform,** worden de beveiligingsmaatregelen, zoals het continuïteitsbeleid, de continuïteitsplannen en de plannen voor fysieke en logische beveiliging, die de ondernemingen dienen in te voeren in het kader van het prudentieel toezichtsstatuut dat op hen van toepassing is en/of in het kader van het toezicht (oversight) dat de Nationale Bank van België op hen uitoefent, gelijkgesteld met het B.P.E. |
| § 6. De exploitant is verantwoordelijk voor het organiseren van oefeningen en voor het actualiseren van het B.P.E., in functie van de lessen getrokken uit de oefeningen of uit elke wijziging van de risicoanalyse. | § 6. De exploitant is verantwoordelijk voor het organiseren van oefeningen en voor het actualiseren van het B.P.E., in functie van de lessen getrokken uit de oefeningen of uit elke wijziging van de risicoanalyse. |
| Voor de sector financiën worden de oefeningen en de bijwerkingen van de beveiligingsmaatregelen als bedoeld in paragraaf 5bis gelijkgesteld met de | Voor de sector financiën **met uitzondering van de kritieke infrastructuren die worden uitgebaat door een exploitant van een handelsplatform,** worden de oefeningen en de bijwerkingen van de |

**COÖRDINATIE VAN DE ARTIKELEN**

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| oefeningen en de bijwerkingen van het B.P.E. als bedoeld in deze paragraaf. | beveiligingsmaatregelen als bedoeld in paragraaf 5bis gelijkgesteld met de oefeningen en de bijwerkingen van het B.P.E. als bedoeld in deze paragraaf. |
| De Koning bepaalt, voor een bepaalde sector of een deelsector, de frequentie van de oefeningen en van de bijwerkingen van het B.P.E. | De Koning bepaalt, voor een bepaalde sector of een deelsector, de frequentie van de oefeningen en van de bijwerkingen van het B.P.E. |
| De Koning bepaalt voor een bepaalde sector of, in voorkomend geval, per deelsector de nadere regels van de deelneming van de politiediensten aan de oefeningen georganiseerd door de exploitant. | De Koning bepaalt voor een bepaalde sector of, in voorkomend geval, per deelsector de nadere regels van de deelneming van de politiediensten aan de oefeningen georganiseerd door de exploitant. |
| § 7. Voor een welbepaalde sector of, in voorkomend geval, per deelsector, kan de Koning aan de exploitanten de uitwerking van een intern noodplan opleggen, waarvan het doel, wat de kritieke infrastructuur betreft, erin bestaat de nefaste gevolgen van een noodsituatie te beperken door te voorzien in aangepaste materiële en organisatorische noodmaatregelen. | § 7. Voor een welbepaalde sector of, in voorkomend geval, per deelsector, kan de Koning aan de exploitanten de uitwerking van een intern noodplan opleggen, waarvan het doel, wat de kritieke infrastructuur betreft, erin bestaat de nefaste gevolgen van een noodsituatie te beperken door te voorzien in aangepaste materiële en organisatorische noodmaatregelen. |
| **Art. 14.** § 1. Onverminderd de wettelijke of reglementaire bepalingen die opleggen, in een bepaalde sector of een deelsector, bepaalde diensten te informeren, is de exploitant ertoe gehouden, wanneer zich een gebeurtenis voordoet die van aard is om de veiligheid van de kritieke infrastructuur te bedreigen, onmiddellijk het SICAD, via de noodnummers 101 of 112, de door de bevoegde sectorale overheid aangewezen dienst en de ADCC te verwittigen. | **Art. 14.** § 1. Onverminderd de wettelijke of reglementaire bepalingen die opleggen, in een bepaalde sector of een deelsector, bepaalde diensten te informeren, is de exploitant ertoe gehouden, wanneer zich een gebeurtenis voordoet die van aard is om de veiligheid van de kritieke infrastructuur te bedreigen, onmiddellijk het SICAD, via de noodnummers 101 of 112, de door de bevoegde sectorale overheid aangewezen dienst en de ADCC te verwittigen. |
| § 1/1. Wanneer de melding van de gebeurtenis, bedoeld in de eerste paragraaf, niet vanuit de infrastructuur zelf wordt gedaan, verstrekt de federale politie aan de beveiligingscontactpunten aangeduid krachtens artikel 12 de noodzakelijke informatie om rechtstreekse meldingen aan het territoriaal bevoegde SICAD te kunnen uitvoeren. | § 1/1. Wanneer de melding van de gebeurtenis, bedoeld in de eerste paragraaf, niet vanuit de infrastructuur zelf wordt gedaan, verstrekt de federale politie aan de beveiligingscontactpunten aangeduid krachtens artikel 12 de noodzakelijke informatie om rechtstreekse meldingen aan het territoriaal bevoegde SICAD te kunnen uitvoeren. |
| § 2. Overeenkomstig de nadere regels bepaald door de minister van Binnenlandse Zaken, verwittigt het SICAD de ADCC van elke gebeurtenis waarvan het kennis heeft en die van aard is de veiligheid van de kritieke infrastructuur te bedreigen. | § 2. Overeenkomstig de nadere regels bepaald door de minister van Binnenlandse Zaken, verwittigt het SICAD de ADCC van elke gebeurtenis waarvan het kennis heeft en die van aard is de veiligheid van de kritieke infrastructuur te bedreigen **en, in voorkomend geval, de autoriteit bedoeld in artikel 7, § 1, van de wet van xx 2018 wat de beveiliging van netwerk- en informatiesystemen betreft.** |

## COÖRDINATIE VAN DE ARTIKELEN

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| § 3. Indien de gebeurtenis van aard is om de verstoring van de werking of de vernietiging van de betrokken kritieke infrastructuur als gevolg te hebben, verwittigt het EPCIP-contactpunt de bevoegde sectorale overheid en, in geval van een Europese kritieke infrastructuur, de bevoegde overheid van de betrokken lidstaten. | § 3. Indien de gebeurtenis van aard is om de verstoring van de werking of de vernietiging van de betrokken kritieke infrastructuur als gevolg te hebben, verwittigt het EPCIP-contactpunt de bevoegde sectorale overheid en, in geval van een Europese kritieke infrastructuur, de bevoegde overheid van de betrokken lidstaten. |
| **Art. 18.** De ADCC, de politiediensten en het OCAD wisselen de nuttige informatie voor het nemen van externe beschermingsmaatregelen voor de kritieke infrastructuren uit. | **Art. 18. De ADCC, de politiediensten, het OCAD, en, in voorkomend geval, de autoriteit bedoeld in artikel 7, § 1, van de wet van xx 2018, wat de beveiliging van netwerk- en informatiesystemen betreft**, de nuttige informatie voor het nemen van externe beschermingsmaatregelen voor de kritieke infrastructuren wisselen uit. |
| **Art. 19.** De exploitant, het beveiligingscontactpunt, de sectorale overheid, de ADCC, het OCAD en de politiediensten werken te allen tijde samen, door een adequate informatie-uitwisseling betreffende de beveiliging en de bescherming van de kritieke infrastructuur, teneinde te waken over een overeenstemming tussen de interne beveiligingsmaatregelen en de externe beschermingsmaatregelen. | **Art. 19. 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 xx 2018, wat de beveiliging van netwerk- en informatiesystemen betreft,** werken te allen tijde samen, door een adequate informatie-uitwisseling betreffende de beveiliging en de bescherming van de kritieke infrastructuur, teneinde te waken over een overeenstemming tussen de interne beveiligingsmaatregelen en de externe beschermingsmaatregelen. |
| **Art. 22.** De sectorale overheid, de ADCC, het OCAD en de politiediensten beperken de toegang tot de informatie bedoeld, in hoofdstuk 2 tot de personen die er de kennis van nodig hebben en er toegang toe moeten hebben voor de uitoefening van hun functies of hun opdracht die de veiligheid en/of de bescherming van de kritieke infrastructuren tot doel hebben. | **Art. 22. De sectorale overheid, de ADCC, het OCAD, de politiediensten en de autoriteit bedoeld in artikel 7, § 1, van de wet van xx 2018,** beperken de toegang tot de informatie bedoeld, in hoofdstuk 2 tot de personen die er de kennis van nodig hebben en er toegang toe moeten hebben voor de uitoefening van hun functies of hun opdracht die de veiligheid en/of de bescherming van de kritieke infrastructuren tot doel hebben. |
| **Art. 22bis**. Voor de sector financiën maakt de Nationale Bank van België aan de Minister van Financiën een verslag over met betrekking tot de taken die zij krachtens deze wet vervult, volgens een passende frequentie van ten hoogste drie jaar. De Nationale Bank van België brengt de Minister echter onmiddellijk op de hoogte van elke concrete en nakende dreiging voor een kritieke infrastructuur van de sector financiën. | **Art. 22bis**. Voor de sector financiën **met uitzondering van de deelsector van de exploitanten van een handelsplatform,** maakt de Nationale Bank van België aan de Minister van Financiën een verslag over met betrekking tot de taken die zij krachtens deze wet vervult, volgens een passende frequentie van ten hoogste drie jaar. De Nationale Bank van België brengt de Minister echter onmiddellijk op de hoogte van elke concrete en nakende dreiging voor een kritieke infrastructuur van de sector financiën. |

## COÖRDINATIE VAN DE ARTIKELEN

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| | **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 sector valt.** |
| **Art. 24.** § 1. Onverminderd de bevoegdheden van de officieren van gerechtelijke politie, wordt per sector, of in voorkomend geval per deelsector, een inspectiedienst ingesteld, belast met de controle op de naleving door de exploitanten van die sector of deelsector van de bepalingen van deze wet en van haar uitvoeringsbesluiten. | **Art. 24.** § 1. Onverminderd de bevoegdheden van de officieren van gerechtelijke politie, wordt per sector, of in voorkomend geval per deelsector, een inspectiedienst ingesteld, belast met de controle op de naleving door de exploitanten van die sector of deelsector van de bepalingen van deze wet en van haar uitvoeringsbesluiten. |
| § 2. De Koning wijst, voor een bepaalde sector, of in voorkomend geval, per deelsector, de bevoegde inspectiedienst aan om de controle uit te voeren. | § 2. De Koning wijst, voor een bepaalde sector, of in voorkomend geval, per deelsector, de bevoegde inspectiedienst aan om de controle uit te voeren. |
| Hij kan de nadere regels van de controle vastleggen. | Hij kan de nadere regels van de controle vastleggen. |
| Voor de sector financiën wordt de Nationale Bank van België aangeduid als inspectiedienst belast met het controleren van de toepassing van de bepalingen van deze wet en haar uitvoeringsbesluiten. Daartoe mag de Nationale Bank van België gebruik maken van de informatie waarover zij beschikt in het kader van haar wettelijke opdrachten met betrekking tot het prudentieel toezicht en het toezicht (oversight) en houdt zij, in het bijzonder, rekening met de vaststellingen die in dit kader zijn gedaan. Evenzo mag de Nationale Bank van België in het kader van haar wettelijke opdrachten met betrekking tot het prudentieel toezicht en het toezicht (oversight) de informatie gebruiken waarover zij met toepassing van deze wet beschikt. | Voor de sector financiën **met uitzondering van de deelsector van de exploitanten van een handelsplatform,** wordt de Nationale Bank van België aangeduid als inspectiedienst belast met het controleren van de toepassing van de bepalingen van deze wet en haar uitvoeringsbesluiten. Daartoe mag de Nationale Bank van België gebruik maken van de informatie waarover zij beschikt in het kader van haar wettelijke opdrachten met betrekking tot het prudentieel toezicht en het toezicht (oversight) en houdt zij, in het bijzonder, rekening met de vaststellingen die in dit kader zijn gedaan. Evenzo mag de Nationale Bank van België in het kader van haar wettelijke opdrachten met betrekking tot het prudentieel toezicht en het toezicht (oversight) de informatie gebruiken waarover zij met toepassing van deze wet beschikt. **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** |

**COÖRDINATIE VAN DE ARTIKELEN**

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| | **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.** |
| § 3. De leden van de inspectiedienst die belast zijn met de controleopdrachten bedoeld in paragraaf 1,zijn voorzien van een legitimatiekaart waarvan het model wordt vastgesteld door de Koning, per sector. | § 3. De leden van de inspectiedienst die belast zijn met de controleopdrachten bedoeld in paragraaf 1,zijn voorzien van een legitimatiekaart waarvan het model wordt vastgesteld door de Koning, per sector. |
| Deze paragraaf is niet van toepassing op de inspectiedienst die is aangeduid krachtens paragraaf 2, derde lid. | Deze paragraaf is niet van toepassing op de inspectiedienst die is aangeduid krachtens paragraaf 2, derde lid. |
| § 4. De Koning kan de voorwaarden van vorming bepalen waaraan de leden van de inspectiedienst moeten voldoen voor een bepaalde sector of deelsector. | § 4. De Koning kan de voorwaarden van vorming bepalen waaraan de leden van de inspectiedienst moeten voldoen voor een bepaalde sector of deelsector. |
| **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** | **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** |
| **Artikel 1.** Voor de toepassing van deze wet en haar uitvoeringsmaatregelen wordt verstaan onder : | **Artikel 1.** Voor de toepassing van deze wet en haar uitvoeringsmaatregelen wordt verstaan onder : |
| - ioniserende stralingen : stralingen samengesteld uit fotonen of deeltjes welke in staat zijn direct of indirect de vorming van ionen te veroorzaken; | - ioniserende stralingen : stralingen samengesteld uit fotonen of deeltjes welke in staat zijn direct of indirect de vorming van ionen te veroorzaken; |
| - radioactieve stof : elke stof of elk materiaal die/dat één of meer radionucliden bevat waarvan de activiteit of de concentratie om redenen van stralingsbescherming niet mag worden verwaarloosd; | - radioactieve stof : elke stof of elk materiaal die/dat één of meer radionucliden bevat waarvan de activiteit of de concentratie om redenen van stralingsbescherming niet mag worden verwaarloosd; |
| - bevoegde overheid : de overheid aangewezen krachtens deze wet en krachtens haar uitvoeringsbesluiten; | - bevoegde overheid : de overheid aangewezen krachtens deze wet en krachtens haar uitvoeringsbesluiten; |
| - algemeen reglement : het koninklijk besluit van 20 juli 2001 houdende algemeen reglement op de bescherming van de bevolking, van de werknemers en het leefmilieu tegen het gevaar van de ioniserende stralingen; | - algemeen reglement : het koninklijk besluit van 20 juli 2001 houdende algemeen reglement op de bescherming van de bevolking, van de werknemers en het leefmilieu tegen het gevaar van de ioniserende stralingen; |

## COÖRDINATIE VAN DE ARTIKELEN

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| - erkende instellingen : de instellingen die door het algemeen reglement met bepaalde taken worden belast; | - erkende instellingen : de instellingen die door het algemeen reglement met bepaalde taken worden belast; |
| - dienst voor fysische controle : de dienst die krachtens het algemeen reglement door de bedrijfsleider moet worden opgericht en die belast is met de organisatie van en het toezicht op de maatregelen die nodig zijn om de bepalingen van dat reglement te doen naleven; | - dienst voor fysische controle : de dienst die krachtens het algemeen reglement door de bedrijfsleider moet worden opgericht en die belast is met de organisatie van en het toezicht op de maatregelen die nodig zijn om de bepalingen van dat reglement te doen naleven; |
| - het Agentschap : de openbare instelling opgericht door deze wet voor de nucleaire controle; | - het Agentschap : de openbare instelling opgericht door deze wet voor de nucleaire controle; |
| - kernmateriaal : de volgende bijzondere splijtbare producten en kerngrondstoffen : | - kernmateriaal : de volgende bijzondere splijtbare producten en kerngrondstoffen : |
| a) de bijzondere splijtbare producten zijn plutonium 239, uranium 233, uranium verrijkt in uranium 235 of 233 : elk product dat één of meerdere van de hierboven vermelde isotopen bevat. | a) de bijzondere splijtbare producten zijn plutonium 239, uranium 233, uranium verrijkt in uranium 235 of 233 : elk product dat één of meerdere van de hierboven vermelde isotopen bevat. |
| Uranium verrijkt in uranium 235 of 233 is uranium dat hetzij uranium 235 bevat hetzij uranium 233, dan wel deze beide isotopen in een zodanige hoeveelheid dat de verhouding tussen de som van beide isotopen en de isotoop 238 groter is dan de verhouding tussen de isotoop 235 en de isotoop 238 in natuurlijk uranium; | Uranium verrijkt in uranium 235 of 233 is uranium dat hetzij uranium 235 bevat hetzij uranium 233, dan wel deze beide isotopen in een zodanige hoeveelheid dat de verhouding tussen de som van beide isotopen en de isotoop 238 groter is dan de verhouding tussen de isotoop 235 en de isotoop 238 in natuurlijk uranium; |
| b) de kerngrondstoffen zijn het uranium dat een mengeling aan isotopen bevat die in de natuur voorkomen en uranium verarmd in uranium 235; thorium; de voornoemde materialen onder de vorm van metaal, legering, de chemische verbindingen of concentraten; | b) de kerngrondstoffen zijn het uranium dat een mengeling aan isotopen bevat die in de natuur voorkomen en uranium verarmd in uranium 235; thorium; de voornoemde materialen onder de vorm van metaal, legering, de chemische verbindingen of concentraten; |
| - nationaal nucleair vervoer : het vervoer, met om het even welk vervoermiddel, van kernmateriaal dat geconditioneerd is met het oog op een zending, wanneer dit uitsluitend binnen Belgisch grondgebied plaatsvindt; | - nationaal nucleair vervoer : het vervoer, met om het even welk vervoermiddel, van kernmateriaal dat geconditioneerd is met het oog op een zending, wanneer dit uitsluitend binnen Belgisch grondgebied plaatsvindt; |
| - internationaal nucleair vervoer : het vervoer, met om het even welk vervoermiddel, van kernmateriaal, dat geconditioneerd is met het oog op een zending, dat de grenzen van het grondgebied moet overschrijden, te rekenen vanaf het vertrek uit de installatie van de expediteur in de Staat van | - internationaal nucleair vervoer : het vervoer, met om het even welk vervoermiddel, van kernmateriaal, dat geconditioneerd is met het oog op een zending, dat de grenzen van het grondgebied moet overschrijden, te rekenen vanaf het vertrek uit de installatie van de expediteur in de Staat van |

**COÖRDINATIE VAN DE ARTIKELEN**

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| oorsprong tot de aankomst in een installatie van de geadresseerde op het grondgebied van de Staat van eindbestemming; | oorsprong tot de aankomst in een installatie van de geadresseerde op het grondgebied van de Staat van eindbestemming; |
| - fysieke beveiligingsmaatregelen : alle administratieve, organisatorische en technische maatregelen met als doel het beschermen van kernmateriaal tijdens de productie, het gebruik, de opslag of het vervoer tegen de risico's van ongeoorloofd bezit en diefstal en het beschermen van kernmateriaal tijdens de productie, het gebruik, de opslag alsook de nucleaire installaties, het nationaal en internationaal nucleair vervoer tegen de risico's van sabotage. De genoemde maatregelen hebben eveneens tot doel de nucleaire documenten te beschermen tegen voornoemde handelingen; | - fysieke beveiligingsmaatregelen : alle administratieve, organisatorische en technische maatregelen met als doel het beschermen van kernmateriaal tijdens de productie, het gebruik, de opslag of het vervoer tegen de risico's van ongeoorloofd bezit en diefstal en het beschermen van kernmateriaal tijdens de productie, het gebruik, de opslag alsook de nucleaire installaties, het nationaal en internationaal nucleair vervoer tegen de risico's van sabotage. De genoemde maatregelen hebben eveneens tot doel de nucleaire documenten te beschermen tegen voornoemde handelingen; |
| - beveiligingsmaatregelen voor radioactieve stoffen: alle administratieve, organisatorische en technische maatregelen, met als doel: | - beveiligingsmaatregelen voor radioactieve stoffen: alle administratieve, organisatorische en technische maatregelen, met als doel: |
| a) om de radioactieve stoffen, met uitzondering van het kernmateriaal, tijdens de productie, het gebruik, de opslag of het vervoer tegen de risico's van ongeoorloofd bezit en diefstal te beschermen; | a) om de radioactieve stoffen, met uitzondering van het kernmateriaal, tijdens de productie, het gebruik, de opslag of het vervoer tegen de risico's van ongeoorloofd bezit en diefstal te beschermen; |
| b) om wat volgt tegen de risico's van sabotage of elk kwaadwillig gebruik te beschermen: | b) om wat volgt tegen de risico's van sabotage of elk kwaadwillig gebruik te beschermen: |
| 1) de radioactieve stoffen, met uitzondering van het kernmateriaal, tijdens de productie, het gebruik of de opslag ervan; | 1) de radioactieve stoffen, met uitzondering van het kernmateriaal, tijdens de productie, het gebruik of de opslag ervan; |
| 2) de inrichtingen waar deze stoffen worden geproduceerd, vervaardigd, gehouden of gebruikt, alsook hun vervoer; | 2) de inrichtingen waar deze stoffen worden geproduceerd, vervaardigd, gehouden of gebruikt, alsook hun vervoer; |
| - beveiligingsmaatregelen voor toestellen of installaties die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is: alle administratieve, organisatorische en technische maatregelen met als doel: | - beveiligingsmaatregelen voor toestellen of installaties die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is: alle administratieve, organisatorische en technische maatregelen met als doel: |
| a) om voormelde toestellen of installaties tegen de risico's van ongeoorloofd bezit en diefstal te beschermen; | a) om voormelde toestellen of installaties tegen de risico's van ongeoorloofd bezit en diefstal te beschermen; |
| b) om wat volgt tegen de risico's van sabotage of elk kwaadwillig gebruik te beschermen: | b) om wat volgt tegen de risico's van sabotage of elk kwaadwillig gebruik te beschermen: |

## COÖRDINATIE VAN DE ARTIKELEN

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| 1) voornoemde toestellen of installaties, alsook het vervoer van deze toestellen of installaties; | 1) voornoemde toestellen of installaties, alsook het vervoer van deze toestellen of installaties; |
| 2) de inrichtingen waar deze toestellen of installaties zich bevinden. | 2) de inrichtingen waar deze toestellen of installaties zich bevinden. |
| - sabotage : alle opzettelijke handelingen: | - sabotage : alle opzettelijke handelingen: |
| a) die zijn gericht tegen: | a) die zijn gericht tegen: |
| 1) kernmateriaal tijdens de productie, het gebruik, de opslag of het vervoer ervan; | 1) kernmateriaal tijdens de productie, het gebruik, de opslag of het vervoer ervan; |
| 2) nucleaire installaties; | 2) nucleaire installaties; |
| 3) het nationaal of internationaal nucleair vervoer; | 3) het nationaal of internationaal nucleair vervoer; |
| 4) radioactieve stoffen, met uitzondering van het kernmateriaal, tijdens de productie, het gebruik, de opslag of het vervoer ervan; | 4) radioactieve stoffen, met uitzondering van het kernmateriaal, tijdens de productie, het gebruik, de opslag of het vervoer ervan; |
| 5) inrichtingen of delen van inrichtingen waar radioactieve stoffen worden geproduceerd, vervaardigd, gehouden of gebruikt; | 5) inrichtingen of delen van inrichtingen waar radioactieve stoffen worden geproduceerd, vervaardigd, gehouden of gebruikt; |
| 6) toestellen of installaties die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is; | 6) toestellen of installaties die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is; |
| 7) het vervoer van toestellen of installaties die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is; | 7) het vervoer van toestellen of installaties die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is; |
| 8) inrichtingen, delen van inrichtingen en plaatsen waar zich toestellen of installaties bevinden die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is; | 8) inrichtingen, delen van inrichtingen en plaatsen waar zich toestellen of installaties bevinden die ioniserende straling uitzenden die niet van radioactieve stoffen afkomstig is; |
| En | en |
| b) die op rechtstreekse of onrechtstreekse wijze de gezondheid en veiligheid van het personeel, de bevolking en het milieu in gevaar kunnen brengen door een blootstelling aan straling, of de uitstoot van radioactieve stoffen; | b) die op rechtstreekse of onrechtstreekse wijze de gezondheid en veiligheid van het personeel, de bevolking en het milieu in gevaar kunnen brengen door een blootstelling aan straling, of de uitstoot van radioactieve stoffen; |
| - vermogensreactor een kernreactor, ontworpen voor de productie van elektriciteit, die vergund is of werd als inrichting van klasse I met toepassing van de regelgeving inzake de bescherming tegen | - vermogensreactor een kernreactor, ontworpen voor de productie van elektriciteit, die vergund is of werd als inrichting van klasse I met toepassing van de regelgeving inzake de bescherming tegen |

**COÖRDINATIE VAN DE ARTIKELEN**

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| ioniserende stralingen en waarvoor nog geen ontmantelingsvergunning werd afgeleverd. | ioniserende stralingen en waarvoor nog geen ontmantelingsvergunning werd afgeleverd. |
| - beroepshalve blootgestelde persoon : iedere natuurlijke persoon die ingevolge zijn beroepsactiviteiten, een blootstelling aan ioniserende stralingen ondergaat die kan leiden tot de overschrijding van één van de dosislimieten vastgesteld voor de personen van het publiek; | - beroepshalve blootgestelde persoon : iedere natuurlijke persoon die ingevolge zijn beroepsactiviteiten, een blootstelling aan ioniserende stralingen ondergaat die kan leiden tot de overschrijding van één van de dosislimieten vastgesteld voor de personen van het publiek; |
| - aan dosimetrisch toezicht onderworpen persoon : iedere natuurlijke persoon die activiteiten van ongeacht welke aard uitvoert waarbij hij/zij een blootstelling aan ioniserende stralingen ondergaat die kan leiden tot de overschrijding van één van de dosislimieten vastgesteld voor de personen van het publiek; | - aan dosimetrisch toezicht onderworpen persoon : iedere natuurlijke persoon die activiteiten van ongeacht welke aard uitvoert waarbij hij/zij een blootstelling aan ioniserende stralingen ondergaat die kan leiden tot de overschrijding van één van de dosislimieten vastgesteld voor de personen van het publiek; |
| - exploitant : elke natuurlijke of rechtspersoon die verantwoordelijk is voor de inrichting onderhevig aan de vergunnings- of aangifteplicht overeenkomstig de bepalingen die voortvloeien uit artikel 17; | - exploitant : elke natuurlijke of rechtspersoon die verantwoordelijk is voor de inrichting onderhevig aan de vergunnings- of aangifteplicht overeenkomstig de bepalingen die voortvloeien uit artikel 17; |
| - externe onderneming : elke natuurlijke of rechtspersoon, die activiteiten van om het even welke aard verricht in een inrichting onderhevig aan de vergunnings- of aangifteplicht overeenkomstig de bepalingen die voortvloeien uit artikel 17, waarbij één van de dosislimieten vastgesteld voor de personen van het publiek zou kunnen overschreden worden, met uitzondering van de exploitant van die inrichting, en zijn personeelsleden; | - externe onderneming : elke natuurlijke of rechtspersoon, die activiteiten van om het even welke aard verricht in een inrichting onderhevig aan de vergunnings- of aangifteplicht overeenkomstig de bepalingen die voortvloeien uit artikel 17, waarbij één van de dosislimieten vastgesteld voor de personen van het publiek zou kunnen overschreden worden, met uitzondering van de exploitant van die inrichting, en zijn personeelsleden; |
| - erkende geneesheer : de preventieadviseur-arbeidsgeneesheer werkzaam in een interne of externe dienst voor preventie en bescherming op het werk, deskundig op gebied van arbeidsgeneeskunde overeenkomstig de bepalingen van de wet van 4 augustus 1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk, en de uitvoeringsbesluiten ervan en die bovendien erkend is overeenkomstig de uitvoeringsmaatregelen genomen op grond van de artikelen 3 en 19; | - erkende geneesheer : de preventieadviseur-arbeidsgeneesheer werkzaam in een interne of externe dienst voor preventie en bescherming op het werk, deskundig op gebied van arbeidsgeneeskunde overeenkomstig de bepalingen van de wet van 4 augustus 1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk, en de uitvoeringsbesluiten ervan en die bovendien erkend is overeenkomstig de uitvoeringsmaatregelen genomen op grond van de artikelen 3 en 19; |
| - externe werker : iedere aan dosimetrisch toezicht onderworpen persoon, die een opdracht met blootstellingsrisico uitvoert bij een exploitant, ongeacht of hij dit doet als tijdelijk of vast werknemer van een externe onderneming, of als zelfstandige; | - externe werker : iedere aan dosimetrisch toezicht onderworpen persoon, die een opdracht met blootstellingsrisico uitvoert bij een exploitant, ongeacht of hij dit doet als tijdelijk of vast werknemer van een externe onderneming, of als zelfstandige; |

## COÖRDINATIE VAN DE ARTIKELEN

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| - opdracht met blootstellingsrisico : de activiteit van ongeacht welke aard, van een externe werker bij een exploitant, waarbij één van de dosislimieten vastgesteld voor de personen van het publiek zou kunnen overschreden worden; | - opdracht met blootstellingsrisico : de activiteit van ongeacht welke aard, van een externe werker bij een exploitant, waarbij één van de dosislimieten vastgesteld voor de personen van het publiek zou kunnen overschreden worden; |
| - blootstellingsregister : het gecentraliseerd registratiesysteem bedoeld in artikel 25/2, dat de dosimetriegegevens van aan dosimetrisch toezicht onderworpen personen bevat; | - blootstellingsregister : het gecentraliseerd registratiesysteem bedoeld in artikel 25/2, dat de dosimetriegegevens van aan dosimetrisch toezicht onderworpen personen bevat; |
| - stralingspaspoort : het individueel document opgesteld voor externe werkers, dat toelaat om hun dosimetrisch toezicht te verzekeren tijdens de opdrachten met blootstellingsrisico uitgevoerd in het buitenland; | - stralingspaspoort : het individueel document opgesteld voor externe werkers, dat toelaat om hun dosimetrisch toezicht te verzekeren tijdens de opdrachten met blootstellingsrisico uitgevoerd in het buitenland; |
| - beroepsbeoefenaar in de gezondheidszorg : de beroepsbeoefenaar in de gezondheidszorg bedoeld in artikel 7, § 4, van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, zoals aangesteld binnen het Agentschap. Zolang geen uitvoering wordt gegeven aan de voormelde bepaling van de wet van 8 december 1992, wordt begrepen onder 'beroepsbeoefenaar in de gezondheidszorg' : de persoon die houder is van het wettelijk diploma van doctor in de genees-, heel- en verloskunde; | - beroepsbeoefenaar in de gezondheidszorg : de beroepsbeoefenaar in de gezondheidszorg bedoeld in artikel 7, § 4, van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, zoals aangesteld binnen het Agentschap. Zolang geen uitvoering wordt gegeven aan de voormelde bepaling van de wet van 8 december 1992, wordt begrepen onder 'beroepsbeoefenaar in de gezondheidszorg' : de persoon die houder is van het wettelijk diploma van doctor in de genees-, heel- en verloskunde; |
| - consulent inzake informatieveiligheid en bescherming van de persoonlijke levenssfeer : de consulent bedoeld in artikel 4, § 5, van de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid, zoals aangewezen binnen het Agentschap; | - consulent inzake informatieveiligheid en bescherming van de persoonlijke levenssfeer : de consulent bedoeld in artikel 4, § 5, van de wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid, zoals aangewezen binnen het Agentschap; |
| - verantwoordelijke voor de verwerking : de persoon bedoeld in artikel 1, § 4, van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, in casu het Agentschap; | - verantwoordelijke voor de verwerking : de persoon bedoeld in artikel 1, § 4, van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, in casu het Agentschap; |
| - vestigingseenheid : een plaats die men geografisch gezien kan identificeren door een adres, waar ten minste een activiteit van de onderneming wordt uitgeoefend of waaruit de activiteit wordt uitgeoefend; | - vestigingseenheid : een plaats die men geografisch gezien kan identificeren door een adres, waar ten minste een activiteit van de onderneming wordt uitgeoefend of waaruit de activiteit wordt uitgeoefend; |

## COÖRDINATIE VAN DE ARTIKELEN

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| - werknemer : de werknemer bedoeld in artikel 2, § 1, eerste en tweede lid, 1°, van de wet van 4 augustus 1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk; | - werknemer : de werknemer bedoeld in artikel 2, § 1, eerste en tweede lid, 1°, van de wet van 4 augustus 1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk; |
| - werkgever : de werkgever bedoeld in artikel 2, § 1, eerste en tweede lid, 2°, van de wet van 4 augustus 1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk; | - werkgever : de werkgever bedoeld in artikel 2, § 1, eerste en tweede lid, 2°, van de wet van 4 augustus 1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk; |
| - dosimetrisch toezicht : het dosimetrisch toezicht zoals bedoeld in artikel 30.6 van het Algemeen reglement; | - dosimetrisch toezicht : het dosimetrisch toezicht zoals bedoeld in artikel 30.6 van het Algemeen reglement; |
| - authentieke bronnen : het Rijksregister opgericht bij de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, de Kruispuntbank der ondernemingen opgericht bij wet van 16 januari 2003 tot oprichting van een Kruispuntbank van Ondernemingen, tot modernisering van het handelsregister, tot oprichting van erkende ondernemingsloketten en houdende diverse bepalingen, en de Registers van de Kruispuntbank van de Sociale Zekerheid (Bis-register en Register van de geschrapten) opgericht bij wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid; | - authentieke bronnen : het Rijksregister opgericht bij de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, de Kruispuntbank der ondernemingen opgericht bij wet van 16 januari 2003 tot oprichting van een Kruispuntbank van Ondernemingen, tot modernisering van het handelsregister, tot oprichting van erkende ondernemingsloketten en houdende diverse bepalingen, en de Registers van de Kruispuntbank van de Sociale Zekerheid (Bis-register en Register van de geschrapten) opgericht bij wet van 15 januari 1990 houdende oprichting en organisatie van een Kruispuntbank van de sociale zekerheid; |
| - anonieme gegevens : de gegevens die niet met een geïdentificeerd of identificeerbaar persoon in verband kunnen worden gebracht en derhalve geen persoonsgegevens zijn; | - anonieme gegevens : de gegevens die niet met een geïdentificeerd of identificeerbaar persoon in verband kunnen worden gebracht en derhalve geen persoonsgegevens zijn; |
| **- "de wet van xx xx 2018": de wet van xx xx 2018 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;".** | **- "de wet van xx xx 2018": de wet van xx xx 2018 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;".** |
| **(…)** | **Art. 15ter. Het Agentschap wordt aangewezen als inspectiedienst, in de zin van artikel 42 van de wet van xx 2018, 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.** |

## COÖRDINATIE VAN DE ARTIKELEN

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| **De Koning bepaalt de praktische inspectiemodaliteiten, na advies van het Agentschap.** | **De Koning bepaalt de praktische inspectiemodaliteiten, na advies van het Agentschap.** |
| **Wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector** | **Wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector** |
| **Art. 1/1.** Hoofdstukken III en V voorzien in een gedeeltelijke omzetting van Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische-communicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming en van Richtlijn 2009/140/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/21/EG inzake een gemeenschappelijk regelgevingskader voor elektronische-communicatienetwerken en -diensten, Richtlijn 2002/19/EG inzake de toegang tot en interconnectie van elektronische-communicatienetwerken en bijbehorende faciliteiten, en Richtlijn 2002/20/EG betreffende de machtiging voor elektronische-communicatienetwerken en -diensten. | **Art. 1/1.** Hoofdstukken III en V voorzien in een gedeeltelijke omzetting van Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische-communicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming en van Richtlijn 2009/140/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/21/EG inzake een gemeenschappelijk regelgevingskader voor elektronische-communicatienetwerken en -diensten, Richtlijn 2002/19/EG inzake de toegang tot en interconnectie van elektronische-communicatienetwerken en bijbehorende faciliteiten, en Richtlijn 2002/20/EG betreffende de machtiging voor elektronische-communicatienetwerken en -diensten.<br><br>**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. 14.** § 1. Onverminderd zijn wettelijke bevoegdheden, heeft het Instituut de volgende taken met betrekking tot elektronische communicatienetwerken en elektronische communicatiediensten, eindapparatuur, radioapparatuur en met betrekking tot postdiensten en openbare postnetwerken zoals gedefinieerd door | **Art. 14.** § 1. Onverminderd zijn wettelijke bevoegdheden, heeft het Instituut de volgende taken met betrekking tot elektronische communicatienetwerken en elektronische communicatiediensten, eindapparatuur, radioapparatuur, **met betrekking tot de sector digitale infrastructuren in de zin van de wet van xx 2018 tot vaststelling van een kader voor de** |

**COÖRDINATIE VAN DE ARTIKELEN**

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| artikel 2 van de wet van 26 januari 2018 betreffende de postdiensten: | **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,** met betrekking tot postdiensten en openbare postnetwerken zoals gedefinieerd door artikel 2 van de wet van 26 januari 2018 betreffende de postdiensten: |
| 1° het formuleren van adviezen op eigen initiatief, in de gevallen waarin de wetten en besluiten erin voorzien of op verzoek van de minister of van de Kamer van volksvertegenwoordigers; | 1° het formuleren van adviezen op eigen initiatief, in de gevallen waarin de wetten en besluiten erin voorzien of op verzoek van de minister of van de Kamer van volksvertegenwoordigers; |
| 2° het nemen van administratieve beslissingen; | 2° het nemen van administratieve beslissingen; |
| 3° het toezicht op de naleving van de wet van 13 juni 2005 betreffende de elektronische communicatie, van Titel I, hoofdstuk X, en Titel III van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, van de wet van 26 januari 2018 betreffende de postdiensten, van 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 Belgische post- en telecommunicatiesector, van 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, van de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad en hun uitvoeringsbesluiten, en van Verordening (EU) nr. 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; | **3° het toezicht op de naleving van de volgende normen en van hun uitvoeringsbesluiten :**<br><br>**a) de wet van 13 juni 2005 betreffende de elektronische communicatie;**<br><br>**b) Titel I, hoofdstuk X, en Titel III van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven;**<br><br>**c) de wet van 26 januari 2018 betreffende de postdiensten;**<br><br>**d) 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 Belgische post- en telecommunicatiesector;**<br><br>**e) 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;**<br><br>**f) de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad;**<br><br>**g) de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren,** |

**COÖRDINATIE VAN DE ARTIKELEN**

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| | **wat de sectoren elektronische communicatie en digitale infrastructuren betreft;** |
| | **h) de wet van xx 2018 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 xx 2018 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.** |
| 4° in geval van een geschil tussen aanbieders van telecommunicatienetwerken, -diensten of -apparatuur, of in geval van een geschil tussen aanbieders van postdiensten, of in geval van een geschil tussen de in de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad bedoelde aanbieders van audiovisuele mediadiensten, het formuleren van voorstellen om de partijen te verzoenen binnen de termijn van één maand. De Koning legt de nadere regels van die procedure vast op advies van het Instituut; | 4° in geval van een geschil tussen aanbieders van telecommunicatienetwerken, -diensten of -apparatuur, of in geval van een geschil tussen aanbieders van postdiensten, of in geval van een geschil tussen de in de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad bedoelde aanbieders van audiovisuele mediadiensten, het formuleren van voorstellen om de partijen te verzoenen binnen de termijn van één maand. De Koning legt de nadere regels van die procedure vast op advies van het Instituut; |
| 4°/1 in geval van geschil tussen aanbieders van telecommunicatienetwerken, -diensten of -apparatuur, of in geval van een geschil tussen aanbieders van postdiensten, of in geval van een geschil tussen de in de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad bedoelde aanbieders van audiovisuele mediadiensten, het nemen van een administratieve beslissing op basis van artikel 4 of 4/1 van de wet van 17 januari 2003 | 4°/1 in geval van geschil tussen aanbieders van telecommunicatienetwerken, -diensten of -apparatuur, of in geval van een geschil tussen aanbieders van postdiensten, of in geval van een geschil tussen de in de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad bedoelde aanbieders van audiovisuele mediadiensten, het nemen van een administratieve beslissing op basis van artikel 4 of 4/1 van de wet van 17 januari 2003 |

## COÖRDINATIE VAN DE ARTIKELEN

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| 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; | 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; |
| 5° het stellen van alle nuttige daden die als doel hebben de voorbereiding van de toepassing van inwerking getreden Europese richtlijnen in de sectoren post en telecommunicatie. | 5° het stellen van alle nuttige daden die als doel hebben de voorbereiding van de toepassing van inwerking getreden Europese richtlijnen in de sectoren post en telecommunicatie. |
| 6° Het Instituut houdt toezicht op de uitvoering van de opdrachten van openbare dienst die door de Staat uitbesteed worden in de postsector en in de sector van de elektronische communicatie, onder voorbehoud van de opdrachten van openbare dienst toegekend in het kader van artikel 141, § 1bis, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven. Het Instituut informeert zowel de Minister bevoegd voor de Postsector als de minister bevoegd voor Overheidsbedrijven over de uitvoering van het beheerscontract. | 6° Het Instituut houdt toezicht op de uitvoering van de opdrachten van openbare dienst die door de Staat uitbesteed worden in de postsector en in de sector van de elektronische communicatie, onder voorbehoud van de opdrachten van openbare dienst toegekend in het kader van artikel 141, § 1bis, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven. Het Instituut informeert zowel de Minister bevoegd voor de Postsector als de minister bevoegd voor Overheidsbedrijven over de uitvoering van het beheerscontract. |
| § 2. In het kader van zijn bevoegdheden : | § 2. In het kader van zijn bevoegdheden : |
| 1° kan het Instituut op een niet discriminerende wijze alle onderzoeken en openbare raadplegingen organiseren; het moet dergelijke openbare raadplegingen organiseren zodat het rekening houdt met de standpunten van de eindgebruikers, consumenten met inbegrip van met name consumenten met een handicap, fabrikanten en ondernemingen die elektronische-communicatienetwerken en/of -diensten aanbieden over aangelegenheden die verband houden met alle eindgebruikers- en consumentenrechten met betrekking tot openbare elektronische-communicatiediensten, met name wanneer zij een belangrijke invloed hebben op de markt; deze raadplegingen waarborgen dat bij de besluitvorming van het Instituut inzake vraagstukken die verband houden met de rechten van eindgebruikers en consumenten wat openbare elektronische-communicatiediensten betreft het op passende wijze rekening houdt met de belangen van de consumenten op het gebied van elektronische communicatie; | 1° kan het Instituut op een niet discriminerende wijze alle onderzoeken en openbare raadplegingen organiseren; het moet dergelijke openbare raadplegingen organiseren zodat het rekening houdt met de standpunten van de eindgebruikers, consumenten met inbegrip van met name consumenten met een handicap, fabrikanten en ondernemingen die elektronische-communicatienetwerken en/of -diensten aanbieden over aangelegenheden die verband houden met alle eindgebruikers- en consumentenrechten met betrekking tot openbare elektronische-communicatiediensten, met name wanneer zij een belangrijke invloed hebben op de markt; deze raadplegingen waarborgen dat bij de besluitvorming van het Instituut inzake vraagstukken die verband houden met de rechten van eindgebruikers en consumenten wat openbare elektronische-communicatiediensten betreft het op passende wijze rekening houdt met de belangen van de consumenten op het gebied van elektronische communicatie; |

## COÖRDINATIE VAN DE ARTIKELEN

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| 2° kan het Instituut van elke betrokken persoon op gemotiveerde wijze alle nuttige informatie opvragen. Het Instituut bepaalt de termijn waarbinnen de inlichtingen moeten worden meegedeeld; | 2° kan het Instituut van elke betrokken persoon op gemotiveerde wijze alle nuttige informatie opvragen. Het Instituut bepaalt de termijn waarbinnen de inlichtingen moeten worden meegedeeld; |
| 3° werkt het Instituut samen met en verstrekt het informatie aan : | 3° werkt het Instituut samen met en verstrekt het informatie aan : |
| a) de Europese Commissie, ENISA, het Bureau en aan BEREC; | a) de Europese Commissie, ENISA, het Bureau en aan BEREC; |
| b) de buitenlandse regulerende instanties voor postdiensten en telecommunicatie; | b) de buitenlandse regulerende instanties voor postdiensten en telecommunicatie; |
| c) de regulerende instanties in de overige economische sectoren; | c) de regulerende instanties in de overige economische sectoren; |
| d) de federale overheidsdiensten die belast zijn met consumentenbescherming; | d) de federale overheidsdiensten die belast zijn met consumentenbescherming; |
| e) de Belgische instanties die belast zijn met mededinging. | e) de Belgische instanties die belast zijn met mededinging. |
| De Koning kan, na raadpleging van deze instanties en van het Instituut en op gezamenlijk voorstel van de minister die bevoegd is voor Economie en van de minister de nadere regels vastleggen inzake samenwerking, raadpleging en uitwisseling van informatie tussen deze instanties en het Instituut; | De Koning kan, na raadpleging van deze instanties en van het Instituut en op gezamenlijk voorstel van de minister die bevoegd is voor Economie en van de minister de nadere regels vastleggen inzake samenwerking, raadpleging en uitwisseling van informatie tussen deze instanties en het Instituut; |
| f) de regulerende instanties van Gemeenschappen en Gewesten en dit volgens de nadere regels die werden afgesproken in samenwerkingsakkoorden met deze beleidsniveaus; | f) de regulerende instanties van Gemeenschappen en Gewesten en dit volgens de nadere regels die werden afgesproken in samenwerkingsakkoorden met deze beleidsniveaus; |
| g) de openbare diensten die bevoegd zijn op het stuk van openbare veiligheid, of civiele veiligheid en bescherming, of civiele verdediging, of crisisplanning, of veiligheid of bescherming van het economische en wetenschappelijke potentieel van het land; | g) de openbare diensten die bevoegd zijn op het stuk van openbare veiligheid, of civiele veiligheid en bescherming, of civiele verdediging, of crisisplanning, of veiligheid of bescherming van het economische en wetenschappelijke potentieel van het land; |
| h) de Commissie voor de bescherming van de persoonlijke levenssfeer; | h) de Commissie voor de bescherming van de persoonlijke levenssfeer; |
| i) de federale overheidsdienst die belast is met statistiek en economische informatie; | i) de federale overheidsdienst die belast is met statistiek en economische informatie; |
| 4° verleent het Instituut zijn medewerking aan de gemengde Commissie voor telecommunicatie, opgericht bij het koninklijk besluit van 10 december | 4° verleent het Instituut zijn medewerking aan de gemengde Commissie voor telecommunicatie, opgericht bij het koninklijk besluit van 10 december |

## COÖRDINATIE VAN DE ARTIKELEN

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| 1957 en gewijzigd bij het koninklijk besluit van 24 september 1993; | 1957 en gewijzigd bij het koninklijk besluit van 24 september 1993; |
| 5° kan het Instituut enkel besluiten nemen met betrekking tot die elektronische communicatienetwerken waarvoor de gemeenschappen eveneens bevoegd zijn nadat er omtrent de uitoefening van bevoegdheden met betrekking tot deze elektronische communicatienetwerken een samenwerkingsakkoord met de Gemeenschappen in werking is getreden. | 5° kan het Instituut enkel besluiten nemen met betrekking tot die elektronische communicatienetwerken waarvoor de gemeenschappen eveneens bevoegd zijn nadat er omtrent de uitoefening van bevoegdheden met betrekking tot deze elektronische communicatienetwerken een samenwerkingsakkoord met de Gemeenschappen in werking is getreden. |
| 6° mag het Instituut, mits de redenen voor de nietigverklaring worden geëerbiedigd en de omvang van het toepassingsgebied niet wordt gewijzigd, overgaan tot de vervanging van een door een rechterlijke autoriteit vernietigd besluit wanneer, wegens die nietigverklaring, één of meer doelstellingen beoogd in de artikelen 6 tot 8 van de wet van 13 juni 2005 betreffende de elektronische communicatie niet langer worden gehaald. Het Instituut kan in een dergelijke vervanging tevens voorzien wanneer het vernietigde besluit betrekking heeft op de postsector en één of meer van de volgende doelstellingen niet langer worden gehaald : | 6° mag het Instituut, mits de redenen voor de nietigverklaring worden geëerbiedigd en de omvang van het toepassingsgebied niet wordt gewijzigd, overgaan tot de vervanging van een door een rechterlijke autoriteit vernietigd besluit wanneer, wegens die nietigverklaring, één of meer doelstellingen beoogd in de artikelen 6 tot 8 van de wet van 13 juni 2005 betreffende de elektronische communicatie niet langer worden gehaald. Het Instituut kan in een dergelijke vervanging tevens voorzien wanneer het vernietigde besluit betrekking heeft op de postsector en één of meer van de volgende doelstellingen niet langer worden gehaald : |
| - waken over de kwaliteit en het voortbestaan van de universele dienst; | - waken over de kwaliteit en het voortbestaan van de universele dienst; |
| - waken over de belangen van de gebruikers van postdiensten; | - waken over de belangen van de gebruikers van postdiensten; |
| - bijdragen tot de ontwikkeling van een interne markt voor postdiensten; | - bijdragen tot de ontwikkeling van een interne markt voor postdiensten; |
| - het bevorderen van de concurrentie in de postsector. | - het bevorderen van de concurrentie in de postsector. |
| § 3. In het kader van de samenwerking met de in de vorige paragraaf onder punt 3 opgesomde instanties kunnen de leden van de Raad en de leden van het personeel van het Instituut vertrouwelijke informatie waarvan ze kennis hebben in het kader van de uitvoering van hun functie, meedelen aan deze instanties, voor zover deze mededeling noodzakelijk is voor de uitvoering van de opdrachten van deze autoriteiten. | § 3. In het kader van de samenwerking met de in de vorige paragraaf onder punt 3 opgesomde instanties kunnen de leden van de Raad en de leden van het personeel van het Instituut vertrouwelijke informatie waarvan ze kennis hebben in het kader van de uitvoering van hun functie, meedelen aan deze instanties, voor zover deze mededeling noodzakelijk is voor de uitvoering van de opdrachten van deze autoriteiten. |

## COÖRDINATIE VAN DE ARTIKELEN

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| **Art. 24.** Op voorstel van het Instituut kan de Koning de hoedanigheid van officier van gerechtelijke politie toekennen aan de statutaire personeelsleden van het Instituut die hij belast met de vaststelling van inbreuken op de wet van 6 juli 1971 houdende oprichting van bpost en betreffende sommige postdiensten, de wet van 13 juni 2005 betreffende de elektronische communicatie, de wet van 26 januari 2018 betreffende de postdiensten, de wet van 21 maart 1991 en de wet van 30 maart 1995 betreffende de elektronische communicatienetwerken en -diensten en de uitoefening van omroepactiviteiten in het tweetalig gebied Brussel-Hoofdstad en hun uitvoeringbesluiten alsook het koninklijk besluit van 18 mei 1994 betreffende elektromagnetische compatibiliteit. | **Art. 24.** Op voorstel van het Instituut kan de Koning de hoedanigheid van officier van gerechtelijke politie toekennen aan de statutaire personeelsleden van het Instituut die hij belast met de vaststelling van inbreuken op de wet van 6 juli 1971 houdende oprichting van bpost en betreffende sommige postdiensten, de wet van 13 juni 2005 betreffende de elektronische communicatie, de wet van 26 januari 2018 betreffende de postdiensten, de wet van 21 maart 1991 en de wet van 30 maart 1995 betreffende de elektronische communicatienetwerken en -diensten en de uitoefening van omroepactiviteiten in het tweetalig gebied Brussel-Hoofdstad, **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 xx 2018, wat de sector digitale infrastructuren betreft,** en hun uitvoeringbesluiten alsook het koninklijk besluit van 18 mei 1994 betreffende elektromagnetische compatibiliteit. |
| Deze personeelsleden zijn eveneens belast met de vaststelling van inbreuken op de wet van 13 juni 2005 betreffende de elektronische communicatie, het Strafwetboek en de bijzondere wetten indien deze gepleegd worden door middel van apparatuur, elektronische communicatienetwerken of -diensten of radiocommunicatie in de zin van de voornoemde wet betreffende de elektronische communicatie. | Deze personeelsleden zijn eveneens belast met de vaststelling van inbreuken op de wet van 13 juni 2005 betreffende de elektronische communicatie, het Strafwetboek en de bijzondere wetten indien deze gepleegd worden door middel van apparatuur, elektronische communicatienetwerken of -diensten of radiocommunicatie in de zin van de voornoemde wet betreffende de elektronische communicatie. |
| **Wet van 21 november 2017 over de infrastructuren voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU** | **Wet van 21 november 2017 over de infrastructuren voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU** |
| **Art. 71.** De FSMA ziet toe op de toepassing van de bepalingen van deze wet en de besluiten en reglementen genomen ter uitvoering ervan, alsook van Verordening 600/2014. | **Art. 71.** De FSMA ziet toe op de toepassing van de bepalingen van deze wet en de besluiten en reglementen genomen ter uitvoering ervan, alsook van Verordening 600/2014 **en van titel 2 van de wet van […] 2018 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 […] 2018 kan de FSMA niettemin een gespecialiseerde externe dienstverlener belasten met de uitvoering van welbepaalde toezichttaken of de bijstand van een dergelijke dienstverlener verkrijgen.** |

## COÖRDINATIE VAN DE ARTIKELEN

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| **Art. 79.** § 1. Wanneer de FSMA een inbreuk vaststelt op de bepalingen van deze wet of de besluiten en reglementen genomen ter uitvoering ervan, of van Verordening 600/2014, kan zij de voor de inbreuk verantwoordelijke persoon bevelen om, binnen de termijn die zij bepaalt, de vastgestelde toestand te verhelpen alsook, desgevallend, om af te zien van herhaling van de gedraging die een inbreuk vormt. De FSMA kan ook elke natuurlijke of rechtspersoon die onjuiste of misleidende informatie heeft gepubliceerd of verspreid, bevelen om een rechtzetting te publiceren. | **Art. 79.** § 1. Wanneer de FSMA een inbreuk vaststelt op de bepalingen van deze wet of de besluiten en reglementen genomen ter uitvoering ervan, of van Verordening 600/2014, kan zij de voor de inbreuk verantwoordelijke persoon bevelen om, binnen de termijn die zij bepaalt, de vastgestelde toestand te verhelpen alsook, desgevallend, om af te zien van herhaling van de gedraging die een inbreuk vormt. De FSMA kan ook elke natuurlijke of rechtspersoon die onjuiste of misleidende informatie heeft gepubliceerd of verspreid, bevelen om een rechtzetting te publiceren. |
| Onverminderd de overige maatregelen bepaald door de wet, kan de FSMA, indien de persoon tot wie zij een bevel heeft gericht met toepassing van het eerste lid, in gebreke blijft bij afloop van de hem opgelegde termijn, en op voorwaarde dat die persoon zijn middelen heeft kunnen laten gelden: | Onverminderd de overige maatregelen bepaald door de wet, kan de FSMA, indien de persoon tot wie zij een bevel heeft gericht met toepassing van het eerste lid, in gebreke blijft bij afloop van de hem opgelegde termijn, en op voorwaarde dat die persoon zijn middelen heeft kunnen laten gelden: |
| 1° haar standpunt over de krachtens het eerste lid gedane vaststellingen openbaar maken, waarbij zij de identiteit van diegene die verantwoordelijk is voor de overtreding, en de aard van de overtreding verduidelijkt. Deze openbaarmaking gebeurt op kosten van de betrokken persoon; | 1° haar standpunt over de krachtens het eerste lid gedane vaststellingen openbaar maken, waarbij zij de identiteit van diegene die verantwoordelijk is voor de overtreding, en de aard van de overtreding verduidelijkt. Deze openbaarmaking gebeurt op kosten van de betrokken persoon; |
| 2° de betaling van een dwangsom opleggen die per kalenderdag dat het bevel niet wordt nageleefd niet meer mag bedragen dan 50 000 euro, noch in het totaal 2 500 000 euro mag overschrijden; | 2° de betaling van een dwangsom opleggen die per kalenderdag dat het bevel niet wordt nageleefd niet meer mag bedragen dan 50 000 euro, noch in het totaal 2 500 000 euro mag overschrijden; |
| In spoedeisende gevallen kan de FSMA de maatregelen bedoeld in het tweede lid, 1°, nemen zonder voorafgaand bevel met toepassing van het eerste lid, mits de persoon zijn middelen heeft kunnen laten gelden. Ook wanneer er geen duidelijk identificeerbare voor de inbreuk verantwoordelijke persoon is, kan de FSMA zonder voorafgaand bevel een waarschuwing bekendmaken waarin desgevallend de aard van de inbreuk wordt genoemd. | In spoedeisende gevallen kan de FSMA de maatregelen bedoeld in het tweede lid, 1°, nemen zonder voorafgaand bevel met toepassing van het eerste lid, mits de persoon zijn middelen heeft kunnen laten gelden. Ook wanneer er geen duidelijk identificeerbare voor de inbreuk verantwoordelijke persoon is, kan de FSMA zonder voorafgaand bevel een waarschuwing bekendmaken waarin desgevallend de aard van de inbreuk wordt genoemd. |
| § 2. Onverminderd de overige maatregelen bepaald door de wet, kan de FSMA, indien zij overeenkomstig de artikelen 70 tot 72 van de wet van 2 augustus 2002 een inbreuk vaststelt op de bepalingen bedoeld in dit hoofdstuk of de besluiten of reglementen genomen ter uitvoering ervan, of van Verordening 600/2014, | § 2. Onverminderd de overige maatregelen bepaald door de wet, kan de FSMA, indien zij overeenkomstig de artikelen 70 tot 72 van de wet van 2 augustus 2002 een inbreuk vaststelt op de bepalingen bedoeld in dit hoofdstuk of de besluiten of reglementen genomen ter uitvoering ervan, of van Verordening 600/2014, |

**COÖRDINATIE VAN DE ARTIKELEN**

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| aan de overtreder een administratieve geldboete opleggen. | aan de overtreder een administratieve geldboete opleggen. |
| Een administratieve geldboete kan ook worden opgelegd aan één of meer leden van het wettelijk bestuursorgaan en aan elke persoon die instaat voor de effectieve leiding, alsook aan elke andere natuurlijke persoon die verantwoordelijk wordt geacht voor de inbreuk. | Een administratieve geldboete kan ook worden opgelegd aan één of meer leden van het wettelijk bestuursorgaan en aan elke persoon die instaat voor de effectieve leiding, alsook aan elke andere natuurlijke persoon die verantwoordelijk wordt geacht voor de inbreuk. |
| § 3. Het bedrag van de in paragraaf 2 bedoelde administratieve geldboetes wordt als volgt bepaald: | § 3. Het bedrag van de in paragraaf 2 bedoelde administratieve geldboetes wordt als volgt bepaald: |
| 1° wanneer het een rechtspersoon betreft, mag de administratieve geldboete, voor hetzelfde feit of geheel van feiten, niet meer bedragen dan 5 000 000 euro, of, indien dit hoger is, tien procent van de totale jaaromzet van die rechtspersoon volgens de recentste jaarrekening die door het leidinggevend orgaan is opgesteld. Indien de betrokken rechtspersoon geen omzet realiseert, wordt onder "totale jaaromzet" begrepen de met omzet corresponderende soort inkomsten, hetzij overeenkomstig de toepasselijke Europese jaarrekeningenrichtlijnen hetzij, indien die niet van toepassing zijn op de betrokken rechtspersoon, overeenkomstig het nationale recht van de lidstaat waar de rechtspersoon gevestigd is. Indien de rechtspersoon een moederonderneming is of een dochteronderneming van de moederonderneming die een geconsolideerde jaarrekening moet opstellen, is de in aanmerking te nemen totale jaaromzet gelijk aan de totale jaaromzet, volgens de laatst beschikbare geconsolideerde jaarrekening als goedgekeurd door het leidinggevend orgaan van de uiteindelijke moederonderneming; | 1° wanneer het een rechtspersoon betreft, mag de administratieve geldboete, voor hetzelfde feit of geheel van feiten, niet meer bedragen dan 5 000 000 euro, of, indien dit hoger is, tien procent van de totale jaaromzet van die rechtspersoon volgens de recentste jaarrekening die door het leidinggevend orgaan is opgesteld. Indien de betrokken rechtspersoon geen omzet realiseert, wordt onder "totale jaaromzet" begrepen de met omzet corresponderende soort inkomsten, hetzij overeenkomstig de toepasselijke Europese jaarrekeningenrichtlijnen hetzij, indien die niet van toepassing zijn op de betrokken rechtspersoon, overeenkomstig het nationale recht van de lidstaat waar de rechtspersoon gevestigd is. Indien de rechtspersoon een moederonderneming is of een dochteronderneming van de moederonderneming die een geconsolideerde jaarrekening moet opstellen, is de in aanmerking te nemen totale jaaromzet gelijk aan de totale jaaromzet, volgens de laatst beschikbare geconsolideerde jaarrekening als goedgekeurd door het leidinggevend orgaan van de uiteindelijke moederonderneming; |
| 2° wanneer het een natuurlijk persoon betreft, mag de administratieve geldboete, voor hetzelfde feit of geheel van feiten, niet meer bedragen dan 5 000 000 euro. | 2° wanneer het een natuurlijk persoon betreft, mag de administratieve geldboete, voor hetzelfde feit of geheel van feiten, niet meer bedragen dan 5 000 000 euro. |
| Wanneer de overtreding de overtreder winst heeft opgeleverd of ervoor heeft gezorgd dat een verlies kon worden vermeden, mag dit maximum, ongeacht wat voorafgaat, tot het dubbele van die winst of dat verlies worden verhoogd. | Wanneer de overtreding de overtreder winst heeft opgeleverd of ervoor heeft gezorgd dat een verlies kon worden vermeden, mag dit maximum, ongeacht wat voorafgaat, tot het dubbele van die winst of dat verlies worden verhoogd. |
| | **§ 4. In geval van schending van de toepasselijke bepalingen van de wet van […] 2018 tot vaststelling** |

## COÖRDINATIE VAN DE ARTIKELEN

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| | **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.** |
| **Wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten** | **Wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten** |
| **Art. 75.** § 1. In afwijking van artikel 74, eerste lid, en binnen de grenzen van het recht van de Europese Unie mag de FSMA vertrouwelijke informatie meedelen : | **Art. 75.** § 1. In afwijking van artikel 74, eerste lid, en binnen de grenzen van het recht van de Europese Unie mag de FSMA vertrouwelijke informatie meedelen : |
| 1° aan de Europese Centrale Bank, aan de Bank en aan de andere centrale banken en instellingen met een gelijkaardige opdracht als monetaire overheid, alsook aan andere overheidsinstanties die belast zijn met het toezicht op de betalings- en afwikkelingssystemen; | 1° aan de Europese Centrale Bank, aan de Bank en aan de andere centrale banken en instellingen met een gelijkaardige opdracht als monetaire overheid, alsook aan andere overheidsinstanties die belast zijn met het toezicht op de betalings- en afwikkelingssystemen; |
| aan de Europese Centrale Bank, aan de Bank en aan de andere centrale banken en instellingen met een soortgelijke taak in hun hoedanigheid van monetaire autoriteit als deze gegevens van belang zijn voor de uitoefening van hun respectieve wettelijke taken, waaronder het voeren van monetair beleid en de daarmee samenhangende beschikbaarstelling van liquide middelen, de uitoefening van toezicht op betalings-, clearing- en afwikkelingssystemen en de waarborging van de stabiliteit van het financiële stelsel, alsook aan andere overheidsinstanties die belast zijn met het toezicht op de betalingssystemen. | aan de Europese Centrale Bank, aan de Bank en aan de andere centrale banken en instellingen met een soortgelijke taak in hun hoedanigheid van monetaire autoriteit als deze gegevens van belang zijn voor de uitoefening van hun respectieve wettelijke taken, waaronder het voeren van monetair beleid en de daarmee samenhangende beschikbaarstelling van liquide middelen, de uitoefening van toezicht op betalings-, clearing- en afwikkelingssystemen en de waarborging van de stabiliteit van het financiële stelsel, alsook aan andere overheidsinstanties die belast zijn met het toezicht op de betalingssystemen. |
| Wanneer zich een noodsituatie voordoet, waaronder ongunstige ontwikkelingen op de financiële markten, die de liquiditeit van de markt en de stabiliteit van het financiële stelsel kan ondermijnen in een van de lidstaten waar aan entiteiten van een groep met beleggingsondernemingen vergunning is verleend of significante bijkantoren zijn gevestigd in de zin van artikel 59, §§ 6 en 7, van de wet van 25 oktober 2016, kan de FSMA gegevens overzenden aan centrale banken van het Europees stelsel van centrale banken als deze gegevens van belang zijn voor de uitoefening van hun wettelijke taken, waaronder het voeren van monetair beleid en de daarmee samenhangende beschikbaarstelling van liquide middelen, de uitoefening van toezicht op betalings-, clearing- en | Wanneer zich een noodsituatie voordoet, waaronder ongunstige ontwikkelingen op de financiële markten, die de liquiditeit van de markt en de stabiliteit van het financiële stelsel kan ondermijnen in een van de lidstaten waar aan entiteiten van een groep met beleggingsondernemingen vergunning is verleend of significante bijkantoren zijn gevestigd in de zin van artikel 59, §§ 6 en 7, van de wet van 25 oktober 2016, kan de FSMA gegevens overzenden aan centrale banken van het Europees stelsel van centrale banken als deze gegevens van belang zijn voor de uitoefening van hun wettelijke taken, waaronder het voeren van monetair beleid en de daarmee samenhangende beschikbaarstelling van liquide middelen, de uitoefening van toezicht op betalings-, clearing- en |

**COÖRDINATIE VAN DE ARTIKELEN**

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| effectenafwikkelingssystemen en de waarborging van de stabiliteit van het financiële stelsel. | effectenafwikkelingssystemen en de waarborging van de stabiliteit van het financiële stelsel. |
| In een noodsituatie zoals hierboven bedoeld, kan de FSMA gegevens meedelen die van belang zijn voor de centrale overheidsdiensten in alle betrokken lidstaten die bevoegd zijn voor de wetgeving inzake toezicht op de kredietinstellingen, financiële instellingen, beleggingsdiensten en verzekeringsmaatschappijen; | In een noodsituatie zoals hierboven bedoeld, kan de FSMA gegevens meedelen die van belang zijn voor de centrale overheidsdiensten in alle betrokken lidstaten die bevoegd zijn voor de wetgeving inzake toezicht op de kredietinstellingen, financiële instellingen, beleggingsdiensten en verzekeringsmaatschappijen; |
| 1°bis aan de Bank, aan de Europese Centrale Bank met betrekking tot de taken die haar zijn opgedragen door Verordening (EU) nr. 1024/2013 van de Raad van 15 oktober 2013 waarbij aan de Europese Centrale Bank specifieke taken worden opgedragen betreffende het beleid inzake het prudentieel toezicht op kredietinstellingen, en aan de andere leden van het ESCB; | 1°bis aan de Bank, aan de Europese Centrale Bank met betrekking tot de taken die haar zijn opgedragen door Verordening (EU) nr. 1024/2013 van de Raad van 15 oktober 2013 waarbij aan de Europese Centrale Bank specifieke taken worden opgedragen betreffende het beleid inzake het prudentieel toezicht op kredietinstellingen, en aan de andere leden van het ESCB; |
| 2° aan het Federaal Agentschap van de Schuld; | 2° aan het Federaal Agentschap van de Schuld; |
| 3° aan de bevoegde autoriteiten van andere Lidstaten van de Europese Economische Ruimte die één of meer bevoegdheden uitoefenen die vergelijkbaar zijn met die als bedoeld in artikel 45; | 3° aan de bevoegde autoriteiten van andere Lidstaten van de Europese Economische Ruimte die één of meer bevoegdheden uitoefenen die vergelijkbaar zijn met die als bedoeld in artikel 45; |
| 4° aan de bevoegde autoriteiten van derde Staten die één of meer bevoegdheden uitoefenen die vergelijkbaar zijn met die als bedoeld in artikel 45 en waarmee de FSMA een samenwerkingsovereenkomst voor de uitwisseling van informatie heeft gesloten; | 4° aan de bevoegde autoriteiten van derde Staten die één of meer bevoegdheden uitoefenen die vergelijkbaar zijn met die als bedoeld in artikel 45 en waarmee de FSMA een samenwerkingsovereenkomst voor de uitwisseling van informatie heeft gesloten; |
| 5° aan het Agentschap voor de samenwerking tussen energieregulators (ACER) en de nationale regulerende instanties bedoeld in artikel 2, punt 10, van Verordening 1227/2011, en, voor Verordening 596/2014, aan de Europese Commissie en de overige instanties bedoeld in artikel 25 van die verordening | 5° aan het Agentschap voor de samenwerking tussen energieregulators (ACER) en de nationale regulerende instanties bedoeld in artikel 2, punt 10, van Verordening 1227/2011, en, voor Verordening 596/2014, aan de Europese Commissie en de overige instanties bedoeld in artikel 25 van die verordening |
| 6° aan de Belgische instellingen of aan instellingen van andere lidstaten van de Europese Economische Ruimte die een beschermingsregeling voor deposito's, beleggers of levensverzekeringen beheren; | 6° aan de Belgische instellingen of aan instellingen van andere lidstaten van de Europese Economische Ruimte die een beschermingsregeling voor deposito's, beleggers of levensverzekeringen beheren; |
| 7° aan de centrale tegenpartijen of de centrale effectenbewaarinstellingen die gemachtigd zijn om verrekenings- of afwikkelingsdiensten te verstrekken | 7° aan de centrale tegenpartijen of de centrale effectenbewaarinstellingen die gemachtigd zijn om verrekenings- of afwikkelingsdiensten te verstrekken |

**COÖRDINATIE VAN DE ARTIKELEN**

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| voor transacties in financiële instrumenten verricht op een Belgische georganiseerde markt, als de FSMA van oordeel is dat de mededeling van de betrokken informatie noodzakelijk is om de regelmatige werking van die instellingen te vrijwaren voor tekortkomingen, zelfs potentiële, van marktdeelnemers op de betrokken markt; | voor transacties in financiële instrumenten verricht op een Belgische georganiseerde markt, als de FSMA van oordeel is dat de mededeling van de betrokken informatie noodzakelijk is om de regelmatige werking van die instellingen te vrijwaren voor tekortkomingen, zelfs potentiële, van marktdeelnemers op de betrokken markt; |
| 8° aan de marktexploitanten voor de goede werking van, de controle van en het toezicht op de markten die zij inrichten; | 8° aan de marktexploitanten voor de goede werking van, de controle van en het toezicht op de markten die zij inrichten; |
| 9° tijdens burgerrechtelijke of handelsrechtelijke procedures, aan de autoriteiten en gerechtelijke mandatarissen die betrokken zijn bij procedures van faillissement of gerechtelijke reorganisatie of bij analoge collectieve procedures betreffende ondernemingen die onder het toezicht van de FSMA staan of waarvan de verrichtingen onder haar toezicht staan, met uitzondering van de vertrouwelijke informatie over het aandeel van derden in pogingen om de instelling te redden vóór de betrokken procedures werden ingesteld; | 9° tijdens burgerrechtelijke of handelsrechtelijke procedures, aan de autoriteiten en gerechtelijke mandatarissen die betrokken zijn bij procedures van faillissement of gerechtelijke reorganisatie of bij analoge collectieve procedures betreffende ondernemingen die onder het toezicht van de FSMA staan of waarvan de verrichtingen onder haar toezicht staan, met uitzondering van de vertrouwelijke informatie over het aandeel van derden in pogingen om de instelling te redden vóór de betrokken procedures werden ingesteld; |
| 10° aan de commissarissen, de bedrijfsrevisoren en de andere personen die belast zijn met de wettelijke controle van de rekeningen van de ondernemingen die onder het toezicht van de FSMA vallen, van de rekeningen van andere Belgische financiële instellingen of van gelijkaardige buitenlandse ondernemingen; | 10° aan de commissarissen, de bedrijfsrevisoren en de andere personen die belast zijn met de wettelijke controle van de rekeningen van de ondernemingen die onder het toezicht van de FSMA vallen, van de rekeningen van andere Belgische financiële instellingen of van gelijkaardige buitenlandse ondernemingen; |
| 11° aan de sekwesters, voor de uitoefening van hun opdracht als bedoeld in de wetten tot regeling van de opdrachten die aan de FSMA zijn toevertrouwd; | 11° aan de sekwesters, voor de uitoefening van hun opdracht als bedoeld in de wetten tot regeling van de opdrachten die aan de FSMA zijn toevertrouwd; |
| 12° aan het College van toezicht op de bedrijfsrevisoren en aan de autoriteiten van lidstaten of derde landen die toezicht houden op de personen die belast zijn met de wettelijke controle op de jaarrekening van de ondernemingen die onder het toezicht van de FSMA staan; | 12° aan het College van toezicht op de bedrijfsrevisoren en aan de autoriteiten van lidstaten of derde landen die toezicht houden op de personen die belast zijn met de wettelijke controle op de jaarrekening van de ondernemingen die onder het toezicht van de FSMA staan; |
| 13° aan de Federale Overheidsdienst Economie; K.M.O., Middenstand en Energie in het kader van het toezicht op het consumentenkrediet, op het hypothecair krediet, op de marktpraktijken en op de betalingsdiensten, aan de bevoegde autoriteiten van andere Lidstaten van de Europese Economische Ruimte die een vergelijkbare bevoegdheid | 13° aan de Federale Overheidsdienst Economie; K.M.O., Middenstand en Energie in het kader van het toezicht op het consumentenkrediet, op het hypothecair krediet, op de marktpraktijken en op de betalingsdiensten, aan de bevoegde autoriteiten van andere Lidstaten van de Europese Economische Ruimte die een vergelijkbare bevoegdheid |

**COÖRDINATIE VAN DE ARTIKELEN**

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| uitoefenen, alsook aan de bevoegde autoriteiten van derde Staten die een vergelijkbare bevoegdheid uitoefenen en waarmee de FSMA een samenwerkingsovereenkomst voor de uitwisseling van informatie heeft gesloten; | uitoefenen, alsook aan de bevoegde autoriteiten van derde Staten die een vergelijkbare bevoegdheid uitoefenen en waarmee de FSMA een samenwerkingsovereenkomst voor de uitwisseling van informatie heeft gesloten; |
| 14° aan de Belgische Mededingingsautoriteit; | 14° aan de Belgische Mededingingsautoriteit; |
| 15° (opgeheven) | **15° binnen de grenzen van het recht van de Europese Unie, aan de autoriteiten bedoeld in artikel 7 van de wet van xx 2018 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;** |
| 16° aan de administratie van de Thesaurie, krachtens de wettelijke en reglementaire bepalingen die zijn genomen voor de tenuitvoerlegging van de maatregelen die gelden inzake financiële embargo's. | 16° aan de administratie van de Thesaurie, krachtens de wettelijke en reglementaire bepalingen die zijn genomen voor de tenuitvoerlegging van de maatregelen die gelden inzake financiële embargo's. |
| 17° aan de van de ondernemingen onafhankelijke actuarissen die krachtens de wet een opdracht vervullen waarbij zij controle uitoefenen op die ondernemingen, alsook aan de instanties die met het toezicht op die actuarissen zijn belast; | 17° aan de van de ondernemingen onafhankelijke actuarissen die krachtens de wet een opdracht vervullen waarbij zij controle uitoefenen op die ondernemingen, alsook aan de instanties die met het toezicht op die actuarissen zijn belast; |
| 18° aan Fedris; | 18° aan Fedris; |
| 19° aan de Controledienst voor de ziekenfondsen en de landsbonden van ziekenfondsen in zijn hoedanigheid van toezichthouder op de maatschappijen voor onderlinge bijstand zoals bedoeld in de artikelen 43bis, § 5 en 70, §§ 6, 7 en 8, van de wet van 6 augustus 1990 betreffende de ziekenfondsen en de landsbonden van ziekenfondsen alsook op hun verrichtingen. | 19° aan de Controledienst voor de ziekenfondsen en de landsbonden van ziekenfondsen in zijn hoedanigheid van toezichthouder op de maatschappijen voor onderlinge bijstand zoals bedoeld in de artikelen 43bis, § 5 en 70, §§ 6, 7 en 8, van de wet van 6 augustus 1990 betreffende de ziekenfondsen en de landsbonden van ziekenfondsen alsook op hun verrichtingen. |
| 20° (opgeheven) | 20° (opgeheven) |
| 21° aan de ESMA, de EIOPA en de EBA en aan het Europees Comité voor systeemrisico's. | 21° aan de ESMA, de EIOPA en de EBA en aan het Europees Comité voor systeemrisico's. |
| 22° binnen de grenzen van de Europese verordeningen en richtlijnen, aan de autoriteiten die toezicht houden op personen die actief zijn op markten voor emissierechten; | 22° binnen de grenzen van de Europese verordeningen en richtlijnen, aan de autoriteiten die toezicht houden op personen die actief zijn op markten voor emissierechten; |

## COÖRDINATIE VAN DE ARTIKELEN

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| 23° binnen de grenzen van de Europese verordeningen en richtlijnen, aan de autoriteiten die toezicht houden op personen die actief zijn op markten voor landbouwgrondstoffenderivaten. | 23° binnen de grenzen van de Europese verordeningen en richtlijnen, aan de autoriteiten die toezicht houden op personen die actief zijn op markten voor landbouwgrondstoffenderivaten. |
| 24° aan de Belgische Gegevensbeschermingsautoriteit. | 24° aan de Belgische Gegevensbeschermingsautoriteit. |
| 24° aan de Cel voor financiële informatieverwerking bedoeld in artikel 76 van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten. | 24° aan de Cel voor financiële informatieverwerking bedoeld in artikel 76 van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten. |
| § 2. De FSMA mag enkel vertrouwelijke informatie overeenkomstig § 1 meedelen op voorwaarde dat de autoriteiten of instellingen die er de geadresseerde van zijn, die informatie gebruiken voor de uitvoering van hun opdrachten, en dat zij, wat die informatie betreft, aan een gelijkwaardig beroepsgeheim gebonden zijn als bedoeld in artikel 74. Bovendien mag de informatie die afkomstig is van een autoriteit van een andere Lidstaat van de Europese Economische Ruimte enkel met de uitdrukkelijke instemming van die autoriteit worden doorgegeven in de gevallen als bedoeld in 7°, 9°, 10° en 17° van § 1 alsook aan de autoriteiten of organismen van derde Staten in de gevallen als bedoeld in 4°, 6°, 10° en 13° van § 1, en, in voorkomend geval, enkel voor de doeleinden waarmee die autoriteit heeft ingestemd. | § 2. De FSMA mag enkel vertrouwelijke informatie overeenkomstig § 1 meedelen op voorwaarde dat de autoriteiten of instellingen die er de geadresseerde van zijn, die informatie gebruiken voor de uitvoering van hun opdrachten, en dat zij, wat die informatie betreft, aan een gelijkwaardig beroepsgeheim gebonden zijn als bedoeld in artikel 74. Bovendien mag de informatie die afkomstig is van een autoriteit van een andere Lidstaat van de Europese Economische Ruimte enkel met de uitdrukkelijke instemming van die autoriteit worden doorgegeven in de gevallen als bedoeld in 7°, 9°, 10° en 17° van § 1 alsook aan de autoriteiten of organismen van derde Staten in de gevallen als bedoeld in 4°, 6°, 10° en 13° van § 1, en, in voorkomend geval, enkel voor de doeleinden waarmee die autoriteit heeft ingestemd. |
| § 3. De FSMA mag de vertrouwelijke informatie als bedoeld in artikel 74, eerste lid, of de vertrouwelijke informatie die zij van de in § 1 bedoelde autoriteiten en instellingen heeft ontvangen, gebruiken voor de uitvoering van al haar opdrachten als bedoeld in artikel 45. | § 3. De FSMA mag de vertrouwelijke informatie als bedoeld in artikel 74, eerste lid, of de vertrouwelijke informatie die zij van de in § 1 bedoelde autoriteiten en instellingen heeft ontvangen, gebruiken voor de uitvoering van al haar opdrachten als bedoeld in artikel 45. |
| § 4. Onverminderd de strengere bepalingen van de bijzondere wetten die op hen van toepassing zijn, zijn de in § 1 bedoelde Belgische autoriteiten en instellingen, wat de vertrouwelijke informatie betreft die zij van de FSMA ontvangen met toepassing van § 1, gebonden door het beroepsgeheim als bedoeld in artikel 74. | § 4. Onverminderd de strengere bepalingen van de bijzondere wetten die op hen van toepassing zijn, zijn de in § 1 bedoelde Belgische autoriteiten en instellingen, wat de vertrouwelijke informatie betreft die zij van de FSMA ontvangen met toepassing van § 1, gebonden door het beroepsgeheim als bedoeld in artikel 74. |
| § 5. Dit artikel is van toepassing onverminderd de meer restrictieve bepalingen van het recht van de Europese Unie inzake het beroepsgeheim die rechtstreeks van toepassing zijn. | § 5. Dit artikel is van toepassing onverminderd de meer restrictieve bepalingen van het recht van de Europese Unie inzake het beroepsgeheim die rechtstreeks van toepassing zijn. |

## COÖRDINATIE VAN DE ARTIKELEN

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| **Wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België** | **Wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België** |
| **Art. 36/1.** Definities : Voor de toepassing van dit hoofdstuk en hoofdstuk VII wordt verstaan onder : | **Art. 36/1.** Definities : Voor de toepassing van dit hoofdstuk en hoofdstuk VII wordt verstaan onder : |
| 1° " de wet van 2 augustus 2002 " : de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten; | 1° " de wet van 2 augustus 2002 " : de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten; |
| 2° " financieel instrument " : een instrument als gedefinieerd in artikel 2, 1° van de wet van 2 augustus 2002; | 2° " financieel instrument " : een instrument als gedefinieerd in artikel 2, 1° van de wet van 2 augustus 2002; |
| 3° " kredietinstelling " : een instelling als bedoeld in Boek II en in de Titels I en II van Boek III van de wet van 25 april 2014 op het statuut van en het toezicht op kredietinstellingen en beursvennootschappen; | 3° " kredietinstelling " : een instelling als bedoeld in Boek II en in de Titels I en II van Boek III van de wet van 25 april 2014 op het statuut van en het toezicht op kredietinstellingen en beursvennootschappen; |
| 4° "instelling voor elektronisch geld" : een instelling als bedoeld in artikel 2, 74° van de wet van 11 maart 2018 op het statuut van en het toezicht op de betalingsinstellingen en de instellingen voor elektronisch geld, de toegang tot het bedrijf van betalingsdienstaanbieder en tot de activiteit van uitgifte van elektronisch geld, en de toegang tot betalingssystemen; | 4° "instelling voor elektronisch geld" : een instelling als bedoeld in artikel 2, 74° van de wet van 11 maart 2018 op het statuut van en het toezicht op de betalingsinstellingen en de instellingen voor elektronisch geld, de toegang tot het bedrijf van betalingsdienstaanbieder en tot de activiteit van uitgifte van elektronisch geld, en de toegang tot betalingssystemen; |
| 5° " beleggingsonderneming met het statuut van beursvennootschap " : een beleggingsonderneming als bedoeld in Boek XII van de wet van 25 april 2014 op het statuut van en het toezicht op kredietinstellingen en beursvennootschappen, die een vergunning heeft als beursvennootschap of beleggingsdiensten mag verlenen die, indien zij door een Belgische beleggingsonderneming zouden worden verleend, een vergunning als beursvennootschap zouden vereisen; | 5° " beleggingsonderneming met het statuut van beursvennootschap " : een beleggingsonderneming als bedoeld in Boek XII van de wet van 25 april 2014 op het statuut van en het toezicht op kredietinstellingen en beursvennootschappen, die een vergunning heeft als beursvennootschap of beleggingsdiensten mag verlenen die, indien zij door een Belgische beleggingsonderneming zouden worden verleend, een vergunning als beursvennootschap zouden vereisen; |
| 6° "verzekeringsonderneming of herverzekeringsonderneming": een onderneming als bedoeld in artikel 5, eerste lid, 1°, of 2°, van de wet van 13 maart 2016 op het statuut van en het toezicht op de verzekerings- of herverzekeringsondernemingen; | 6° "verzekeringsonderneming of herverzekeringsonderneming": een onderneming als bedoeld in artikel 5, eerste lid, 1°, of 2°, van de wet van 13 maart 2016 op het statuut van en het toezicht op de verzekerings- of herverzekeringsondernemingen; |
| 7° (…) | 7° (…) |

## COÖRDINATIE VAN DE ARTIKELEN

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| 8° " maatschappij voor onderlinge borgstelling " : een maatschappij als bedoeld in artikel 57 van de programmawet van 10 februari 1998 tot bevordering van het zelfstandig ondernemerschap; | 8° " maatschappij voor onderlinge borgstelling " : een maatschappij als bedoeld in artikel 57 van de programmawet van 10 februari 1998 tot bevordering van het zelfstandig ondernemerschap; |
| 9° "betalingsinstelling" : een instelling als bedoeld in artikel 2, 8° van de wet van 11 maart 2018 op het statuut van en het toezicht op de betalingsinstellingen en de instellingen voor elektronisch geld, de toegang tot het bedrijf van betalingsdienstaanbieder en tot de activiteit van uitgifte van elektronisch geld, en de toegang tot betalingssystemen; | 9° "betalingsinstelling" : een instelling als bedoeld in artikel 2, 8° van de wet van 11 maart 2018 op het statuut van en het toezicht op de betalingsinstellingen en de instellingen voor elektronisch geld, de toegang tot het bedrijf van betalingsdienstaanbieder en tot de activiteit van uitgifte van elektronisch geld, en de toegang tot betalingssystemen; |
| 10° " gereglementeerde markt " : een Belgische of buitenlandse gereglementeerde markt; | 10° " gereglementeerde markt " : een Belgische of buitenlandse gereglementeerde markt; |
| 11° " Belgische gereglementeerde markt " : een door een marktonderneming geëxploiteerd en/of beheerd multilateraal systeem dat verschillende koop- en verkoopintenties van derden met betrekking tot financiële instrumenten - binnen dit systeem en volgens de niet-discretionaire regels van dit systeem - samenbrengt of het samenbrengen daarvan vergemakkelijkt op zodanige wijze dat er een overeenkomst uit voortvloeit met betrekking tot financiële instrumenten die volgens de regels en/of de systemen van de markt tot de handel zijn toegelaten, en waaraan vergunning is verleend en die regelmatig werkt, overeenkomstig het bepaalde in hoofdstuk II van de wet van 2 augustus 2002; | 11° " Belgische gereglementeerde markt " : een door een marktonderneming geëxploiteerd en/of beheerd multilateraal systeem dat verschillende koop- en verkoopintenties van derden met betrekking tot financiële instrumenten - binnen dit systeem en volgens de niet-discretionaire regels van dit systeem - samenbrengt of het samenbrengen daarvan vergemakkelijkt op zodanige wijze dat er een overeenkomst uit voortvloeit met betrekking tot financiële instrumenten die volgens de regels en/of de systemen van de markt tot de handel zijn toegelaten, en waaraan vergunning is verleend en die regelmatig werkt, overeenkomstig het bepaalde in hoofdstuk II van de wet van 2 augustus 2002; |
| 12° " buitenlandse gereglementeerde markt " : een markt voor financiële instrumenten die is georganiseerd door een marktonderneming waarvan de Staat van herkomst een andere lidstaat van de Europese Economische Ruimte is dan België, en waaraan in deze lidstaat een vergunning als gereglementeerde markt met toepassing van titel III van Richtlijn 2014/65/EU is verleend; | 12° " buitenlandse gereglementeerde markt " : een markt voor financiële instrumenten die is georganiseerd door een marktonderneming waarvan de Staat van herkomst een andere lidstaat van de Europese Economische Ruimte is dan België, en waaraan in deze lidstaat een vergunning als gereglementeerde markt met toepassing van titel III van Richtlijn 2014/65/EU is verleend; |
| 13° "centrale tegenpartij" : een centrale tegenpartij als gedefinieerd in artikel 2, punt 1), van Verordering (EU) Nr. 648/2012 van het Europees Parlement en de Raad van 4 juli 2012 betreffende otc-derivaten, centrale tegenpartijen en transactieregisters; | 13° "centrale tegenpartij" : een centrale tegenpartij als gedefinieerd in artikel 2, punt 1), van Verordering (EU) Nr. 648/2012 van het Europees Parlement en de Raad van 4 juli 2012 betreffende otc-derivaten, centrale tegenpartijen en transactieregisters; |
| 14° " vereffeningsinstelling " : een instelling die de vereffening verzekert van orders van overdracht van | 14° " vereffeningsinstelling " : een instelling die de vereffening verzekert van orders van overdracht van |

**COÖRDINATIE VAN DE ARTIKELEN**

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| financiële instrumenten, van rechten met betrekking tot deze financiële instrumenten of van termijnverrichtingen op deviezen, met of zonder afwikkeling in contanten; | financiële instrumenten, van rechten met betrekking tot deze financiële instrumenten of van termijnverrichtingen op deviezen, met of zonder afwikkeling in contanten; |
| 15° " FSMA " : de Autoriteit voor Financiële Diensten en Markten, in het Duits " Kommission für das Bank-, Finanz- und Versicherungswesen "; | 15° " FSMA " : de Autoriteit voor Financiële Diensten en Markten, in het Duits " Kommission für das Bank-, Finanz- und Versicherungswesen "; |
| 16° "bevoegde autoriteit" : de Bank, de FSMA of de autoriteit die door elke lidstaat wordt aangewezen met toepassing van artikel 67 van Richtlijn 2014/65/EU, artikel 22 van Verordening 648/2012 of artikel 11 van Verordening 909/2014, tenzij anders is bepaald in de Richtlijn en de respectieve verordeningen; | 16° "bevoegde autoriteit" : de Bank, de FSMA of de autoriteit die door elke lidstaat wordt aangewezen met toepassing van artikel 67 van Richtlijn 2014/65/EU, artikel 22 van Verordening 648/2012 of artikel 11 van Verordening 909/2014, tenzij anders is bepaald in de Richtlijn en de respectieve verordeningen; |
| 17° "Richtlijn 2014/65/EU" : Richtlijn 2014/65/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende markten voor financiële instrumenten en tot wijziging van Richtlijn 2002/92/EG en Richtlijn 2011/61/EU; | 17° "Richtlijn 2014/65/EU" : Richtlijn 2014/65/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende markten voor financiële instrumenten en tot wijziging van Richtlijn 2002/92/EG en Richtlijn 2011/61/EU; |
| 18° " CSRSFI " : het Comité voor systeemrisico's en systeemrelevante financiële instellingen. | 18° " CSRSFI " : het Comité voor systeemrisico's en systeemrelevante financiële instellingen. |
| 19° " instelling voor bedrijfspensioenvoorziening " : een instelling als bedoeld in artikel 2, 1° van de wet van 27 oktober 2006 betreffende het toezicht op de instellingen voor bedrijfspensioenvoorziening. | 19° " instelling voor bedrijfspensioenvoorziening " : een instelling als bedoeld in artikel 2, 1° van de wet van 27 oktober 2006 betreffende het toezicht op de instellingen voor bedrijfspensioenvoorziening. |
| 20° "Europese Bankautoriteit" : de Europese Bankautoriteit opgericht bij Verordening nr. 1093/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Bankautoriteit), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/78/EG van de Commissie; | 20° "Europese Bankautoriteit" : de Europese Bankautoriteit opgericht bij Verordening nr. 1093/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Bankautoriteit), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/78/EG van de Commissie; |
| 21° "Europese Autoriteit voor verzekeringen en bedrijfspensioenen" : de Europese Autoriteit voor verzekeringen en bedrijfspensioenen opgericht bij Verordening nr. 1094/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Autoriteit voor verzekeringen en bedrijfspensioenen), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/79/EG van de Commissie; | 21° "Europese Autoriteit voor verzekeringen en bedrijfspensioenen" : de Europese Autoriteit voor verzekeringen en bedrijfspensioenen opgericht bij Verordening nr. 1094/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Autoriteit voor verzekeringen en bedrijfspensioenen), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/79/EG van de Commissie; |

## COÖRDINATIE VAN DE ARTIKELEN

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| 21°/1 "Europese Autoriteit voor effecten en markten" : de Europese Autoriteit voor effecten en markten opgericht bij Verordening 1095/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Autoriteit voor effecten en markten), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/77/EG van de Commissie; | 21°/1 "Europese Autoriteit voor effecten en markten" : de Europese Autoriteit voor effecten en markten opgericht bij Verordening 1095/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Autoriteit voor effecten en markten), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/77/EG van de Commissie; |
| 22° "Verordering 648/2012" : Verordering (EU) nr. 648/2012 van het Europees Parlement en de Raad van 4 juli 2012 betreffende otc-derivaten, centrale tegenpartijen en transactieregisters; | 22° "Verordering 648/2012" : Verordering (EU) nr. 648/2012 van het Europees Parlement en de Raad van 4 juli 2012 betreffende otc-derivaten, centrale tegenpartijen en transactieregisters; |
| 23° "financiële tegenpartij" : een tegenpartij als gedefinieerd in artikel 2, punt 8), van Verordering 648/2012 of in artikel 3, punt 3), van Verordening 2015/2365; | 23° "financiële tegenpartij" : een tegenpartij als gedefinieerd in artikel 2, punt 8), van Verordering 648/2012 of in artikel 3, punt 3), van Verordening 2015/2365; |
| 24° "niet-financiële tegenpartij" : een tegenpartij als gedefinieerd in artikel 2, punt 9), van Verordering 648/2012 of in artikel 3, punt 4), van Verordening 2015/2365; | 24° "niet-financiële tegenpartij" : een tegenpartij als gedefinieerd in artikel 2, punt 9), van Verordering 648/2012 of in artikel 3, punt 4), van Verordening 2015/2365; |
| 25° "centrale effectenbewaarinstelling" : een centrale effectenbewaarinstelling als omschreven in artikel 2, lid 1, punt 1), van Verordening 909/2014; | 25° "centrale effectenbewaarinstelling" : een centrale effectenbewaarinstelling als omschreven in artikel 2, lid 1, punt 1), van Verordening 909/2014; |
| 26° "Verordening 909/2014" : Verordening (EU) nr. 909/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende de verbetering van de effectenafwikkeling in de Europese Unie, betreffende centrale effectenbewaarinstellingen en tot wijziging van Richtlijnen 98/26/EG en 2014/65/EU en Verordening (EU) nr. 236/2012; | 26° "Verordening 909/2014" : Verordening (EU) nr. 909/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende de verbetering van de effectenafwikkeling in de Europese Unie, betreffende centrale effectenbewaarinstellingen en tot wijziging van Richtlijnen 98/26/EG en 2014/65/EU en Verordening (EU) nr. 236/2012; |
| 27° "Verordening 2015/2365" : Verordening (EU) 2015/2365 van het Europees Parlement en de Raad van 25 november 2015 betreffende de transparantie van effectenfinancieringstransacties en van hergebruik en tot wijziging van Verordening (EU) nr. 648/2012. | 27° "Verordening 2015/2365" : Verordening (EU) 2015/2365 van het Europees Parlement en de Raad van 25 november 2015 betreffende de transparantie van effectenfinancieringstransacties en van hergebruik en tot wijziging van Verordening (EU) nr. 648/2012; |
| | **28° "de wet van xx xx 2018": de wet van xx xx 2018 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.** |

**COÖRDINATIE VAN DE ARTIKELEN**

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| | **(…)** |
| **Art. 36/14.** § 1. In afwijking van artikel 35 mag de Bank tevens vertrouwelijke informatie meedelen : | **Art. 36/14.** § 1. In afwijking van artikel 35 mag de Bank tevens vertrouwelijke informatie meedelen : |
| 1° aan de Europese Centrale Bank en aan de andere centrale banken en instellingen met een soortgelijke taak in hun hoedanigheid van monetaire autoriteit als deze gegevens van belang zijn voor de uitoefening van hun respectieve wettelijke taken, waaronder het voeren van monetair beleid en de daarmee samenhangende beschikbaarstelling van liquide middelen, de uitoefening van toezicht op betalings-, clearing- en afwikkelingssystemen en de waarborging van de stabiliteit van het financiële stelsel, alsook aan andere overheidsinstanties die belast zijn met het toezicht op de betalingssystemen. | 1° aan de Europese Centrale Bank en aan de andere centrale banken en instellingen met een soortgelijke taak in hun hoedanigheid van monetaire autoriteit als deze gegevens van belang zijn voor de uitoefening van hun respectieve wettelijke taken, waaronder het voeren van monetair beleid en de daarmee samenhangende beschikbaarstelling van liquide middelen, de uitoefening van toezicht op betalings-, clearing- en afwikkelingssystemen en de waarborging van de stabiliteit van het financiële stelsel, alsook aan andere overheidsinstanties die belast zijn met het toezicht op de betalingssystemen. |
| Wanneer zich een noodsituatie voordoet, waaronder ongunstige ontwikkelingen op de financiële markten, die de liquiditeit van de markt en de stabiliteit van het financiële stelsel kan ondermijnen in een van de lidstaten waar aan entiteiten van een groep met kredietinstellingen of beleggingsondernemingen vergunning is verleend of significante bijkantoren zijn gevestigd in de zin van artikel 3, 65° van de wet van 25 april 2014 op het statuut van en het toezicht op kredietinstellingen en beursvennootschappen, kan de Bank gegevens overzenden aan centrale banken van het Europees stelsel van centrale banken als deze gegevens van belang zijn voor de uitoefening van hun wettelijke taken, waaronder het voeren van monetair beleid en de daarmee samenhangende beschikbaarstelling van liquide middelen, de uitoefening van toezicht op betalings-, clearing- en effectenafwikkelingssystemen en de waarborging van de stabiliteit van het financiële stelsel. | Wanneer zich een noodsituatie voordoet, waaronder ongunstige ontwikkelingen op de financiële markten, die de liquiditeit van de markt en de stabiliteit van het financiële stelsel kan ondermijnen in een van de lidstaten waar aan entiteiten van een groep met kredietinstellingen of beleggingsondernemingen vergunning is verleend of significante bijkantoren zijn gevestigd in de zin van artikel 3, 65° van de wet van 25 april 2014 op het statuut van en het toezicht op kredietinstellingen en beursvennootschappen, kan de Bank gegevens overzenden aan centrale banken van het Europees stelsel van centrale banken als deze gegevens van belang zijn voor de uitoefening van hun wettelijke taken, waaronder het voeren van monetair beleid en de daarmee samenhangende beschikbaarstelling van liquide middelen, de uitoefening van toezicht op betalings-, clearing- en effectenafwikkelingssystemen en de waarborging van de stabiliteit van het financiële stelsel. |
| In een noodsituatie zoals hierboven bedoeld, kan de Bank gegevens meedelen die van belang zijn voor de centrale overheidsdiensten in alle betrokken lidstaten die bevoegd zijn voor de wetgeving inzake toezicht op de kredietinstellingen, financiële instellingen, beleggingsdiensten en verzekeringsmaatschappijen; | In een noodsituatie zoals hierboven bedoeld, kan de Bank gegevens meedelen die van belang zijn voor de centrale overheidsdiensten in alle betrokken lidstaten die bevoegd zijn voor de wetgeving inzake toezicht op de kredietinstellingen, financiële instellingen, beleggingsdiensten en verzekeringsmaatschappijen; |
| 2° binnen de grenzen van de Europese richtlijnen, aan de bevoegde autoriteiten van de Europese Unie en van andere Lidstaten van de Europese Economische Ruimte die één of meerdere | 2° binnen de grenzen van de Europese richtlijnen, aan de bevoegde autoriteiten van de Europese Unie en van andere Lidstaten van de Europese Economische Ruimte die één of meerdere |

**COÖRDINATIE VAN DE ARTIKELEN**

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| bevoegdheden uitoefenen die vergelijkbaar zijn met die als bedoeld in de artikelen 36/2 en 36/3, met inbegrip van de Europese Centrale Bank voor wat betreft de taken die haar zijn opgedragen bij Verordening (EU) nr. 1024/2013 van de Raad van 15 oktober 2013 waarbij aan de Europese Centrale Bank specifieke taken worden opgedragen betreffende het beleid inzake het prudentieel toezicht op kredietinstellingen; | bevoegdheden uitoefenen die vergelijkbaar zijn met die als bedoeld in de artikelen 36/2 en 36/3, met inbegrip van de Europese Centrale Bank voor wat betreft de taken die haar zijn opgedragen bij Verordening (EU) nr. 1024/2013 van de Raad van 15 oktober 2013 waarbij aan de Europese Centrale Bank specifieke taken worden opgedragen betreffende het beleid inzake het prudentieel toezicht op kredietinstellingen; |
| 3° met inachtneming van de Europese richtlijnen, aan de bevoegde autoriteiten van derde Staten die één of meerdere bevoegdheden uitoefenen die vergelijkbaar zijn met die als bedoeld in de artikelen 36/2 en 36/3 en waarmee de Bank een samenwerkingsovereenkomst voor de uitwisseling van informatie heeft gesloten; | 3° met inachtneming van de Europese richtlijnen, aan de bevoegde autoriteiten van derde Staten die één of meerdere bevoegdheden uitoefenen die vergelijkbaar zijn met die als bedoeld in de artikelen 36/2 en 36/3 en waarmee de Bank een samenwerkingsovereenkomst voor de uitwisseling van informatie heeft gesloten; |
| 4° aan de FSMA; | 4° aan de FSMA; |
| 5° aan de Belgische instellingen of aan instellingen van een andere Lidstaat van de Europese Economische Ruimte die een beschermingsregeling voor deposito's, beleggers of levensverzekeringen beheren en aan het orgaan dat bevoegd is voor de financieringsregelingen voor de afwikkeling; | 5° aan de Belgische instellingen of aan instellingen van een andere Lidstaat van de Europese Economische Ruimte die een beschermingsregeling voor deposito's, beleggers of levensverzekeringen beheren en aan het orgaan dat bevoegd is voor de financieringsregelingen voor de afwikkeling; |
| 6° aan de centrale tegenpartijen de instellingen voor vereffening van financiële instrumenten of de centrale effectenbewaarinstellingen die gemachtigd zijn om verrekenings- of vereffeningsdiensten te verstrekken voor transacties in financiële instrumenten verricht op een Belgische gereglementeerde markt, als de Bank van oordeel is dat de mededeling van de betrokken informatie noodzakelijk is om de regelmatige werking van die centrale tegenpartijen, instellingen voor vereffening en centrale effectenbewaarinstellingen te vrijwaren voor tekortkomingen, zelfs potentiële, van marktdeelnemers op de betrokken markt; | 6° aan de centrale tegenpartijen de instellingen voor vereffening van financiële instrumenten of de centrale effectenbewaarinstellingen die gemachtigd zijn om verrekenings- of vereffeningsdiensten te verstrekken voor transacties in financiële instrumenten verricht op een Belgische gereglementeerde markt, als de Bank van oordeel is dat de mededeling van de betrokken informatie noodzakelijk is om de regelmatige werking van die centrale tegenpartijen, instellingen voor vereffening en centrale effectenbewaarinstellingen te vrijwaren voor tekortkomingen, zelfs potentiële, van marktdeelnemers op de betrokken markt; |
| 7° binnen de grenzen van de Europese richtlijnen, aan de marktondernemingen voor de goede werking van, de controle van en het toezicht op de markten die deze inrichten; | 7° binnen de grenzen van de Europese richtlijnen, aan de marktondernemingen voor de goede werking van, de controle van en het toezicht op de markten die deze inrichten; |
| 8° tijdens burgerrechtelijke of handelsrechtelijke procedures, aan de autoriteiten en gerechtelijke mandatarissen die betrokken zijn bij procedures van faillissement of gerechtelijke reorganisatie of bij | 8° tijdens burgerrechtelijke of handelsrechtelijke procedures, aan de autoriteiten en gerechtelijke mandatarissen die betrokken zijn bij procedures van faillissement of gerechtelijke reorganisatie of bij |

## COÖRDINATIE VAN DE ARTIKELEN

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| analoge collectieve procedures betreffende instellingen die onder het toezicht van de Bank staan, met uitzondering van de vertrouwelijke informatie over het aandeel van derden in reddingspogingen vóór de betrokken procedures werden ingesteld; | analoge collectieve procedures betreffende instellingen die onder het toezicht van de Bank staan, met uitzondering van de vertrouwelijke informatie over het aandeel van derden in reddingspogingen vóór de betrokken procedures werden ingesteld; |
| 9° aan de commissarissen, de bedrijfsrevisoren en de andere personen die belast zijn met de wettelijke controle van de rekeningen van de instellingen die onder het toezicht van de Bank vallen, van de rekeningen van andere Belgische financiële instellingen of van soortgelijke buitenlandse instellingen; | 9° aan de commissarissen, de bedrijfsrevisoren en de andere personen die belast zijn met de wettelijke controle van de rekeningen van de instellingen die onder het toezicht van de Bank vallen, van de rekeningen van andere Belgische financiële instellingen of van soortgelijke buitenlandse instellingen; |
| 10° aan de sekwesters, voor de uitoefening van hun opdracht als bedoeld in de wetten tot regeling van de opdrachten die aan de Bank zijn toevertrouwd; | 10° aan de sekwesters, voor de uitoefening van hun opdracht als bedoeld in de wetten tot regeling van de opdrachten die aan de Bank zijn toevertrouwd; |
| 11° aan het College van toezicht op de bedrijfsrevisoren en aan de autoriteiten van lidstaten of derde landen die toezicht houden op de personen die belast zijn met de wettelijke controle op de jaarrekening van de instellingen die onder het toezicht van de Bank staan; | 11° aan het College van toezicht op de bedrijfsrevisoren en aan de autoriteiten van lidstaten of derde landen die toezicht houden op de personen die belast zijn met de wettelijke controle op de jaarrekening van de instellingen die onder het toezicht van de Bank staan; |
| 12° binnen de grenzen van het recht van de Europese Unie, aan de Belgische mededingingsautoriteit; | 12° binnen de grenzen van het recht van de Europese Unie, aan de Belgische mededingingsautoriteit; |
| 13° binnen de grenzen van de Europese richtlijnen, aan de erkenningsraad voor effectenmakelaars als bedoeld in artikel 21 van de wet van 2 augustus 2002; | 13° binnen de grenzen van de Europese richtlijnen, aan de erkenningsraad voor effectenmakelaars als bedoeld in artikel 21 van de wet van 2 augustus 2002; |
| 14° binnen de grenzen van de Europese richtlijnen, aan de Algemene Administratie van de Thesaurie, krachtens de wettelijke en reglementaire bepalingen die zijn genomen voor de tenuitvoerlegging van de maatregelen die gelden inzake financiële embargo's; | 14° binnen de grenzen van de Europese richtlijnen, aan de Algemene Administratie van de Thesaurie, krachtens de wettelijke en reglementaire bepalingen die zijn genomen voor de tenuitvoerlegging van de maatregelen die gelden inzake financiële embargo's; |
| 15° binnen de grenzen van de Europese richtlijnen, aan de van de instellingen onafhankelijke actuarissen die krachtens de wet een opdracht vervullen waarbij ze controle uitoefenen op die instellingen, alsook aan de instanties die met het toezicht op die actuarissen zijn belast; | 15° binnen de grenzen van de Europese richtlijnen, aan de van de instellingen onafhankelijke actuarissen die krachtens de wet een opdracht vervullen waarbij ze controle uitoefenen op die instellingen, alsook aan de instanties die met het toezicht op die actuarissen zijn belast; |
| 16° aan Fedris; | 16° aan Fedris; |
| 17° de ambtenaren aangesteld door de minister die, in het raam van hun opdracht bedoeld in artikel XV. 2 van het Wetboek van economisch recht bevoegd zijn om de inbreuken op de bepalingen van artikel XV. | 17° de ambtenaren aangesteld door de minister die, in het raam van hun opdracht bedoeld in artikel XV. 2 van het Wetboek van economisch recht bevoegd zijn om de inbreuken op de bepalingen van artikel XV. |

## COÖRDINATIE VAN DE ARTIKELEN

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| 89, 1° tot 18°, 20° 11 , 21°, 22° en 23°, van het Wetboek van economisch recht, op te sporen en vast te stellen; | 89, 1° tot 18°, 20° 11 , 21°, 22° en 23°, van het Wetboek van economisch recht, op te sporen en vast te stellen; |
| 18° aan de autoriteiten die onder het recht van lidstaten van de Europese Unie ressorteren en die bevoegd zijn op het vlak van macroprudentieel toezicht, evenals aan het Europees Comité voor Systeemrisico's, ingesteld bij Europese Verordening (EU) nr. 1092/2010 van het Europees Parlement en de Raad van 24 november 2010; | 18° aan de autoriteiten die onder het recht van lidstaten van de Europese Unie ressorteren en die bevoegd zijn op het vlak van macroprudentieel toezicht, evenals aan het Europees Comité voor Systeemrisico's, ingesteld bij Europese Verordening (EU) nr. 1092/2010 van het Europees Parlement en de Raad van 24 november 2010; |
| 19° binnen de grenzen van de Europese verordeningen en richtlijnen, aan de Europese Autoriteit voor effecten en markten, aan de Europese Autoriteit voor verzekeringen en bedrijfspensioenen en aan de Europese Bankautoriteit; | 19° binnen de grenzen van de Europese verordeningen en richtlijnen, aan de Europese Autoriteit voor effecten en markten, aan de Europese Autoriteit voor verzekeringen en bedrijfspensioenen en aan de Europese Bankautoriteit; |
| 20° binnen de grenzen van het recht van de Europese Unie, aan het Coördinatie- en Crisiscentrum van de Regering van de FOD Binnenlandse Zaken, aan het Coördinatieorgaan voor de dreigingsanalyse, ingesteld door de wet van 10 juli 2006 betreffende de analyse van de dreiging, en aan de politiediensten bedoeld in de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus, in de mate dat de toepassing van artikel 19 van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren zulks vereist; | 20° binnen de grenzen van het recht van de Europese Unie, aan het Coördinatie- en Crisiscentrum van de Regering van de FOD Binnenlandse Zaken, aan het Coördinatieorgaan voor de dreigingsanalyse, ingesteld door de wet van 10 juli 2006 betreffende de analyse van de dreiging, **aan de autoriteit bedoeld in artikel 7, §1, van de wet van xx 2018** en aan de politiediensten bedoeld in de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus, in de mate dat de toepassing van artikel 19 van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren zulks vereist; |
| 21° aan de Controledienst voor de ziekenfondsen en de landsbonden van ziekenfondsen, voor de uitoefening van zijn wettelijke opdrachten als bedoeld in artikel 303, § 3, van de wet van 13 maart 2016 op het statuut van en het toezicht op de verzekerings- of herverzekeringsondernemingen, met betrekking tot de maatschappijen van onderlinge bijstand als bedoeld in artikel 43bis, § 5 of artikel 70, §§ 6, 7 en 8 van de wet van 6 augustus 1990 betreffende de ziekenfondsen en de landsbonden van ziekenfondsen en hun verrichtingen; | 21° aan de Controledienst voor de ziekenfondsen en de landsbonden van ziekenfondsen, voor de uitoefening van zijn wettelijke opdrachten als bedoeld in artikel 303, § 3, van de wet van 13 maart 2016 op het statuut van en het toezicht op de verzekerings- of herverzekeringsondernemingen, met betrekking tot de maatschappijen van onderlinge bijstand als bedoeld in artikel 43bis, § 5 of artikel 70, §§ 6, 7 en 8 van de wet van 6 augustus 1990 betreffende de ziekenfondsen en de landsbonden van ziekenfondsen en hun verrichtingen; |
| 22° binnen de grenzen van het recht van de Europese Unie, aan de afwikkelingsautoriteiten als bedoeld in artikel 3 van Richtlijn 2014/59/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende | 22° binnen de grenzen van het recht van de Europese Unie, aan de afwikkelingsautoriteiten als bedoeld in artikel 3 van Richtlijn 2014/59/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende |

**COÖRDINATIE VAN DE ARTIKELEN**

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| de totstandbrenging van een kader voor het herstel en de afwikkeling van kredietinstellingen en beleggingsondernemingen, aan de autoriteiten van derde Staten die belast zijn met taken die te vergelijken zijn met die als bedoeld in artikel 12ter, § 1, waarmee de Bank een samenwerkingsakkoord heeft gesloten waarin wordt voorzien in de uitwisseling van informatie, alsook aan de bevoegde ministeries van de lidstaten van de Europese Economische Ruimte, wanneer dit noodzakelijk is voor het plannen of uitvoeren van afwikkelingsmaatregel; | de totstandbrenging van een kader voor het herstel en de afwikkeling van kredietinstellingen en beleggingsondernemingen, aan de autoriteiten van derde Staten die belast zijn met taken die te vergelijken zijn met die als bedoeld in artikel 12ter, § 1, waarmee de Bank een samenwerkingsakkoord heeft gesloten waarin wordt voorzien in de uitwisseling van informatie, alsook aan de bevoegde ministeries van de lidstaten van de Europese Economische Ruimte, wanneer dit noodzakelijk is voor het plannen of uitvoeren van afwikkelingsmaatregel; |
| 23° aan eenieder die een taak uitvoert die door of krachtens de wet is vastgesteld en die deelneemt of bijdraagt aan de uitoefening van de toezichtsopdracht van de Bank, wanneer die persoon door of met instemming van de Bank werd aangeduid voor die taak, zoals, met name: | 23° aan eenieder die een taak uitvoert die door of krachtens de wet is vastgesteld en die deelneemt of bijdraagt aan de uitoefening van de toezichtsopdracht van de Bank, wanneer die persoon door of met instemming van de Bank werd aangeduid voor die taak, zoals, met name: |
| a) de portefeuillesurveillant bedoeld in artikel 16 van Bijlage III bij de wet van 25 april 2014 op het statuut van en het toezicht op kredietinstellingen en beursvennootschappen; | a) de portefeuillesurveillant bedoeld in artikel 16 van Bijlage III bij de wet van 25 april 2014 op het statuut van en het toezicht op kredietinstellingen en beursvennootschappen; |
| b) de portefeuillebeheerder bedoeld in artikel 8 van Bijlage III bij de wet van 25 april 2014 op het statuut van en het toezicht op kredietinstellingen en beursvennootschappen; en | b) de portefeuillebeheerder bedoeld in artikel 8 van Bijlage III bij de wet van 25 april 2014 op het statuut van en het toezicht op kredietinstellingen en beursvennootschappen; en |
| c) de speciaal commissaris bedoeld in artikel 236, § 1, 1°, van de voornoemde wet, in artikel 517, § 1, 1°, van de wet van 13 maart 2016 op het statuut van en het toezicht op de verzekerings- of herverzekeringsondernemingen, artikel 35, § 1, tweede lid, 1°, van de wet van 21 december 2009 op het statuut van de betalingsinstellingen en van de instellingen voor elektronisch geld, de toegang tot het bedrijf van betalingsdienstaanbieder en tot de activiteit van uitgifte van elektronisch geld en de toegang tot betalingssystemen, artikel 87, § 1, tweede lid, 1°, van de voornoemde wet, artikel 48, eerste lid, 1°, van het koninklijk besluit van 30 april 1999 betreffende het statuut en de controle der maatschappijen voor onderlinge borgstelling en artikel 36/30, § 1, tweede lid, 3°, van deze wet. | c) de speciaal commissaris bedoeld in artikel 236, § 1, 1°, van de voornoemde wet, in artikel 517, § 1, 1°, van de wet van 13 maart 2016 op het statuut van en het toezicht op de verzekerings- of herverzekeringsondernemingen, artikel 35, § 1, tweede lid, 1°, van de wet van 21 december 2009 op het statuut van de betalingsinstellingen en van de instellingen voor elektronisch geld, de toegang tot het bedrijf van betalingsdienstaanbieder en tot de activiteit van uitgifte van elektronisch geld en de toegang tot betalingssystemen, artikel 87, § 1, tweede lid, 1°, van de voornoemde wet, artikel 48, eerste lid, 1°, van het koninklijk besluit van 30 april 1999 betreffende het statuut en de controle der maatschappijen voor onderlinge borgstelling en artikel 36/30, § 1, tweede lid, 3°, van deze wet. |
| | **24° binnen de grenzen van het recht van de Europese Unie, aan de autoriteiten bedoeld in artikel 7 van de wet van xx 2018 voor de uitvoering** |

**COÖRDINATIE VAN DE ARTIKELEN**

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| | **van de bepalingen van de wet van xx 2018 en van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren.** |
| § 2. De Bank mag enkel vertrouwelijke informatie overeenkomstig § 1 meedelen op voorwaarde dat de autoriteiten of instellingen die er de geadresseerden van zijn, die informatie gebruiken voor de uitvoering van hun opdrachten, en dat zij, wat die informatie betreft, aan een gelijkwaardig beroepsgeheim gebonden zijn als bedoeld in artikel 35. Bovendien mag de informatie die afkomstig is van een autoriteit van een andere Lidstaat van de Europese Economische Ruimte enkel met de uitdrukkelijke instemming van die autoriteit worden doorgegeven in de gevallen als bedoeld in 7°, 9°, 10°, 12°, en 16° van § 1 alsook aan de autoriteiten of organismen van derde Staten in de gevallen als bedoeld in 4°, 6° en 10° van § 1, en, in voorkomend geval, enkel voor de doeleinden waarmee die autoriteit heeft ingestemd. | § 2. De Bank mag enkel vertrouwelijke informatie overeenkomstig § 1 meedelen op voorwaarde dat de autoriteiten of instellingen die er de geadresseerden van zijn, die informatie gebruiken voor de uitvoering van hun opdrachten, en dat zij, wat die informatie betreft, aan een gelijkwaardig beroepsgeheim gebonden zijn als bedoeld in artikel 35. Bovendien mag de informatie die afkomstig is van een autoriteit van een andere Lidstaat van de Europese Economische Ruimte enkel met de uitdrukkelijke instemming van die autoriteit worden doorgegeven in de gevallen als bedoeld in 7°, 9°, 10°, 12°, en 16° van § 1 alsook aan de autoriteiten of organismen van derde Staten in de gevallen als bedoeld in 4°, 6° en 10° van § 1, en, in voorkomend geval, enkel voor de doeleinden waarmee die autoriteit heeft ingestemd. |
| § 3. Onverminderd de strengere bepalingen van de bijzondere wetten die op hen van toepassing zijn, zijn de in § 1 bedoelde Belgische personen, autoriteiten en instellingen, wat de vertrouwelijke informatie betreft die zij van de Bank ontvangen met toepassing van § 1, gebonden door het beroepsgeheim als bedoeld in artikel 35. | § 3. Onverminderd de strengere bepalingen van de bijzondere wetten die op hen van toepassing zijn, zijn de in § 1 bedoelde Belgische personen, autoriteiten en instellingen, wat de vertrouwelijke informatie betreft die zij van de Bank ontvangen met toepassing van § 1, gebonden door het beroepsgeheim als bedoeld in artikel 35. |
| § 4. Dit artikel is van toepassing onverminderd de meer restrictieve bepalingen van het recht van de Europese Unie inzake het beroepsgeheim. | § 4. Dit artikel is van toepassing onverminderd de meer restrictieve bepalingen van het recht van de Europese Unie inzake het beroepsgeheim. |
| | **(…)** |
| | **Hoofdstuk IV/4 Toezicht door de Bank in het kader van de wet van … 2018 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 xx 2018 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** |

**COÖRDINATIE VAN DE ARTIKELEN**

| BESTAANDE TEKST | ONTWERP VAN WET |
|---|---|
| | **2014/65/EU. De artikelen 36/19 en 36/20 zijn van toepassing.**<br><br>**De Sanctiecommissie oordeelt over het opleggen van de administratieve geldboetes bedoeld in artikel 52 van de wet van … 2018. De artikelen 36/8 tot 36/12/3 en artikel 36/21 zijn van toepassing.**<br><br>**De Bank deelt relevante informatie over incidentmeldingen die zij ontvangt krachtens de wet van … 2018 zo snel mogelijk met de ECB.** |

## COORDINATION DES ARTICLES

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| **Loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques** | **Loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques** |
| **Art. 2.** La présente loi transpose partiellement la Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection. | **Art. 2.** La présente loi transpose partiellement la Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection. |
| La DGCC, telle que définie à l'article 3, 1°, est désignée comme point de contact national pour la protection des infrastructures critiques européennes, ci-après dénommé « point de contact EPCIP », pour l'ensemble des secteurs et sous-secteurs, pour la Belgique dans ses relations avec la Commission européenne et les Etats membres de l'Union européenne. | La DGCC, telle que définie à l'article 3, 1°, est désignée comme point de contact national pour la protection des infrastructures critiques européennes, ci-après dénommé « point de contact EPCIP », pour l'ensemble des secteurs et sous-secteurs, pour la Belgique dans ses relations avec la Commission européenne et les Etats membres de l'Union européenne. |
| | **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 de sécurité des réseaux et systèmes d'information dans l'Union.** |
| **Art. 3.** Pour l'application de la présente loi et de ses arrêtés d'exécution, l'on entend par : | **Art. 3.** Pour l'application de la présente loi et de ses arrêtés d'exécution, l'on entend par : |
| 1° "DGCC" : Direction générale Centre de Crise du Service public fédéral Intérieur, chargée de la protection spéciale des biens et des personnes et de la coordination nationale en matière d'ordre public ; | 1° "DGCC" : Direction générale Centre de Crise du Service public fédéral Intérieur, chargée de la protection spéciale des biens et des personnes et de la coordination nationale en matière d'ordre public ; |
| 2° "OCAM" : Organe de coordination pour l'analyse de la menace institué par la loi du 10 juillet 2006 relative à l'analyse de la menace ; | 2° "OCAM" : Organe de coordination pour l'analyse de la menace institué par la loi du 10 juillet 2006 relative à l'analyse de la menace ; |
| 3° "autorité sectorielle" : | 3° "autorité sectorielle" : |
| a) pour le secteur des transports : le Ministre ayant les Transports dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration ; | a) pour le secteur des transports : le Ministre ayant les Transports dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration ; |
| b) pour le secteur de l'énergie : le Ministre ayant l'Energie dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration ; | b) pour le secteur de l'énergie : le Ministre ayant l'Energie dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration ; |

## COORDINATION DES ARTICLES

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| c) pour le secteur des finances : la Banque nationale de Belgique; | **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;** |
| | **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)** ; |
| d) pour le secteur des communications électroniques : le Ministre ayant les Communications électroniques dans ses attributions ou, par délégation de celui-ci, un membre dirigeant du personnel de son administration ou un membre de l'Institut belge des services postaux et des télécommunications ; | **e) pour le secteur des communications électroniques et des infrastructures numériques : l'Institut belge des services postaux et des télécommunications ;** |
| | **f) pour le secteur de la santé : l'autorité publique désignée par la loi ou par le Roi, par arrêté délibéré en Conseil des Ministres ;** |
| | **g) pour le secteur de l'eau : l'autorité publique désignée par la loi ou par le Roi, par arrêté délibéré en Conseil des Ministres ;** |
| 4° "infrastructure critique" : installation, système ou partie de celui- ci, d'intérêt fédéral, qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, et dont l'interruption du fonctionnement ou la destruction aurait une incidence significative du fait de la défaillance de ces fonctions ; | 4° "infrastructure critique" : installation, système ou partie de celui- ci, d'intérêt fédéral, qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, et dont l'interruption du fonctionnement ou la destruction aurait une incidence significative du fait de la défaillance de ces fonctions ; |
| 5° "infrastructure critique nationale" : l'infrastructure critique située sur le territoire belge, dont l'interruption du fonctionnement ou la destruction aurait une incidence significative dans le pays ; | 5° "infrastructure critique nationale" : l'infrastructure critique située sur le territoire belge, dont l'interruption du fonctionnement ou la destruction aurait une incidence significative dans le pays ; |
| 6° "infrastructure critique européenne" : l'infrastructure critique nationale dont l'interruption du fonctionnement ou la destruction aurait une incidence significative sur deux États membres de | 6° "infrastructure critique européenne" : l'infrastructure critique nationale dont l'interruption du fonctionnement ou la destruction aurait une incidence significative sur deux États membres de |

## COORDINATION DES ARTICLES

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| l'Union européenne au moins ou l'infrastructure critique qui n'est pas située sur le territoire belge mais sur celui d'un autre Etat membre de l'Union européenne, dont l'interruption du fonctionnement ou la destruction aurait une incidence significative sur au moins deux Etats membres de l'Union européenne, dont la Belgique ; | l'Union européenne au moins ou l'infrastructure critique qui n'est pas située sur le territoire belge mais sur celui d'un autre Etat membre de l'Union européenne, dont l'interruption du fonctionnement ou la destruction aurait une incidence significative sur au moins deux Etats membres de l'Union européenne, dont la Belgique ; |
| 7° "autres points d'intérêt fédéral" : les lieux qui ne sont pas désignés comme infrastructure critique mais qui présentent un intérêt particulier pour l'ordre public, pour la protection spéciale des personnes et des biens, pour la gestion de situations d'urgence ou pour les intérêts militaires et qui font l'objet de mesures de protection prises par la DGCC ; | 7° "autres points d'intérêt fédéral" : les lieux qui ne sont pas désignés comme infrastructure critique mais qui présentent un intérêt particulier pour l'ordre public, pour la protection spéciale des personnes et des biens, pour la gestion de situations d'urgence ou pour les intérêts militaires et qui font l'objet de mesures de protection prises par la DGCC ; |
| 8° "points d'intérêt local" : les lieux qui ne sont ni des infrastructures critiques, ni des autres points d'intérêt fédéral, mais qui présentent un intérêt particulier pour l'exécution des missions de police administrative au niveau local et qui font l'objet de mesures de protection prises par le bourgmestre; | 8° "points d'intérêt local" : les lieux qui ne sont ni des infrastructures critiques, ni des autres points d'intérêt fédéral, mais qui présentent un intérêt particulier pour l'exécution des missions de police administrative au niveau local et qui font l'objet de mesures de protection prises par le bourgmestre; |
| 9° "communications électroniques" : les communications électroniques visées par la loi du 13 juin 2005 relative aux communications électroniques ; | 9° "communications électroniques" : les communications électroniques visées par la loi du 13 juin 2005 relative aux communications électroniques ; |
| 10° "exploitant" : toute personne physique ou morale responsable des investissements relatifs à ou de la gestion quotidienne d'une infrastructure critique nationale ou européenne ; | 10° "exploitant" : toute personne physique ou morale responsable des investissements relatifs à ou de la gestion quotidienne d'une infrastructure critique nationale ou européenne ; |
| 11° "services de police" : les services de police visés par la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux ; | 11° "services de police" : les services de police visés par la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux ; |
| 12° « SICAD » : service d'information et de communication de l'arrondissement, tel que visé par la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux. | 12° « SICAD » : service d'information et de communication de l'arrondissement, tel que visé par la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux. |
| | **13° « la loi du xx xx 2018 » : la loi du xx xx 2018 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique ;** |
| | **14°« sécurité des réseaux et systèmes d'information » : la sécurité des réseaux et** |

## COORDINATION DES ARTICLES

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| | **systèmes d'information au sens de l'article 6, 8° et 9°, de la loi du xx xx 2018 ;** |
| | **15° « infrastructures numériques » : opérateurs visés au point 6 de l'annexe 1 de la loi du xx xx 2018;** |
| | **16° « eau » : opérateurs visés au point 5 de l'annexe 1 de la loi du xx xx 2018 ;** |
| | **17° « santé » : opérateurs visés au point 4 de l'annexe 1 de la loi du xx xx 2018.** |
| **Art. 4.** § 1er. Le présent chapitre s'applique au secteur des transports et au secteur de l'énergie en ce qui concerne la sécurité et la protection des infrastructures critiques nationales et européennes. | **Art. 4.** § 1er. Le présent chapitre s'applique au secteur des transports et au secteur de l'énergie en ce qui concerne la sécurité et la protection des infrastructures critiques nationales et européennes. |
| Toutefois, il ne s'applique pas aux installations nucléaires visées par 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, à l'exception des éléments d'une installation nucléaire destinée à la production industrielle d'électricité qui servent au transport de l'électricité. | Toutefois, il ne s'applique pas aux installations nucléaires visées par 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, à l'exception des éléments d'une installation nucléaire destinée à la production industrielle d'électricité qui servent au transport de l'électricité. |
| L'article 8 et les articles 12 à 26 s'appliquent uniquement aux infrastructures critiques situées sur le territoire belge. | L'article 8 et les articles 12 à 26 s'appliquent uniquement aux infrastructures critiques situées sur le territoire belge. |
| § 2. Le secteur de l'Energie comporte les sous-secteurs suivants : | § 2. Le secteur de l'Energie comporte les sous-secteurs suivants : |
| 1° l'électricité, composée des infrastructures et installations permettant la production et le transport d'électricité, en vue de la fourniture d'électricité ; | 1° l'électricité, composée des infrastructures et installations permettant la production et le transport d'électricité, en vue de la fourniture d'électricité ; |
| 2° le pétrole, composé de la production pétrolière, du raffinage, du traitement, du stockage et de la distribution par oléoducs ; | 2° le pétrole, composé de la production pétrolière, du raffinage, du traitement, du stockage et de la distribution par oléoducs ; |
| 3° le gaz, composé de la production gazière, du raffinage, du traitement, du stockage, du transport par gazoducs et des terminaux de gaz naturel liquéfié. | 3° le gaz, composé de la production gazière, du raffinage, du traitement, du stockage, du transport par gazoducs et des terminaux de gaz naturel liquéfié. |
| Le secteur des Transports comporte les sous-secteurs suivants : | Le secteur des Transports comporte les sous-secteurs suivants : |

## COORDINATION DES ARTICLES

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| 1° transport par route ;<br>2° transport ferroviaire ;<br>3° transport aérien ;<br>4° navigation intérieure ;<br>5° transport hauturier et transport maritime à courte distance et ports. | 1° transport par route ;<br>2° transport ferroviaire ;<br>3° transport aérien ;<br>4° navigation intérieure ;<br>5° transport hauturier et transport maritime à courte distance et ports. |
| § 3. Par dérogation au § 1er, alinéa 1er, le présent chapitre ne s'applique pas au sous-secteur du transport aérien. | § 3. Par dérogation au § 1er, alinéa 1er, le présent chapitre ne s'applique pas au sous-secteur du transport aérien. |
| Sans préjudice de l'article 2, alinéa 2, le Roi prend, par arrêté délibéré en Conseil des ministres, les mesures nécessaires, y compris l'abrogation, l'ajout, la modification ou le remplacement de dispositions légales, pour assurer la transposition de la Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection en ce qui concerne le transport aérien. | Sans préjudice de l'article 2, alinéa 2, le Roi prend, par arrêté délibéré en Conseil des ministres, les mesures nécessaires, y compris l'abrogation, l'ajout, la modification ou le remplacement de dispositions légales, pour assurer la transposition de la Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection en ce qui concerne le transport aérien. |
| § 4. Le présent chapitre s'applique au secteur des finances et au secteur des communications électroniques en ce qui concerne la sécurité et la protection des infrastructures critiques nationales. | **§ 4. Le présent chapitre s'applique au secteur des finances, aux opérateurs de plate-forme de négociation visés à l'article 3,3°, de la loi au secteur des communications électroniques, au secteur des infrastructures numériques, au secteur de la santé et au secteur de l'eau, en ce qui concerne la sécurité et la protection des infrastructures critiques nationales.** |
| **Art. 5.** § 1er. Afin d'identifier les infrastructures critiques relevant de sa compétence, l'autorité sectorielle se concerte au préalable avec la DGCC, et consulte, si elle l'estime utile, les représentants du secteur et les exploitants d'infrastructures critiques potentielles. | **Art. 5.** § 1er. Afin d'identifier les infrastructures critiques relevant de sa compétence, l'autorité sectorielle se concerte au préalable avec la DGCC, et consulte, si elle l'estime utile, les représentants du secteur et les exploitants d'infrastructures critiques potentielles. |
| | **§ 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 xx xx 2018 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.** |
| A cette même fin, l'autorité sectorielle procède à la consultation au préalable des régions, pour les | A cette même fin, l'autorité sectorielle procède à la consultation au préalable des régions, pour les |

**COORDINATION DES ARTICLES**

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| infrastructures critiques potentielles relevant de leurs compétences. | infrastructures critiques potentielles relevant de leurs compétences. |
| § 2. La procédure à suivre pour l'identification des infrastructures critiques nationales et européennes est déterminée à l'annexe. | § 2. La procédure à suivre pour l'identification des infrastructures critiques nationales et européennes est déterminée à l'annexe. |
| | **§ 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 xx xx 2018 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. 13.** § 1er. L'exploitant d'une infrastructure critique élabore un plan de sécurité de l'exploitant, ci-après dénommé P.S.E., visant à prévenir, à atténuer et à neutraliser les risques d'interruption du fonctionnement ou de destruction de l'infrastructure critique par la mise au point de mesures matérielles et organisationnelles internes. | **Art. 13.** § 1er. L'exploitant d'une infrastructure critique élabore un plan de sécurité de l'exploitant, ci-après dénommé P.S.E., visant à prévenir, à atténuer et à neutraliser les risques d'interruption du fonctionnement ou de destruction de l'infrastructure critique par la mise au point de mesures matérielles et organisationnelles internes. |
| § 2. Le P.S.E. comprend au minimum : | § 2. Le P.S.E. comprend au minimum : |
| 1° des mesures internes de sécurité permanentes, devant être appliquées en toutes circonstances ; | 1° des mesures internes de sécurité permanentes, devant être appliquées en toutes circonstances ; |
| 2° des mesures internes de sécurité graduelles à appliquer en fonction de la menace. | 2° des mesures internes de sécurité graduelles à appliquer en fonction de la menace. |
| Pour un secteur déterminé ou le cas échéant par sous-secteur, le Roi peut détailler ces mesures et imposer d'inclure au P.S.E. certaines informations. | Pour un secteur déterminé ou le cas échéant par sous-secteur, le Roi peut détailler ces mesures et imposer d'inclure au P.S.E. certaines informations. |
| § 3. La procédure d'élaboration du P.S.E. comprend au moins les étapes suivantes: | § 3. La procédure d'élaboration du P.S.E. comprend au moins les étapes suivantes: |
| 1° l'inventaire et la localisation des points de l'infrastructure qui, s'ils étaient touchés, pourraient causer l'interruption de son fonctionnement ou sa destruction ; | 1° l'inventaire et la localisation des points de l'infrastructure qui, s'ils étaient touchés, pourraient causer l'interruption de son fonctionnement ou sa destruction ; |
| 2° une analyse des risques, consistant en une identification des principaux scénarios de menaces potentielles pertinents d'actes intentionnels visant à interrompre le fonctionnement de l'infrastructure critique ou à la détruire ; | 2° une analyse des risques, consistant en une identification des principaux scénarios de menaces potentielles pertinents d'actes intentionnels visant à interrompre le fonctionnement de l'infrastructure critique ou à la détruire ; |

## COORDINATION DES ARTICLES

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| 3° une analyse des vulnérabilités de l'infrastructure critique et des impacts potentiels de l'interruption de son fonctionnement ou de sa destruction en fonction des différents scénarios retenus ; | 3° une analyse des vulnérabilités de l'infrastructure critique et des impacts potentiels de l'interruption de son fonctionnement ou de sa destruction en fonction des différents scénarios retenus ; |
| 4° pour chaque scénario de l'analyse de risques, l'identification, la sélection et la désignation par ordre de priorité des mesures de sécurité internes. | 4° pour chaque scénario de l'analyse de risques, l'identification, la sélection et la désignation par ordre de priorité des mesures de sécurité internes. |
| § 4. L'exploitant élabore le P.S.E. dans un délai d'un an à dater de la notification de la désignation de son infrastructure comme infrastructure critique. | § 4. L'exploitant élabore le P.S.E. dans un délai d'un an à dater de la notification de la désignation de son infrastructure comme infrastructure critique. |
| Dans un délai de vingt-quatre mois au plus tard à dater de la notification de la désignation de son infrastructure comme infrastructure critique, il met en œuvre les mesures internes de sécurité prévues dans le P.S.E. | Dans un délai de vingt-quatre mois au plus tard à dater de la notification de la désignation de son infrastructure comme infrastructure critique, il met en œuvre les mesures internes de sécurité prévues dans le P.S.E. |
| 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 le P.S.E. | 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 le P.S.E. |
| § 5. Pour les ports qui tombent sous le champ d'application de la loi du 5 février 2007 relative à la sûreté maritime, le plan de sûreté portuaire imposé par cette loi est assimilé au P.S.E. | § 5. Pour les ports qui tombent sous le champ d'application de la loi du 5 février 2007 relative à la sûreté maritime, le plan de sûreté portuaire imposé par cette loi est assimilé au P.S.E. |
| § 5bis. Pour les infrastructures critiques relevant du secteur des finances, les mesures de sécurité, telles que les politiques de continuité, les plans de continuité et les plans de sécurité physique et logique, que les entreprises sont tenues de mettre en place dans le cadre du statut de contrôle prudentiel qui leur est applicable et/ou dans le cadre de la surveillance (oversight) dont elles font l'objet par la Banque nationale de Belgique, sont assimilées au P.S.E. | § 5bis. Pour les infrastructures critiques relevant du secteur des finances, **à l'exception de celles exploitées par un opérateur de plate-forme de négociation**, les mesures de sécurité, telles que les politiques de continuité, les plans de continuité et les plans de sécurité physique et logique, que les entreprises sont tenues de mettre en place dans le cadre du statut de contrôle prudentiel qui leur est applicable et/ou dans le cadre de la surveillance (oversight) dont elles font l'objet par la Banque nationale de Belgique, sont assimilées au P.S.E. |
| § 6. L'exploitant est responsable d'organiser des exercices et d'actualiser le P.S.E., en fonction des enseignements des exercices ou de toute modification de l'analyse des risques. | § 6. L'exploitant est responsable d'organiser des exercices et d'actualiser le P.S.E., en fonction des enseignements des exercices ou de toute modification de l'analyse des risques. |
| Pour le secteur des finances, les exercices et les mises à jour des mesures de sécurité visées au paragraphe 5bis, sont assimilés aux exercices et mises à jour du P.S.E. visés au présent paragraphe. | Pour le secteur des finances, **à l'exception des infrastructures critiques exploitées par un opérateur de plate-forme de négociation**, les exercices et les mises à jour des mesures de sécurité |

## COORDINATION DES ARTICLES

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| | visées au paragraphe 5bis, sont assimilés aux exercices et mises à jour du P.S.E. visés au présent paragraphe. |
| Le Roi détermine pour un secteur ou un sous-secteur déterminé la fréquence des exercices et des mises à jour du P.S.E. | Le Roi détermine pour un secteur ou un sous-secteur déterminé la fréquence des exercices et des mises à jour du P.S.E. |
| Le Roi détermine pour un secteur déterminé ou, le cas échéant, par sous-secteur les modalités de la participation des services de police aux exercices organisés par l'exploitant. | Le Roi détermine pour un secteur déterminé ou, le cas échéant, par sous-secteur les modalités de la participation des services de police aux exercices organisés par l'exploitant. |
| § 7. Pour un secteur déterminé ou, le cas échéant, par sous-secteur, le Roi peut imposer aux exploitants l'élaboration d'un plan interne d'urgence, visant à limiter, au niveau de l'infrastructure critique, les conséquences néfastes d'une situation d'urgence par la mise au point de mesures matérielles et organisationnelles d'urgence adaptées. | § 7. Pour un secteur déterminé ou, le cas échéant, par sous-secteur, le Roi peut imposer aux exploitants l'élaboration d'un plan interne d'urgence, visant à limiter, au niveau de l'infrastructure critique, les conséquences néfastes d'une situation d'urgence par la mise au point de mesures matérielles et organisationnelles d'urgence adaptées. |
| **Art. 14.** § 1er. Sans préjudice des dispositions légales ou réglementaires imposant, dans un secteur ou un sous-secteur déterminé, d'informer des services déterminés, lorsqu'un événement se produit, de nature à menacer la sécurité de l'infrastructure critique, l'exploitant est tenu de prévenir immédiatement le SICAD, via les numéros d'urgence 101 ou 112, le service désigné par l'autorité sectorielle compétente et la DGCC. | **Art. 14.** § 1er. Sans préjudice des dispositions légales ou réglementaires imposant, dans un secteur ou un sous-secteur déterminé, d'informer des services déterminés, lorsqu'un événement se produit, de nature à menacer la sécurité de l'infrastructure critique, l'exploitant est tenu de prévenir immédiatement le SICAD, via les numéros d'urgence 101 ou 112, le service désigné par l'autorité sectorielle compétente et la DGCC. |
| § 1er /1. Lorsque la notification de l'événement visé au paragraphe 1er ne se fait pas depuis l'infrastructure critique concernée, la police fédérale fournit aux points de contact pour la sécurité désignés en vertu de l'article 12 les informations nécessaires leur permettant de contacter directement le SICAD territorialement compétent. | § 1er /1. Lorsque la notification de l'événement visé au paragraphe 1er ne se fait pas depuis l'infrastructure critique concernée, la police fédérale fournit aux points de contact pour la sécurité désignés en vertu de l'article 12 les informations nécessaires leur permettant de contacter directement le SICAD territorialement compétent. |
| § 2. Conformément aux modalités déterminées par le ministre de l'Intérieur, le SICAD avertit la DGCC de tout événement dont il a connaissance et qui est de nature à menacer la sécurité de l'infrastructure critique. | § 2. Conformément aux modalités déterminées par le ministre de l'Intérieur, le SICAD avertit la DGCC de tout événement dont il a connaissance et qui est de nature à menacer la sécurité de l'infrastructure critique **et, le cas échéant, l'autorité visée à l'article 7, § 1er, de la loi du xx xx 2018, pour ce qui concerne la sécurité des réseaux et systèmes d'information.** |
| **Art. 18.** La DGCC, les services de police et l'OCAM s'échangent les informations utiles pour la prise de | **Art. 18. La DGCC, les services de police, l'OCAM et, le cas échéant, l'autorité visée à l'article 7, § 1er, de** |

## COORDINATION DES ARTICLES

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| mesures externes de protection des infrastructures critiques. | **la loi du xx xx 2018 pour ce qui concerne la sécurité des réseaux et systèmes d'information**, s'échangent les informations utiles pour la prise de mesures externes de protection des infrastructures critiques. |
| **Art. 19.** L'exploitant, le point de contact pour la sécurité, l'autorité sectorielle, la DGCC, l'OCAM et les services de police collaborent en tout temps, par un échange adéquat d'informations concernant la sécurité et la protection de l'infrastructure critique, afin de veiller à une concordance entre les mesures internes de sécurité et les mesures externes de protection. | **Art. 19. 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 xx xx 2018 pour ce qui concerne la sécurité des réseaux et systèmes d'information**, collaborent en tout temps, par un échange adéquat d'informations concernant la sécurité et la protection de l'infrastructure critique, afin de veiller à une concordance entre les mesures internes de sécurité et les mesures externes de protection. |
| **Art. 22.** L'autorité sectorielle, la DGCC, l'OCAM et les services de police limitent l'accès aux informations visées au chapitre 2 aux personnes ayant besoin d'en connaître et d'y avoir accès pour l'exercice de leurs fonctions ou de leur mission s'inscrivant dans une finalité de sécurité et/ou de protection des infrastructures critiques. | **Art. 22. L'autorité sectorielle, la DGCC, l'OCAM et les services de police et l'autorité visée à l'article 7, § 1er, de la loi du xx xx 2018**, limitent l'accès aux informations visées au chapitre 2 aux personnes ayant besoin d'en connaître et d'y avoir accès pour l'exercice de leurs fonctions ou de leur mission s'inscrivant dans une finalité de sécurité et/ou de protection des infrastructures critiques. |
| **Art. 22bis**. Pour le secteur des finances, la Banque nationale de Belgique 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 Banque nationale de Belgique l'informe toutefois sans délai de toute menace concrète et imminente pesant sur une infrastructure critique du secteur des finances. | **Art. 22bis**. Pour le secteur des finances **à l'exception du sous-secteur des opérateurs de plate-forme de négociation**, la Banque nationale de Belgique 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 Banque nationale de Belgique l'informe toutefois sans délai de toute menace concrète et imminente pesant sur une infrastructure critique du secteur des finances.<br><br>**Pour les opérateurs de plate-forme de négociation, la FSMA communique au Ministre des Finances un rapport relatif aux tâches qu'elle accomplit en vertu de la présente loi selon une périodicité appropriée n'excédant toutefois pas trois ans. La FSMA l'informe toutefois sans délai de toute menace concrète et imminente pesant sur une infrastructure critique relevant de son secteur.** |
| **Art. 24.** § 1er. Sans préjudice des attributions des officiers de police judiciaire, un service d'inspection par secteur, ou le cas échéant par sous-secteur, est mis en place, chargé du contrôle du respect des | **Art. 24.** § 1er. Sans préjudice des attributions des officiers de police judiciaire, un service d'inspection par secteur, ou le cas échéant par sous-secteur, est mis en place, chargé du contrôle du respect des |

## COORDINATION DES ARTICLES

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| dispositions de la présente loi et de ses arrêtés d'exécution par les exploitants dudit secteur ou sous-secteur. | dispositions de la présente loi et de ses arrêtés d'exécution par les exploitants dudit secteur ou sous-secteur. |
| § 2. Le Roi désigne, pour un secteur déterminé ou, le cas échéant, par sous-secteur, le service d'inspection compétent pour effectuer le contrôle. | § 2. Le Roi désigne, pour un secteur déterminé ou, le cas échéant, par sous-secteur, le service d'inspection compétent pour effectuer le contrôle. |
| Il peut fixer les modalités du contrôle. | Il peut fixer les modalités du contrôle. |
| Pour le secteur des finances, la Banque nationale de Belgique 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. A cette fin, la Banque nationale de Belgique peut faire usage des informations dont elle dispose dans le cadre de ses missions légales de contrôle prudentiel et de surveillance (oversight) et tient compte, notamment, des constats effectués dans ce cadre. De même, dans le cadre de ses missions légales de contrôle prudentiel et de surveillance (oversight), la Banque nationale de Belgique peut utiliser les informations dont elle dispose en application de la présente loi. | Pour le secteur des finances **à l'exception du sous-secteur des opérateurs de plate-forme de négociation**, la Banque nationale de Belgique 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. A cette fin, la Banque nationale de Belgique peut faire usage des informations dont elle dispose dans le cadre de ses missions légales de contrôle prudentiel et de surveillance (oversight) et tient compte, notamment, des constats effectués dans ce cadre. De même, dans le cadre de ses missions légales de contrôle prudentiel et de surveillance (oversight), la Banque nationale de Belgique peut utiliser les informations dont elle dispose en application de la présente loi. **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 est sans préjudice de la possibilité pour la FSMA de, pour l'exécution des missions qui lui sont confiées par la présente loi, charger un prestataire externe spécialisé de l'exécution de tâches déterminées ou d'obtenir l'assistance d'un tel prestataire**. |
| § 3. Les membres du service d'inspection qui effectuent les opérations prévues à l'article 25, § 1er, sont dotés d'une carte de légitimation dont le modèle est fixé par le Roi, par secteur. | § 3. Les membres du service d'inspection qui effectuent les opérations prévues à l'article 25, § 1er, sont dotés d'une carte de légitimation dont le modèle est fixé par le Roi, par secteur. |
| Le présent paragraphe n'est pas applicable au service d'inspection désigné en vertu du paragraphe 2, alinéa 3. | Le présent paragraphe n'est pas applicable au service d'inspection désigné en vertu du paragraphe 2, alinéa 3. |

## COORDINATION DES ARTICLES

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| § 4. Le Roi peut déterminer les conditions de formation auxquelles doivent répondre les membres du service d'inspection pour un secteur ou un sous-secteur déterminé. | § 4. Le Roi peut déterminer les conditions de formation auxquelles doivent répondre les membres du service d'inspection pour un secteur ou un sous-secteur déterminé. |
| **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** | **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** |
| **Article 1er.** Pour l'application de la présente loi, et de ses mesures d'exécution, il y a lieu d'entendre par : | **Article 1er.** Pour l'application de la présente loi, et de ses mesures d'exécution, il y a lieu d'entendre par : |
| - rayonnements ionisants : rayonnements composés de photos ou de particules capables de déterminer la formation d'ions directement ou indirectement; | - rayonnements ionisants : rayonnements composés de photos ou de particules capables de déterminer la formation d'ions directement ou indirectement; |
| - substance radioactive : toute substance ou toute matière contenant un ou plusieurs radionucléides dont l'activité ou la concentration ne peut être négligée pour des raisons de radioprotection; | - substance radioactive : toute substance ou toute matière contenant un ou plusieurs radionucléides dont l'activité ou la concentration ne peut être négligée pour des raisons de radioprotection; |
| - autorités compétentes : les autorités désignées en vertu de la présente loi et de ses arrêtés d'exécution; | - autorités compétentes : les autorités désignées en vertu de la présente loi et de ses arrêtés d'exécution; |
| - règlement général : règlement général : l'arrêté royal du 20 juillet 2001 portant règlement général de la protection de la population, des travailleurs et de l'environnement contre le danger des rayonnements ionisants; | - règlement général : règlement général : l'arrêté royal du 20 juillet 2001 portant règlement général de la protection de la population, des travailleurs et de l'environnement contre le danger des rayonnements ionisants; |
| - organismes agréés : les organismes chargés de certaines missions par le règlement général; | - organismes agréés : les organismes chargés de certaines missions par le règlement général; |
| - service de contrôle physique : le service qu'est tenu d'organiser le chef d'entreprise en vertu du règlement général, qui est chargé de l'organisation et de la surveillance des mesures nécessaires pour assurer l'observation des dispositions dudit règlement; | - service de contrôle physique : le service qu'est tenu d'organiser le chef d'entreprise en vertu du règlement général, qui est chargé de l'organisation et de la surveillance des mesures nécessaires pour assurer l'observation des dispositions dudit règlement; |
| - l'Agence : l'établissement public créé par la présente loi pour le contrôle nucléaire; | - l'Agence : l'établissement public créé par la présente loi pour le contrôle nucléaire; |
| - matières nucléaires : les produits fissiles spéciaux et les matières brutes suivantes : | - matières nucléaires : les produits fissiles spéciaux et les matières brutes suivantes : |
| a) les produits fissiles spéciaux sont le plutonium 239, l'uranium 233, l'uranium enrichi en uranium 235 ou | a) les produits fissiles spéciaux sont le plutonium 239, l'uranium 233, l'uranium enrichi en uranium 235 ou |

**COORDINATION DES ARTICLES**

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| 233; tout produit contenant un ou plusieurs des isotopes ci-dessus. | 233; tout produit contenant un ou plusieurs des isotopes ci-dessus. |
| L'uranium enrichi en uranium 235 ou 233 est de l'uranium qui contient soit de l'uranium 235 soit de l'uranium 233, soit ces deux isotopes en quantité telle que le rapport entre la somme de ces deux isotopes et l'isotope 238 est supérieur au rapport entre l'isotope 235 et l'isotope 238 dans l'uranium naturel; | L'uranium enrichi en uranium 235 ou 233 est de l'uranium qui contient soit de l'uranium 235 soit de l'uranium 233, soit ces deux isotopes en quantité telle que le rapport entre la somme de ces deux isotopes et l'isotope 238 est supérieur au rapport entre l'isotope 235 et l'isotope 238 dans l'uranium naturel; |
| b) les matières brutes sont l'uranium contenant le mélange d'isotopes qui se trouve dans la nature, et l'uranium appauvri en uranium 235; le thorium; toutes les matières mentionnées ci-dessus sous forme de métal, d'alliage, de composés chimiques ou de concentrés; | b) les matières brutes sont l'uranium contenant le mélange d'isotopes qui se trouve dans la nature, et l'uranium appauvri en uranium 235; le thorium; toutes les matières mentionnées ci-dessus sous forme de métal, d'alliage, de composés chimiques ou de concentrés; |
| - transport nucléaire national : le transport de matières nucléaires conditionnées en vue d'un envoi par tout moyen de transport lorsque celui-ci se déroule exclusivement à l'intérieur du territoire belge; | - transport nucléaire national : le transport de matières nucléaires conditionnées en vue d'un envoi par tout moyen de transport lorsque celui-ci se déroule exclusivement à l'intérieur du territoire belge; |
| - transport nucléaire international : le transport de matières nucléaires conditionnées en vue d'un envoi par tout moyen de transport lorsqu'il doit franchir les frontières du territoire au départ d'une installation de l'expéditeur située dans l'Etat d'origine jusqu'à son arrivée dans une installation du destinataire sur le territoire de l'Etat de destination finale; | - transport nucléaire international : le transport de matières nucléaires conditionnées en vue d'un envoi par tout moyen de transport lorsqu'il doit franchir les frontières du territoire au départ d'une installation de l'expéditeur située dans l'Etat d'origine jusqu'à son arrivée dans une installation du destinataire sur le territoire de l'Etat de destination finale; |
| - mesures de protection physique : toute mesure administrative, organisationnelle et technique qui a pour objectif de protéger les matières nucléaires en cours de production, d'utilisation, d'entreposage ou de transport contre les risques de détention illicite et de vol comme de protéger les matières nucléaires en cours de production, d'utilisation, d'entreposage ainsi que les installations nucléaires et les transports nucléaires nationaux et internationaux contre les risques de sabotage. Lesdites mesures ont également pour objectif de protéger des actes précités les documents nucléaires; | - mesures de protection physique : toute mesure administrative, organisationnelle et technique qui a pour objectif de protéger les matières nucléaires en cours de production, d'utilisation, d'entreposage ou de transport contre les risques de détention illicite et de vol comme de protéger les matières nucléaires en cours de production, d'utilisation, d'entreposage ainsi que les installations nucléaires et les transports nucléaires nationaux et internationaux contre les risques de sabotage. Lesdites mesures ont également pour objectif de protéger des actes précités les documents nucléaires; |
| - mesures de sécurité pour les substances radioactives: toute mesure administrative, organisationnelle et technique qui a pour objectif: | - mesures de sécurité pour les substances radioactives: toute mesure administrative, organisationnelle et technique qui a pour objectif: |

## COORDINATION DES ARTICLES

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| a) de protéger les substances radioactives autres que les matières nucléaires, en cours de production, d'utilisation, d'entreposage ou de transport contre les risques de détention illicite et de vol; | a) de protéger les substances radioactives autres que les matières nucléaires, en cours de production, d'utilisation, d'entreposage ou de transport contre les risques de détention illicite et de vol; |
| b) de protéger contre les risques de sabotage ou de toute utilisation malveillante: | b) de protéger contre les risques de sabotage ou de toute utilisation malveillante: |
| 1) les substances radioactives autres que les matières nucléaires et qui sont en cours de production, d'utilisation ou d'entreposage; | 1) les substances radioactives autres que les matières nucléaires et qui sont en cours de production, d'utilisation ou d'entreposage; |
| 2) les établissements où ces substances sont produites, fabriquées, détenues ou utilisées ainsi que leur transport; | 2) les établissements où ces substances sont produites, fabriquées, détenues ou utilisées ainsi que leur transport; |
| - mesures de sécurité pour les appareils ou installations émettant des rayonnements ionisants ne provenant pas de substances radioactives: toute mesure administrative, organisationnelle et technique qui a pour objectif: | - mesures de sécurité pour les appareils ou installations émettant des rayonnements ionisants ne provenant pas de substances radioactives: toute mesure administrative, organisationnelle et technique qui a pour objectif: |
| a) de protéger les dits appareils ou installations contre les risques de détention illicite et de vol; | a) de protéger les dits appareils ou installations contre les risques de détention illicite et de vol; |
| b) de protéger contre les risques de sabotage ou de toute utilisation malveillante: | b) de protéger contre les risques de sabotage ou de toute utilisation malveillante: |
| 1) lesdits appareils ou installations, ainsi que le transport de ces appareils ou installations; | 1) lesdits appareils ou installations, ainsi que le transport de ces appareils ou installations; |
| 2) les établissements et lieux où se trouvent ces appareils et installations; | 2) les établissements et lieux où se trouvent ces appareils et installations; |
| - sabotage : tout acte délibéré: | - sabotage : tout acte délibéré: |
| a) qui est dirigé contre: | a) qui est dirigé contre: |
| 1) des matières nucléaires en cours de production, d'utilisation, d'entreposage ou de transport; | 1) des matières nucléaires en cours de production, d'utilisation, d'entreposage ou de transport; |
| 2) des installations nucléaires; | 2) des installations nucléaires; |
| 3) des transports nucléaires nationaux ou internationaux; | 3) des transports nucléaires nationaux ou internationaux; |
| 4) des substances radioactives autres que les matières nucléaires et qui sont en cours de production, l'utilisation, d'entreposage ou de transport; | 4) des substances radioactives autres que les matières nucléaires et qui sont en cours de production, l'utilisation, d'entreposage ou de transport; |

## COORDINATION DES ARTICLES

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| 5) des établissements ou parties d'établissements, où des substances radioactives sont produites, fabriquées, détenues ou utilisées; | 5) des établissements ou parties d'établissements, où des substances radioactives sont produites, fabriquées, détenues ou utilisées; |
| 6) des appareils ou installations émettant des rayonnements ionisants ne provenant pas de substances radioactives; | 6) des appareils ou installations émettant des rayonnements ionisants ne provenant pas de substances radioactives; |
| 7) le transport des appareils ou installations émettant des rayonnements ionisants ne provenant pas de substances radioactives; | 7) le transport des appareils ou installations émettant des rayonnements ionisants ne provenant pas de substances radioactives; |
| 8) des établissements, parties d'établissement et lieux où se trouvent des appareils ou installations émettant des rayonnements ionisants ne provenant pas de substances radioactives;<br>Et | 8) des établissements, parties d'établissement et lieux où se trouvent des appareils ou installations émettant des rayonnements ionisants ne provenant pas de substances radioactives;<br>Et |
| b) qui pourrait mettre directement ou indirectement en danger la santé et la sécurité du personnel, de la population et de l'environnement par une exposition aux radiations ou l'émission de substances radioactives; | b) qui pourrait mettre directement ou indirectement en danger la santé et la sécurité du personnel, de la population et de l'environnement par une exposition aux radiations ou l'émission de substances radioactives; |
| - réacteur de puissance : un réacteur nucléaire, conçu à des fins de production électrique, qui est ou a été autorisé en tant qu'établissement de classe I en application de la réglementation relative à la protection contre les rayonnements ionisants et pour lequel aucune autorisation de démantèlement n'a encore été délivrée. | - réacteur de puissance : un réacteur nucléaire, conçu à des fins de production électrique, qui est ou a été autorisé en tant qu'établissement de classe I en application de la réglementation relative à la protection contre les rayonnements ionisants et pour lequel aucune autorisation de démantèlement n'a encore été délivrée. |
| - personne professionnellement exposée : chaque personne physique soumise, dans le cadre de ses activités professionnelles, à une exposition aux rayonnements ionisants susceptible d'entraîner le dépassement de l'une des limites de dose fixées pour les personnes du public; | - personne professionnellement exposée : chaque personne physique soumise, dans le cadre de ses activités professionnelles, à une exposition aux rayonnements ionisants susceptible d'entraîner le dépassement de l'une des limites de dose fixées pour les personnes du public; |
| - personne soumise à la surveillance dosimétrique : chaque personne physique qui exécute des activités de quelque nature que ce soit lors desquelles elle est soumise à une exposition aux rayonnements ionisants susceptible d'entraîner le dépassement de l'une des limites de dose fixées pour les personnes du public; | - personne soumise à la surveillance dosimétrique : chaque personne physique qui exécute des activités de quelque nature que ce soit lors desquelles elle est soumise à une exposition aux rayonnements ionisants susceptible d'entraîner le dépassement de l'une des limites de dose fixées pour les personnes du public; |
| - exploitant : toute personne physique ou morale qui assume la responsabilité de l'établissement devant | - exploitant : toute personne physique ou morale qui assume la responsabilité de l'établissement devant |

**COORDINATION DES ARTICLES**

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| faire l'objet d'une autorisation ou d'une déclaration conformément aux dispositions découlant de l'article 17; | faire l'objet d'une autorisation ou d'une déclaration conformément aux dispositions découlant de l'article 17; |
| - entreprise extérieure : toute personne physique ou morale appelée à exécuter des activités de quelque nature que ce soit dans un établissement devant faire l'objet d'une autorisation ou d'une déclaration conformément aux dispositions découlant de l'article 17, au cours desquelles l'une des limites de dose fixées pour les personnes du public pourraient être dépassées, à l'exception de l'exploitant de cet établissement et des membres de son personnel; | - entreprise extérieure : toute personne physique ou morale appelée à exécuter des activités de quelque nature que ce soit dans un établissement devant faire l'objet d'une autorisation ou d'une déclaration conformément aux dispositions découlant de l'article 17, au cours desquelles l'une des limites de dose fixées pour les personnes du public pourraient être dépassées, à l'exception de l'exploitant de cet établissement et des membres de son personnel; |
| - médecin agréé : le conseiller en prévention-médecin du travail travaillant dans un service interne ou externe pour la prévention et la protection au travail, compétent dans le domaine de la médecine du travail conformément aux dispositions de la loi du 4 août 1996 relative au bien-être des travailleurs dans la cadre de l'exécution de leur travail et à ses arrêtés d'exécution et qui, en outre, est agréé conformément aux mesures d'exécution prises en vertu des articles 3 et 19; | - médecin agréé : le conseiller en prévention-médecin du travail travaillant dans un service interne ou externe pour la prévention et la protection au travail, compétent dans le domaine de la médecine du travail conformément aux dispositions de la loi du 4 août 1996 relative au bien-être des travailleurs dans la cadre de l'exécution de leur travail et à ses arrêtés d'exécution et qui, en outre, est agréé conformément aux mesures d'exécution prises en vertu des articles 3 et 19; |
| - travailleur extérieur : toute personne soumise à la surveillance dosimétrique qui exécute chez un exploitant une mission comportant un risque d'exposition, qu'elle soit employée à titre temporaire ou permanent par une entreprise extérieure, ou qu'elle preste ses services en qualité de travailleur indépendant; | - travailleur extérieur : toute personne soumise à la surveillance dosimétrique qui exécute chez un exploitant une mission comportant un risque d'exposition, qu'elle soit employée à titre temporaire ou permanent par une entreprise extérieure, ou qu'elle preste ses services en qualité de travailleur indépendant; |
| - mission comportant un risque d'exposition : l'activité de quelque nature que ce soit prestée par un travailleur extérieur chez un exploitant au cours de laquelle l'une des limites de dose fixées pour les personnes du public pourrait être dépassée; | - mission comportant un risque d'exposition : l'activité de quelque nature que ce soit prestée par un travailleur extérieur chez un exploitant au cours de laquelle l'une des limites de dose fixées pour les personnes du public pourrait être dépassée; |
| - registre d'exposition : le système d'enregistrement centralisé des données dosimétriques des personnes soumises à la surveillance dosimétrique, visé à l'article 25/2; | - registre d'exposition : le système d'enregistrement centralisé des données dosimétriques des personnes soumises à la surveillance dosimétrique, visé à l'article 25/2; |
| - passeport radiologique : le document individuel établi pour les travailleurs extérieurs permettant d'assurer leur surveillance dosimétrique pendant les missions comportant un risque d'exposition qu'ils exécutent à l'étranger; | - passeport radiologique : le document individuel établi pour les travailleurs extérieurs permettant d'assurer leur surveillance dosimétrique pendant les missions comportant un risque d'exposition qu'ils exécutent à l'étranger; |

**COORDINATION DES ARTICLES**

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| - professionnel des soins de santé : le professionnel des soins de santé visé à l'article 7, § 4, de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et désigné au sein de l'Agence. Tant que les mesures d'exécution de la disposition précitée de la loi du 8 décembre 1992 ne sont pas prises, on entend par 'professionnel des soins de santé' : la personne titulaire du diplôme légal de docteur en médecine, chirurgie et accouchements; | - professionnel des soins de santé : le professionnel des soins de santé visé à l'article 7, § 4, de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et désigné au sein de l'Agence. Tant que les mesures d'exécution de la disposition précitée de la loi du 8 décembre 1992 ne sont pas prises, on entend par 'professionnel des soins de santé' : la personne titulaire du diplôme légal de docteur en médecine, chirurgie et accouchements; |
| - consultant en sécurité de l'information et protection de la vie privée : le consultant visé à l'article 4, § 5, de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la Sécurité sociale et désigné au sein de l'Agence; | - consultant en sécurité de l'information et protection de la vie privée : le consultant visé à l'article 4, § 5, de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la Sécurité sociale et désigné au sein de l'Agence; |
| - responsable du traitement : la personne visée à l'article 1er, § 4, de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, en l'occurrence l'Agence; | - responsable du traitement : la personne visée à l'article 1er, § 4, de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, en l'occurrence l'Agence; |
| - unité d'implantation : le lieu d'activité, géographiquement identifiable par une adresse, où s'exerce au moins une activité de l'entreprise ou à partir duquel elle est exercée; | - unité d'implantation : le lieu d'activité, géographiquement identifiable par une adresse, où s'exerce au moins une activité de l'entreprise ou à partir duquel elle est exercée; |
| - travailleur : le travailleur visé à l'article 2, § 1er, alinéas 1er et 2, 1°, de la loi du 4 août 1996 relative au bien-être des travailleurs lors de l'exécution de leur travail; | - travailleur : le travailleur visé à l'article 2, § 1er, alinéas 1er et 2, 1°, de la loi du 4 août 1996 relative au bien-être des travailleurs lors de l'exécution de leur travail; |
| - employeur : l'employeur visé à l'article 2, § 1er, alinéas 1er et 2, 2°, de la loi du 4 août 1996 relative au bien-être des travailleurs lors de l'exécution de leur travail; | - employeur : l'employeur visé à l'article 2, § 1er, alinéas 1er et 2, 2°, de la loi du 4 août 1996 relative au bien-être des travailleurs lors de l'exécution de leur travail; |
| - surveillance dosimétrique : la surveillance dosimétrique telle que visée à l'article 30.6 du Règlement général; | - surveillance dosimétrique : la surveillance dosimétrique telle que visée à l'article 30.6 du Règlement général; |
| - sources authentiques : le Registre national créé par la loi du 8 août 1983 organisant un Registre national des personnes physiques, la Banque-Carrefour des entreprises créée par la loi du 16 janvier 2003 portant création d'une Banque-Carrefour des Entreprises, modernisation du registre de commerce, création de guichets-entreprises agréés et portant diverses | - sources authentiques : le Registre national créé par la loi du 8 août 1983 organisant un Registre national des personnes physiques, la Banque-Carrefour des entreprises créée par la loi du 16 janvier 2003 portant création d'une Banque-Carrefour des Entreprises, modernisation du registre de commerce, création de guichets-entreprises agréés et portant diverses |

**COORDINATION DES ARTICLES**

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| dispositions, et les Registres de la Banque-Carrefour de la Sécurité sociale (Registre bis et Registre des radiés) créés par la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la Sécurité sociale; | dispositions, et les Registres de la Banque-Carrefour de la Sécurité sociale (Registre bis et Registre des radiés) créés par la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la Sécurité sociale; |
| - données anonymes : les données qui ne peuvent être mises en relation avec une personne identifiée ou identifiable et qui ne sont, en conséquence, pas des données à caractère personnel; | - données anonymes : les données qui ne peuvent être mises en relation avec une personne identifiée ou identifiable et qui ne sont, en conséquence, pas des données à caractère personnel; |
| | **- « la loi du xx xx 2018 » : la loi du xx xx 2018 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique ;** |
| (…) | **Art. 15ter. L'Agence est désignée comme service d'inspection, au sens de l'article 42 de la loi du xx 2018 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.** |
| **Loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges** | **Loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges** |
| **Art. 1er/1.** Les chapitres III et V transposent partiellement la Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la Directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la Directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le Règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs et la Directive 2009/140/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant les Directives | **Art. 1er/1.** Les chapitres III et V transposent partiellement la Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la Directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la Directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le Règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs et la Directive 2009/140/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant les Directives |

**COORDINATION DES ARTICLES**

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| 2002/21/CE relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, 2002/19/CE relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion, et 2002/20/CE relative à l'autorisation des réseaux et services de communications électroniques. | 2002/21/CE relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, 2002/19/CE relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion, et 2002/20/CE relative à l'autorisation des réseaux et services de communications électroniques.<br><br>**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. 14.** § 1er. Sans préjudice de ses compétences légales, les missions de l'Institut en ce qui concerne les réseaux de communications électroniques et les services de communications électroniques, équipement terminal équipement hertzien et en ce qui concerne les services postaux et les réseaux postaux publics tels que définis à l'article 2 de la loi du 26 janvier 2018 relative aux services postaux, sont les suivantes : | **Art. 14.** § 1er. Sans préjudice de ses compétences légales, les missions de l'Institut en ce qui concerne les réseaux de communications électroniques et les services de communications électroniques, équipement terminal équipement hertzien**, en ce qui concerne le secteur des infrastructures numériques au sens de la loi du xx 2018 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,** et en ce qui concerne les services postaux et les réseaux postaux publics tels que définis à l'article 2 de la loi du 26 janvier 2018 relative aux services postaux, sont les suivantes : |
| 1° la formulation d'avis d'initiative, dans les cas prévus par les lois et arrêtés ou à la demande du ministre ou de la Chambre des représentants; | 1° la formulation d'avis d'initiative, dans les cas prévus par les lois et arrêtés ou à la demande du ministre ou de la Chambre des représentants; |
| 2° la prise de décisions administratives; | 2° la prise de décisions administratives; |
| 3° le contrôle du respect de la loi du 13 juin 2005 relative aux communications électroniques, du Titre Ier, chapitre X et du Titre III de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, de la loi du 26 janvier 2018 relative aux services postaux, des 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, des articles 4 et 4/1 de la loi du 17 janvier 2003 concernant les recours et le | **3° le contrôle du respect des normes suivantes et de leurs arrêtés d'exécution :**<br><br>**a) la loi du 13 juin 2005 relative aux communications électroniques ;**<br><br>**b) le Titre I[er], chapitre X et le Titre III de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques ;** |

**COORDINATION DES ARTICLES**

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| 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, de la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale et de leurs arrêtés d'exécution, et du Règlement (UE) n° 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; | **c) la loi du 26 janvier 2018 relative aux services postaux ;**<br><br>**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 ;**<br><br>**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 ;**<br><br>**f) la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale ;**<br><br>**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 ;**<br><br>**h) la loi du xx 2018 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 ;**<br><br>**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.**<br><br>**Pour l'application de la loi du xx 2018 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.** |
| 4° en cas de litige entre des fournisseurs de réseaux, de services ou d'équipements de télécommunications ou en cas de litige entre des prestataires de services postaux, ou en cas de litige entre les fournisseurs de services ou de réseaux de communications électroniques ou de fournisseurs de | 4° en cas de litige entre des fournisseurs de réseaux, de services ou d'équipements de télécommunications ou en cas de litige entre des prestataires de services postaux, ou en cas de litige entre les fournisseurs de services ou de réseaux de communications électroniques ou de fournisseurs de |

**COORDINATION DES ARTICLES**

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| services de médias audiovisuels visés par la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale, la formulation de propositions tendant à concilier les parties dans le délai d'un mois. Le Roi fixe, sur avis de l'Institut, les modalités de cette procédure; | services de médias audiovisuels visés par la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale, la formulation de propositions tendant à concilier les parties dans le délai d'un mois. Le Roi fixe, sur avis de l'Institut, les modalités de cette procédure; |
| 4°/1 en cas de litige entre fournisseurs de réseaux, de services ou d'équipements de télécommunications ou en cas de litige entre des prestataires de services postaux, ou en cas de litige entre les fournisseurs de services ou de réseaux de communications électroniques ou de fournisseurs de services de médias audiovisuels visés par la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale, la prise de décision administrative sur base de l'article 4 ou 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; | 4°/1 en cas de litige entre fournisseurs de réseaux, de services ou d'équipements de télécommunications ou en cas de litige entre des prestataires de services postaux, ou en cas de litige entre les fournisseurs de services ou de réseaux de communications électroniques ou de fournisseurs de services de médias audiovisuels visés par la loi du 5 mai 2017 relative aux services de médias audiovisuels en région bilingue de Bruxelles-Capitale, la prise de décision administrative sur base de l'article 4 ou 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; |
| 5° poser tous les actes utiles qui ont pour objet la préparation de l'application des directives européennes entrées en vigueur dans le secteur des postes et des télécommunications. | 5° poser tous les actes utiles qui ont pour objet la préparation de l'application des directives européennes entrées en vigueur dans le secteur des postes et des télécommunications. |
| 6° L'Institut est chargé de contrôler l'exécution de toutes les missions de service public qui sont attribuées par l'Etat dans le secteur postal et dans le secteur des communications électroniques, sous réserve des missions de service publics attribué dans le cadre d'article 141, § 1erbis, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques. L'Institut informe tant le Ministre en charge du Secteur postal que le Ministre en charge des Entreprises publiques de l'exécution du contrat de gestion. | 6° L'Institut est chargé de contrôler l'exécution de toutes les missions de service public qui sont attribuées par l'Etat dans le secteur postal et dans le secteur des communications électroniques, sous réserve des missions de service publics attribué dans le cadre d'article 141, § 1erbis, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques. L'Institut informe tant le Ministre en charge du Secteur postal que le Ministre en charge des Entreprises publiques de l'exécution du contrat de gestion. |
| § 2. Dans le cadre de ses compétences, l'Institut : | § 2. Dans le cadre de ses compétences, l'Institut : |
| 1° peut organiser de manière non discriminatoire toute forme d'enquêtes et de consultations publiques ; il doit organiser de telles consultations publiques afin qu'il tienne compte des points de vue des utilisateurs finals, des consommateurs (y compris notamment, des consommateurs handicapés), des fabricants et des entreprises qui fournissent des réseaux et/ou des services de communications | 1° peut organiser de manière non discriminatoire toute forme d'enquêtes et de consultations publiques ; il doit organiser de telles consultations publiques afin qu'il tienne compte des points de vue des utilisateurs finals, des consommateurs (y compris notamment, des consommateurs handicapés), des fabricants et des entreprises qui fournissent des réseaux et/ou des services de communications |

**COORDINATION DES ARTICLES**

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| électroniques sur toute question relative à tous les droits des utilisateurs finals et des consommateurs en ce qui concerne les services de communications électroniques accessibles au public, en particulier lorsqu'ils ont une incidence importante sur le marché; ces consultations garantissent que, lorsque l'Institut statue sur des questions relatives aux droits des utilisateurs finals et des consommateurs en ce qui concerne les services de communications électroniques accessibles au public, les intérêts des consommateurs en matière de communications électroniques sont dûment pris en compte; | électroniques sur toute question relative à tous les droits des utilisateurs finals et des consommateurs en ce qui concerne les services de communications électroniques accessibles au public, en particulier lorsqu'ils ont une incidence importante sur le marché; ces consultations garantissent que, lorsque l'Institut statue sur des questions relatives aux droits des utilisateurs finals et des consommateurs en ce qui concerne les services de communications électroniques accessibles au public, les intérêts des consommateurs en matière de communications électroniques sont dûment pris en compte; |
| 2° peut exiger, par demande motivée, de toute personne concernée toute information utile. L'Institut fixe le délai de communication des informations demandées; | 2° peut exiger, par demande motivée, de toute personne concernée toute information utile. L'Institut fixe le délai de communication des informations demandées; |
| 3° coopère avec et communique de l'information à : | 3° coopère avec et communique de l'information à : |
| a) la Commission européenne , l'ENISA, l'Office et à l'ORECE; | a) la Commission européenne , l'ENISA, l'Office et à l'ORECE; |
| b) les autorités de régulation étrangères en matière de services postaux et de télécommunications; | b) les autorités de régulation étrangères en matière de services postaux et de télécommunications; |
| c) les autorités de régulation des autres secteurs économiques; | c) les autorités de régulation des autres secteurs économiques; |
| d) les services publics fédéraux en charge de la protection des consommateurs; | d) les services publics fédéraux en charge de la protection des consommateurs; |
| e) les autorités belges en charge de la concurrence; | e) les autorités belges en charge de la concurrence; |
| Après consultation de ces autorités et de l'Institut et sur proposition conjointe du ministre de l'Economie et du ministre, le Roi peut fixer les modalités de la coopération, de la consultation et de l'échange d'informations entre ces instances et l'Institut; | Après consultation de ces autorités et de l'Institut et sur proposition conjointe du ministre de l'Economie et du ministre, le Roi peut fixer les modalités de la coopération, de la consultation et de l'échange d'informations entre ces instances et l'Institut; |
| f) les autorités régulatrices des Communautés et des Régions, selon les modalités convenues dans les accords de coopération avec ces niveaux de pouvoir; | f) les autorités régulatrices des Communautés et des Régions, selon les modalités convenues dans les accords de coopération avec ces niveaux de pouvoir; |
| g) les services publics qui ont une compétence en matière de sécurité publique, ou de sécurité et protection civile, ou de défense civile, ou de planification de crise, ou de sécurité ou de protection du potentiel économique et scientifique du pays; | g) les services publics qui ont une compétence en matière de sécurité publique, ou de sécurité et protection civile, ou de défense civile, ou de planification de crise, ou de sécurité ou de protection du potentiel économique et scientifique du pays; |

**COORDINATION DES ARTICLES**

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| h) la Commission de la protection de la vie privée; | h) la Commission de la protection de la vie privée; |
| i) le Service public fédéral chargé des statistiques et de l'information économique. | i) le Service public fédéral chargé des statistiques et de l'information économique. |
| 4° apporte sa collaboration aux activités de la Commission mixte des télécommunications, créée par l'arrêté royal du 10 décembre 1957, modifié par l'arrêté royal du 24 septembre 1993; | 4° apporte sa collaboration aux activités de la Commission mixte des télécommunications, créée par l'arrêté royal du 10 décembre 1957, modifié par l'arrêté royal du 24 septembre 1993; |
| 5° l'Institut peut uniquement prendre des décisions relatives aux réseaux de communications électroniques pour lesquels les Communautés sont également compétentes, après l'entrée en vigueur d'un accord de coopération avec les Communautés portant sur l'exercice des compétences en matière de réseaux de communications électroniques. | 5° l'Institut peut uniquement prendre des décisions relatives aux réseaux de communications électroniques pour lesquels les Communautés sont également compétentes, après l'entrée en vigueur d'un accord de coopération avec les Communautés portant sur l'exercice des compétences en matière de réseaux de communications électroniques. |
| 6° peut procéder, en respectant les motifs de l'annulation et sans modifier l'étendue de son champ d'application, à la réfection d'une décision annulée par une autorité juridictionnelle lorsque, du fait de cette annulation, un ou plusieurs des objectifs visés aux articles 6 à 8 de la loi du 13 juin 2005 relative aux communications électroniques ne sont plus réalisés. L'Institut peut procéder à une même réfection lorsque la décision annulée concerne le secteur postal et qu'un ou plusieurs des objectifs suivants ne sont plus réalisés : | 6° peut procéder, en respectant les motifs de l'annulation et sans modifier l'étendue de son champ d'application, à la réfection d'une décision annulée par une autorité juridictionnelle lorsque, du fait de cette annulation, un ou plusieurs des objectifs visés aux articles 6 à 8 de la loi du 13 juin 2005 relative aux communications électroniques ne sont plus réalisés. L'Institut peut procéder à une même réfection lorsque la décision annulée concerne le secteur postal et qu'un ou plusieurs des objectifs suivants ne sont plus réalisés : |
| - veiller à la qualité et à la pérennité du service universel; | - veiller à la qualité et à la pérennité du service universel; |
| - veiller aux intérêts des utilisateurs des services postaux; | - veiller aux intérêts des utilisateurs des services postaux; |
| - contribuer au développement d'un marché intérieur des services postaux; | - contribuer au développement d'un marché intérieur des services postaux; |
| - promouvoir la concurrence dans le secteur postal. | - promouvoir la concurrence dans le secteur postal. |
| § 3. Dans le cadre de la coopération avec les autorités énumérées au point 3 du paragraphe précédent, les membres du Conseil et les membres du personnel de l'Institut peuvent communiquer à ces autorités des informations confidentielles dont ils ont connaissance dans l'exercice de leur fonction, dans la mesure où cette communication est nécessaire pour l'accomplissement des missions de ces autorités. | § 3. Dans le cadre de la coopération avec les autorités énumérées au point 3 du paragraphe précédent, les membres du Conseil et les membres du personnel de l'Institut peuvent communiquer à ces autorités des informations confidentielles dont ils ont connaissance dans l'exercice de leur fonction, dans la mesure où cette communication est nécessaire pour l'accomplissement des missions de ces autorités. |

## COORDINATION DES ARTICLES

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| **Art. 24.** Sur proposition de l'Institut, le Roi peut conférer la qualité d'officier de police judiciaire aux membres statutaires du personnel de l'Institut qu'il charge de la constatation des infractions à la loi du 6 juillet 1971 portant création de bpost et à certains services postaux à la loi du 13 juin 2005 relative aux communications électroniques, à la loi du 26 janvier 2018 relative aux services postaux, à la loi du 21 mars 1991 et à la loi du 30 mars 1995 concernant les réseaux de distribution d'émissions de radiodiffusion et l'exercice d'activités de radiodiffusion dans la région bilingue de Bruxelles-Capitale et à leurs arrêtés d'exécution ainsi qu'à l'arrêté royal du 18 mai 1994 concernant la compatibilité électromagnétique. | **Art. 24.** Sur proposition de l'Institut, le Roi peut conférer la qualité d'officier de police judiciaire aux membres statutaires du personnel de l'Institut qu'il charge de la constatation des infractions à la loi du 6 juillet 1971 portant création de bpost et à certains services postaux, à la loi du 13 juin 2005 relative aux communications électroniques, à la loi du 26 janvier 2018 relative aux services postaux, à la loi du 21 mars 1991 et à la loi du 30 mars 1995 concernant les réseaux de distribution d'émissions de radiodiffusion et l'exercice d'activités de radiodiffusion dans la région bilingue de Bruxelles-Capitale**, 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 2018, pour ce qui concerne le secteur des infrastructures numériques,** et à leurs arrêtés d'exécution ainsi qu'à l'arrêté royal du 18 mai 1994 concernant la compatibilité électromagnétique. |
| Ces membres du personnel sont également chargés de constater des infractions à la loi du 13 juin 2005 relative aux communications électroniques, au Code pénal et aux lois spéciales lorsque celles-ci sont commises au moyen d'équipements, de réseaux ou services de communications électroniques ou de radiocommunications au sens de la loi précitée relative aux communications électroniques. | Ces membres du personnel sont également chargés de constater des infractions à la loi du 13 juin 2005 relative aux communications électroniques, au Code pénal et aux lois spéciales lorsque celles-ci sont commises au moyen d'équipements, de réseaux ou services de communications électroniques ou de radiocommunications au sens de la loi précitée relative aux communications électroniques. |
| **Loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la Directive 2014/65/UE** | **Loi du 21 novembre 2017 relative aux infrastructures des marchés d'instruments financiers et portant transposition de la Directive 2014/65/UE** |
| **Art. 71.** La FSMA contrôle l'application des dispositions de la présente loi et des arrêtés et règlements pris pour son exécution ainsi que du Règlement 600/2014. | **Art. 71.** La FSMA contrôle l'application des dispositions de la présente loi et des arrêtés et règlements pris pour son exécution ainsi que du Règlement 600/2014 **et du titre 2 de la loi du […] 2018 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 […] 2018, 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. 79.** § 1er. Lorsque la FSMA constate une infraction aux dispositions de la présente loi ou des | **Art. 79.** § 1er. Lorsque la FSMA constate une infraction aux dispositions de la présente loi ou des |

## COORDINATION DES ARTICLES

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| arrêtés et règlements pris pour son exécution, ou du Règlement 600/2014, elle peut enjoindre à la personne responsable de l'infraction de remédier à la situation constatée dans le délai que la FSMA détermine et, le cas échéant, de s'abstenir de réitérer le comportement constitutif d'une infraction. La FSMA peut également enjoindre à toute personne physique ou morale ayant publié ou diffusé des informations fausses ou trompeuses de publier un communiqué rectificatif. | arrêtés et règlements pris pour son exécution, ou du Règlement 600/2014, elle peut enjoindre à la personne responsable de l'infraction de remédier à la situation constatée dans le délai que la FSMA détermine et, le cas échéant, de s'abstenir de réitérer le comportement constitutif d'une infraction. La FSMA peut également enjoindre à toute personne physique ou morale ayant publié ou diffusé des informations fausses ou trompeuses de publier un communiqué rectificatif. |
| Sans préjudice des autres mesures prévues par la loi, si la personne à laquelle elle a adressé une injonction en application de l'alinéa 1er reste en défaut à l'expiration du délai qui lui a été imparti, la FSMA peut, la personne ayant pu faire valoir ses moyens: | Sans préjudice des autres mesures prévues par la loi, si la personne à laquelle elle a adressé une injonction en application de l'alinéa 1er reste en défaut à l'expiration du délai qui lui a été imparti, la FSMA peut, la personne ayant pu faire valoir ses moyens: |
| 1° rendre publique sa position quant aux constatations faites en vertu de l'alinéa 1er, en précisant l'identité de la personne responsable de la violation et la nature de celle-ci. Les frais de cette publication sont à charge de la personne concernée; | 1° rendre publique sa position quant aux constatations faites en vertu de l'alinéa 1er, en précisant l'identité de la personne responsable de la violation et la nature de celle-ci. Les frais de cette publication sont à charge de la personne concernée; |
| 2° imposer le paiement d'une astreinte qui ne peut être, par jour calendrier de non-respect de l'injonction, supérieure à 50 000 euros, ni, au total, excéder 2 500 000 euros; | 2° imposer le paiement d'une astreinte qui ne peut être, par jour calendrier de non-respect de l'injonction, supérieure à 50 000 euros, ni, au total, excéder 2 500 000 euros; |
| Dans les cas urgents, la FSMA peut prendre les mesures visées à l'alinéa 2, 1°, sans injonction préalable en application de l'alinéa 1er, la personne ayant pu faire valoir ses moyens. Dans le cas également où la personne responsable de l'infraction n'est pas clairement identifiable, la FSMA peut, sans injonction préalable, publier un avertissement indiquant, le cas échéant, la nature de l'infraction. | Dans les cas urgents, la FSMA peut prendre les mesures visées à l'alinéa 2, 1°, sans injonction préalable en application de l'alinéa 1er, la personne ayant pu faire valoir ses moyens. Dans le cas également où la personne responsable de l'infraction n'est pas clairement identifiable, la FSMA peut, sans injonction préalable, publier un avertissement indiquant, le cas échéant, la nature de l'infraction. |
| § 2. Sans préjudice des autres mesures prévues par la loi, lorsque, conformément aux articles 70 à 72 de la loi du 2 août 2002, elle constate une infraction aux dispositions de la présente loi ou dans les arrêtés et règlements pris pour son exécution, ou du Règlement 600/2014, la FSMA peut infliger au contrevenant une amende administrative. | § 2. Sans préjudice des autres mesures prévues par la loi, lorsque, conformément aux articles 70 à 72 de la loi du 2 août 2002, elle constate une infraction aux dispositions de la présente loi ou dans les arrêtés et règlements pris pour son exécution, ou du Règlement 600/2014, la FSMA peut infliger au contrevenant une amende administrative. |
| Une amende administrative peut également être imposée à un ou plusieurs membres de l'organe légal d'administration et à toute personne chargée de la direction effective, ainsi que de toute autre personne | Une amende administrative peut également être imposée à un ou plusieurs membres de l'organe légal d'administration et à toute personne chargée de la direction effective, ainsi que de toute autre personne |

**COORDINATION DES ARTICLES**

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| physique, lorsque celle-ci est reconnue responsable de l'infraction. | physique, lorsque celle-ci est reconnue responsable de l'infraction. |
| § 3. Le montant des amendes administratives visées au paragraphe 2 est déterminé comme suit: | § 3. Le montant des amendes administratives visées au paragraphe 2 est déterminé comme suit: |
| 1° dans le cas d'une personne morale, le montant de l'amende administrative ne peut être supérieur, pour le même fait ou pour le même ensemble de faits, à 5 000 000 euros, ou, si le montant obtenu par application de ce pourcentage est plus élevé, à dix pour cent du chiffre d'affaire annuel total de la personne morale tel qu'il ressort des derniers comptes disponibles établis par l'organe de direction. Si la personne morale concernée ne réalise pas de chiffre d'affaires, il y a lieu d'entendre par "chiffre d'affaires annuel total" le type de revenus correspondant au chiffre d'affaires, soit conformément aux directives comptables européennes pertinentes, soit, si celles-ci ne sont pas applicables à la personne morale concernée, conformément au droit interne de l'Etat membre dans lequel la personne morale a son siège statutaire. Lorsque la personne morale est une entreprise mère ou une filiale de l'entreprise mère qui est tenue d'établir des comptes financiers consolidés, le chiffre d'affaires annuel total à prendre en considération est le chiffre d'affaires annuel total, tel qu'il ressort des derniers comptes consolidés disponibles approuvés par l'organe de direction de l'entreprise mère ultime; | 1° dans le cas d'une personne morale, le montant de l'amende administrative ne peut être supérieur, pour le même fait ou pour le même ensemble de faits, à 5 000 000 euros, ou, si le montant obtenu par application de ce pourcentage est plus élevé, à dix pour cent du chiffre d'affaire annuel total de la personne morale tel qu'il ressort des derniers comptes disponibles établis par l'organe de direction. Si la personne morale concernée ne réalise pas de chiffre d'affaires, il y a lieu d'entendre par "chiffre d'affaires annuel total" le type de revenus correspondant au chiffre d'affaires, soit conformément aux directives comptables européennes pertinentes, soit, si celles-ci ne sont pas applicables à la personne morale concernée, conformément au droit interne de l'Etat membre dans lequel la personne morale a son siège statutaire. Lorsque la personne morale est une entreprise mère ou une filiale de l'entreprise mère qui est tenue d'établir des comptes financiers consolidés, le chiffre d'affaires annuel total à prendre en considération est le chiffre d'affaires annuel total, tel qu'il ressort des derniers comptes consolidés disponibles approuvés par l'organe de direction de l'entreprise mère ultime; |
| 2° dans le cas d'une personne physique, le montant de l'amende administrative ne peut être supérieur, pour le même fait ou pour le même ensemble de faits, à 5 000 000 euros. | 2° dans le cas d'une personne physique, le montant de l'amende administrative ne peut être supérieur, pour le même fait ou pour le même ensemble de faits, à 5 000 000 euros. |
| Nonobstant ce qui précède, lorsque la violation a procuré un profit au contrevenant ou a permis à ce dernier d'éviter une perte, ce maximum peut être porté au double du montant de ce profit ou de cette perte. | Nonobstant ce qui précède, lorsque la violation a procuré un profit au contrevenant ou a permis à ce dernier d'éviter une perte, ce maximum peut être porté au double du montant de ce profit ou de cette perte. |
| | **§ 4. En cas de violation des dispositions applicables de la loi du […] 2018 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.** |

## COORDINATION DES ARTICLES

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| **Loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers** | **Loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers** |
| **Art. 75.** § 1er. Par dérogation à l'article 74, alinéa 1er, et dans les limites du droit de l'Union européenne la FSMA peut communiquer des informations confidentielles : | **Art. 75.** § 1er. Par dérogation à l'article 74, alinéa 1er, et dans les limites du droit de l'Union européenne la FSMA peut communiquer des informations confidentielles : |
| 1° à la Banque centrale européenne, à la Banque et aux autres banques centrales et organismes à vocation similaire en leur qualité d'autorités monétaires, ainsi qu'à d'autres autorités publiques chargées de la surveillance des systèmes de paiement et de règlement; | 1° à la Banque centrale européenne, à la Banque et aux autres banques centrales et organismes à vocation similaire en leur qualité d'autorités monétaires, ainsi qu'à d'autres autorités publiques chargées de la surveillance des systèmes de paiement et de règlement; |
| à la Banque centrale européenne, à la Banque et aux autres banques centrales et organismes à vocation similaire en leur qualité d'autorités monétaires lorsque ces informations sont pertinentes pour l'exercice de leurs missions légales respectives, notamment la conduite de la politique monétaire et la fourniture de liquidité y afférente, la surveillance des systèmes de paiement, de compensation et de règlement, ainsi que la sauvegarde de la stabilité du système financier, de même qu'à d'autres autorités publiques chargées de la surveillance des systèmes de paiement. | à la Banque centrale européenne, à la Banque et aux autres banques centrales et organismes à vocation similaire en leur qualité d'autorités monétaires lorsque ces informations sont pertinentes pour l'exercice de leurs missions légales respectives, notamment la conduite de la politique monétaire et la fourniture de liquidité y afférente, la surveillance des systèmes de paiement, de compensation et de règlement, ainsi que la sauvegarde de la stabilité du système financier, de même qu'à d'autres autorités publiques chargées de la surveillance des systèmes de paiement. |
| Lorsque survient une situation d'urgence, notamment une évolution défavorable des marchés financiers, susceptible de menacer la liquidité du marché et la stabilité du système financier dans un des Etats membres dans lequel des entités d'un groupe comprenant des entreprises d'investissement ont été agréées ou dans lequel sont établies des succursales d'importance significative au sens de l'article 59, §§ 6 et 7, de la loi du 25 octobre 2016, la FSMA peut transmettre des informations aux banques centrales du Système européen de banques centrales lorsque ces informations sont pertinentes pour l'exercice de leurs missions légales, notamment la conduite de la politique monétaire et la fourniture de liquidité y afférente, la surveillance des systèmes de paiement, de compensation et de règlement, ainsi que la sauvegarde de la stabilité du système financier. | Lorsque survient une situation d'urgence, notamment une évolution défavorable des marchés financiers, susceptible de menacer la liquidité du marché et la stabilité du système financier dans un des Etats membres dans lequel des entités d'un groupe comprenant des entreprises d'investissement ont été agréées ou dans lequel sont établies des succursales d'importance significative au sens de l'article 59, §§ 6 et 7, de la loi du 25 octobre 2016, la FSMA peut transmettre des informations aux banques centrales du Système européen de banques centrales lorsque ces informations sont pertinentes pour l'exercice de leurs missions légales, notamment la conduite de la politique monétaire et la fourniture de liquidité y afférente, la surveillance des systèmes de paiement, de compensation et de règlement, ainsi que la sauvegarde de la stabilité du système financier. |
| En cas de situation d'urgence telle que visée ci-dessus, la FSMA peut divulguer, dans tous les Etats membres concernés, des informations qui | En cas de situation d'urgence telle que visée ci-dessus, la FSMA peut divulguer, dans tous les Etats membres concernés, des informations qui |

**COORDINATION DES ARTICLES**

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| présentent un intérêt pour les départements d'administrations centrales responsables de la législation relative à la surveillance des établissements de crédit, des établissements financiers, des services d'investissement et des entreprises d'assurances; | présentent un intérêt pour les départements d'administrations centrales responsables de la législation relative à la surveillance des établissements de crédit, des établissements financiers, des services d'investissement et des entreprises d'assurances; |
| 1° bis à la Banque, à la Banque centrale européenne en ce qui concerne les missions qui lui sont confiées par le Règlement (UE) n° 1024/2013 du Conseil du 15 octobre 2013 confiant à la Banque centrale européenne des missions spécifiques ayant trait aux politiques en matière de surveillance prudentielle des établissements de crédit et aux autres membres du SEBC; | 1° bis à la Banque, à la Banque centrale européenne en ce qui concerne les missions qui lui sont confiées par le Règlement (UE) n° 1024/2013 du Conseil du 15 octobre 2013 confiant à la Banque centrale européenne des missions spécifiques ayant trait aux politiques en matière de surveillance prudentielle des établissements de crédit et aux autres membres du SEBC; |
| 2° à l'Agence Fédérale de la Dette; | 2° à l'Agence Fédérale de la Dette; |
| 3° aux autorités compétentes d'autres Etats membres de l'Espace économique européen qui exercent une ou plusieurs compétences comparables à celles visées à l'article 45; | 3° aux autorités compétentes d'autres Etats membres de l'Espace économique européen qui exercent une ou plusieurs compétences comparables à celles visées à l'article 45; |
| 4° aux autorités compétentes d'Etats tiers qui exercent une ou plusieurs compétences comparables à celles visées à l'article 45 et avec lesquels la FSMA a conclu un accord de coopération prévoyant un échange d'informations; | 4° aux autorités compétentes d'Etats tiers qui exercent une ou plusieurs compétences comparables à celles visées à l'article 45 et avec lesquels la FSMA a conclu un accord de coopération prévoyant un échange d'informations; |
| 5° et aux autorités de régulation nationales visées à l'article 2, point 10, du règlement 1227/2011 et, pour ce qui est du règlement 596/2014, à la Commission européenne et aux autres autorités visées à l'article 25 de ce règlement; | 5° et aux autorités de régulation nationales visées à l'article 2, point 10, du règlement 1227/2011 et, pour ce qui est du règlement 596/2014, à la Commission européenne et aux autres autorités visées à l'article 25 de ce règlement; |
| 6° aux organismes belges ou d'un autre Etat membre de l'Espace économique européen gérant un système de protection des dépôts, des investisseurs ou des assurances sur la vie; | 6° aux organismes belges ou d'un autre Etat membre de l'Espace économique européen gérant un système de protection des dépôts, des investisseurs ou des assurances sur la vie; |
| 7° aux contreparties centrales ou aux dépositaires centraux de titres qui sont autorisés à assurer des services de compensation ou de règlement de transactions sur instruments financiers effectuées sur un marché organisé belge, dans la mesure où la FSMA estime que la communication des informations en question est nécessaire en vue de garantir le fonctionnement régulier de ces organismes par rapport à des manquements, même potentiels, d'intervenants sur le marché concerné; | 7° aux contreparties centrales ou aux dépositaires centraux de titres qui sont autorisés à assurer des services de compensation ou de règlement de transactions sur instruments financiers effectuées sur un marché organisé belge, dans la mesure où la FSMA estime que la communication des informations en question est nécessaire en vue de garantir le fonctionnement régulier de ces organismes par rapport à des manquements, même potentiels, d'intervenants sur le marché concerné; |

## COORDINATION DES ARTICLES

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| 8° aux opérateurs de marché pour le bon fonctionnement, le contrôle et la surveillance des marchés qu'ils organisent; | 8° aux opérateurs de marché pour le bon fonctionnement, le contrôle et la surveillance des marchés qu'ils organisent; |
| 9° au cours de procédures civiles ou commerciales, aux autorités et mandataires de justice impliqués dans des procédures de faillite ou de réorganisation judiciaire ou des procédures collectives analogues concernant des entreprises soumises au contrôle de la FSMA ou dont les opérations sont soumises à son contrôle, à l'exception des informations confidentielles concernant la participation de tiers à des tentatives de sauvetage antérieures à ces procédures; | 9° au cours de procédures civiles ou commerciales, aux autorités et mandataires de justice impliqués dans des procédures de faillite ou de réorganisation judiciaire ou des procédures collectives analogues concernant des entreprises soumises au contrôle de la FSMA ou dont les opérations sont soumises à son contrôle, à l'exception des informations confidentielles concernant la participation de tiers à des tentatives de sauvetage antérieures à ces procédures; |
| 10° aux commissaires et réviseurs d'entreprises et aux autres contrôleurs légaux des comptes des entreprises soumises au contrôle de la FSMA, d'autres établissements financiers belges ou d'entreprises similaires étrangères; | 10° aux commissaires et réviseurs d'entreprises et aux autres contrôleurs légaux des comptes des entreprises soumises au contrôle de la FSMA, d'autres établissements financiers belges ou d'entreprises similaires étrangères; |
| 11° aux séquestres, pour l'exercice de leur mission visée dans les lois régissant les missions confiées à la FSMA; | 11° aux séquestres, pour l'exercice de leur mission visée dans les lois régissant les missions confiées à la FSMA; |
| 12° au Collège de supervision des réviseurs d'entreprises et aux autorités d'Etats membres ou de pays tiers investies de la surveillance des personnes chargées du contrôle légal des comptes annuels des entreprises soumises au contrôle de la FSMA; | 12° au Collège de supervision des réviseurs d'entreprises et aux autorités d'Etats membres ou de pays tiers investies de la surveillance des personnes chargées du contrôle légal des comptes annuels des entreprises soumises au contrôle de la FSMA; |
| 13° au Service public fédéral Economie, PME, Classes moyennes et Energie pour le contrôle relatif au crédit à la consommation, et pour le contrôle relatif au crédit hypothécaire aux pratiques du marché et aux services de paiement, aux autorités compétentes d'autres Etats membres de l'Espace économique européen qui exercent une compétence comparable, ainsi qu'aux autorités compétentes d'Etats tiers qui exercent une compétence comparable et avec lesquelles la FSMA a conclu un accord de coopération prévoyant un échange d'informations; | 13° au Service public fédéral Economie, PME, Classes moyennes et Energie pour le contrôle relatif au crédit à la consommation, et pour le contrôle relatif au crédit hypothécaire aux pratiques du marché et aux services de paiement, aux autorités compétentes d'autres Etats membres de l'Espace économique européen qui exercent une compétence comparable, ainsi qu'aux autorités compétentes d'Etats tiers qui exercent une compétence comparable et avec lesquelles la FSMA a conclu un accord de coopération prévoyant un échange d'informations; |
| 14° à l'Autorité belge de la concurrence; | 14° à l'Autorité belge de la concurrence; |
| 15° (…) | **15° dans les limites du droit de l'Union européenne, les autorités visées à l'article 7 de la loi du xx 2018 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour** |

**COORDINATION DES ARTICLES**

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| | **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 ;** |
| 16° à l'administration de la Trésorerie, en vertu des dispositions légales et réglementaires prises pour la mise en oeuvre des mesures d'embargos financiers. | 16° à l'administration de la Trésorerie, en vertu des dispositions légales et réglementaires prises pour la mise en oeuvre des mesures d'embargos financiers. |
| 17° aux actuaires indépendants des entreprises exerçant, en vertu de la loi, une tâche de contrôle sur ces entreprises ainsi qu'aux organes chargés de la surveillance de ces actuaires; | 17° aux actuaires indépendants des entreprises exerçant, en vertu de la loi, une tâche de contrôle sur ces entreprises ainsi qu'aux organes chargés de la surveillance de ces actuaires; |
| 18° à Fedris ; | 18° à Fedris ; |
| 19° à l'Office de contrôle des mutualités et des unions nationales de mutualités, en sa qualité d'autorité de contrôle des sociétés mutualistes visées aux articles 43bis, § 5, et 70, §§ 6, 7 et 8, de la loi du 6 août 1990 relative aux mutualités et aux unions nationales de mutualités, ainsi que de leurs opérations. | 19° à l'Office de contrôle des mutualités et des unions nationales de mutualités, en sa qualité d'autorité de contrôle des sociétés mutualistes visées aux articles 43bis, § 5, et 70, §§ 6, 7 et 8, de la loi du 6 août 1990 relative aux mutualités et aux unions nationales de mutualités, ainsi que de leurs opérations. |
| 19° (...) | 19° (...) |
| 20° (…) | 20° (…) |
| 21° à l'ESMA, l'EIOPA et l'EBA et au Comité européen du risque systémique. | 21° à l'ESMA, l'EIOPA et l'EBA et au Comité européen du risque systémique. |
| 22° aux autorités investies de la surveillance des personnes exerçant des activités sur les marchés des quotas d'émission; | 22° aux autorités investies de la surveillance des personnes exerçant des activités sur les marchés des quotas d'émission; |
| 23° aux autorités investies de la surveillance des personnes exerçant des activités sur les marchés dérivés de matières premières agricoles; | 23° aux autorités investies de la surveillance des personnes exerçant des activités sur les marchés dérivés de matières premières agricoles; |
| 24° à l'Autorité belge de protection des données; | 24° à l'Autorité belge de protection des données; |
| 4° à la Cellule de traitement des informations financières, visée à l'article 76 de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces. | 4° à la Cellule de traitement des informations financières, visée à l'article 76 de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces. |
| § 2. La FSMA ne peut communiquer des informations confidentielles en vertu du § 1er qu'à condition | § 2. La FSMA ne peut communiquer des informations confidentielles en vertu du § 1er qu'à condition |

**COORDINATION DES ARTICLES**

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| qu'elles soient destinées à l'accomplissement des missions des autorités ou organismes qui en sont les destinataires et que les informations soient dans leur chef couvertes par un devoir de secret professionnel équivalent à celui prévu à l'article 74. En outre, les informations provenant d'une autorité d'un autre Etat membre de l'Espace économique européen ne peuvent être divulguées dans les cas visés aux 7°, 9° et 12° et 17° du § 1er ainsi qu'à des autorités ou organismes d'Etat tiers dans les cas visés aux 4°, 6°, 10° et 13° du § 1er qu'avec l'accord explicite de cette autorité et, le cas échéant, aux seules fins pour lesquelles cette autorité a marqué son accord. | qu'elles soient destinées à l'accomplissement des missions des autorités ou organismes qui en sont les destinataires et que les informations soient dans leur chef couvertes par un devoir de secret professionnel équivalent à celui prévu à l'article 74. En outre, les informations provenant d'une autorité d'un autre Etat membre de l'Espace économique européen ne peuvent être divulguées dans les cas visés aux 7°, 9° et 12° et 17° du § 1er ainsi qu'à des autorités ou organismes d'Etat tiers dans les cas visés aux 4°, 6°, 10° et 13° du § 1er qu'avec l'accord explicite de cette autorité et, le cas échéant, aux seules fins pour lesquelles cette autorité a marqué son accord. |
| § 3. La FSMA peut faire usage des informations confidentielles visées à l'article 74, alinéa 1er, ou reçues de la part des autorités et organismes visés au § 1er pour l'accomplissement de l'ensemble de ses missions visées à l'article 45. | § 3. La FSMA peut faire usage des informations confidentielles visées à l'article 74, alinéa 1er, ou reçues de la part des autorités et organismes visés au § 1er pour l'accomplissement de l'ensemble de ses missions visées à l'article 45. |
| § 4. Sans préjudice des dispositions plus sévères des lois particulières qui les régissent, les autorités et organismes belges visés au § 1er sont tenus au secret professionnel prévu à l'article 74 quant aux informations confidentielles qu'ils reçoivent de la FSMA en application du § 1er. | § 4. Sans préjudice des dispositions plus sévères des lois particulières qui les régissent, les autorités et organismes belges visés au § 1er sont tenus au secret professionnel prévu à l'article 74 quant aux informations confidentielles qu'ils reçoivent de la FSMA en application du § 1er. |
| § 5. Le présent article s'applique sans préjudice de dispositions plus restrictives du droit de l'Union européenne en matière de secret professionnel directement applicables. | § 5. Le présent article s'applique sans préjudice de dispositions plus restrictives du droit de l'Union européenne en matière de secret professionnel directement applicables. |
| **Loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique** | **Loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique** |
| **Art. 36/1.** Définitions : Pour l'application du présent chapitre et du chapitre VII, il y a lieu d'entendre par : | **Art. 36/1.** Définitions : Pour l'application du présent chapitre et du chapitre VII, il y a lieu d'entendre par : |
| 1° " la loi du 2 août 2002 " : la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers; | 1° " la loi du 2 août 2002 " : la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers; |
| 2° " instrument financier " : un instrument tel que défini à l'article 2, 1° de la loi du 2 août 2002; | 2° " instrument financier " : un instrument tel que défini à l'article 2, 1° de la loi du 2 août 2002; |
| 3° " établissement de crédit " : tout établissement visé au Livre II et aux Titres Ier et II du Livre III de la loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourse; | 3° " établissement de crédit " : tout établissement visé au Livre II et aux Titres Ier et II du Livre III de la loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourse; |

## COORDINATION DES ARTICLES

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| 4° "établissement de monnaie électronique" : tout établissement visé à l'article 2, 74° de la loi du 11 mars 2018 relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement et à l'activité d'émission de monnaie électronique, et à l'accès aux systèmes de paiement; | 4° "établissement de monnaie électronique" : tout établissement visé à l'article 2, 74° de la loi du 11 mars 2018 relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement et à l'activité d'émission de monnaie électronique, et à l'accès aux systèmes de paiement; |
| 5° " entreprise d'investissement ayant le statut de société de bourse " : toute entreprise d'investissement visée au Livre XII de la loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourse agréée en qualité de société de bourse ou autorisée à prester des services d'investissement qui, s'ils étaient prestés par une entreprise d'investissement belge, nécessiteraient l'obtention d'un agrément en tant que société de bourse; | 5° " entreprise d'investissement ayant le statut de société de bourse " : toute entreprise d'investissement visée au Livre XII de la loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourse agréée en qualité de société de bourse ou autorisée à prester des services d'investissement qui, s'ils étaient prestés par une entreprise d'investissement belge, nécessiteraient l'obtention d'un agrément en tant que société de bourse; |
| 6° "entreprise d'assurance ou de réassurance": toute entreprise visée à l'article 5, alinéa 1er, 1°, ou 2°, de la loi du 13 mars 2016. relative au statut et au contrôle des entreprises d'assurance ou de réassurance; | 6° "entreprise d'assurance ou de réassurance": toute entreprise visée à l'article 5, alinéa 1er, 1°, ou 2°, de la loi du 13 mars 2016. relative au statut et au contrôle des entreprises d'assurance ou de réassurance; |
| 7° (…) | 7° (…) |
| 8° " société de cautionnement mutuel " : toute société visée à l'article 57 de la loi-programme du 10 février 1998 pour la promotion de l'entreprise indépendante; | 8° " société de cautionnement mutuel " : toute société visée à l'article 57 de la loi-programme du 10 février 1998 pour la promotion de l'entreprise indépendante; |
| 9° "établissement de paiement" : tout établissement visé à l'article 2, 8° de la loi du 11 mars 2018 relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement et à l'activité d'émission de monnaie électronique, et à l'accès aux systèmes de paiement; | 9° "établissement de paiement" : tout établissement visé à l'article 2, 8° de la loi du 11 mars 2018 relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement et à l'activité d'émission de monnaie électronique, et à l'accès aux systèmes de paiement; |
| 10° " marché réglementé " : tout marché réglementé belge ou étranger; | 10° " marché réglementé " : tout marché réglementé belge ou étranger; |
| 11° " marché réglementé belge " : un système multilatéral, exploité et/ou géré par une entreprise de marché, qui assure ou facilite la rencontre - en son sein même et selon ses règles non discrétionnaires - | 11° " marché réglementé belge " : un système multilatéral, exploité et/ou géré par une entreprise de marché, qui assure ou facilite la rencontre - en son sein même et selon ses règles non discrétionnaires - |

**COORDINATION DES ARTICLES**

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| de multiples intérêts acheteurs et vendeurs exprimés par des tiers pour des instruments financiers, d'une manière qui aboutisse à la conclusion de contrats portant sur des instruments financiers admis à la négociation dans le cadre de ses règles et/ou de ses systèmes, et qui est agréé et fonctionne régulièrement conformément aux dispositions du chapitre II de la loi du 2 août 2002; | de multiples intérêts acheteurs et vendeurs exprimés par des tiers pour des instruments financiers, d'une manière qui aboutisse à la conclusion de contrats portant sur des instruments financiers admis à la négociation dans le cadre de ses règles et/ou de ses systèmes, et qui est agréé et fonctionne régulièrement conformément aux dispositions du chapitre II de la loi du 2 août 2002; |
| 12° " marché réglementé étranger " : tout marché d'instruments financiers qui est organisé par une entreprise de marché dont l'Etat d'origine est un Etat membre de l'Espace économique européen autre que la Belgique et qui a été agréé dans cet Etat membre en qualité de marché réglementé en application du titre III de la Directive 2014/65/UE; | 12° " marché réglementé étranger " : tout marché d'instruments financiers qui est organisé par une entreprise de marché dont l'Etat d'origine est un Etat membre de l'Espace économique européen autre que la Belgique et qui a été agréé dans cet Etat membre en qualité de marché réglementé en application du titre III de la Directive 2014/65/UE; |
| 13° "contrepartie centrale" : une contrepartie centrale telle que définie à l'article 2, 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; | 13° "contrepartie centrale" : une contrepartie centrale telle que définie à l'article 2, 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; |
| 14° " organisme de liquidation " : tout établissement assurant la liquidation d'ordres de transfert d'instruments financiers, de droits relatifs à ces instruments financiers ou d'opérations à terme sur devises, avec ou non règlement en espèces; | 14° " organisme de liquidation " : tout établissement assurant la liquidation d'ordres de transfert d'instruments financiers, de droits relatifs à ces instruments financiers ou d'opérations à terme sur devises, avec ou non règlement en espèces; |
| 15° " FSMA " : l'Autorité des services et marchés financiers, en allemand " Kommission für das Bank-, Finanz- und Versicherungswesen "; | 15° " FSMA " : l'Autorité des services et marchés financiers, en allemand " Kommission für das Bank-, Finanz- und Versicherungswesen "; |
| 16° "autorité compétente" : la Banque, la FSMA ou l'autorité désignée par chaque Etat membre en application de l'article 67 de la Directive 2014/65/UE, de l'article 22 du Règlement 648/2012 ou de l'article 11 du Règlement 909/2014, à moins que la Directive et les Règlements respectifs n'en disposent autrement; | 16° "autorité compétente" : la Banque, la FSMA ou l'autorité désignée par chaque Etat membre en application de l'article 67 de la Directive 2014/65/UE, de l'article 22 du Règlement 648/2012 ou de l'article 11 du Règlement 909/2014, à moins que la Directive et les Règlements respectifs n'en disposent autrement; |
| 17° "la Directive 2014/65/UE" : la Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE; | 17° "la Directive 2014/65/UE" : la Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE; |
| 18° " CREFS " : le Comité des risques et établissements financiers systémiques. | 18° " CREFS " : le Comité des risques et établissements financiers systémiques. |

**COORDINATION DES ARTICLES**

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| 19° " institution de retraite professionnelle " : l'établissement visé à l'article 2, 1°, de la loi du 27 octobre 2006 relative au contrôle des institutions de retraite professionnelle; | 19° " institution de retraite professionnelle " : l'établissement visé à l'article 2, 1°, de la loi du 27 octobre 2006 relative au contrôle des institutions de retraite professionnelle; |
| 20° " l'Autorité bancaire européenne " : l'Autorité bancaire européenne instituée par le Règlement n° 1093/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité bancaire européenne), modifiant la Décision n° 716/2009/CE et abrogeant la Décision 2009/78/CE de la Commission; | 20° " l'Autorité bancaire européenne " : l'Autorité bancaire européenne instituée par le Règlement n° 1093/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité bancaire européenne), modifiant la Décision n° 716/2009/CE et abrogeant la Décision 2009/78/CE de la Commission; |
| 21° " l'Autorité européenne des assurances et des pensions professionnelles " : l'Autorité européenne des assurances et des pensions professionnelles instituée par le Règlement n° 1094/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité européenne des assurances et des pensions professionnelles), modifiant la Décision n° 716/2009/CE et abrogeant la Décision 2009/79/CE de la Commission; | 21° " l'Autorité européenne des assurances et des pensions professionnelles " : l'Autorité européenne des assurances et des pensions professionnelles instituée par le Règlement n° 1094/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité européenne des assurances et des pensions professionnelles), modifiant la Décision n° 716/2009/CE et abrogeant la Décision 2009/79/CE de la Commission; |
| 21°/1 " l'Autorité européenne des marchés financiers " : l'Autorité européenne des marchés financiers instituée par le Règlement 1095/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité européenne des marchés financiers), modifiant la Décision n° 716/2009/CE et abrogeant la Décision 2009/77/CE de la Commission. | 21°/1 " l'Autorité européenne des marchés financiers " : l'Autorité européenne des marchés financiers instituée par le Règlement 1095/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité européenne des marchés financiers), modifiant la Décision n° 716/2009/CE et abrogeant la Décision 2009/77/CE de la Commission. |
| 22° "le Règlement 648/2012" : le 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; | 22° "le Règlement 648/2012" : le 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; |
| 23° "contrepartie financière" : une contrepartie telle que définie à l'article 2, 8) du Règlement 648/2012 ou à l'article 3, 3) du Règlement 2015/2365; | 23° "contrepartie financière" : une contrepartie telle que définie à l'article 2, 8) du Règlement 648/2012 ou à l'article 3, 3) du Règlement 2015/2365; |
| 24° "contrepartie non financière" : une contrepartie telle que définie à l'article 2, 9) du Règlement 648/2012 ou à l'article 3, 4) du Règlement 2015/2365; | 24° "contrepartie non financière" : une contrepartie telle que définie à l'article 2, 9) du Règlement 648/2012 ou à l'article 3, 4) du Règlement 2015/2365; |

## COORDINATION DES ARTICLES

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| 25° "dépositaire central de titres" : un dépositaire central de titres tel que défini à l'article 2, paragraphe 1er, 1) du Règlement 909/2014; | 25° "dépositaire central de titres" : un dépositaire central de titres tel que défini à l'article 2, paragraphe 1er, 1) du Règlement 909/2014; |
| 26° "le Règlement 909/2014" : le Règlement (UE) n° 909/2014 du Parlement européen et du Conseil du 23 juillet 2014 concernant l'amélioration du règlement de titres dans l'Union européenne et les dépositaires centraux de titres, et modifiant les directives 98/26/CE et 2014/65/UE ainsi que le Règlement (UE) n° 236/2012; | 26° "le Règlement 909/2014" : le Règlement (UE) n° 909/2014 du Parlement européen et du Conseil du 23 juillet 2014 concernant l'amélioration du règlement de titres dans l'Union européenne et les dépositaires centraux de titres, et modifiant les directives 98/26/CE et 2014/65/UE ainsi que le Règlement (UE) n° 236/2012; |
| 27° "le Règlement 2015/2365" : le Règlement (UE) 2015/2365 du Parlement européen et du Conseil du 25 novembre 2015 relatif à la transparence des opérations de financement sur titres et de la réutilisation et modifiant le règlement (UE) n° 648/2012. | 27° "le Règlement 2015/2365" : le Règlement (UE) 2015/2365 du Parlement européen et du Conseil du 25 novembre 2015 relatif à la transparence des opérations de financement sur titres et de la réutilisation et modifiant le règlement (UE) n° 648/2012. |
| | **28° « la loi du xx xx 2018 » : la loi du xx xx 2018 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.** |
| **Art. 36/14.** § 1er. Par dérogation à l'article 35, la Banque peut également communiquer des informations confidentielles : | **Art. 36/14.** § 1er. Par dérogation à l'article 35, la Banque peut également communiquer des informations confidentielles : |
| 1° à la Banque centrale européenne et aux autres banques centrales et organismes à vocation similaire en leur qualité d'autorités monétaires lorsque ces informations sont pertinentes pour l'exercice de leurs missions légales respectives, notamment la conduite de la politique monétaire et la fourniture de liquidité y afférente, la surveillance des systèmes de paiement, de compensation et de règlement, ainsi que la sauvegarde de la stabilité du système financier, de même qu'à d'autres autorités publiques chargées de la surveillance des systèmes de paiement. | 1° à la Banque centrale européenne et aux autres banques centrales et organismes à vocation similaire en leur qualité d'autorités monétaires lorsque ces informations sont pertinentes pour l'exercice de leurs missions légales respectives, notamment la conduite de la politique monétaire et la fourniture de liquidité y afférente, la surveillance des systèmes de paiement, de compensation et de règlement, ainsi que la sauvegarde de la stabilité du système financier, de même qu'à d'autres autorités publiques chargées de la surveillance des systèmes de paiement. |
| Lorsque survient une situation d'urgence, notamment une évolution défavorable des marchés financiers, susceptible de menacer la liquidité du marché et la stabilité du système financier dans un des Etats membres dans lequel des entités d'un groupe comprenant des établissements de crédit ou des entreprises d'investissement ont été agréées ou dans lequel sont établies des succursales d'importance significative au sens de l'article 3, 65° | Lorsque survient une situation d'urgence, notamment une évolution défavorable des marchés financiers, susceptible de menacer la liquidité du marché et la stabilité du système financier dans un des Etats membres dans lequel des entités d'un groupe comprenant des établissements de crédit ou des entreprises d'investissement ont été agréées ou dans lequel sont établies des succursales d'importance significative au sens de l'article 3, 65° |

## COORDINATION DES ARTICLES

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| de la loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourse la Banque peut transmettre des informations aux banques centrales du Système européen de banques centrales lorsque ces informations sont pertinentes pour l'exercice de leurs missions légales, notamment la conduite de la politique monétaire et la fourniture de liquidité y afférente, la surveillance des systèmes de paiement, de compensation et de règlement, ainsi que la sauvegarde de la stabilité du système financier. | de la loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourse la Banque peut transmettre des informations aux banques centrales du Système européen de banques centrales lorsque ces informations sont pertinentes pour l'exercice de leurs missions légales, notamment la conduite de la politique monétaire et la fourniture de liquidité y afférente, la surveillance des systèmes de paiement, de compensation et de règlement, ainsi que la sauvegarde de la stabilité du système financier. |
| En cas de situation d'urgence telle que visée ci-dessus, la Banque peut divulguer, dans tous les Etats membres concernés, des informations qui présentent un intérêt pour les départements d'administrations centrales responsables de la législation relative à la surveillance des établissements de crédit, des établissements financiers, des services d'investissement et des entreprises d'assurances; | En cas de situation d'urgence telle que visée ci-dessus, la Banque peut divulguer, dans tous les Etats membres concernés, des informations qui présentent un intérêt pour les départements d'administrations centrales responsables de la législation relative à la surveillance des établissements de crédit, des établissements financiers, des services d'investissement et des entreprises d'assurances; |
| 2° dans les limites des directives européennes, aux autorités compétentes de l'Union européenne et d'autres Etats membres de l'Espace économique européen qui exercent une ou plusieurs compétences comparables à celles visées aux articles 36/2 et 36/3, y compris la Banque centrale européenne en ce qui concerne les missions qui lui sont confiées par le Règlement (UE) n° 1024/2013 du Conseil du 15 octobre 2013 confiant à la Banque centrale européenne des missions spécifiques ayant trait aux politiques en matière de surveillance prudentielle des établissements de crédit; | 2° dans les limites des directives européennes, aux autorités compétentes de l'Union européenne et d'autres Etats membres de l'Espace économique européen qui exercent une ou plusieurs compétences comparables à celles visées aux articles 36/2 et 36/3, y compris la Banque centrale européenne en ce qui concerne les missions qui lui sont confiées par le Règlement (UE) n° 1024/2013 du Conseil du 15 octobre 2013 confiant à la Banque centrale européenne des missions spécifiques ayant trait aux politiques en matière de surveillance prudentielle des établissements de crédit; |
| 3° dans le respect des directives européennes, aux autorités compétentes d'Etats tiers qui exercent une ou plusieurs compétences comparables à celles visées aux articles 36/2 et 36/3 et avec lesquelles la Banque a conclu un accord de coopération prévoyant un échange d'informations; | 3° dans le respect des directives européennes, aux autorités compétentes d'Etats tiers qui exercent une ou plusieurs compétences comparables à celles visées aux articles 36/2 et 36/3 et avec lesquelles la Banque a conclu un accord de coopération prévoyant un échange d'informations; |
| 4° à la FSMA; | 4° à la FSMA; |
| 5° aux organismes belges ou d'un autre Etat membre de l'Espace économique européen gérant un système de protection des dépôts, des investisseurs ou des assurances sur la vie et à l'organe chargé des dispositifs de financement pour la résolution; | 5° aux organismes belges ou d'un autre Etat membre de l'Espace économique européen gérant un système de protection des dépôts, des investisseurs ou des assurances sur la vie et à l'organe chargé des dispositifs de financement pour la résolution; |

## COORDINATION DES ARTICLES

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| 6° aux contreparties centrales, aux organismes de liquidation d'instruments financiers ou aux dépositaires centraux de titres qui sont autorisés à assurer des services de compensation ou de liquidation de transactions sur instruments financiers effectuées sur un marché réglementé belge, dans la mesure où la Banque estime que la communication des informations en question est nécessaire en vue de garantir le fonctionnement régulier de ces contreparties centrales, organismes de liquidation et dépositaires centraux de titres par rapport à des manquements, même potentiels, d'intervenants sur le marché concerné; | 6° aux contreparties centrales, aux organismes de liquidation d'instruments financiers ou aux dépositaires centraux de titres qui sont autorisés à assurer des services de compensation ou de liquidation de transactions sur instruments financiers effectuées sur un marché réglementé belge, dans la mesure où la Banque estime que la communication des informations en question est nécessaire en vue de garantir le fonctionnement régulier de ces contreparties centrales, organismes de liquidation et dépositaires centraux de titres par rapport à des manquements, même potentiels, d'intervenants sur le marché concerné; |
| 7° dans les limites des directives européennes, aux entreprises de marché pour le bon fonctionnement, le contrôle et la surveillance des marchés que celles-ci organisent; | 7° dans les limites des directives européennes, aux entreprises de marché pour le bon fonctionnement, le contrôle et la surveillance des marchés que celles-ci organisent; |
| 8° au cours de procédures civiles ou commerciales, aux autorités et mandataires de justice impliqués dans des procédures de faillite ou de réorganisation judiciaire ou des procédures collectives analogues concernant des établissements soumis au contrôle de la Banque, à l'exception des informations confidentielles concernant la participation de tiers à des tentatives de sauvetage antérieures à ces procédures; | 8° au cours de procédures civiles ou commerciales, aux autorités et mandataires de justice impliqués dans des procédures de faillite ou de réorganisation judiciaire ou des procédures collectives analogues concernant des établissements soumis au contrôle de la Banque, à l'exception des informations confidentielles concernant la participation de tiers à des tentatives de sauvetage antérieures à ces procédures; |
| 9° aux commissaires et réviseurs d'entreprises et aux autres contrôleurs légaux des comptes des établissements soumis au contrôle de la Banque, d'autres établissements financiers belges ou d'établissements étrangers similaires; | 9° aux commissaires et réviseurs d'entreprises et aux autres contrôleurs légaux des comptes des établissements soumis au contrôle de la Banque, d'autres établissements financiers belges ou d'établissements étrangers similaires; |
| 10° aux séquestres, pour l'exercice de leur mission visée par les lois régissant les missions confiées à la Banque; | 10° aux séquestres, pour l'exercice de leur mission visée par les lois régissant les missions confiées à la Banque; |
| 11° au Collège de supervision des réviseurs d'entreprises et aux autorités d'Etats membres ou de pays tiers investies de la surveillance des personnes chargées du contrôle légal des comptes annuels des établissements soumis au contrôle de la Banque; | 11° au Collège de supervision des réviseurs d'entreprises et aux autorités d'Etats membres ou de pays tiers investies de la surveillance des personnes chargées du contrôle légal des comptes annuels des établissements soumis au contrôle de la Banque; |
| 12° dans les limites du droit de l'Union européenne, à l'Autorité belge de la concurrence; | 12° dans les limites du droit de l'Union européenne, à l'Autorité belge de la concurrence; |

## COORDINATION DES ARTICLES

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| 13° dans les limites des directives européennes, au conseil d'agrément des agents de change visé à l'article 21 de la loi du 2 août 2002; | 13° dans les limites des directives européennes, au conseil d'agrément des agents de change visé à l'article 21 de la loi du 2 août 2002; |
| 14° dans les limites des directives européennes, à l'Administration générale de la Trésorerie, en vertu des dispositions légales et réglementaires prises pour la mise en oeuvre des mesures d'embargos financiers; | 14° dans les limites des directives européennes, à l'Administration générale de la Trésorerie, en vertu des dispositions légales et réglementaires prises pour la mise en oeuvre des mesures d'embargos financiers; |
| 15° dans les limites des directives européennes, aux actuaires indépendants des établissements exerçant, en vertu de la loi, une tâche de contrôle sur ces établissements ainsi qu'aux organes chargés de la surveillance de ces actuaires; | 15° dans les limites des directives européennes, aux actuaires indépendants des établissements exerçant, en vertu de la loi, une tâche de contrôle sur ces établissements ainsi qu'aux organes chargés de la surveillance de ces actuaires; |
| 16° à Fedris; | 16° à Fedris; |
| 17° aux agents commissionnés par le ministre qui dans le cadre de leur mission viséé à l'article XV. 2 du Code de droit économique sont compétents pour rechercher et constater les infractions aux dispositions de l'article XV. 89, 1° à 18°, 20°, 21°, 22° et 23°, du Code de droit économique; | 17° aux agents commissionnés par le ministre qui dans le cadre de leur mission viséé à l'article XV. 2 du Code de droit économique sont compétents pour rechercher et constater les infractions aux dispositions de l'article XV. 89, 1° à 18°, 20°, 21°, 22° et 23°, du Code de droit économique; |
| 18° aux autorités relevant du droit d'Etats membres de l'Union européenne compétentes dans le domaine de la surveillance macroprudentielle ainsi qu'au Comité européen du risque systémique institué par le Règlement (UE) n° 1092/2010 du Parlement européen et du Conseil du 24 novembre 2010; | 18° aux autorités relevant du droit d'Etats membres de l'Union européenne compétentes dans le domaine de la surveillance macroprudentielle ainsi qu'au Comité européen du risque systémique institué par le Règlement (UE) n° 1092/2010 du Parlement européen et du Conseil du 24 novembre 2010; |
| 19° dans les limites des règlements et directives européens, à l'Autorité européenne des marchés financiers, à l'Autorité européenne des assurances et des pensions professionnelles et à l'Autorité bancaire européenne; | 19° dans les limites des règlements et directives européens, à l'Autorité européenne des marchés financiers, à l'Autorité européenne des assurances et des pensions professionnelles et à l'Autorité bancaire européenne; |
| 20° dans les limites du droit de l'Union européenne, au Centre gouvernemental de Coordination et de Crise du SPF Intérieur, à l'Organe de coordination pour l'analyse de la menace, institué par la loi du 10 juillet 2006 relative à l'analyse de la menace, et aux services de police visés par la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux, dans la mesure où l'application de l'article 19 de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques le requiert; | 20° dans les limites du droit de l'Union européenne, au Centre gouvernemental de Coordination et de Crise du SPF Intérieur, à l'Organe de coordination pour l'analyse de la menace, institué par la loi du 10 juillet 2006 relative à l'analyse de la menace, **à l'autorité visé à l'article 7, §1er, de la loi du xx 2018**, et aux services de police visés par la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux, dans la mesure où l'application de l'article 19 de la loi du 1er juillet 2011 |

**COORDINATION DES ARTICLES**

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| | relative à la sécurité et la protection des infrastructures critiques le requiert; |
| 21° à l'Office de contrôle des mutualités et des unions nationales de mutualités, pour l'exercice de ses missions légales visées à l'article 303, § 3, de la loi du 13 mars 2016 relative au statut et au contrôle des entreprises d'assurance ou de réassurance, en ce qui concerne les sociétés mutualistes visées à l'article 43bis, § 5, ou à l'article 70, §§ 6, 7 et 8, de la loi du 6 août 1990 relative aux mutualités et aux unions nationales de mutualités et leurs opérations; | 21° à l'Office de contrôle des mutualités et des unions nationales de mutualités, pour l'exercice de ses missions légales visées à l'article 303, § 3, de la loi du 13 mars 2016 relative au statut et au contrôle des entreprises d'assurance ou de réassurance, en ce qui concerne les sociétés mutualistes visées à l'article 43bis, § 5, ou à l'article 70, §§ 6, 7 et 8, de la loi du 6 août 1990 relative aux mutualités et aux unions nationales de mutualités et leurs opérations; |
| 22° dans les limites du droit de l'Union européenne, aux autorités de résolution visées à l'article 3 de la Directive 2014/59/UE du Parlement européen et du Conseil du 15 mai 2014 établissant un cadre pour le redressement et la résolution des établissements de crédit et des entreprises d'investissement, aux autorités d'Etats tiers chargées de missions équivalentes à celles visées à l'article 12ter, § 1er avec lesquelles la Banque a conclu un accord de coopération prévoyant un échange d'information, ainsi qu'aux ministères compétents des Etats membres de l'Espace économique européen lorsque cela s'avère nécessaire à la planification ou à la réalisation d'une action de résolution; | 22° dans les limites du droit de l'Union européenne, aux autorités de résolution visées à l'article 3 de la Directive 2014/59/UE du Parlement européen et du Conseil du 15 mai 2014 établissant un cadre pour le redressement et la résolution des établissements de crédit et des entreprises d'investissement, aux autorités d'Etats tiers chargées de missions équivalentes à celles visées à l'article 12ter, § 1er avec lesquelles la Banque a conclu un accord de coopération prévoyant un échange d'information, ainsi qu'aux ministères compétents des Etats membres de l'Espace économique européen lorsque cela s'avère nécessaire à la planification ou à la réalisation d'une action de résolution; |
| 23° à toute personne exerçant une tâche, prévue par ou en vertu de la loi, qui participe ou contribue à l'exercice de la mission de contrôle de la Banque lorsque cette personne a été désignée par ou avec l'accord de la Banque et aux fins de cette tâche, telle notamment: | 23° à toute personne exerçant une tâche, prévue par ou en vertu de la loi, qui participe ou contribue à l'exercice de la mission de contrôle de la Banque lorsque cette personne a été désignée par ou avec l'accord de la Banque et aux fins de cette tâche, telle notamment: |
| a) le surveillant de portefeuille visé à l'article 16 de l'Annexe III à la loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourse; | a) le surveillant de portefeuille visé à l'article 16 de l'Annexe III à la loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourse; |
| b) le gestionnaire de portefeuille visé à l'article 8 de l'Annexe III à la loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourse; et | b) le gestionnaire de portefeuille visé à l'article 8 de l'Annexe III à la loi du 25 avril 2014 relative au statut et au contrôle des établissements de crédit et des sociétés de bourse; et |
| c) le commissaire spécial visé à l'article 236, § 1er, 1°, de la loi précitée, à l'article 517, § 1er, 1°, de la loi du 13 mars 2016 relative au statut et au contrôle des entreprises d'assurance ou de réassurance, l'article 35, § 1er, alinéa 2, 1°, de la loi du 21 décembre 2009 | c) le commissaire spécial visé à l'article 236, § 1er, 1°, de la loi précitée, à l'article 517, § 1er, 1°, de la loi du 13 mars 2016 relative au statut et au contrôle des entreprises d'assurance ou de réassurance, l'article 35, § 1er, alinéa 2, 1°, de la loi du 21 décembre 2009 |

**COORDINATION DES ARTICLES**

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| relative au statut des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement, à l'activité d'émission de monnaie électronique et à l'accès aux systèmes de paiement, l'article 87, § 1er, alinéa 2, 1°, de la loi précitée, l'article 48, alinéa 1er, 1°, de l'arrêté royal du 30 avril 1999 réglementant le statut et le contrôle des sociétés de cautionnement mutuel et l'article 36/30, § 1er, alinéa 2, 3°, de la présente loi. | relative au statut des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement, à l'activité d'émission de monnaie électronique et à l'accès aux systèmes de paiement, l'article 87, § 1er, alinéa 2, 1°, de la loi précitée, l'article 48, alinéa 1er, 1°, de l'arrêté royal du 30 avril 1999 réglementant le statut et le contrôle des sociétés de cautionnement mutuel et l'article 36/30, § 1er, alinéa 2, 3°, de la présente loi. |
| | **24° dans les limites du droit de l'Union européenne, aux autorités visées à l'article 7 de la loi du xx 2018 pour les besoins de l'exécution des dispositions de la loi du xx 2018 et de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.** |
| § 2. La Banque ne peut communiquer des informations confidentielles en vertu du § 1er qu'à la condition qu'elles soient destinées à l'accomplissement des missions des autorités ou organismes qui en sont les destinataires et que les informations soient dans leur chef couvertes par un devoir de secret professionnel équivalent à celui prévu à l'article 35. En outre, les informations provenant d'une autorité d'un autre Etat membre de l'Espace économique européen ne peuvent être divulguées dans les cas visés aux 7°, 9°, 10°, 12°, et 16° du § 1er, ainsi qu'à des autorités ou organismes d'Etats tiers dans les cas visés aux 4°, 6° et 10° du § 1er, qu'avec l'accord explicite de cette autorité et, le cas échéant, aux seules fins pour lesquelles cette autorité a marqué son accord. | § 2. La Banque ne peut communiquer des informations confidentielles en vertu du § 1er qu'à la condition qu'elles soient destinées à l'accomplissement des missions des autorités ou organismes qui en sont les destinataires et que les informations soient dans leur chef couvertes par un devoir de secret professionnel équivalent à celui prévu à l'article 35. En outre, les informations provenant d'une autorité d'un autre Etat membre de l'Espace économique européen ne peuvent être divulguées dans les cas visés aux 7°, 9°, 10°, 12°, et 16° du § 1er, ainsi qu'à des autorités ou organismes d'Etats tiers dans les cas visés aux 4°, 6° et 10° du § 1er, qu'avec l'accord explicite de cette autorité et, le cas échéant, aux seules fins pour lesquelles cette autorité a marqué son accord. |
| § 3. Sans préjudice des dispositions plus sévères des lois particulières qui les régissent, les personnes, autorités et organismes belges visés au § 1er sont tenus au secret professionnel prévu à l'article 35 quant aux informations confidentielles qu'ils reçoivent de la Banque en application du § 1er. | § 3. Sans préjudice des dispositions plus sévères des lois particulières qui les régissent, les personnes, autorités et organismes belges visés au § 1er sont tenus au secret professionnel prévu à l'article 35 quant aux informations confidentielles qu'ils reçoivent de la Banque en application du § 1er. |
| § 4. Le présent article s'applique sans préjudice des dispositions plus restrictives du droit de l'Union européenne en matière de secret professionnel. | § 4. Le présent article s'applique sans préjudice des dispositions plus restrictives du droit de l'Union européenne en matière de secret professionnel. |
| | **(…)** |
| | **Chapitre IV/4 Surveillance par la Banque dans le cadre de la loi du … 2018 établissant un cadre pour** |

**COORDINATION DES ARTICLES**

| TEXTE EN VIGUEUR | PROJET DE LOI |
|---|---|
| | **la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.**<br><br>**Art. 36/47. «Pour l'application de la loi du xx 2018, 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.**<br><br>**La Commission des sanctions statue sur l'imposition des amendes administratives prévues à l'article 52 de la loi du ... 2018. Les articles 36/8 à 36/12/3 et l'article 36/21 sont applicables.**<br><br>**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 … 2018.** |

**Advies nr. 84/2018 van 14 september 2018**

**Betreft:** Wetsontwerp tot vaststelling van een kader voor de beveiliging van netwerk –en informatiesystemen van algemeen belang voor de openbare veiligheid (CO-A-2018-070)

De Gegevensbeschermingsautoriteit (hierna "de Autoriteit");

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit*, inzonderheid de artikelen 23 en 26;

Gelet op het verzoek om advies van Dhr. Michel, Eerste Minister, ontvangen op 20 juli 2018;

Gelet op het verslag van Dhr. F. De Smet;

Brengt op 14 september 2018 het volgend advies uit:

## I. VOORWERP EN CONTEXT VAN DE ADVIESAANVRAAG

1. De Eerste Minister (hierna "de aanvrager") verzocht op 20 juli 2018 het advies van de Autoriteit over een wetsontwerp *tot vaststelling van een kader voor de beveiliging van netwerk –en informatiesystemen van algemeen belang voor de openbare veiligheid* (hierna "het Ontwerp").

2. Het Ontwerp beoogt 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 Richtlijn"). De verplichtingen vervat in de richtlijn gelden voornamelijk voor entiteiten die, ingeval van een incident dat de beveiliging van hun netwerk –en informatiesystemen aantast, de verlening van essentiële diensten en van digitale diensten voor het behoud van kritieke maatschappelijke of economische activiteiten aanzienlijk kunnen verstoren[1]. De richtlijn heeft met name tot doel ervoor te zorgen dat technische –en organisatorische beveiligingsmaatregelen worden genomen door de aanbieders van essentiële diensten en door digitale dienstverleners om incidenten te voorkomen of de impact ervan te beperken, teneinde de continuïteit van deze diensten te waarborgen. In dezelfde geest heeft de in de Richtlijn vervatte meldingsplicht van incidenten betrekking op de incidenten die een aanzienlijke impact hebben op de verleende diensten[2].

3. Verschillende autoriteiten worden belast met de uitvoering van de bepalingen in het Ontwerp. De Koning zal met name meerdere autoriteiten aanwijzen die de volgende rollen zullen opnemen[3]:

   - Nationale autoriteit, die belast is met de opvolging en coördinatie van de uitvoering van deze wet. Deze nationale autoriteit is ook het "Centraal Nationaal Contactpunt". Dit betreft een verbindingsfunctie – gecreëerd door de Richtlijn – die moet zorgen voor Europese samenwerking;
   - Nationaal Computer Security Incident Response Team (hierna het "NCSIRT"), dat belast is met de ontvangst en behandeling van meldingen van incidenten door aanbieders van essentiële diensten en digitale dienstverlener, alsook van meldingen vanuit andere landen;

---

[1] Het betreft bijvoorbeeld elektriciteitsbedrijven, waterleveranciers, luchtvaartmaatschappijen, Kredietinstellingen, zorginstellingen, enz. (zie bijlage 1 bij het Ontwerp).

[2] P. 1 t.e.m. 3 van de Memorie van Toelichting bij het Ontwerp.

[3] Zie artikel 7 van het Ontwerp.

- Sectorale Overheden[4] & Sectorale Computer Security Incident Response Teams (hierna "SCSIRT"), die binnen hun sector belast zijn met het toezicht op de uitvoering van de bepalingen van het Ontwerp;
- Een autoriteit die belast is met *"de actualisering van de nationale strategie voor de beveiliging van netwerk –informatiesystemen"*[5];
- Inspectiediensten die toezien op de naleving van het Ontwerp en haar uitvoeringsbesluiten door de aanbieders van essentiële diensten of digitale dienstverleners.

4. In de context van het Ontwerp zullen (minstens) de volgende gegevensverwerkingen plaatsvinden:
   - algemene informatie-uitwisseling vanuit de aanbieders van essentiële diensten en digitale dienstverleners naar de in randnummer 3 bedoelde autoriteiten en vanuit laatstgenoemde autoriteiten naar andere (buitenlandse) autoriteiten[6];
   - verwerken van informatie die de in randnummer 3 opgesomde autoriteiten ontvangen vanwege de aanbieders van essentiële diensten en vanuit de digitale dienstverleners
     - bij de aanmelding van hun *"contactpunt voor de computerbeveiliging"*[7];
     - in het kader van meldingen van incidenten[8];
   - verwerkingen door de inspectiediensten[9] (cf randnummer 3, laatste bullet) in het kader van het toezicht op de aanbieders van essentiële diensten en digitale dienstverleners en dit met name voor wat betreft de naleving van de beveiligingsvereisten of de eisen inzake het melden van incidenten. Artikel 44 van het Ontwerp verschaft deze inspectiediensten ruime onderzoeksbevoegdheden. Ze kunnen met name *"overgaan tot elk onderzoek, elke controle en elk verhoor"* en ze kunnen alle inlichtingen inwinnen die zij nodig achten voor de uitoefening van hun opdracht[10];
   - verwerkingen door de Hoven en Rechtbanken (bij strafrechtelijke procedures) of door de "sectorale overheden"[11] (bij administratiefrechtelijke procedures) in het kader van de sanctionering van inbreuken op het Ontwerp;

---

[4] Zij zullen o.a. instaan voor de identificatie van de aanbieders van essentiële diensten binnen hun sector (cf. artikel 11 Ontwerp).

[5] Artikel 10, §1, van het Ontwerp.

[6] Artikel 9 van het Ontwerp.

[7] Artikelen 23 & 34 van het Ontwerp.

[8] Artikelen 24 e.v. & 35 e.v. van het Ontwerp.

[9] -Zie randnummer 3, laatste bullet.
-Zie Titel 4: Hoofdstuk 1, afdeling 2 & Hoofdstuk 2 van het Ontwerp.

[10] Artikel 44, §3, 3°, van het Ontwerp.

[11] Zie randnummer 3, derde bullet.

- verwerkingen door het NCSIRT en de SCSIRT in het kader van het beheer van veiligheidsincidenten[12].

## II. ONDERZOEK VAN DE ADVIESAANVRAAG

### 1. Algemene opmerkingen

5. De Autoriteit staat heel positief ten aanzien van de *ratio legis* van het Ontwerp: welbepaalde netwerk –en informatiesystemen die van belang zijn voor de openbare veiligheid zo goed mogelijk beveiligen. Zoals de Memorie van Toelichting bij het Ontwerp (p. 3) correct aangeeft, sluit een dergelijk beheer van veiligheidsrisico's aan bij het opzet van de AVG.

6. Zij staat ook gunstig ten aanzien van de samenwerkingsplicht tussen de in randnummer 3 opgesomde instanties en de Autoriteit[13], alsook ten aanzien van het gemeenschappelijk platform dat zal gecreëerd worden om incidenten te melden[14]. Specifiek ten aanzien van voornoemd meldingsplatform, vestigt de Autoriteit er wel de aandacht op dat er – gelet op het in de AVG vervatte principe van de 'verantwoordingsplicht' – bij de uitbouw van dit platform dient over gewaakt te worden dat het de verantwoordelijkheid van de verwerkingsverantwoordelijke blijft om te beslissen bij welke instantie(s) hij een melding doet en bij welke niet. De realisatie van dit platform kan met andere woorden niet tot gevolg hebben dat deze verantwoordelijkheid van de verwerkingsverantwoordelijke wordt 'verschoven' naar één of meerdere instanties die via dit platform meldingen ontvangen.

7. Verder wijst de Autoriteit er op dat er in de praktijk tal van raakvlakken zullen opduiken tussen de bepalingen in het Ontwerp en de regels inzake dataprotectie. In dit verband onderlijnt de Autoriteit ook dat de AVG onverminderd van toepassing blijft op verwerkingen van persoonsgegevens die in de context van het Ontwerp zullen plaatsvinden. Alle actoren die onderworpen zijn aan de bepalingen in het Ontwerp, zullen dus – voor zover zij persoonsgegevens verwerken – tegelijk rekening moeten houden met de regelgeving inzake dataprotectie. Nochtans zouden zij verkeerdelijk de indruk kunnen krijgen dat ze volledig legaal handelen indien ze enkel de regels in het Ontwerp respecteren terwijl ze misschien de AVG uit het oog verliezen. De Autoriteit pleit er daarom voor om

---

[12] Zie Titel 5 van het Ontwerp.

[13] Artikel 8, §2, van het Ontwerp. De artikelen 48 & 52 van de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit* laat de Autoriteit overigens ook toe om in onderhavige context samen te werken met andere actoren.

[14] Artikel 31, §1, laatste lid & artikel 36, §3, van het Ontwerp.

- in het Ontwerp een bepaling op te nemen die het principe vastlegt dat het Ontwerp geen afbreuk doet aan de AVG en de daarbij horende nationale uitvoeringswetten[15];
- in de Memorie van Toelichting bij het Ontwerp te wijzen op specifieke gelijkenissen en verschillen tussen de regels in het Ontwerp en de verplichtingen in de AVG[16].

## 2. Doeleinde

8. Volgens artikel 5.1.b) AVG is de verwerking van persoonsgegevens enkel toegestaan voor welbepaalde uitdrukkelijk omschreven en gerechtvaardigde doeleinden. De Autoriteit stelt vast dat het Ontwerp een – weliswaar algemeen - duidelijk en legitiem doel beoogt: ervoor zorgen dat technische –en organisatorische beveiligingsmaatregelen worden genomen door de aanbieders van essentiële diensten om incidenten te voorkomen of de impact ervan te beperken, teneinde de continuïteit van essentiële diensten te waarborgen. Tegelijk pleit de Autoriteit ervoor om de subfinaliteit van elke aparte categorie van verwerkingen (cf. randnummer 4), expliciet in het Ontwerp op te nemen (cf. randnummer 12).

## 3. Rechtsgrondslag

9. Elke verwerking van persoonsgegevens moet steunen op een rechtsgrondslag in de zin van artikel 6 AVG. Bovendien is de verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten aan strikte voorwaarden onderworpen (artikel 10 AVG).

10. Voor de verwerking van persoonsgegevens die niet behoren tot de bijzondere categorieën van artikelen 9 & 10 AVG, kan het Ontwerp wellicht steunen op de volgende twee rechtsgronden:

    - artikel 6.1.c) voor wat de verwerkingen betreft die uitgevoerd worden door de aanbieders van essentiële diensten en de digitale dienstverleners. Zij delen

---

[15] Artikel 2 van de Richtlijn lijkt dit toe te laten, aangezien deze bepaling verwijst naar de klassieke regels inzake dataprotectie (met name naar de oude Richtlijn 95/46/EG, die intussen door de AVG vervangen werd) voor wat de verwerking van persoonsgegevens betreft die in onderhavige context zullen plaatsvinden.

[16] Ter illustratie:

- De artikelen 24 e.v. & 35 e.v. van het Ontwerp leggen een meldingsplicht op voor beveiligingsincidenten, terwijl de artikelen 33 & 34 AVG in een meldingsplicht voorzien voor *"inbreuken in verband met persoonsgegevens"*;
- Artikel 23, §1, van het Ontwerp voorziet in een aanmeldingsplicht voor het *"contactpunt voor de beveiliging van netwerk –en informatiesystemen"* en artikel 37.7 AVG bepaalt dat de contactgegevens van de functionaris voor gegevensbescherming aan de toezichthoudende autoriteit moeten medegedeeld worden.

immers bepaalde persoonsgegevens mee aan de actoren bedoeld in randnummer 3, omdat ze hiertoe verplicht worden door het Ontwerp;

- artikel 6.1. e) AVG voor wat de verwerkingen betreft die worden verricht door de actoren bedoeld in randnummer 3. Zij vervullen immers een taak van algemeen belang.

11. De Autoriteit vestigt hierbij de aandacht op artikel 6.3 AVG dat -in samenlezing met artikel 8 EVRM en artikel 22 van de Grondwet-[17] voorschrijft dat regelgeving die de verwerking van persoonsgegevens omkadert, in principe minstens volgende essentiële elementen van die verwerking zou moet vermelden:
    - het doel van de verwerking;
    - de types of categorieën van te verwerken persoonsgegevens;
    - de betrokkenen;
    - de entiteiten waaraan en doeleinden waarvoor de persoonsgegevens mogen worden verstrekt;
    - opslagperioden;
    - evenals de aanduiding van de verwerkingsverantwoordelijke.

12. Het Ontwerp dient in voormelde zin te worden gepreciseerd en aangevuld. Dit zou bijvoorbeeld kunnen door in Titel 6 van het Ontwerp een artikel op te nemen waarin per type verwerking (zie hoger randnummer 4) minstens het doel van de verwerking wordt gepreciseerd. Ook de andere essentiële elementen van de verwerkingen moeten in deze nieuwe bepaling worden opgenomen tenzij hiervoor in een delegatie aan de Koning zou worden voorzien.

13. Hierbij aansluitend vestigt de Autoriteit ook de aandacht op artikel 20 van de Kaderwet inzake dataprotectie[18], dat aan federale overheden[19] de verplichting oplegt om protocolakkoorden af te sluiten voor gegevensuitwisselingen die op artikel 6.1.e) AVG gebaseerd zijn.

---

[17] Zie arresten van het Grondwettelijk Hof: Arrest nr. 44/2015 van 23 april 2015 (p. 63), Arrest nr. 108/2017 van 5 oktober 2017 (p. 17) en Arrest nr. 29/2018 van 15 maart 2018 (p. 26).

[18] Wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens*

[19] Een Vlaams Decreet legt overigens gelijkaardige verplichtingen op aan Vlaamse Overheidsdiensten (Cf Artikel 16 van het decreet van 8 juni 2018 *houdende de aanpassing van de decreten aan de verordening (EU) 2016/679 van het Europees Parlement en de Raad 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)*)

14. Verder stelt de Autoriteit vast dat er ook gegevens zullen worden verwerkt betreffende strafrechtelijke veroordelingen en strafbare feiten[20], wat verwerkingen betreft die krachtens artikel 10 AVG enkel toegestaan zijn onder toezicht van een overheid (of indien de verwerking is toegestaan bij Unierechtelijk of lidstaatrechtelijke bepalingen die passende waarborgen voor de rechten en vrijheden van de betrokkenen bieden). *In casu* zal de verwerking van dit type gegevens uitgevoerd worden onder toezicht van een overheid, met name de actoren bedoeld in randnummer 3, wat strookt met artikel 10 AVG. Deze bepaling uit de AVG dient overigens eveneens samengelezen te worden met de artikelen 6 AVG[21], 22 GW en 8 EVRM, wat impliceert dat – ook al vindt de verwerking van dit type van gegevens plaats onder toezicht van een overheid – de essentiële elementen van de verwerking van dit type van gegevens eveneens in de regelgeving dienen vastgelegd te worden, wat *in casu* nog onvoldoende het geval is (zie randnummers 11-12).

## 4. Principe van de minimale gegevensverwerking

15. Artikel 5.1.c) AVG bepaalt dat persoonsgegevens beperkt moeten zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt ("minimale gegevensverwerking").

16. De Autoriteit constateert vooreerst dat in artikel 9, §3, laatste lid, van het Ontwerp[22] het principe is opgenomen dat uitgewisselde informatie beperkt dient te worden tot *"hetgeen relevant is voor en evenredig is met het doel van die uitwisseling"*. De Autoriteit adviseert om een gelijkaardige bepaling toe te voegen aan Titel 6 van het Ontwerp, opdat deze regel een transversale werking zou krijgen. Er zijn immers nog andere bepalingen in het Ontwerp die gegevensverwerkingen impliceren – zie bijvoorbeeld de artikelen 29, 37, §1, & 62, tweede lid, - waarvoor het vanuit dataprotectie-oogpunt een meerwaarde zou betekenen mochten zij expliciet aan hetzelfde beginsel onderworpen zijn.

17. Verder vestigt de Autoriteit er de aandacht op dat het principe van de "minimale gegevensverwerking" ook impliceert dat wanneer een bepaald doeleinde kan gerealiseerd worden zonder dat hierbij persoonsgegevens worden verwerkt, er voor deze piste dient gekozen te worden. De instanties opgesomd in randnummer 3 dienen zich hier terdege

---

[20] Zie bv. artikel 54, eerste lid, van het Ontwerp: de procureur des Konings zal de sectorale overheid inlichten wanneer strafrechtelijke vervolging is ingesteld.

[21] Zie overweging 51 AVG: *"(...) Naast de specifieke voorschriften voor die verwerking [van gevoelige gegevens] dienen de algemene beginselen en andere regels van deze verordening te worden toegepast, met name wat betreft de voorwaarden voor rechtmatige verwerking. (...)"*

Zie ook p. 15 van het advies 06/2014 van de Groep *on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC:*

[22] Zie randnummer 4, eerste bullet.

bewust van te zijn en daarom kan het nuttig zijn om hier melding van te maken in de Memorie van Toelichting bij het Ontwerp.

## 5. Bewaartermijn

18. Volgens artikel 5.1.e) AVG mogen persoonsgegevens niet langer worden bewaard, in een vorm die het mogelijk maakt de betrokkenen te identificeren, dan noodzakelijk voor de verwezenlijking van de doeleinden waarvoor zij worden verwerkt. Het Ontwerp voorziet enkel voor verwerkingen betreffende inbreuken in een welbepaalde bewaartermijn (cf infra randnummer 22, bullet 6). De Autoriteit adviseert om voor de andere verwerkingsfinaliteiten – ofwel in het Ontwerp, ofwel in een uitvoeringsbesluit – alsnog in specifieke bewaartermijnen of afbakeningscriteria voor de bewaartermijnen te voorzien.

## 6. Verantwoordelijkheid

19. Artikel 4.7 AVG bepaalt dat voor de verwerkingen waarvan de regelgeving het doel en de middelen vastlegt, de verwerkingsverantwoordelijke diegene is die de wetgeving in kwestie aanduidt. Het Ontwerp duidt geen verwerkingsverantwoordelijken aan en de Autoriteit adviseert om deze leemte op te vullen (bv. in Titel 6 van het Ontwerp).

20. De Autoriteit stelt verder vast dat de aanbieders van essentiële diensten, de digitale dienstverleners, alsook de autoriteiten opgesomd in randnummer 3, krachtens het Ontwerp allen een functionaris voor gegevensbescherming moeten aanduiden[23] en zij staat evident positief ten aanzien van deze maatregel.

## 7. Rechten van de betrokkenen

21. Artikel 23 AVG laat de lidstaten toe om binnen welbepaalde grenzen en voor specifieke doeleinden te voorzien in uitzonderingen op de rechten van betrokkenen. De specifieke doeleinden waarvoor dit mogelijk is, staan opgesomd in artikel 23.1 AVG. Iedere wettelijk maatregel die voorziet in beperkingen op de rechten van de betrokkene, moet ten minste specifieke bepalingen bevatten betreffende de elementen opgesomd in artikel 23.2 AVG zoals:
    - de doeleinden van de (categorieën van de) verwerking,
    - de categorieën van persoonsgegevens,
    - het toepassingsgebied van de beperkingen,

[23] Artikel 66 van het Ontwerp. De Autoriteit meent overigens dat dit artikel beter net voor artikel 65 van het Ontwerp zou geplaatst worden, aangezien het nu is ondergebracht tussen twee artikels die over een ander onderwerp handelen (met name over de beperking van de rechten van de betrokkene).

- waarborgen ter voorkoming van misbruik of onrechtmatige toegang of doorgifte,
- specificatie van de (categorieën van) verwerkingsverantwoordelijke(n),
- de opslagperiodes,
- de risico's voor de rechten en vrijheden van de betrokkenen en
- het recht van de betrokkene op kennisgeving inzake de beperking.

22. De Autoriteit analyseert hierna in hoeverre deze voorwaarden gerespecteerd worden:

- wat het doeleinde van de verwerking betreft: In het kader van *"het melden van incidenten" en in het kader van "het toezicht bedoeld in Titel 4 van het Ontwerp"*, worden door het Ontwerp alle rechten bedoeld in de artikelen 12 t.e.m. 22 AVG uitgesloten[24]. De Autoriteit merkt op dat de omschrijving van het doeleinde *"het toezicht bedoeld in Titel 4 van het Ontwerp"* nauwkeuriger zou moeten uitgewerkt worden. Dit zou bijvoorbeeld kunnen door naar de exacte artikels in het Ontwerp te verwijzen waarin de verwerkingen vervat liggen die onderhevig zijn aan de beperkingen van de rechten die in artikel 65 van het Ontwerp zijn vastgelegd. De Autoriteit herinnert er volledigheidshalve aan dat deze beperkingen binnen de grenzen van het strikt noodzakelijke dienen te blijven[25];
- wat de categorieën van persoonsgegevens betreft: *"alle categorieën van persoonsgegevens die door de verwerkingsverantwoordelijke(n) worden verwerkt voor de [hogervermelde] doeleinden"*[26]; De Autoriteit dringt er op aan om deze omschrijving te verduidelijken.
- wat het toepassingsgebied van de beperkingen betreft: Het Ontwerp voorziet ter zake niets en deze leemte dient aldus de Autoriteit te worden opgevuld. Ter illustratie verwijst de Autoriteit naar randnummer 41 van advies nr. 34/2018[27].
- wat de waarborgen ter voorkoming van misbruik of onrechtmatige toegang of doorgifte betreft:
  - *"Elke verwerkingsverantwoordelijke moet passende maatregelen nemen om elke vorm van misbruik of onrechtmatige toegang of overdracht van*

---

[24] Artikel 65, §2, van het Ontwerp.

[25] Cf. randnummer 38 van advies nr. 34/2018.

[26] Artikel 65, § 4, van het Ontwerp.

[27] *" (...) Wat het toepassingsgebied van de beperkingen betreft:*

- *gedurende de periode waarin de betrokkene het voorwerp uitmaakt van een controle of onderzoek (incl. de voorbereidende werkzaamheden van max 1 jaar na ontvangst van het verzoek tot uitoefening van het recht) en gedurende de periode om vervolgingen hieromtrent in te stellen;*
- *voor zover de uitoefening van de rechten nadelig zou zijn voor de controle, het onderzoek of de voorbereidende werkzaamheden of het geheim van het strafonderzoek dreigt te schenden. (...)"*

*voormelde persoonsgegevens te voorkomen"*[28]. De Autoriteit verzoekt de aanvrager om (bv. in de Memorie van Toelichting) te expliciteren welke concrete "passende maatregelen" zullen genomen worden om onrechtmatige toegang te vermijden;

- "*De functionaris voor gegevensbescherming vermeldt de feitelijke en juridische redenen waarop zijn beslissing steunt en deze inlichtingen worden ter beschikking gehouden van de bevoegde toezichthoudende autoriteit*"[29]. Deze procedure lijkt echter enkel te gelden voor beperkingen op het recht op rectificatie wat dus onvoldoende is (cf. infra randnummer 23);

- wat de specificatie van de verwerkingsverantwoordelijken betreft: de aanbieder van essentiële diensten, de digitale dienstverlener of de autoriteiten bedoeld in randnummer 3[30];
- wat de opslagperiodes betreft: de gegevens betreffende inbreuken mogen niet langer bewaard worden dan noodzakelijk is voor de vooropgestelde doeleinden en maximaal voor de duur van de verjaringstermijnen[31]. De artikels van het Ontwerp waarnaar hierbij verwezen wordt bevatten echter geen verjaartermijnen. De Autoriteit verzoekt dan ook om voor iedere verwerking de termijnen expliciet in het Ontwerp op te nemen.
- wat de risico's voor de rechten en vrijheden van de betrokkenen betreft:
  - De functionaris voor gegevensbescherming informeert de betrokkene over de mogelijkheid om klacht in te dienen bij de bevoegde toezichthoudende overheid of om een jurisdictioneel beroep in te stellen[32];
  - De functionaris voor gegevensbescherming vermeldt de feitelijke en juridische redenen waarop zijn beslissing steunt en deze inlichtingen worden ter beschikking gehouden van de bevoegde toezichthoudende overheid[33];

  De Autoriteit merkt op dat deze procedures enkel lijken te gelden voor beperkingen op het recht op rectificatie (cf. infra randnummer 23).

  Zij adviseert verder om in artikel 67 van het Ontwerp ook een bepaling op te nemen die stipuleert dat de functionaris voor gegevensbescherming de betrokkene onverwijld in kennis stelt van de opheffing van een beperking en dit onmiddellijk na afsluiting van controle of onderzoek (tenzij het dossier

[28] Artikel 65, §4, van het Ontwerp.
[29] Artikel 67, §3, tweede lid, van het Ontwerp.
[30] Artikel 65, §3, van het Ontwerp.
[31] Artikel 65, §5, van het Ontwerp.
[32] Artikel 67, §3, eerste lid, van het Ontwerp.
[33] Artikel 67, §3, tweede lid, van het Ontwerp.

wordt overgemaakt aan het openbaar ministerie of aan de bevoegde instelling om over de bevindingen van het onderzoek te beslissen).

- wat het recht van de betrokkene op kennisgeving inzake de beperking betreft: In dit verband zijn twee bepalingen uit het Ontwerp relevant:
  - *"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 recht op rectificatie, 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 65 zou ondermijnen."*[34]
  - de verwerkingsverantwoordelijke kan de betrokkene toegang verlenen 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."*[35]

De Autoriteit heeft dienaangaande twee opmerkingen:

- Ten eerste stelt zij zich de vraag wat met *"beperkte informatie"* bedoeld wordt. Een verduidelijking in het Ontwerp zou dit kunnen ophelderen;
- Ten tweede verzoekt zij om de inhoud en draagwijdte van de zinsnede *"de doelstellingen van deze wet"* en de *"de doelstellingen vermeld in artikel 65"* te verduidelijken.

23. Verder vestigt de Autoriteit er in het algemeen de aandacht op dat de redactie van artikel 67 van het Ontwerp dient bijgestuurd te worden. De eerste paragraaf stipuleert dat betrokkenen *"een verzoek in verband met hun rechten"* kunnen richten tot de functionaris voor gegevensbescherming, terwijl de tweede en derde paragraaf de procedure beschrijft die deze functionaris hierbij dient te volgen. Deze procedure lijkt echter te worden beperkt tot de gevallen waarin een betrokkene zijn recht op rectificatie (artikel 16 AVG) uitoefent. De Autoriteit verzoekt bijgevolg om deze procedure ook te laten gelden voor de gevallen waarin betrokkenen andere AVG-rechten dan het recht op rectificatie wensen uit te oefenen. Zoniet zijn de hoger geschetste waarborgen (randnummer 22, bullets 4, 7 & 8) niet op deze gevallen van toepassing en beantwoorden deze beperkingen aldus helemaal niet aan de vereisten van artikel 23 AVG.

---

[34] Artikel 67, §2, van het Ontwerp.

[35] Artikel 67, §4, van het Ontwerp.

24. Om de redactie van de artikelen 65 en 67 van het Ontwerp in bovengenoemde zin te verbeteren, zou overigens inspiratie kunnen gevonden worden in de artikelen 59 e.v. van de wet *tot oprichting van het informatieveiligheidscomité en tot wijziging van diverse wetten betreffende de uitvoering van Verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad 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.*

25. Tot slot stelt de Autoriteit ook vast dat de meldingsplicht vervat in artikel 34 AVG wordt beperkt, met name in artikel 67, §5, van het Ontwerp. Er wordt niet gemotiveerd waarom deze afwijking noodzakelijk zou zijn. De redactie van artikel 67, §5, is bovendien niet duidelijk, aangezien eveneens dezelfde vage zinsnede (*"de doelstellingen van deze wet"*) wordt gebruikt die hoger in randnummer 22, bullet 8, reeds wordt bekritiseerd. Daarenboven stemt de tekst van deze bepaling niet overeen met de uitleg die er in de Memorie van Toelichting (p. 35) aan gegeven wordt. In de Memorie staat namelijk dat er toestemming nodig is van de toezichthoudende autoriteit vooraleer een verwerkingsverantwoordelijke zou ontslaan worden van de meldingsplicht vervat in artikel 34 AVG, terwijl deze voorwaarde niet blijkt uit de tekst van artikel 67, §5. De Autoriteit dringt er dan ook op aan om deze bepaling grondig te herwerken.

## III. BESLUIT

26. Op voorwaarde dat de volgende opmerkingen in de tekst worden geïntegreerd:
    - de betrokken actoren via (de Memorie van Toelichting bij) het Ontwerp sensibiliseren opdat de gegevensverwerkingen die ingevolge het Ontwerp zullen plaatsvinden AVG-conform zouden zijn (zie randnummer 7);
    - alle essentiële elementen van de geplande gegevensverwerkingen in het Ontwerp integreren (zie randnummers 11, 12, 14, 18 & 19);
    - het principe van de "minimale gegevensverwerking" nog meer implementeren in (de Memorie van Toelichting bij) het Ontwerp (zie randnummers 16 & 17);
    - de artikelen 65 & 67 van het Ontwerp herwerken conform de suggesties in de randnummers 22 t.e.m. 25.

is de Autoriteit van oordeel dat het Ontwerp voldoende waarborgen biedt wat de bescherming van de persoonsgegevens van de betrokkenen betreft.

**OM DEZE REDENEN**

Brengt de Autoriteit een **gunstig advies** uit over het wetsontwerp *tot vaststelling van een kader voor de beveiliging van netwerk –en informatiesystemen van algemeen belang voor de openbare veiligheid* en dit onder de uitdrukkelijke voorwaarde dat voormelde opmerkingen bijkomend worden geïntegreerd.

De Wnd. Administrateur,

An Machtens

De Voorzitter,

Willem Debeuckelaere

**Avis n° 84/2018 du 14 septembre 2018**

**Objet :** Projet de loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (CO-A-2018-070)

L'Autorité de protection des données (ci-après "l'Autorité") ;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26 ;

Vu la demande d'avis de M. Michel, Premier ministre, reçue le 20 juillet 2018 ;

Vu le rapport de Monsieur F. De Smet ;

Émet, le 14 septembre 2018, l'avis suivant :

## I. OBJET ET CONTEXTE DE LA DEMANDE D'AVIS

1. Le 20 juillet 2018, le Premier ministre (ci-après "le demandeur") a sollicité l'avis de l'Autorité sur un projet de loi *établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique* (ci-après "le Projet").

2. Le Projet vise la transposition de la Directive européenne (EU) 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 "la Directive"). Les principaux destinataires des obligations de la Directive sont les entités susceptibles, en cas d'incident affectant la sécurité de leurs réseaux et systèmes d'information, de perturber de manière importante la fourniture de services essentiels et de services numériques essentiels au maintien d'activités sociétales ou économiques critiques[1]. La Directive a notamment pour objectif de veiller à ce que des mesures de sécurité techniques et organisationnelles soient prises par les opérateurs de services essentiels et les fournisseurs de service numérique afin de prévenir les incidents ou d'en limiter l'impact, en vue d'assurer la continuité de ces services. Dans le même esprit, l'obligation de notification d'incidents reprise dans la Directive concerne les incidents ayant un impact significatif sur les services fournis[2].

3. Différentes autorités sont chargées de l'exécution des dispositions du Projet. Le Roi désignera notamment plusieurs autorités qui assureront les rôles suivants[3]:

   - L'Autorité nationale, chargée du suivi et de la coordination de la mise en œuvre de cette loi. Cette Autorité nationale est aussi le "point de contact national unique". Il s'agit d'une fonction de liaison – créée par la Directive – qui doit assurer une coopération européenne ;
   - le centre national de réponse aux incidents de sécurité informatique (ci-après le "NCSIRT"), chargé de recevoir et de traiter les notifications d'incidents des opérateurs de services essentiels et du fournisseur de service numérique, ainsi que des notifications d'autres pays ;
   - les Autorité sectorielles[4] et les centres sectoriels de réponse aux incidents de sécurité informatique (ci-après "SCSIRT"), chargés au sein de leur secteur de veiller à la mise en œuvre des dispositions du Projet ;
   - une autorité chargée de "*maintenir à jour la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information*"[5];

[1] Il s'agit par exemple d'entreprises d'électricité, de fournisseurs d'eau, de transporteurs aériens, d'établissements de crédit, d'établissements de soins de santé, etc. (voir l'annexe 1 du Projet).

- Les services d'inspection qui veillent au respect du Projet et de ses arrêtés d'exécution par les opérateurs de services essentiels ou les fournisseurs de service numérique.

4. Dans le contexte du Projet, les traitements de données réalisés seront (au moins) les suivants :
   - échange général d'informations depuis les opérateurs de services essentiels et les fournisseurs de service numérique vers les autorités visées au point 3 et depuis ces autorités vers d'autres autorités (étrangères)[6];
   - traitement d'informations que les autorités énoncées au point 3 reçoivent de la part des opérateurs de services essentiels et des fournisseurs de service numérique
     - o lors de la notification de leur "*point de contact pour la sécurité informatique*"[7];
     - o dans le cadre de notifications d'incidents[8];
   - traitements par les services d'inspection[9] (cf. point 3, dernière puce) dans le cadre de la surveillance des opérateurs de services essentiels et des fournisseurs de service numérique, et ce notamment en ce qui concerne le respect des exigences de sécurité ou des exigences en matière de notification d'incidents. L'article 44 du Projet octroie à ces services d'inspection de larges pouvoirs d'enquête. Ils peuvent notamment "*procéder à tout examen, contrôle et audition*" et peuvent requérir toutes les informations qu'ils estiment nécessaires à l'exercice de leur mission[10];
   - traitements par les Cours et Tribunaux (dans les procédures pénales) ou par les "autorités sectorielles"[11] (dans les procédures administratives) dans le cadre de la répression d'infractions au Projet ;
   - traitements par le NCSIRT et les SCSIRT dans le cadre de la gestion d'incidents de sécurité[12].

---

[2] Pages 1 à 3 de l'Exposé des motifs du Projet.

[3] Voir l'article 7 du Projet.

[4] Elles seront notamment chargées de l'identification des opérateurs de services essentiels dans leur secteur (cf. article 11 du Projet).

[5] Article 10, § 1 du projet.

[6] Article 9 du projet.

[7] Articles 23 et 34 du Projet.

[8] Articles 24 e.s. et 35 e.s. du Projet.

[9] - Voir le point 3, dernière puce.
- Voir le Titre 4 : Chapitre 1, section 2 & Chapitre 2 du Projet.

[10] Article 44, § 3, 3° du Projet.

[11] Voir le point 3, dernière puce.

[12] Voir le Titre 5 du Projet.

## II. EXAMEN DE LA DEMANDE D'AVIS

### 1. Remarques générales

5. L'Autorité est très positive à l'égard de la *ratio legis* du Projet : protéger au mieux certains réseaux et systèmes d'information qui sont importants pour la sécurité publique. Comme l'indique à juste titre l'Exposé des motifs du Projet (p. 3), une telle gestion des risques de sécurité est conforme au RGPD.

6. L'Autorité accueille également favorablement l'obligation de coopération entre elle-même et les instances énoncées au point 3[13], ainsi que la plateforme commune qui sera créée en vue de notifier les incidents[14]. Spécifiquement à propos de cette plateforme de notification, l'Autorité attire toutefois l'attention sur le fait que – vu le principe de "responsabilité" du RGPD – il faudra veiller, lors de sa conception, à ce qu'il incombe toujours au responsable du traitement de décider à quelle(s) instance(s) il adresse la notification et à laquelle/auxquelles il ne le fait pas. En d'autres termes, la réalisation de cette plateforme ne peut pas impliquer un report de cette responsabilité du responsable du traitement vers une ou plusieurs instances qui reçoivent des notifications via cette plateforme.

7. Par ailleurs, l'Autorité attire l'attention sur le fait que dans la pratique, de nombreux points communs apparaîtront entre les dispositions du Projet et les règles en matière de protection des données. À cet égard, l'Autorité souligne aussi que le RGPD reste intégralement d'application aux traitements de données à caractère personnel qui auront lieu dans le contexte du Projet. Tous les acteurs soumis aux dispositions du Projet devront donc (dans la mesure où ils traitent des données à caractère personnel) tenir compte également de la réglementation en matière de protection des données. Ils pourraient toutefois avoir l'impression erronée qu'ils agissent en toute légalité en respectant les règles du Projet alors qu'ils perdent peut-être le RGPD de vue. L'Autorité plaide dès lors pour :
   - insérer dans le Projet une disposition établissant le principe selon lequel le Projet ne porte pas préjudice au RGPD ainsi qu'aux lois d'exécution nationales y afférentes[15];

---

[13] Article 8, § 2 du Projet. Les articles 48 et 52 de la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données* permet d'ailleurs aussi à l'Autorité de collaborer avec d'autres acteurs dans ce contexte.

[14] Article 31, § 1, dernier alinéa et article 36, § 3 du Projet.

[15] L'article 2 de la Directive semble le permettre, étant donné que cette disposition renvoie aux règles classiques en matière de protection des données (à savoir à l'ancienne Directive 95/46/CE, qui a entre-temps été remplacée par le RGPD) en ce qui concerne le traitement de données à caractère personnel qui sera réalisé dans le présent contexte.

- signaler dans l'Exposé des motifs du Projet les similitudes et différences spécifiques entre les règles du Projet et les obligations du RGPD[16].

## 2. Finalité

8. Conformément à l'article 5.1.b) du RGPD, le traitement de données à caractère personnel n'est autorisé que pour des finalités déterminées, explicites et légitimes. L'Autorité constate que le Projet vise une finalité (certes générale) claire et légitime : veiller à ce que des mesures de sécurité techniques et organisationnelles soient prises par les opérateurs de services essentiels afin de prévenir les incidents ou d'en limiter l'impact, en vue d'assurer la continuité de services essentiels. Parallèlement, l'Autorité plaide pour que l'on reprenne explicitement dans le Projet (cf. point 12) la sous-finalité de chaque catégorie distincte de traitements (cf. point 4).

## 3. Fondement juridique

9. Tout traitement de données à caractère personnel doit reposer sur un fondement juridique au sens de l'article 6 du RGPD. En outre, le traitement de données à caractère personnel relatives aux condamnations pénales et aux infractions est soumis à des conditions strictes (article 10 du RGPD).

10. Pour le traitement de données à caractère personnel qui n'appartiennent pas aux catégories particulières des articles 9 et 10 du RGPD, le Projet peut éventuellement se baser sur les deux fondements juridiques suivants :

- l'article 6.1.c) du RGPD en ce qui concerne les traitements qui sont réalisés par les opérateurs de services essentiels et les fournisseurs de service numérique. Ils communiquent en effet certaines données à caractère personnel aux acteurs visés au point 3, parce que le Projet les y oblige ;
- l'article 6.1. e) du RGPD en ce qui concerne les traitements réalisés par les acteurs visés au point 3. Ils accomplissent en effet une mission d'intérêt public.

---

[16] À titre d'exemple :

- les articles 24 e.s. et 35 e.s. du Projet imposent une obligation de notification pour les incidents de sécurité, alors que les articles 33 et 34 du RGPD prévoient une obligation de notification pour les "*violations de données à caractère personnel*" ;
- l'article 23, § 1 du Projet prévoit une obligation de notification pour le "*point de contact pour la sécurité des réseaux et systèmes d'information*" et l'article 37.7 du RGPD dispose que les coordonnées du délégué à la protection des données doivent être communiquées à l'autorité de contrôle.

11. À cet égard, l'Autorité attire l'attention sur l'article 6.3 du RGPD qui – lu conjointement avec l'article 8 de la CEDH et l'article 22 de la Constitution -[17] prescrit que la réglementation qui encadre le traitement de données à caractère personnel doit en principe mentionner au moins les éléments essentiels suivants de ce traitement :
    - la finalité du traitement ;
    - les types ou catégories de données à caractère personnel qui feront l'objet du traitement ;
    - les personnes concernées ;
    - les entités auxquelles les données à caractère personnel peuvent être communiquées et les finalités pour lesquelles elles peuvent l'être ;
    - les durées de conservation ;
    - ainsi que la désignation du responsable du traitement.

12. Le Projet doit être précisé et complété en ce sens. Cela pourrait par exemple se faire en insérant dans le Titre 6 du Projet un article précisant, par type de traitement (voir le point 4 ci-avant), au moins la finalité du traitement. Les autres éléments essentiels des traitements doivent également être repris dans cette nouvelle disposition, sauf si une délégation au Roi est prévue à cet effet.

13. À cet égard, l'Autorité attire également l'attention sur l'article 20 de la loi-cadre en matière de protection des données[18] qui impose aux autorités fédérales[19] l'obligation de conclure des protocoles d'accord pour les échanges de données qui sont basés sur l'article 6.1.e) du RGPD.

14. Par ailleurs, l'Autorité constate que des données seront également traitées au sujet de condamnations pénales et d'infractions pénales[20], ce qui concerne des traitements qui, en vertu de l'article 10 du RGPD, ne sont permis que sous le contrôle d'une autorité publique (ou si le traitement est autorisé par le droit de l'Union ou par le droit d'un État membre qui prévoit des garanties appropriées pour les droits et libertés des personnes concernées). En l'occurrence, le traitement de ce type de données sera réalisé sous le contrôle d'une autorité publique, à savoir les acteurs visés au point 3, ce qui est conforme à l'article 10 du RGPD. Cette disposition du RGPD doit par ailleurs aussi être lue conjointement avec les articles

---

[17] Voir les arrêts de la Cour constitutionnelle : arrêt n° 44/2015 du 23 avril 2015 (p. 63), arrêt n° 108/2017 du 5 octobre 2017 (p. 17) et arrêt n° 29/2018 du 15 mars 2018 (p. 26).

[18] Loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*

[19] Un décret flamand impose d'ailleurs des obligations similaires aux services publics flamands (voir l'article 16 du décret du 8 juin 2018 *contenant l'ajustement des décrets au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).*)

[20] Voir par exemple l'article 54, premier alinéa, du Projet : le procureur du Roi informera l'autorité sectorielle lorsque que des poursuites pénales ont été engagées.

6 du RGPD[21], 22 de la Constitution et 8 de la CEDH, ce qui implique que – même si le traitement de ce type de données a lieu sous le contrôle d'une autorité publique – les éléments essentiels du traitement de ce type de données doivent également être fixés dans la réglementation, ce qui est encore insuffisamment le cas en l'espèce (voir les points 11-12).

### 4. Principe de minimisation des données

15. L'article 5.1.c) du RGPD dispose que les données à caractère personnel doivent être limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ("minimisation des données").

16. L'Autorité constate avant tout que l'article 9, § 3, dernier alinéa du Projet[22] reprend le principe selon lequel les informations échangées doivent être limitées "au minimum nécessaire et sont proportionnées à l'objectif de cet échange". L'Autorité conseille d'ajouter une disposition similaire au Titre 6 du Projet, afin que cette règle ait un effet transversal. Le Projet comporte en effet encore d'autres dispositions impliquant des traitements de données – voir par exemple les articles 29, 37, § 1 et 62, deuxième alinéa – qui bénéficieraient d'une plus-value du point de vue de la protection des données si elles étaient explicitement soumises au même principe.

17. L'Autorité attire ensuite l'attention sur le fait que le principe de "minimisation des données" implique aussi que lorsqu'une certaine finalité peut être réalisée sans traiter des données à caractère personnel, il faut opter pour cette solution. Les instances énoncées au point 3 doivent avoir pleinement conscience de cela et il peut dès lors être utile de le mentionner dans l'Exposé des motifs du Projet.

### 5. Délai de conservation

18. Selon l'article 5.1.e) du RGPD, les données doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées. Le Projet ne prévoit un délai de conservation déterminé que pour les traitements relatifs à des infractions (cf. ci-après, point 22, puce 6). Pour les autres finalités de traitements, l'Autorité recommande d'encore prévoir

---

[21] Voir le considérant 51 du RGPD : "(...) *Outre les exigences spécifiques applicables à ce traitement [de données sensibles], les principes généraux et les autres règles du présent règlement devraient s'appliquer, en particulier en ce qui concerne les conditions de licéité du traitement. (...)*"

Voir aussi la p. 15 de l'avis n° 06/2014 du Groupe 29 *sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE.*

[22] Voir le point 4, première puce.

- soit dans le Projet, soit dans un arrêté d'exécution - des délais de conservation spécifiques ou des critères de délimitation pour les délais de conservation.

## 6. Responsabilité

19. L'article 4.7. du RGPD prévoit que pour les traitements dont les finalités et les moyens sont déterminés par la réglementation, le responsable du traitement est celui qui est désigné par la réglementation en question. Le Projet ne désigne aucun responsable du traitement et l'Autorité recommande de combler cette lacune (par exemple au Titre 6 du Projet).

20. L'Autorité constate par ailleurs que les opérateurs de services essentiels, les fournisseurs de service numérique ainsi que les autorités énoncées au point 3, doivent tous, en vertu du Projet, désigner un délégué à la protection des données[23]. Elle accueille bien entendu favorablement cette mesure.

## 7. Droit des personnes concernées

21. L'article 23 du RGPD autorise les États membres à prévoir, dans certaines limites déterminées et pour des objectifs spécifiques, des exceptions aux droits des personnes concernées. Les finalités spécifiques pour lesquelles c'est possible sont énoncées à l'article 23.1 du RGPD. Toute mesure législative prévoyant des limitations aux droits de la personne concernée doit au moins contenir des dispositions spécifiques relatives aux éléments énumérés à l'article 23.2 du RGPD, comme :
    - les finalités du traitement (ou des catégories de traitement),
    - les catégories de données à caractère personnel,
    - l'étendue des limitations introduites,
    - les garanties destinées à prévenir les abus ou l'accès ou le transfert illicites,
    - la détermination du (des) responsable(s) du traitement (ou des catégories de responsables du traitement),
    - les durées de conservation,
    - les risques pour les droits et libertés des personnes concernées et
    - le droit des personnes concernées d'être informées de la limitation.

22. L'Autorité analyse ci-après dans quelle mesure ces conditions sont respectées :
    - en ce qui concerne la finalité du traitement : dans le cadre de *"la notification des incidents" et des "contrôles visés au Titre 4 du Projet"*, le Projet exclut tous les

[23] Article 66 du Projet. L'Autorité estime d'ailleurs que cet article devrait se situer juste avant l'article 65 du Projet, étant donné qu'il est à présent situé entre deux articles qui traitent d'un autre sujet (à savoir la limitation des droits de la personne concernée).

droits visés aux articles 12 à 22 inclus du RGPD[24]. L'Autorité fait remarquer que la description de la finalité "*les contrôles visés au Titre 4 du Projet*" devrait être développée avec plus de précision. Cela pourrait par exemple se faire en renvoyant aux articles précis du Projet qui contiennent les traitements soumis aux limitations des droits établis à l'article 65 du Projet. L'Autorité rappelle, par souci d'exhaustivité, que ces limitations doivent rester dans les limites du strict nécessaire[25];

- en ce qui concerne les catégories de données à caractère personnel : *"toutes les catégories de données à caractère personnel traitées par le ou les responsables du traitement en lien avec les finalités [précitées]"*[26] ; l'Autorité insiste pour que l'on précise cette description.
- en ce qui concerne l'étendue des limitations : le Projet ne prévoit rien en la matière et l'Autorité estime que cette lacune doit être comblée. À titre d'illustration, l'Autorité renvoie au point 41 de l'avis n° 34/2018[27].
- en ce qui concerne les garanties visant à prévenir un abus ou un accès ou une transmission illicite :
  - *"Chaque responsable du traitement est tenu de prendre des mesures appropriées pour éviter toute forme d'abus, d'accès ou de transfert illicites desdites données à caractère personnel"*[28]. L'Autorité prie le demandeur de clarifier (par exemple dans l'Exposé des motifs) quelles "mesures appropriées" concrètes seront prises pour éviter un accès illicite ;
  - "*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.*"[29] Cette procédure ne semble toutefois s'appliquer que pour les limitations du droit de rectification ce qui est donc insuffisant (cf. infra, point 23).

---

[24] Article 65, § 2 du Projet.

[25] Cf. point 38 de l'avis n° 34/2018.

[26] Article 65, § 4 du Projet.

[27] *"(...) En ce qui concerne l'étendue des limitations :*

- *pendant la période au cours de laquelle la personne concernée fait l'objet d'un contrôle ou d'une enquête (y compris les actes préparatoires de maximum 1 an après réception de la demande d'exercice du droit) et pendant la période en vue d'exercer les poursuites en la matière ;*
- *dans la mesure où l'exercice des droits nuirait aux besoins du contrôle, de l'enquête ou des actes préparatoires ou risque de violer le secret de l'enquête pénale. (...)"*

[28] Article 65, § 4 du Projet.

[29] Article 67, § 3, deuxième alinéa du Projet.

- en ce qui concerne la détermination des responsables du traitement : l'opérateur de services essentiels, le fournisseur de service numérique ou les autorités visées au point 3[30];
- en ce qui concerne les durées de conservation : les données relatives à des infractions ne peuvent pas être conservées plus longtemps que nécessaire au regard des finalités pour lesquelles elles sont traitées et au maximum pour la durée des délais de prescription[31]. Les articles du Projet auquel il est renvoyé à cet égard ne contiennent toutefois aucun délai de prescription. L'Autorité demande dès lors de reprendre les délais explicitement dans le Projet pour chaque traitement.
- en ce qui concerne les risques pour les droits et libertés des personnes concernées :
  - le délégué à la protection des données informe la personne concernée de la possibilité d'introduire une réclamation auprès de l'autorité de contrôle compétente ou de former un recours juridictionnel[32] ;
  - le délégué à la protection des données consigne les motifs de fait ou de droit sur lesquels se fonde sa décision et ces informations sont mises à la disposition de l'autorité de contrôle compétente[33];

  L'Autorité observe que ces procédures ne semblent s'appliquer que pour les limitations du droit de rectification (cf. infra, point 23).

  Elle recommande par ailleurs de reprendre aussi à l'article 67 du Projet une disposition qui précise que le délégué à la protection des données informe immédiatement la personne concernée de la levée d'une limitation, et ce directement après la clôture du contrôle ou de l'enquête (sauf si le dossier est transmis au ministère public ou à l'instance compétente pour statuer sur les constatations de l'enquête).

- en ce qui concerne le droit de la personne concernée d'être informée de la limitation : à cet égard, deux dispositions du Projet sont pertinentes :
  - *"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 à son droit de rectification, ainsi que des motifs du refus ou de la limitation. Ces informations concernant le*

[30] Article 65, § 3 du Projet.
[31] Article 65, § 5 du Projet.
[32] Article 67, § 3, premier alinéa du Projet.
[33] Article 67, § 3, deuxième alinéa du Projet.

*refus ou la limitation peuvent ne pas être fournies lorsque leur communication risque de compromettre l'une des finalités énoncées à l'article 65.*"[34]

- le responsable du traitement peut donner accès à la personne concernée aux "*informations limitées*" concernant le traitement de ses données à caractère personnel, "*dans la mesure où cette communication ne compromet pas la réalisation des objectifs de la présente loi.*"[35]

L'Autorité a deux remarques à formuler à cet égard :

- elle se demande tout d'abord ce que l'on entend par "*informations limitées*". Une explication dans le Projet pourrait clarifier ces termes ;
- Deuxièmement, elle demande de préciser le contenu et la portée des termes "*des objectifs de la présente loi*" et "*des finalités énoncées à l'article 65*".

23. Ensuite, l'Autorité attire l'attention de manière générale sur la nécessité de corriger la rédaction de l'article 67 du Projet. Le premier paragraphe dispose que les personnes concernées peuvent "*adresser une demande concernant leur droits au délégué à la protection des données*" et les deuxième et troisième paragraphes décrivent la procédure que ce délégué doit suivre à cet égard. Cette procédure semble toutefois se limiter aux cas dans lesquels une personne concernée exerce son droit de rectification (article 16 du RGPD). L'Autorité demande dès lors que cette procédure soit également appliquée aux cas dans lesquels les personnes concernées souhaitent exercer d'autres droits que le droit de rectification. À défaut, les garanties précitées (point 22, puces 4, 7 et 8) ne s'appliqueront pas à ces cas et ces limitations ne répondront absolument pas aux exigences de l'article 23 du RGPD.

24. Pour améliorer la rédaction des articles 65 et 67 du Projet en ce sens, on pourrait d'ailleurs s'inspirer des articles 59 e.s. de la loi *instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.*

25. Enfin, l'Autorité constate aussi que l'obligation de notification de l'article 34 du RGPD est limitée, à savoir à l'article 67, § 5 du Projet. On ne motive pas la nécessité de cette dérogation. La rédaction de l'article 67, § 5 n'est en outre pas claire, étant donné que l'on utilise également les mêmes termes vagues (les "*objectifs de la présente loi*") qui font déjà l'objet de critiques ci-avant au point 22, puce 8. Le texte de cette disposition ne correspond en outre pas à

[34] Article 67, § 2 du Projet.
[35] Article 67, § 4 du Projet.

l'explication qui en est donnée dans l'Exposé des motifs (p. 35). L'Exposé des motifs indique en effet qu'il faut une autorisation de l'autorité de contrôle avant qu'un responsable du traitement soit déchargé de l'obligation de notification reprise à l'article 34 du RGPD, alors que cette condition ne ressort pas du texte de l'article 67, § 5. L'Autorité insiste dès lors pour que cette disposition soit retravaillée en profondeur.

## III. CONCLUSION

26. À condition que les remarques suivantes soient intégrées dans le texte :

- sensibiliser les acteurs concernés via le Projet (ou l'Exposé des motifs du Projet) afin que les traitements de données qui auront lieu en vertu du Projet soient conformes au RGPD (voir le point 7) ;
- intégrer tous les éléments essentiels des traitements de données envisagés dans le Projet (voir les points 11, 12, 14, 18 et 19) ;
- implémenter encore davantage le principe de "minimisation des données" dans (l'Exposé des motifs du) Projet (voir les points 16 & 17) ;
- retravailler les articles 65 et 67 du Projet conformément aux suggestions reprises aux points 22 à 25 inclus.

l'Autorité estime que le Projet offre suffisamment de garanties quant à la protection des données à caractère personnel des personnes concernées.

**PAR CES MOTIFS,**

l'Autorité émet un **avis favorable** sur le projet de loi *établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique*, et ce à la condition explicite que les remarques précitées soient intégrées.

L'Administrateur f.f., La Présidente,


An Machtens Willem Debeuckelaere