MEMORIE VAN TOELICHTING

MEVROUWEN, MIJNE HEREN,

ALGEMENE BESCHOUWINGEN

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 beveiligings-maatregelen 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

EXPOSÉ DES MOTIFS

MESDAMES, MESSIEURS,

CONSIDÉRATIONS GÉNÉRALES

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.

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.

De bescherming, de beveiliging en de betrouwbaarheid van de netwerk- en informatie-systemen 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 beveiligings-voorschriften 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 informatie-systemen, 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

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.

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.

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.

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.

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.

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.

Het wetsontwerp wil een aanpak van het beheer van beveiligingsrisico's bevorderen die aansluit bij 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).

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

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.

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.

De inhoud van de verplichtingen vervat in de NIS-richtlijn heeft betrekking op het beveiligings-niveau 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.

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'Etat 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

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

worden geraadpleegd wanneer sommige aanbieders van essentiële diensten (publiek-rechtelijke 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.

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.

ARTIKELSGEWIJZE BESPREKING

TITEL 1

Definities en algemene bepalingen

HOOFDSTUK 1

Onderwerp en toepassingsgebied

COMMENTAIRE DES ARTICLES

TITRE 1er

Définitions et dispositions générales

CHAPITRE 1er

Objet et champ d'application

Artikel 1

Dit artikel bevat de grondwettelijke grondslag van de wet.

Article 1er

Cet article précise le fondement constitutionnel de la loi.

Artikel 2

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

Article 2

Cet article précise la directive transposée par la loi.

Artikel 3

Dit artikel verduidelijkt het territoriale toepassingsgebied van de wet. Het wijst erop dat de wet ook van toepassing is op potentiële aanbieders van essentiële diensten die niet geïdentificeerd zijn krachtens de wet. Daarom somt het artikel de wetsbepalingen op die van toepassing zijn op deze potentiële aanbieders van essentiële diensten.

Article 3

Cet article précise le champ d'application territorial de la loi. Il est précisé que la loi s'applique également aux opérateurs de services essentiels potentiels, non identifiés en vertu de la loi. L'article énumère donc les dispositions de la loi qui s'appliquent à de tels opérateurs de services essentiels potentiels.

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.

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.

Artikel 4

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

Article 4

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

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 van essentiële diensten) en van artikel 26 (modaliteiten inzake het melden van incidenten) en de artikelen 65, 66 et 67 (afwijkingen van de verplichtingen en rechten van de Algemene Verordening Gegevensbescherming) zijn echter wel van toepassing op de aanbieders van essentiële diensten die deel uitmaken van de sector financiën.

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 1 de la loi (le champ d'application, les définitions, la coopération au niveau national, l'échange d'informations et la stratégie nationale), du chapitre 1 du Titre 2 (identification des opérateurs de services essentiels) et de l'article 26 (modalités relatives aux notification des incidents) ainsi que des articles 65, 66 et 67 (dérogations aux obligations et droits prévus par le Règlement Général sur la protection des données) sont néanmoins applicables aux opérateurs de services essentiels appartenant au secteur des finances.

Toutefois, les articles 65 à 67 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 Règlement pour

De artikelen 65 tot 67 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 Verordening 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).

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).

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.

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.

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.

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.

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.

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.

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.

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

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

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 verduidelijkt 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.

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 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 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.

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 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.

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.

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 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.

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 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.

HOOFDSTUK 3

Bevoegde autoriteiten en samenwerking op nationaal niveau

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 représentant de l'Etat 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 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.

CHAPITRE 3

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 (B.I.P.T.), 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

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 Etats membres de l'Union européenne, ainsi qu'avec les autorités concernées des autres Etats 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 (I.B.P.T.), 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

instrumenten en houdende 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

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), 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

autoriteiten, de gerechtelijke autoriteiten en de toezichthoudende autoriteiten persoonsgegevens.

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.

HOOFDSTUK 5

Nationale strategie voor de beveiliging van

autres services administratifs de l'Etat, aux autres autorités administratives, aux autorités judiciaires et aux autorités de contrôle des données à caractère personnel.

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.

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.

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.

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 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 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.

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 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.

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.

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

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

L'autorité sectorielle fait connaître, en collaboration avec celui-ci, à l'opérateur de service essentiel désigné 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 réfragable, il demeure toujours possible de la renverser en apportant la preuve du contraire.

Ainsi, dans le cas où un opérateur de service essentiel

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.

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

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, §§ 1 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.

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, §§ 1 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, §§ 1 et 4, de la loi, afin d’assurer une cohérence entre les différents secteurs et les autres Etats 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.

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.

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 een potentiële aanbieder 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

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.

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 qu'unopérateur potentiel fournit un ou des services essentiels dans au moins un autre Etat 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,

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 essentiële 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 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

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 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.

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 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,

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 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.

§ 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.

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.

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.

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

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.

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

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 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

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 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

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 conformiteits-beoordeling 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.

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, §§ 1 et 4 de communiquer facilement avec les opérateurs identifiés en cas d'incidents ou de les informer de menaces éventuelles.

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. 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

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. 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

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 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.

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 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

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 essentiële 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 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

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 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.

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.

Dit platform kan ook worden gebruikt voor verplichte meldingen door aanbieders van essentiële diensten en digitaledienstverleners krachtens 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.

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 algemene informatie aan het publiek mee te delen om redenen van sensibilisering en incidentpreventie of -beheer.

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 pour les notifications imposées aux opérateurs de services essentiels et aux fournisseurs de service numérique, en vertu 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.

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 au public à des fins de sensibilisation et de prévention ou de gestion d'incidents.

TITEL 3

Netwerk- en informatiesystemen van digitaledienstverleners

TITRE 3

Réseaux et systèmes d'information des fournisseurs de service numérique

Artikel 32

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

Article 32

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

HOOFDSTUK 1

De beveiligingseisen

CHAPITRE 1

Les exigences de sécurité

Artikel 33

Dit artikel verplicht digitaledienstverleners om de

Article 33

Cet article impose aux fournisseurs de service

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. Zo bepaalt de wet dat deze beveiligingsmaatregelen aan de uitvoeringsverordeningen van de Europese Commissie moeten voldoen.

Artikel 34

Het artikel bepaalt dat de digitaledienstverleners ook een contactpunt moeten aanwijzen, om dezelfde redenen als de aanbieders van essentiële diensten.

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

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. La loi précise ainsi que ces mesures de sécurité doivent être conformes aux règlements d'exécution de la Commission européenne.

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.

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.

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 of, als dit niet bestaat, via de door de Koning bepaalde beveiligde middelen.

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 verstrekte informatie.

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.

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 ou, à défaut, par les moyens sécurisés que le Roi définit.

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.

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

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 erkennings-akkoorden 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 kader van hun controle-opdrachten 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 conformiteits-beoordeling 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

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 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

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 instelling voor de conformiteitsbeoordeling moet 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 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 beveiligings-maatregelen en het melden van incidenten door de aanbieders worden nageleefd.

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 de certification, 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 sectorielle 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 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.

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 controle-modaliteiten 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 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.

Artikel 45

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. 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.

Article 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.

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 sectorale overheid 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

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.

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 à l'autorité sectorielle 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 1
Procédure

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 ingebreke-stelling, 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 proces-verbaal. Hetzelfde geldt voor de potentiële aanbieder van essentiële diensten 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.

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

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 va de même de l'opérateur de services essentiels potentiel 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.

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.

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.

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

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.

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.

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.

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

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.

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

CSIRT-netwerk, de vaststelling van procedures voor de behandeling van incidenten of nog alarmmeldingen 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

De artikelen 65 en 66 voeren uitzonderingen in op sommige bepalingen van verordening (EU) nr. 2016/679 van 27 april 2016 ("algemene verordening gegevensbescherming", hierna "AVG"). Deze uitzonderingen zijn gebaseerd op artikel 23 van de AVG en blijven binnen de grenzen van dat artikel.

Gelet op de verplichtingen in deze wet moeten immers 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, 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.

De afwijkingen in deze wet zijn beperkt tot de verplichtingen inzake het melden van incidenten bedoeld in hoofdstuk 3 van titel 2 en hoofdstuk 2 van titel 3, en tot het toezicht bedoeld in titel 4 van deze wet.

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

Les articles 65 et 66 introduisent des exceptions à certaines dispositions du Règlement (UE) n° 2016/679 du 27 avril 2016 (« règlement général sur la protection des données », ci-après « RGPD »). Ces exceptions sont introduites sur le fondement de et dans les limites permises par l'article 23 du RGPD.

Les obligations prévues par la présente loi nécessitent en effet 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, 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 réglementation liée à l'exercice de l'autorité publique.

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

Ces dérogations bénéficient aux opérateurs de

Deze afwijkingen komen de aanbieders van essentiële diensten en digitaledienstverleners ten goede, alsook de inspectiediensten en de autoriteiten bedoeld in artikel 7 van deze wet, voor zover dit noodzakelijk is voor het nagestreefde doel.

In overeenstemming met artikel 23 van de AVG bepaalt deze wet de betrokken doeleinden en gegevenscategorieën, de reikwijdte van de ingevoerde beperkingen, de garanties ter voorkoming van misbruik en de periode tijdens dewelke de afwijkingen van toepassing zijn. Deze wet bepaalt ook in hoeverre de betrokkenen al dan niet mogen worden geïnformeerd over deze beperkingen van hun rechten. Met inachtneming van het evenredigheidsbeginsel mag de verwerkingsverantwoordelijke beslissen om beperkte informatie aan de betrokkenen te verstrekken.

De artikelen 66 en 67 bepalen dat de aanbieders van essentiële diensten, de digitaledienstverleners of de autoriteiten bedoeld in artikel 7 van de wet die persoonsgegevens verwerken, een functionaris voor gegevensbescherming moeten aanwijzen in de zin van de AVG.

Een andere, beperktere afwijking betreft artikel 34 van de AVG en de verplichting om een inbreuk in verband met persoonsgegevens individueel mee te delen. Enkel met de toestemming van de autoriteit bedoeld in artikel 7, § 1, van de wet, en voor zover dit noodzakelijk is om de doelstellingen van de wet of de efficiëntie van onderzoeken te waarborgen, zou deze individuele kennisgeving niet meer verplicht zijn.

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.

Comme le prévoit l'article 23 du RGPD, la présente loi précise les finalités et catégories de données concernées, l'étendue des limitations introduites, les garanties en vue de prévenir les abus et la période pendant laquelle les dérogations sont applicables. Elle détermine aussi la mesure dans laquelle les personnes concernées peuvent ou non être informées de ces limitations à leur droit. Dans le respect du principe de proportionnalité, le responsable du traitement peut choisir de fournir certaines informations limitées aux personnes concernées.

Les articles 66 et 67 précisent que les opérateurs de services essentiels, les fournisseurs de service numérique ou les autorités visées à l'article 7 de la loi qui traitent des données à caractère personnel doivent désigner un délégué à la protection des données au sens du RGPD.

Une autre dérogation, plus limitée, concerne 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 dans la mesure nécessaire pour préserver les objectifs de la loi ou l'efficacité d'enquêtes, que cette notification individuelle ne serait plus obligatoire.

TITEL 7
Slotbepalingen
HOOFDSTUK 1
Bescherming van de uitvoerende personeelsleden

Artikel 68

Dit artikel bepaalt dat de personeelsleden en aangestelden van aanbieders van essentiële diensten en digitaledienstverleners die de in deze wet vermelde verplichtingen te goeder trouw en in het kader van hun functie uitvoeren, niet louter op basis daarvan kunnen worden bestraft, noch benadeeld.

TITRE 7
Disposition finales
CHAPITRE 1
Protection des agents d'exécution

Article 68

Cet article prévoit que les agents ou préposés des opérateurs de services essentiels ou fournisseurs de

HOOFDSTUK 2

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

De artikelen 69 tot en met 77 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 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

De artikelen 77 en 78 passen de wet van 15 april 1994 aan en behoeven geen verdere commentaar.

HOOFDSTUK 4

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

De artikelen 79 tot 82 passen de wet van 17 januari 2003 aan en behoeven geen verdere commentaar.

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

service numérique qui exécutent, de bonne foi et dans le cadre de leurs fonctions, les obligations prévues par la présente loi ne peuvent être pénalisés ni désavantagés de ce seul fait.

CHAPITRE 2

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

Les articles 69 à 77 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 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

Les articles 77 et 78 visent à adapter la loi du 15 avril 1994 et n'appellent pas de commentaire particulier.

CHAPITRE 4

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

Les articles 79 à 82 visent à adapter la loi du 17 janvier 2003 et n'appellent pas de commentaire particulier.

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

Les articles 83 et 84 visent à adapter les lois du 21 novembre 2017 et 2 août 2002 et n'appellent pas de

De artikelen 83 en 84 passen de wetten van 21 november 2017 en 2 augustus 2002 aan en behoeven geen verdere commentaar.

HOOFDSTUK 6

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

De artikelen 85 tot 87 passen de wet van 22 februari 1998 aan en behoeven geen verdere commentaar.

HOOFDSTUK 7

Inwerkingtreding

Artikel 88 bepaalt de datum van inwerkingtreding van de wet en behoeft geen verdere commentaar.

BIJLAGE I

Deze bijlage bevat de soorten aanbieders van essentiële diensten die minstens in aanmerking moeten worden genomen voor de identificatie-procedure.

BIJLAGE II

Deze bijlage bevat de soorten digitaledienstverleners.

commentaire particulier.

CHAPITRE 6

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

Les articles 85 à 87 visent à adapter la loi du 22 février 1998 et n'appellent pas de commentaire particulier.

CHAPITRE 7

Entrée en vigueur

L'article 88 fixe la date d'entrée en vigueur de la loi et n'appelle pas de commentaire particulier.

ANNEXE I

Cette annexe reprend les types d'opérateurs de services essentiels qui doivent au minimum être pris en compte par la procédure d'identification.

ANNEXE II

Cette annexe reprend les types de fournisseurs de service numérique.

Wetsontwerp tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.	**Projet de loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.**
Titel 1. - Definities en algemene bepalingen	**Titre 1er. - Définitions et dispositions générales**
Hoofdstuk 1. Onderwerp en toepassingsgebied	**Chapitre 1er. Objet et champ d'application**
Afdeling 1. Onderwerp	**Section 1re. Objet**
Art. 1. Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.	**Art. 1er**. La présente loi règle une matière visée à l'article 74 de la Constitution.
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.	**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".
Afdeling 2. Toepassingsgebied	**Section 2. Champ d'application**
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	**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 1, 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

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.	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. § 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.	**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 1 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.

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. §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.	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. 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. § 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 259bis, 314bis, 380, 382quinquies, 383bis, 383bis/1, 433septies, 433novies/1, 458bis, 550bis en 550ter 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.	**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 259bis, 314bis, 380, 382quinquies, 383bis, 383bis/1, 433septies, 433novies/1, 458bis, 550bis et 550ter du Code pénal, ou d'autres dispositions du droit belge transposant la directive 2011/93/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. 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.	§ 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.
Hoofdstuk 2. Definities	**Chapitre 2. Définitions**
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; 5° "instelling voor de conformiteitsbeoordeling": instelling bedoeld in artikel I.9 van het Wetboek van economisch recht die conformiteitsbeoordelings-activiteiten 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	**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° "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

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 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	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 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

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 netwerk-	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 ;

infrastructuur 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° "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° “domeinnaamsysteem” of “DNS”: een hiërarchisch opgebouwd adresseringssysteem in een netwerk dat een zoekvraag naar een domeinnaam beantwoordt;	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° “DNS-dienstverlener”: een entiteit die DNS-diensten op het internet verleent;	25° "fournisseur de services DNS" : une entité qui fournit des services DNS sur l'internet ;
26° “register voor topleveldomeinnamen”: een entiteit die de internetdomeinnamen van een specifiek topleveldomein registreert en beheert;	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° “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;	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° “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° "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° “cloudcomputerdienst”: een digitale dienst die toegang mogelijk maakt tot een schaalbare en elastische pool van deelbare computercapaciteit;	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° “wet van 1 juli 2011”: de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren;	30° «loi du 1er juillet 2011 » : la loi du 1er juillet 2011 relative à la sécurité et à la protection des infrastructures critiques ;
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.	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	**Chapitre 3. Autorités compétentes et coopération au niveau national**
Afdeling 1. Bevoegde autoriteiten	**Section 1re. Autorités compétentes**
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	**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'Etat fédéral, des Communautés et des Régions, conformément aux modalités prévues à l'article 92*ter* de la loi spéciale du

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.	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	**Section 2. Coopération au niveau national**
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.	**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'Etat, 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.
Hoofdstuk 4. Informatie-uitwisseling	**Chapitre 4. Echanges d'information**
Art. 9. § 1. Dit artikel doet geen afbreuk aan de	**Art. 9.** § 1er. Le présent article ne porte pas préjudice

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 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 digitaledienst-verleners beschermd.	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 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.
Hoofdstuk 5. Nationale strategie voor de beveiliging van netwerk- en informatiesystemen	**Chapitre 5. Stratégie nationale en matière de sécurité des réseaux et des systèmes d'information**
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.	**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. De in paragraaf 1 bedoelde strategie wordt geactualiseerd na advies van de autoriteiten bedoeld in artikel 7 en, in voorkomend geval, van de toezichthoudende autoriteiten persoonsgegevens. Ze heeft minstens betrekking op de sectoren bedoeld in bijlage I en de diensten bedoeld in bijlage II. In deze strategie worden passende strategische en regelgevingsdoelstellingen bepaald om een hoog niveau van beveiliging van netwerk- en informatiesystemen tot stand te brengen en te handhaven. § 3. De nationale strategie voor de beveiliging van netwerk- en informatiesystemen betreft onder meer de volgende punten: a) de doelstellingen en de prioriteiten van de nationale strategie voor de beveiliging van netwerk- en informatiesystemen; b) een governancekader ter verwezenlijking van de doelstellingen en de prioriteiten van de nationale strategie voor de beveiliging van netwerk- en informatiesystemen, met inbegrip van de taken en verantwoordelijkheden van de overheidsorganen en de andere betrokken actoren; c) de bepaling van maatregelen inzake paraatheid, reactie en herstel, met inbegrip van samenwerking tussen de publieke en de particuliere sector; d) een overzicht van de onderwijs-, bewustmakings- en opleidingsprogramma's met betrekking tot de nationale strategie voor de beveiliging van netwerk- en informatiesystemen; e) een overzicht van de plannen voor onderzoek en ontwikkeling met betrekking tot de nationale strategie voor de beveiliging van netwerk- en informatiesystemen; f) een risicobeoordelingsplan om risico's te identificeren; g) een lijst van de verschillende actoren die betrokken zijn bij de uitvoering van de nationale strategie voor de beveiliging van netwerk- en informatiesystemen.	§ 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) 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.
Titel 2. - Netwerk- en informatiesystemen van de aanbieders van essentiële diensten	**Titre 2. - Réseaux et systèmes d'information des opérateurs de services essentiels**
Hoofdstuk 1. Identificatie van de aanbieders van	**Chapitre 1er. Identification des opérateurs de**

essentiële diensten	services essentiels
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. 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, §§ 1 et 4.
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	**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

weerslagniveaus of drempelwaarden. § 2. Behoudens tegenbewijs wordt de verlening van een essentiële dienst geacht afhankelijk te zijn van netwerk- en informatiesystemen.	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. § 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.	**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 foumi 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	**Art. 14.** L'opérateur de services essentiels potentiel transmet à la demande d'une autorité visée à l'article

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.	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. § 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. 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 Etat membre de l'Union européenne, elle en informe les autorités visées à l'article 7, §§ 1er et 4. Ces derniers, en collaboration avec les autorités sectorielles concernées, organisent les discussions avec la ou les autorités nationales étrangères concernées et, le cas échéant, avec les régions ou les communautés concernées. § 3. L'autorité sectorielle notifie à l'opérateur sa décision motivée de désignation en qualité d'opérateur de services essentiels. Cette notification est réalisée de manière sécurisée. Elle communique également copie de cette décision aux autorités visées à l'article 7, §§ 1er et 4. L'autorité sectorielle en informe, le cas échéant, les régions et/ou les communautés concernées.

Art. 16. 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. 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. 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. 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. § 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	**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

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.	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. De Koning kan, bij in Ministerraad overlegd besluit, andere sectoren of soorten aanbieders toevoegen aan bijlage I van deze wet.	**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	**Chapitre 2. Mesures de sécurité**
Artikel 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. 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. § 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	**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

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 het luchtvervoer, worden gelijkgesteld met het I.B.B. indien alle in paragraaf 2 bedoelde informatie erin opgenomen is.	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 P.S.I. lorsque toutes les informations visées au paragraphe 2 y sont reprises.
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 conformiteits-beoordeling die volgens de norm ISO/IEC 17021 of ISO/IEC 17065 geaccrediteerd is door de accreditatie-autoriteit 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	**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, § 1. § 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

conformiteitsbeoordeling geaccrediteerd is en op de volledige inhoud van het I.B.B.	contenu de la PSI.
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.	**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	**Chapitre 3. Notification d'incidents**
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.	**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

§ 4. De Koning kan verschillende meldingscategorieën creëren volgens de mate van impact van het incident.	notification en fonction du degré d'impact de l'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. 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. 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. 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. 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. § 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	**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

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.	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. 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. § 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. 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. § 1. De Koning is belast met de modaliteiten	**Art. 31**. § 1er. Le Roi est chargé de déterminer les

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.	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.
Titel 3. - Netwerk- en informatiesystemen van digitaledienstverleners	**Titre 3. - Réseaux et systèmes d'information des fournisseurs de service numérique**
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).	**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).
Hoofdstuk 1. De beveiligingseisen	**Chapitre 1er. Les exigences de sécurité**
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;	**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;

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 toepassings-bepalingen 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.	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. 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.	**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.
Hoofdstuk 2. Melding van incidenten	**Chapitre 2. Notification d'incidents**
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 toepassings-bepalingen voor Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad wat betreft de nadere	**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

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.	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. 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. 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. § 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	**Art. 37.** § 1er. Lorsque c'est approprié, et notamment si l'incident visé au paragraphe 1er concerne au moins un autre Etat 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

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.	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	**Titre 4. - Contrôle et sanctions**
Hoofdstuk 1. Toezicht op de aanbieders van essentiële diensten	**Chapitre 1er. Les contrôles des opérateurs de services essentiels**
Afdeling 1. Audits	**Section 1re. 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 conformiteits-beoordeling 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. 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. § 1. Na advies van de sectorale overheid en de autoriteit bedoeld in artikel 7, § 1, bepaalt de Koning:	**Art. 39.** § 1er. Après avis de l'autorité sectorielle et de l'autorité visée à l'article 7, § 1er, le Roi fixe :

1° de algemene accreditatievoorwaarden op basis van de eisen van de normen ISO/IEC 17021 of ISO/IEC 17065; 2° de bijkomende sectorale eisen waaraan de instelling voor de conformiteitsbeoordeling onderworpen kan zijn; 3° de regels die van toepassing zijn op de interne audit; 4° de regels die van toepassing zijn op de externe audit. § 2. Bij 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 conformiteits-beoordeling wordt verleend. § 3. De lijst van de geaccrediteerde of erkende instellingen voor de conformiteitsbeoordeling is beschikbaar bij de sectorale overheid die ze actueel houdt.	1° les conditions générales d'accréditation sur base des exigences des normes ISO/IEC 17021 ou ISO/IEC 17065 ; 2° les exigences supplémentaires sectorielles auxquelles peut être soumis l'organisme d'évaluation de la conformité ; 3° les règles applicables à l'audit interne ; 4° les règles applicables à l'audit externe. § 2. Par arrêté délibéré en Conseil des Ministres, le Roi peut également déterminer, après avis de l'autorité sectorielle et de l'autorité visée à l'article 7, § 1er, les conditions d'un éventuel agrément accordé par l'autorité sectorielle à un organisme d'évaluation de la conformité. § 3. La liste des organismes d'évaluation de la conformité accrédités ou agréés est disponible auprès de l'autorité sectorielle qui la tient à jour.
Art. 40. § 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. 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. 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.	**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.
Afdeling 2. Inspectiedienst	**Section 2. Service d'inspection**
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.	**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

§ 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.	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 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. § 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	**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

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.	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.	§ 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. 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;	§ 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° 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 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.	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 ou de l'autorité sectorielle peuvent saisir, contre récépissé contenant un inventaire, le système informatique et les données qu'il contient.
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. 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. § 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.	**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.
Hoofdstuk 2. Toezicht op de digitaledienstverleners	**Chapitre 2. Contrôle des fournisseurs de service numérique**
Art. 47. § 1. De Koning bepaalt de praktische modaliteiten van het toezicht op de digitaledienst-verleners. § 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; 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	**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) 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

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.	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 Etat membre de l'Union européenne. § 7. L'autorité visée à l'article 7, § 1er, peut solliciter du service d'inspection la transmission des rapports 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.
Hoofdstuk 3. De sancties	**Chapitre 3. Les sanctions**
Afdeling 1. Procedure	**Section 1re. Procédure**
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	**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

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.	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. § 1. Als de inspectiedienst vaststelt dat de aanbieder van essentiële diensten of digitaledienst-verlener 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. 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. Inbreuken op deze wet of de uitvoeringsbesluiten ervan kunnen aanleiding geven tot strafrechtelijke of administratieve sancties.	**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.
Afdeling 2. Strafrechtelijke sancties	**Section 2. Sanctions pénales**
Art. 51. § 1. Niet-naleving van een van de meldings-verplichtingen 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.	**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. 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.	§ 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. 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.	§ 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. 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.	§ 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. 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.	§ 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. 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.	§. 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. 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.	§ 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. Inbreuken op artikel 9, paragrafen 2 en 3, van deze wet geven aanleiding tot de straffen bepaald in artikel 458 van het Strafwetboek.	§ 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.
Afdeling 3. Administratieve sancties	**Section 3. Sanctions administratives**
Art. 52. § 1. Elke inbreuk op deze wet, op de	**Art. 52.** § 1er. Toute infraction à la présente loi, à ses

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 €. § 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 €.	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. 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. 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. 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. 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	**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.

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. § 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. 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. 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. 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. 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. 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.	**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

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.	conformément aux articles 1035 à 1038, 1040 et 1041 du Code judiciaire. Ce recours ne suspend pas l'exécution de la décision.
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. 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.	**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. 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. 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.	§ 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. 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.	**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	**Titre 5. CSIRT**
Hoofdstuk 1. Het nationale CSIRT	**Chapitre 1er. Le CSIRT national**
Afdeling 1. Taken van het nationale CSIRT	**Section 1re. Tâches du CSIRT national**
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;	**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 ;

Na advies van het nationale CSIRT kan de Koning dit CSIRT extra taken toevertrouwen.	Après avis du CSIRT national, le Roi peut lui confier des tâches supplémentaires.
Afdeling 2. Voorschriften voor het nationale CSIRT	**Section 2. Obligations du CSIRT national**
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. 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. 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	**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

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.	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	**Chapitre 2. Le CSIRT sectoriel**
Afdeling 1. Taken van het sectoraal CSIRT	**Section 1re. Tâches du CSIRT sectoriel**
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.	**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.
Afdeling. 2. Voorschriften voor een sectoraal CSIRT	**Section 2. Obligations d'un CSIRT sectoriel**
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.	**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

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.	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.
Titel 6. Verwerking van persoonsgegevens	**Titre 6. Traitement des données à caractère personnel**
Art. 65. § 1. Overeenkomstig artikel 23.1, a), b), c), d), e), h), van 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	**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.

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.	§ 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. 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 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. 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 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. § 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	**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

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.	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	**Titre 7. - Dispositions finales**
Hoofdstuk 1. Bescherming van de uitvoerende personeelsleden	**Chapitre 1er. Protection des agents d'exécution**
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.	**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.
Hoofdstuk 2. Wijzigingen van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren	**Chapitre 2. Modifications de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques**
Art. 69. Artikel 2 van de wet van 1 juli 2011 wordt aangevuld met een derde lid, als volgt:	**Art. 69.** L'article 2 de la loi du 1er juillet 2011 est complété par un troisième alinéa rédigé comme suit :

"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.".	« 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. 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); 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;";	**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) 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. ».

- 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. 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. 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. 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. 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. 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. 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. 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 beveiligings-contactpunt, 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. 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. In artikel 22 van de wet van 1 juli 2011 worden	**Art. 76.** A l'article 22 de la loi du 1er juillet 2011, les

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,”.	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. 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. 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.	**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. 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. 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. In de wet van 15 april 1994 wordt een artikel 15ter ingevoegd, dat als volgt luidt: “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. De Koning bepaalt de praktische inspectiemodaliteiten, na advies van het Agentschap.”.	**Art. 79.** Il est inséré un article 15ter dans la loi du 15 avril 1994, rédigé comme suit : « 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. ».

Hoofdstuk 4. Wijzigingen van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector	**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. 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. 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. 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: - 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	**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 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

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.”.	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. 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”.	**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	**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. § 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	**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. ».

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”.	**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	**Chapitre 6. Modifications de la loi du 22 février 1998 fixant le statut organique de la Banque Nationale de Belgique**
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. 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. 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. 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. 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	**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

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. De Bank deelt relevante informatie over incidentmeldingen die zij ontvangt krachtens de wet van … 2018 zo snel mogelijk met de ECB.".	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. 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. ».
Hoofdstuk 7. Inwerkingtreding	**Chapitre 7. Entrée en vigueur**
Art. 88. Deze wet treedt in werking de dag waarop ze in het Belgisch Staatsblad wordt bekendgemaakt.	**Art. 88.** La présente loi entre en vigueur le jour de sa publication au Moniteur belge.

Bijlage I

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. Water		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

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		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 **Soorten digitale diensten** 1. Onlinemarktplaats 2. Onlinezoekmachines 3. Cloudcomputerdiensten	**Annexe II** **Types de services numériques** 1. Place de marché en ligne 2. Moteurs de recherche en ligne 3. Service d'informatique en nuage