Publicatie : 2019-05-03
Numac : 2019011507

einde

FEDERALE OVERHEIDSDIENST KANSELARIJ VAN DE EERSTE MINISTER

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

FILIP, Koning der Belgen,
Aan allen die nu zijn en hierna wezen zullen, Onze Groet.
De Kamer van volksvertegenwoordigers heeft aangenomen en Wij bekrachtigen, hetgeen volgt :
TITEL 1. - Definities en algemene bepalingen
HOOFDSTUK 1. - Onderwerp en toepassingsgebied
Afdeling 1. - Onderwerp
Artikel 1. Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.
Art. 2. Deze wet voorziet met name in de omzetting van de Europese Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, hierna de "NIS-richtlijn" genoemd.
Afdeling 2. - Toepassingsgebied
Art. 3. § 1. Deze wet is van toepassing op de aanbieders van essentiële diensten, zoals gedefinieerd in artikel 6, 11°, die minstens één vestiging op Belgisch grondgebied hebben en daadwerkelijk een activiteit uitoefenen die betrekking heeft op de verlening van minstens één essentiële dienst op Belgisch grondgebied.
De bepalingen van titel 1, de artikelen 13, 14 en 30, alsook hoofdstuk 3 van titel 4 zijn van toepassing op de potentiële aanbieders van essentiële diensten.
§ 2. Deze wet is van toepassing op de digitaledienstverleners, zoals gedefinieerd in artikel 6, 21°, die hun hoofdkantoor in België hebben. Een digitaledienstverlener wordt geacht zijn hoofdkantoor in België te hebben als zijn maatschappelijke zetel zich daar bevindt.
Deze wet is ook van toepassing op de digitaledienstverleners die niet in de Europese Unie gevestigd zijn wanneer zij in België diensten verlenen als bedoeld in bijlage II en hun vertegenwoordiger in België gevestigd is in het kader van de NIS-richtlijn.
Art. 4. § 1. De beveiligings- en meldingseisen bedoeld in deze wet zijn niet van toepassing op ondernemingen die onderworpen zijn aan de eisen van de artikelen 114 en 114/1 van de wet van 13 juni 2005 betreffende de elektronische communicatie, wat hun activiteiten betreft op het gebied van het aanbieden van openbare 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 eerste lid, nader te bepalen.
§ 3. Deze wet is niet van toepassing op de aanbieders die behoren tot de sector financiën in de zin van bijlage I bij deze wet, met uitzondering van de bepalingen van titel I, hoofdstuk 1 van titel II en van artikel 26.
In afwijking van het eerste lid is artikel 52 van toepassing op de aanbieders die behoren tot de sector financiën in de zin van bijlage I bij deze wet, met uitzondering van de exploitanten van een handelsplatform in de zin van artikel 3, 6°, van de wet van 21 november 2017 over de infrastructuren voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU.
De sectorale overheden en de aanbieders die behoren tot de sector financiën in de zin van bijlage I bij deze wet zijn onderworpen aan de artikelen 65 tot 73.
In afwijking op wat voorafgaat zijn de artikelen 65 tot 73 niet van toepassing op de betrokken sectorale overheid wanneer deze laatste optreedt in de gevallen bedoeld in artikel 46bis van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten, of in artikel 12quater van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België.
§ 4. Deze wet is niet van toepassing wanneer en voor zover er maatregelen voor de beveiliging van netwerk- en informatiesystemen bestaan krachtens de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle.
In afwijking van het eerste lid is deze wet van toepassing op de elementen van een nucleaire installatie bestemd voor de industriële productie van elektriciteit die dienen voor de transmissie van de elektriciteit.
Art. 5. § 1. Onder voorbehoud van de bepalingen van titel 6 doet deze wet geen afbreuk aan de toepassing van Verordening EU 2016/679 of aan de wettelijke en reglementaire bepalingen die deze verordening aanvullen of verduidelijken.
§ 2. Deze wet doet geen afbreuk aan de toepassing van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, aan de artikelen 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 2011/92/EU van het Europees Parlement en de Raad van 13 december 2011 ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie, en ter vervanging van Kaderbesluit 2004/68/JBZ van de Raad, en van Richtlijn 2013/40/EU van het

Europees Parlement en de Raad van 12 augustus 2013 over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad.
§ 3. Deze wet doet geen afbreuk aan de regels die van toepassing zijn op de verwerking van informatie, documenten of gegevens, materieel, materialen of stoffen, in welke vorm ook, die geclassificeerd zijn overeenkomstig de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheids-adviezen.
§ 4. Deze wet doet geen afbreuk aan de regels die van toepassing zijn op de nucleaire documenten, in de zin van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle.
HOOFDSTUK 2. - Definities
Art. 6. Voor de toepassing van deze wet moet worden verstaan onder:
1° "nationaal CSIRT": het nationale computer security incident response team, aangewezen door de Koning;
2° "sectorale overheid": de overheid aangewezen door de wet of de Koning bij besluit vastgesteld na overleg in de Ministerraad;
3° "sectoraal CSIRT": het sectorale computer security incident response team, aangewezen door de Koning;
4° "toezichthoudende autoriteit persoonsgegevens": toezichthoudende autoriteit in de zin van artikel 4, 21°, van Verordening EU 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming);
5° "instelling voor de conformiteitsbeoordeling": instelling bedoeld in artikel I.9.7° van het Wetboek van economisch recht;
6° "certificeringsaudit": een audit uitgevoerd in het kader van een certificering bedoeld in artikel 22, § 2;
7° "nationale accreditatieautoriteit": instelling die door de Koning is opgericht in uitvoering van artikel VIII.30 van het Wetboek van economisch recht;
8° "netwerk- en informatiesysteem":
a) een elektronische-communicatienetwerk in de zin van artikel 2, 3°, van de wet van 13 juni 2005 betreffende de elektronische communicatie;
b) een apparaat of groep van permanent of tijdelijk gekoppelde of bij elkaar behorende apparaten, waarvan een of meer elementen, in uitvoering van een programma, digitale gegevens automatisch verwerken, met inbegrip van de digitale, elektronische of mechanische componenten van dat apparaat die met name de automatisering van het operationele proces, de controle op afstand of het verkrijgen van werkingsgegevens in real time mogelijk maken;
c) of digitale gegevens die via in de bepalingen onder a) en b), bedoelde elementen worden opgeslagen, verwerkt, opgehaald of verzonden met het oog op de werking, het gebruik, de beveiliging en het onderhoud ervan;
9° "beveiliging van netwerk- en informatiesystemen": het vermogen van netwerk- en informatiesystemen om met een bepaalde mate van betrouwbaarheid bestand te zijn tegen acties die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van de opgeslagen, verzonden of verwerkte gegevens of de daaraan gerelateerde diensten die via die netwerk- en informatiesystemen worden aangeboden of toegankelijk zijn, in gevaar brengen;

10° "nationale strategie voor de beveiliging van netwerk- en informatiesystemen": een kader met strategische doelstellingen en prioriteiten op het gebied van de beveiliging van netwerk- en informatiesystemen op nationaal niveau;
11° "aanbieder van essentiële diensten": een publieke of private entiteit die actief is in België in een van de sectoren opgenomen in bijlage I bij deze wet, die aan de criteria bedoeld in artikel 12, § 1, voldoet en die als dusdanig is aangewezen door de sectorale overheid;
12° "potentiële aanbieder van essentiële diensten": een publieke of private entiteit die in België actief is in een van de sectoren opgenomen in bijlage I bij deze wet, maar niet is aangewezen als aanbieder van essentiële diensten;
13° "incident": elke gebeurtenis met een reële negatieve impact op de beveiliging van netwerk- en informatiesystemen;
14° "incidentenbehandeling": alle procedures ter ondersteuning van de opsporing, analyse en beheersing van en reactie op een incident;
15° "risico": elke redelijkerwijs vast te stellen omstandigheid of gebeurtenis met een mogelijke negatieve impact op de beveiliging van netwerk- en informatiesystemen;
16° "intersectoraal criterium": factor die gemeenschappelijk is voor alle sectoren bedoeld in bijlage I bij deze wet en die het belang van een verstorend effect voor de verlening van een essentiële dienst in de zin van artikel 12, § 1, c), bepaalt;
17° "sectoraal criterium": factor die eigen is aan een sector of deelsector bedoeld in bijlage I bij deze wet en die het belang van een verstorend effect voor de verlening van een essentiële dienst in de zin van artikel 12, § 1, c), bepaalt;
18° "beveiligingsbeleid voor de netwerk- en informatiesystemen (I.B.B.)" : een document als bedoeld in artikel 21, § 1, met de maatregelen voor de beveiliging van de netwerk- en informatiesystemen die een aanbieder van essentiële diensten heeft genomen;
19° "contactpunt voor de beveiliging van netwerk- en informatiesystemen": het contactpunt aangewezen door de aanbieder van essentiële diensten of de digitaledienstverlener dat de functie van contactpunt uitoefent ten aanzien van de autoriteiten bedoeld in artikel 7, voor elke vraag in verband met de beveiliging van de netwerk- en informatiesystemen waarvan de verleende essentiële diensten afhankelijk zijn.
20° "digitale dienst": een dienst in de zin van artikel 1, lid 1, punt b), van de Europese Richtlijn 2015/1535 van het Europees Parlement en de Raad van 9 september 2015 betreffende een informatieprocedure op het gebied van technische voorschriften en regels betreffende de diensten van de informatiemaatschappij, en waarvan de soort is vermeld in de lijst in bijlage II;
21° "digitaledienstverlener": elke rechtspersoon die een digitale dienst aanbiedt als bedoeld in bijlage II bij deze wet;
22° "vertegenwoordiger van een digitaledienstverlener": elke in België gevestigde natuurlijke of rechtspersoon die uitdrukkelijk is aangewezen om voor rekening van een niet in de Unie gevestigde digitaledienstverlener op te treden en die door de nationale autoriteit bedoeld in artikel 7, § 1, de bevoegde sectorale overheid of de bevoegde inspectiedienst kan worden gecontacteerd in plaats van de digitaledienstverlener, wat de uit deze wet voortvloeiende verplichtingen van deze laatste betreft;
23° "internetknooppunt (IXP)": een netwerkinfrastructuur die de onderlinge verbinding van meer dan twee onafhankelijke autonome systemen mogelijk maakt, voornamelijk met als doel de uitwisseling van internetverkeer te vergemakkelijken;

een internetknooppunt zorgt enkel voor onderlinge verbinding voor autonome systemen; een internetknooppunt vereist niet dat het internetverkeer tussen twee deelnemende autonome systemen via een derde autonoom systeem verloopt, noch dat het internetknooppunt dergelijk verkeer wijzigt of anderszins daartussen komt;
24° "domeinnaamsysteem" of "DNS": een hiërarchisch opgebouwd adresseringssysteem in een netwerk dat een zoekvraag naar een domeinnaam beantwoordt;
25° "DNS-dienstverlener": een entiteit die DNS-diensten op het internet verleent;
26° "register voor topleveldomeinnamen": een entiteit die de internetdomeinnamen van een specifiek topleveldomein registreert en beheert;
27° "onlinemarktplaats": een digitale dienst die het consumenten, zoals gedefinieerd in artikel I.1., eerste lid, 2°, van het Wetboek van economisch recht, en/of ondernemingen, zoals gedefinieerd in artikel I.8, 39°, van hetzelfde Wetboek, mogelijk maakt online verkoop- of dienstenovereenkomsten met ondernemingen te sluiten op de website van de onlinemarktplaats of op de website van een onderneming die gebruikmaakt van door de onlinemarktplaats aangeboden informaticadiensten;
28° "onlinezoekmachine": een digitale dienst die het gebruikers mogelijk maakt zoekacties uit te voeren op in principe alle websites of websites in een bepaalde taal op basis van een zoekvraag over om het even welk onderwerp in de vorm van een trefwoord, een zin of andere input; het resultaat zijn hyperlinks naar informatie over de opgevraagde inhoud;
29° "cloudcomputerdienst": een digitale dienst die toegang mogelijk maakt tot een schaalbare en elastische pool van deelbare computercapaciteit;
30° "wet van 1 juli 2011": de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren;
31° "wet van 11 december 1998": de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen;
32° "wet van 15 april 1994": de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle.
33° "Verordening EU 2016/679": de Europese Verordening 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).
HOOFDSTUK 3. - Bevoegde autoriteiten en samenwerking op nationaal niveau
Afdeling 1. - Bevoegde autoriteiten
Art. 7. § 1. De Koning wijst de autoriteit aan die, als nationale autoriteit, belast is met de opvolging en coördinatie van de uitvoering van deze wet.
De autoriteit bedoeld in het eerste lid is ook het centraal nationaal contactpunt voor de beveiliging van netwerk- en informatiesystemen, voor alle aanbieders van essentiële diensten en digitaledienstverleners, voor België in zijn relatie met de Europese Commissie, de lidstaten van de Europese Unie, de in artikel 11 van de NIS-richtlijn bedoelde Samenwerkingsgroep en het CSIRT-netwerk. Daartoe vertegenwoordigt het contactpunt België binnen de Samenwerkingsgroep.
§ 2. De Koning wijst de autoriteit aan die de rol van nationaal CSIRT vervult.
Het nationale CSIRT vertegenwoordigt België binnen het CSIRT-netwerk bedoeld in

artikel 12 van de NIS-richtlijn. Het werkt op doeltreffende, efficiënte en beveiligde wijze mee aan de opdrachten van het CSIRT-netwerk.
§ 3. De Koning wijst, bij besluit vastgesteld na overleg in de Ministerraad, de sectorale overheden aan die, voor hun respectie-velijke 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 nadere regels bepaald in artikel 92ter van de bijzondere wet van 8 augustus 1980 tot hervorming der instellingen.
In afwijking van het eerste lid wijst de wet zelf de bij wet opgerichte en geregelde sectorale overheden aan.
§ 4. De Koning wijst de autoriteit aan die, in samenwerking met de nationale autoriteit bedoeld in paragraaf 1, de identificatie van aanbieders van essentiële diensten coördineert.
§ 5. Per sector of, in voorkomend geval, per deelsector wordt een inspectiedienst opgericht die toeziet op de naleving van de bepalingen van deze wet en van de uitvoeringsbesluiten ervan door aanbieders van essentiële diensten of digitaledienstverleners.
De Koning wijst voor een welbepaalde sector of, in voorkomend geval, per deelsector de inspectiedienst aan die bevoegd is voor het toezicht.
In afwijking van het tweede lid wijst de wet de door haar opgerichte en geregelde inspectiediensten aan.
Afdeling 2. - Samenwerking op nationaal niveau
Art. 8. § 1. De autoriteiten bedoeld in artikel 7 werken nauw samen om de in deze wet vastgestelde verplichtingen te vervullen.
§ 2. Naargelang de behoeften die nodig zijn voor de uitvoering van de wet en overeenkomstig de toepasselijke wettelijke bepalingen werken de in paragraaf 1 bedoelde autoriteiten, op nationaal niveau, ook samen met de administratieve diensten van de Staat, de administratieve autoriteiten, de gerechtelijke autoriteiten, de inlichtingen- en veiligheidsdiensten bedoeld in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, de politiediensten bedoeld in de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus, en met de toezichthoudende autoriteiten persoonsgegevens.
§ 3. De aanbieder van essentiële diensten, de digitaledienstverlener en de autoriteiten bedoeld in artikel 7 werken te allen tijde samen door een adequate uitwisseling van informatie over de beveiliging van de netwerk- en informatiesystemen.
HOOFDSTUK 4. - Informatie-uitwisseling
Art. 9. § 1. Dit artikel doet geen afbreuk aan de toepassing van de wet van 11 december 1998, de wet van 15 april 1994, de wet van 11 april 1994 betreffende de openbaarheid van bestuur of andere wettelijke bepalingen die de vertrouwelijkheid van de informatie m.b.t. de wezenlijke belangen van de nationale openbare veiligheid waarborgen.
De autoriteiten bedoeld in artikel 7, de aanbieder van essentiële diensten, de digitaledienstverlener, of hun onderaannemers, beperken de toegang tot de informatie over de uitvoering van deze wet tot de personen die er de kennis van nodig hebben en er toegang toe moeten hebben voor de uitoefening van hun functie of opdracht die verband houdt met deze wet.
§ 2. De personeelsleden van de aanbieder van essentiële diensten, de

digitaledienstverlener, of hun onderaannemers, zijn gebonden aan het beroepsgeheim wat de informatie over de uitvoering van deze wet betreft.
Personen die uit hoofde van hun staat of beroep kennis dragen van geheimen die hun zijn toevertrouwd, mogen deze geheimen bekendmaken voor de uitvoering van deze wet.
§ 3. De informatie die door aanbieders van essentiële diensten en digitaledienstverleners aan de autoriteiten bedoeld in artikel 7 wordt bezorgd, mag worden uitgewisseld met autoriteiten van de Europese Unie, Belgische of buitenlandse autoriteiten, wanneer die uitwisseling noodzakelijk is voor de toepassing van wettelijke bepalingen.
De uitgewisselde informatie wordt beperkt tot hetgeen relevant is voor en evenredig is met het doel van die uitwisseling, met name overeenkomstig Verordening EU 2016/679. Bij die uitwisseling van informatie wordt de vertrouwelijkheid van de informatie gewaarborgd en worden de veiligheid en de commerciële belangen van de aanbieders van essentiële diensten en de digitaledienstverleners beschermd.
HOOFDSTUK 5. - Nationale strategie voor de beveiliging van netwerk- en informatiesystemen
Art. 10. § 1. De Koning wijst, bij besluit vastgesteld na overleg in de Ministerraad, de autoriteit aan die belast is met de actualisering van de bestaande nationale strategie voor de beveiliging van netwerk- en informatiesystemen.
§ 2. De in paragraaf 1 bedoelde strategie wordt geactualiseerd na advies van de autoriteiten bedoeld in artikel 7 en, in voorkomend geval, van de toezichthoudende autoriteiten persoonsgegevens. Ze heeft minstens betrekking op de sectoren bedoeld in bijlage I en de diensten bedoeld in bijlage II.
In deze strategie worden passende strategische en regelgevingsdoelstellingen bepaald om een hoog niveau van beveiliging van netwerk- en informatiesystemen tot stand te brengen en te handhaven.
§ 3. De nationale strategie voor de beveiliging van netwerk- en informatiesystemen betreft onder meer de volgende punten:
a) de doelstellingen en de prioriteiten van de nationale strategie voor de beveiliging van netwerk- en informatiesystemen;
b) een governancekader ter verwezenlijking van de doelstellingen en de prioriteiten van de nationale strategie voor de beveiliging van netwerk- en informatiesystemen, met inbegrip van de taken en verantwoordelijkheden van de overheidsorganen en de andere betrokken actoren;
c) de bepaling van maatregelen inzake paraatheid, reactie en herstel, met inbegrip van samenwerking tussen de publieke en de particuliere sector;
d) een overzicht van de onderwijs-, bewustmakings- en opleidingsprogramma's met betrekking tot de nationale strategie voor de beveiliging van netwerk- en informatiesystemen;
e) een overzicht van de plannen voor onderzoek en ontwikkeling met betrekking tot de nationale strategie voor de beveiliging van netwerk- en informatiesystemen;
f) een risicobeoordelingsplan om risico's te identificeren;
g) een lijst van de verschillende actoren die betrokken zijn bij de uitvoering van de nationale strategie voor de beveiliging van netwerk- en informatiesystemen.
TITEL 2. - Netwerk- en informatiesystemen van de aanbieders van essentiële diensten
HOOFDSTUK 1. - Identificatie van de aanbieders van essentiële diensten
Art. 11. § 1. De sectorale overheid identificeert de aanbieders van essentiële diensten van haar sector en houdt hierbij minstens rekening met de soorten aanbieders

bedoeld in bijlage I van deze wet.
Binnen de grenzen van hun respectievelijke bevoegdheden overleggen de autoriteiten bedoeld in artikel 7, §§ 1 en 4, met de sectorale overheid om over te gaan tot deze identificatie.
De sectorale overheid raadpleegt, in voorkomend geval, de betrokken gewesten of gemeenschappen en de vertegenwoordigers van de in bijlage I bedoelde entiteiten.
§ 2. Na raadpleging van de potentiële aanbieder van essentiële diensten deelt de sectorale overheid deze aanbieder mee welke door hem verleende dienst of diensten als essentieel worden beschouwd.
§ 3. De sectorale overheid zorgt voor een permanente opvolging van het identificatie- en aanwijzingsproces van de aanbieders van essentiële diensten en van hun essentiële diensten, volgens de in dit hoofdstuk beschreven procedures. Dit proces vindt voor het eerst plaats uiterlijk binnen zes maanden na de inwerkingtreding van deze wet.
De sectorale overheid evalueert en, in voorkomend geval, actualiseert minstens om de twee jaar de identificatie van de aanbieders van essentiële diensten en van hun essentiële diensten.
De actualiseringen worden naar de autoriteiten bedoeld in artikel 7, §§ 1 en 4, gestuurd.
Art. 12. § 1. Om de in artikel 11 bedoelde aanbieders te identificeren, past de sectorale overheid de volgende criteria toe:
a) de entiteit verleent een dienst die van essentieel belang is voor de instandhouding van kritieke maatschappelijke en/of economische activiteiten;
b) de verlening van die dienst is afhankelijk van netwerk- en informatiesystemen; en
c) een incident kan aanzienlijke verstorende effecten hebben voor de verlening van die dienst, rekening houdend met de in artikel 13 bedoelde criteria en weerslagniveaus of drempelwaarden.
§ 2. Behoudens tegenbewijs wordt de verlening van een essentiële dienst geacht afhankelijk te zijn van netwerk- en informatiesystemen.
Art. 13. § 1. Om het belang van het in artikel 12, § 1, c), bedoelde verstorende effect vast te stellen, bepaalt de sectorale overheid sectorale en/of intersectorale criteria, weerslagniveaus of drempelwaarden voor haar sector.
Het aanzienlijke verstorende effect staat vast zodra de potentiële aanbieder van essentiële diensten aan een drempelwaarde of weerslagniveau voldoet.
Binnen de grenzen van hun respectievelijke bevoegdheden overleggen de autoriteiten bedoeld in artikel 7, §§ 1 en 4, met de sectorale overheid om de criteria, weerslagniveaus en drempelwaarden te bepalen, in voorkomend geval na raadpleging van de betrokken gewesten of gemeenschappen en van de vertegenwoordigers van de in bijlage I bedoelde entiteiten.
§ 2. De sectorale overheid houdt minstens rekening met de volgende intersectorale criteria op basis van de beschikbare informatie:
a) het aantal gebruikers dat afhankelijk is van de door de betrokken entiteit verleende dienst;
b) de afhankelijkheid van de andere in bijlage I bedoelde sectoren van de door die entiteit verleende dienst;
c) de gevolgen die incidenten kunnen hebben, wat betreft mate en duur, voor economische of maatschappelijke activiteiten of de openbare veiligheid;
d) het marktaandeel van die entiteit;
e) de omvang van het geografische gebied dat door een incident kan worden

getroffen;
f) het belang van de entiteit voor de instandhouding van een toereikend dienstverleningsniveau, rekening houdend met de beschikbare alternatieven voor het verlenen van die dienst.
§ 3. Na advies van de autoriteiten bedoeld in artikel 7 en raadpleging van de betrokken gewesten en gemeenschappen kan de Koning deze intersectorale criteria aanvullen.
Art. 14. De potentiële aanbieder van essentiële diensten bezorgt, op verzoek van een autoriteit bedoeld in artikel 7, alle nuttige informatie over zijn eventuele identificatie als aanbieder van essentiële diensten, met inbegrip van de informatie die toelaat te objectiveren of de verlening van de essentiële dienst al dan niet afhankelijk is van netwerk- en informatiesystemen.
De door de potentiële aanbieder overgezonden relevante informatie wordt meegedeeld aan de andere autoriteiten bedoeld in artikel 7.
Art. 15. § 1. De sectorale overheid bezorgt de autoriteiten bedoeld in artikel 7, §§ 1 en 4, een met redenen omkleed voorstel van lijst van aanbieders van essentiële diensten van haar sector, samen met een of meer toegepaste identificatiecriteria.
Wanneer de sectorale overheid geen enkele aanbieder van essentiële diensten binnen een sector of deelsector heeft voorgesteld, licht ze de redenen hiervoor schriftelijk toe.
De autoriteiten bedoeld in artikel 7, §§ 1 en 4, brengen, binnen de grenzen van hun respectievelijke bevoegdheden, advies uit over het met redenen omklede voorstel van lijst, in voorkomend geval na raadpleging van de gewesten en gemeenschappen.
§ 2. Wanneer de sectorale overheid vaststelt dat de entiteit die zij voornemens is aan te wijzen als aanbieder van essentiële diensten een of meer essentiële diensten in minstens één andere lidstaat van de Europese Unie verleent, brengt ze de autoriteiten bedoeld in artikel 7, §§ 1 en 4, daarvan op de hoogte. Deze laatsten organiseren, in samenwerking met de betrokken sectorale overheden, de besprekingen met de betrokken buitenlandse nationale autoriteit of autoriteiten en, in voorkomend geval, met de betrokken gewesten of gemeenschappen.
§ 3. De sectorale overheid stelt de aanbieder in kennis van haar met redenen omklede beslissing betreffende zijn aanwijzing als aanbieder van essentiële diensten. Deze kennisgeving gebeurt op beveiligde wijze.
Ze bezorgt ook een kopie van deze beslissing aan de autoriteiten bedoeld in artikel 7, §§ 1 en 4.
In voorkomend geval brengt de sectorale overheid de betrokken gewesten en/of gemeenschappen hiervan op de hoogte.
Art. 16. Binnen drie maanden na zijn aanwijzing bezorgt de aanbieder van essentiële diensten de sectorale overheid een beschrijving van de netwerk- en informatiesystemen waarvan de verlening van de betrokken essentiële dienst of diensten afhankelijk is.
De sectorale overheid bezorgt deze beschrijving aan de autoriteit bedoeld in artikel 7, § 1.
Art. 17. Onverminderd de eventuele toepassing van de wet van 11 december 1998 worden de bestuursdocumenten betreffende de toepassing van dit hoofdstuk als bestuursdocumenten beschouwd die verband houden met de veiligheid van de bevolking, de openbare orde en de veiligheid, in de zin van artikel 6, § 1, van de wet van 11 april 1994 betreffende de openbaarheid van bestuur, en die niet het voorwerp mogen uitmaken van inzage, uitleg of mededeling in afschrift voor het publiek.

Art. 18. § 1. In afwijking van artikel 11 wijst de sectorale overheid de exploitanten van kritieke infrastructuren aan, zoals aangeduid krachtens artikel 8 van de wet van 1 juli 2011 en artikel 6 van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer, als aanbieders van essentiële diensten, wanneer hun sector is opgenomen in bijlage I van deze wet en de verlening van hun essentiële diensten afhankelijk is van netwerk- en informatiesystemen.
Deze aanwijzing gebeurt in overleg met de autoriteiten bedoeld in artikel 7, §§ 1 en 4, binnen de grenzen van hun respectievelijke bevoegdheden.
§ 2. Behoudens tegenbewijs wordt de exploitatie van een kritieke infrastructuur geacht afhankelijk te zijn van netwerk- en informatiesystemen.
§ 3. De exploitant bezorgt de sectorale overheid, op haar verzoek of op verzoek van de autoriteiten bedoeld in artikel 7, §§ 1 en 4, alle nuttige informatie over zijn eventuele identificatie als aanbieder van essentiële diensten, met inbegrip van de informatie die toelaat te objectiveren of hij al dan niet afhankelijk is van netwerk- en informatiesystemen.
De sectorale overheid bezorgt de door de exploitant meegedeelde relevante informatie aan de autoriteiten bedoeld in artikel 7, §§ 1 en 4.
§ 4. Artikel 15, § 3, is van toepassing op de met redenen omklede beslissing tot aanwijzing van een exploitant van een kritieke infrastructuur als aanbieder van essentiële diensten.
Art. 19. De Koning kan, bij besluit vastgesteld na overleg in de Ministerraad, andere sectoren of soorten aanbieders toevoegen aan bijlage I van deze wet.
HOOFDSTUK 2. - Beveiligingsmaatregelen
Art. 20. De aanbieder van essentiële diensten neemt passende en evenredige technische en organisatorische maatregelen om de risico's voor de beveiliging van netwerk- en informatiesystemen waarvan zijn essentiële diensten afhankelijk zijn, te beheersen.
Deze maatregelen zorgen, rekening houdend met de stand van de technische kennis, voor een niveau van fysieke en logische beveiliging van netwerk- en informatiesystemen dat is afgestemd op de risico's die zich voordoen.
De aanbieder neemt ook passende maatregelen om incidenten die de beveiliging van de voor de verlening van die essentiële diensten gebruikte netwerk- en informatiesystemen aantasten, te voorkomen of de gevolgen ervan te minimaliseren, teneinde de continuïteit van deze diensten te waarborgen.
Art. 21. § 1. De aanbieder van essentiële diensten werkt een beveiligingsbeleid uit voor zijn netwerk- en informatiesystemen (hierna "I.B.B." genoemd) dat minstens de in artikel 20 bedoelde concrete beveiligingsdoelstellingen en -maatregelen bevat.
§ 2. De aanbieder van essentiële diensten werkt zijn I.B.B. uiterlijk uit binnen een termijn van twaalf maanden na de kennisgeving van zijn aanwijzing. Hij implementeert de in zijn I.B.B. beschreven maatregelen uiterlijk binnen een termijn van vierentwintig maanden na de kennisgeving van zijn aanwijzing.
Voor een welbepaalde sector of, in voorkomend geval, per deelsector kan de bevoegde sectorale overheid deze termijn aanpassen in functie van het soort maatregelen waarin het I.B.B. voorziet.
§ 3. Na advies van de autoriteiten bedoeld in artikel 7 en, in voorkomend geval, na raadpleging van de betrokken gewesten of gemeenschappen kan de Koning de aanbieders van essentiële diensten van een of meer sectoren beveiligingsmaatregelen opleggen.

§ 4. In overleg met de autoriteit bedoeld in artikel 7, § 1, en, in voorkomend geval, na raadpleging van de gewesten of gemeenschappen kan de sectorale overheid, bij individuele administratieve beslissing, bijkomende beveiligingsmaatregelen opleggen.
§ 5. De maatregelen voor de fysieke en logische beveiliging van netwerk- en informatiesystemen die zijn opgenomen in het beveiligingsplan van de exploitant (B.P.E.) bedoeld in artikel 13 van de wet van 1 juli 2011 en in artikel 11 van het koninklijk besluit van 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer, worden gelijkgesteld met het I.B.B. indien alle in paragraaf 2 bedoelde informatie erin opgenomen is.
Art. 22. § 1. Het I.B.B. bedoeld in artikel 21, § 1, wordt tot bewijs van het tegendeel geacht conform te zijn met de beveiligingseisen bedoeld in artikel 20, indien de beveiligingsmaatregelen die het invoert voldoen aan de eisen van de norm ISO/IEC 27001 of aan een nationale, buitenlandse of internationale norm die door de Koning als gelijkwaardig wordt erkend, bij besluit vastgesteld na overleg in de Ministerraad.
Het in het eerste lid bedoelde besluit wordt genomen na advies van de nationale accreditatieautoriteit, de sectorale overheid en de autoriteit bedoeld in artikel 7, § 1.
§ 2. De naleving van de eisen bedoeld in paragraaf 1 wordt aangetoond aan de hand van een certificaat uitgereikt door een instelling voor de conformiteitsbeoordeling die volgens de norm ISO/IEC 17021 of ISO/IEC 17065 geaccrediteerd is door de nationale accreditatieautoriteit of door een instelling die de erkenningsakkoorden van de "European Cooperation for Accreditation" medeondertekend heeft.
Het uitgereikte certificaat moet betrekking hebben op het certificeringsdomein waarvoor de instelling voor de conformiteitsbeoordeling geaccrediteerd is en op de volledige inhoud van het I.B.B.
Art. 23. § 1. De aanbieder van essentiële diensten wijst zijn contactpunt aan voor de beveiliging van netwerk- en informatiesystemen en deelt de gegevens ervan mee aan de bevoegde sectorale overheid binnen een termijn van drie maanden na de kennisgeving van de aanwijzing als aanbieder van essentiële diensten, en, onverwijld, na elke actualisering van deze gegevens.
De sectorale overheid stelt deze gegevens ter beschikking van de autoriteiten bedoeld in artikel 7, §§ 1, en 4.
§ 2. Indien er reeds een beveiligingscontactpunt bestaat krachtens nationale of internationale bepalingen die van toepassing zijn in een sector of een deelsector, bezorgt de aanbieder van essentiële diensten de contactgegevens ervan aan de sectorale overheid binnen de in paragraaf 1 bedoelde termijnen.
§ 3. Het in paragraaf 1 bedoelde contactpunt voor de beveiliging van netwerk- en informatiesystemen is te allen tijde beschikbaar.
HOOFDSTUK 3. - Melding van incidenten
Art. 24. § 1. De aanbieder van essentiële diensten meldt onverwijld alle incidenten die aanzienlijke gevolgen hebben voor de beschikbaarheid, vertrouwelijkheid, integriteit of authenticiteit van de netwerk- en informatiesystemen waarvan de door hem verleende essentiële dienst of diensten afhankelijk zijn.
§ 2. Na advies van het nationale CSIRT, de autoriteit bedoeld in artikel 7, § 4, de sectorale overheid en, in voorkomend geval, van de betrokken gewesten of gemeenschappen, kan de Koning, per sector of deelsector, de weerslagniveaus en/of de drempelwaarden bepalen die minstens aanzienlijke gevolgen hebben in de zin van paragraaf 1.
§ 3. Indien geen weerslagniveaus en/of drempelwaarden als bedoeld in paragraaf 2 zijn bepaald, meldt de aanbieder alle incidenten die gevolgen hebben voor de

beschikbaarheid, vertrouwelijkheid, integriteit of authenticiteit van de netwerk- en informatiesystemen waarvan de door hem verleende essentiële dienst of diensten afhankelijk zijn.
§ 4. De Koning kan verschillende meldingscategorieën creëren volgens de mate van impact van het incident.
Art. 25. De melding bedoeld in artikel 24 gebeurt tegelijkertijd bij het nationale CSIRT, de sectorale overheid of haar sectorale CSIRT, en de autoriteit bedoeld in artikel 7, § 4.
De meldingsplicht is van toepassing zelfs wanneer de aanbieder van essentiële diensten slechts gedeeltelijk over de relevante informatie beschikt om te bepalen of het incident een aanzienlijke impact heeft.
Art. 26. § 1. Dit hoofdstuk is van toepassing op de exploitanten van een handelsplatform in de zin van artikel 3, 6°, van de wet van 21 november 2017 over de infrastructuren voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU.
§ 2. Aanbieders die behoren tot de sector financiën in de zin van bijlage I van de wet, met uitzondering van de exploitanten van een handelsplatform, melden onverwijld aan de Nationale Bank van België (NBB) alle incidenten die aanzienlijke gevolgen hebben voor de beschikbaarheid, vertrouwelijkheid, integriteit of authenticiteit van de netwerk- en informatiesystemen waarvan de door hen verleende essentiële dienst of diensten afhankelijk zijn. De NBB bepaalt de aanzienlijke gevolgen bedoeld in dit lid.
De NBB bezorgt de melding vervolgens onverwijld aan het nationale CSIRT en de autoriteit bedoeld in artikel 7, § 4.
Art. 27. De onderneming die een digitale dienst verleent aan een aanbieder van essentiële diensten en die onderworpen is aan deze wet, meldt deze aanbieder onverwijld alle incidenten die aanzienlijke gevolgen, in de zin van artikel 24, hebben voor de continuïteit van zijn essentiële diensten.
Vervolgens meldt de aanbieder van essentiële diensten dit incident volgens de in dit hoofdstuk beschreven procedures.
Art. 28. § 1. Wanneer een aanbieder van essentiële diensten getroffen is door een incident met aanzienlijke gevolgen in de zin van artikel 24, is hij verplicht het incident aan te pakken en reactieve maatregelen te nemen om het op te lossen.
De aanbieder van essentiële diensten blijft verantwoordelijk voor de aanpak van het incident.
§ 2. De aanbieder van essentiële diensten onderzoekt incidenten of verdachte gebeurtenissen die hem door het nationale CSIRT, de sectorale overheid of de autoriteit bedoeld in artikel 7, § 4, worden gemeld.
Art. 29. Op basis van de informatie in de melding van de aanbieder van essentiële diensten informeert het nationale CSIRT de andere getroffen lidstaten van de Europese Unie als het incident aanzienlijke gevolgen heeft voor de continuïteit van essentiële diensten in die lidstaten. Het nationale CSIRT beschermt daarbij, overeenkomstig het Unierecht of nationale wetgeving die met het Unierecht in overeenstemming is, de veiligheids- en commerciële belangen van de aanbieder van essentiële diensten alsook de vertrouwelijkheid van de informatie in diens melding.
Het nationale CSIRT bezorgt de in het eerste lid bedoelde meldingen aan de centrale contactpunten van de andere getroffen lidstaten.
Art. 30. § 1. De potentiële aanbieders van essentiële diensten mogen op vrijwillige basis incidenten melden die aanzienlijke gevolgen hebben voor de continuïteit van de

door hen in België verleende diensten.
Vrijwillige melding mag niet leiden tot het opleggen aan de meldende entiteit van verplichtingen waaraan zij niet zou zijn onderworpen als zij die melding niet had gedaan.
§ 2. Bij de behandeling van meldingen mogen het nationale CSIRT, de sectorale overheid of haar sectorale CSIRT, en de autoriteit bedoeld in artikel 7, § 4, de door deze wet opgelegde verplichte meldingen prioritair verwerken ten opzichte van vrijwillige meldingen.
Vrijwillige meldingen worden enkel verwerkt wanneer die verwerking geen onevenredige of overmatige belasting vormt voor het nationale CSIRT, de sectorale overheid of haar sectorale CSIRT, en de autoriteit bedoeld in artikel 7, § 4.
Art. 31. § 1. De Koning is ermee belast de nadere regels voor de melding en rapportering van incidenten te bepalen, en een beveiligd meldingsplatform op te richten.
Via dit platform kunnen aanbieders van essentiële diensten ook inbreuken in verband met persoonsgegevens melden aan de toezichthoudende autoriteiten, zoals opgelegd door artikel 33, eerste alinea, van Verordening EU 2016/679.
§ 2. Wanneer publieke bewustwording nodig is om een incident te voorkomen of een lopend incident te beheersen, kan het nationale CSIRT na raadpleging van de aanbieder die de melding heeft ingediend en van de bevoegde sectorale overheid, het publiek over afzonderlijke incidenten informeren. Hierbij wordt uitsluitend algemene informatie over het incident meegedeeld.
TITEL 3. - Netwerk- en informatiesystemen van digitaledienstverleners
HOOFDSTUK 1. - Toepassingsgebied
Art. 32. Deze titel is niet van toepassing op micro- en kleine ondernemingen zoals gedefinieerd in de aanbeveling van de Europese Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (2003/361/EG).
HOOFDSTUK 2. - De beveiligingseisen
Art. 33. § 1. De digitaledienstverleners identificeren de risico's voor de beveiliging van de netwerk- en informatiesystemen die zij gebruiken voor het aanbieden in de Europese Unie van de in bijlage II bedoelde diensten en nemen passende en evenredige technische en organisatorische maatregelen om die risico's te beheersen. Deze maatregelen zorgen, rekening houdend met de stand van de technische kennis, voor een niveau van beveiliging van netwerk- en informatiesystemen dat is afgestemd op de risico's die zich voordoen, en houden rekening met de volgende aspecten:
a) de beveiliging van systemen en voorzieningen;
b) de behandeling van incidenten;
c) het beheer van de bedrijfscontinuïteit;
d) toezicht, controle en testen;
e) de inachtneming van de internationale normen.
§ 2. De digitaledienstverleners nemen ook maatregelen om incidenten die de beveiliging van hun netwerk- en informatiesystemen aantasten, voor de in bijlage II van deze wet bedoelde diensten die in de Europese Unie worden aangeboden, te voorkomen en te minimaliseren, teneinde de continuïteit van deze diensten te waarborgen.
Art. 34. De digitaledienstverleners wijzen een contactpunt aan voor de computerbeveiliging en delen de gegevens ervan mee aan de sectorale overheid die bevoegd is voor de digitaledienstverleners, alsook na elke actualisering van deze

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

HOOFDSTUK 3. - Melding van incidenten

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

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

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

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

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

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

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

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

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

TITEL 4. - Toezicht en sancties

HOOFDSTUK 1. - Toezicht op de aanbieders van essentiële diensten

Afdeling 1. - Audits

Art. 38. § 1. De aanbieder van essentiële diensten voert, jaarlijks en op zijn kosten,

een interne audit uit van de netwerk- en informatiesystemen waarvan de door hem verleende essentiële diensten afhankelijk zijn. Deze interne audit moet de aanbieder van essentiële diensten toelaten zich ervan te vergewissen dat de in zijn I.B.B. bepaalde maatregelen en processen goed worden toegepast en regelmatig worden gecontroleerd.
De aanbieder van essentiële diensten bezorgt de interne auditverslagen binnen de dertig dagen aan de sectorale overheid.
§ 2. De aanbieder van essentiële diensten laat, minstens om de drie jaar en op zijn kosten, een externe audit uitvoeren door een instelling voor de conformiteitsbeoordeling die geaccrediteerd is door de nationale accreditatieautoriteit of door een instelling die de erkenningsakkoorden van de "European Cooperation for Accreditation" medeondertekend heeft.
De aanbieder van essentiële diensten bezorgt de externe auditverslagen binnen de dertig dagen aan de sectorale overheid.
§ 3. De aanbieder van essentiële diensten voert zijn eerste interne audit uit uiterlijk binnen de drie maanden na de uitwerking van zijn I.B.B. Hij voert zijn eerste externe audit uit uiterlijk binnen de vierentwintig maanden na de uitvoering van zijn eerste interne audit.
Art. 39. § 1. Na advies van de sectorale overheid en de autoriteit bedoeld in artikel 7, § 1, bepaalt de Koning:
1° de algemene accreditatievoorwaarden op basis van de eisen van de normen ISO/IEC 17021 of ISO/IEC 17065;
2° de bijkomende sectorale eisen waaraan de instelling voor de conformiteitsbeoordeling onderworpen kan zijn;
3° de regels die van toepassing zijn op de interne audit;
4° de regels die van toepassing zijn op de externe audit.
§ 2. Bij besluit vastgesteld na overleg in de Ministerraad kan de Koning, na advies van de sectorale overheid en de autoriteit bedoeld in artikel 7, § 1, ook de voorwaarden bepalen voor een eventuele erkenning die door de sectorale overheid aan een instelling voor de conformiteitsbeoordeling wordt verleend.
§ 3. De lijst van de geaccrediteerde of erkende instellingen voor de conformiteitsbeoordeling is beschikbaar bij de sectorale overheid die ze actueel houdt.
Art. 40. § 1. Certificeringsaudits kunnen door de inspectiedienst of de sectorale overheid worden gelijkgesteld met de verplichte jaarlijkse interne audit bedoeld in artikel 39, § 1. De verslagen van deze audits worden binnen de dertig dagen door de aanbieder van essentiële diensten aan de sectorale overheid bezorgd.
§ 2. Certificeringsaudits kunnen door de inspectiedienst of de sectorale overheid worden gelijkgesteld met de verplichte externe audit bedoeld in artikel 39, § 2. De verslagen van deze audits worden binnen de dertig dagen door de aanbieder van essentiële diensten aan de sectorale overheid bezorgd.
Art. 41. De autoriteit bedoeld in artikel 7, § 1, kan de sectorale overheid of de inspectiedienst, mits motivering, vragen haar de certificerings- of auditverslagen van een aanbieder van essentiële diensten te bezorgen.
Afdeling 2. - Inspectiedienst
Art. 42. § 1. De inspectiediensten kunnen op elk ogenblik controles uitvoeren op de naleving door de aanbieder van essentiële diensten van de beveiligingsmaatregelen en de regels voor het melden van incidenten.
§ 2. De autoriteit bedoeld in artikel 7, § 1, of de sectorale overheid kan de

inspectiedienst, mits motivering, aanbevelen om controles uit te voeren.
Na advies van de sectorale overheid en de autoriteit bedoeld in artikel 7, § 1, kan de Koning de eventuele sectorale praktische controlemodaliteiten bepalen.
§ 3. Bij het formuleren van een verzoek om informatie of bewijzen vermeldt de inspectiedienst het doel van het verzoek en de termijn waarbinnen de informatie of bewijzen moeten worden verstrekt.
De inspectiedienst kan een beroep doen op experten.
Art. 43. Wanneer de netwerk- en informatiesystemen van een aanbieder van essentiële diensten zich buiten het Belgische grondgebied bevinden, kan de inspectiedienst, in overleg met de autoriteit bedoeld in artikel 7, § 1, de bevoegde toezichthoudende autoriteiten van deze andere landen om samenwerking en bijstand verzoeken. Deze bijstand en samenwerking kunnen betrekking hebben op informatie-uitwisseling en verzoeken om toezichtmaatregelen.
Art. 44. § 1. De leden van de inspectiedienst beschikken over een legitimatiekaart waarvan het model, per sector of, in voorkomend geval, per deelsector, door de Koning wordt bepaald.
§ 2. De leden van de inspectiedienst of de experten die deelnemen aan de inspectie, mogen geen enkel rechtstreeks of onrechtstreeks belang hebben in de ondernemingen of instellingen waarop zij toezicht dienen uit te oefenen, waardoor hun objectiviteit in het gedrang zou kunnen komen. Ze leggen de eed af bij de leidend ambtenaar van hun dienst.
§ 3. Onverminderd de bevoegdheden van de officieren van gerechtelijke politie bedoeld in artikel 8 van het Wetboek van strafvordering beschikken de beëdigde leden van de inspectiedienst op elk ogenblik over de volgende toezichtbevoegdheden bij de uitoefening van hun opdracht, en dit zowel in het kader van administratieve handelingen als in het kader van de vaststelling van inbreuken bij proces-verbaal:
1° zonder voorafgaande verwittiging, op vertoon van hun legitimatiekaart, alle plaatsen betreden die de aanbieder van essentiële diensten gebruikt; zij hebben slechts toegang tot bewoonde lokalen mits een machtiging die vooraf is uitgereikt door de onderzoeksrechter;
2° ter plaatse kennis nemen van het I.B.B., de auditverslagen, alle bescheiden, documenten en andere informatiebronnen die nodig zijn voor de uitoefening van hun opdracht en hiervan een kopie verkrijgen;
3° overgaan tot elk onderzoek, elke controle en elk verhoor, alsook alle inlichtingen inwinnen die zij nodig achten voor de uitoefening van hun opdracht;
4° de identiteit opnemen van de personen die zich bevinden op de plaatsen die de aanbieder van essentiële diensten gebruikt en van wie ze het verhoor noodzakelijk achten voor de uitoefening van hun opdracht. Daartoe kunnen ze van deze personen eisen dat ze hun officiële identiteitsdocumenten voorleggen;
5° de bijstand vorderen van de federale of lokale politiediensten;
6° inlichtingen inwinnen bij de personeelsleden bedoeld in artikel 9 van de wet van 15 april 1994 voor de uitvoering van de bepalingen van deze wet en van de wet van 1 juli 2011.
§ 4. Om een machtiging tot betreding van bewoonde lokalen te bekomen, richten de personeelsleden van de inspectiedienst een met redenen omkleed verzoek aan de onderzoeksrechter. Dit verzoek bevat minstens de volgende gegevens:
1° de identificatie van de bewoonde ruimten waartoe de personeelsleden van de inspectiedienst of van de sectorale overheid toegang wensen te hebben;
2° de eventuele inbreuken die het voorwerp zijn van het toezicht;

3° alle documenten en inlichtingen waaruit blijkt dat het gebruik van dit middel nodig is.
De onderzoeksrechter beslist binnen een termijn van maximum 48 uur na ontvangst van het verzoek. De beslissing van de onderzoeksrechter is met redenen omkleed. Bij gebrek aan een beslissing binnen de voorgeschreven termijn wordt het plaatsbezoek geacht te zijn geweigerd. De inspectiedienst kan beroep instellen tegen de weigeringsbeslissing of het gebrek aan een beslissing bij de kamer van inbeschuldigingstelling binnen vijftien dagen na de kennisgeving van de beslissing of het verstrijken van de termijn.
Bezoeken aan bewoonde lokalen zonder toestemming van de bewoner gebeuren tussen vijf en eenentwintig uur door minstens twee leden van de inspectiedienst die samen optreden.
§ 5. Bij het begin van elk verhoor wordt aan de ondervraagde persoon meegedeeld:
1° dat zijn verklaringen voor een rechtbank als bewijs kunnen worden gebruikt;
2° dat hij kan vragen dat alle vragen die hem worden gesteld en de antwoorden die hij geeft, worden genoteerd in de gebruikte bewoordingen;
3° dat hij het recht heeft om te zwijgen en niet bij te dragen tot zijn eigen beschuldiging.
Elke ondervraagde persoon mag de documenten in zijn bezit gebruiken, zonder dat daardoor het verhoor uitgesteld wordt. Hij mag tijdens het verhoor of later vragen om die documenten bij het verhoor te voegen.
Het verhoor vermeldt nauwkeurig het tijdstip waarop het wordt aangevat, eventueel onderbroken en hervat, alsook beëindigd. Het vermeldt de identiteit van de personen die tussenkomen tijdens het verhoor of een deel ervan.
Aan het einde van het verhoor heeft de ondervraagde persoon het recht om zijn verhoor te lezen of het te laten voorlezen. Hij mag zijn verklaringen laten verbeteren of er iets aan laten toevoegen.
De personeelsleden van de inspectiedienst die een persoon ondervragen, delen hem mee dat hij een kopie mag vragen van de tekst van zijn verhoor. Deze kopie wordt gratis verstrekt.
§ 6. De leden van de inspectiedienst mogen alle informatiedragers en de erin opgenomen gegevens raadplegen. Zij mogen zich ter plaatse het informaticasysteem en de erin opgenomen gegevens die zij nodig hebben voor hun onderzoeken en vaststellingen doen voorleggen en er kosteloos uittreksels, duplicaten of kopieën van nemen of vragen in een door hen gevraagde leesbare en verstaanbare vorm.
Indien het niet mogelijk is om ter plaatse kopieën te nemen, mogen de leden van de inspectiedienst, tegen een ontvangstbewijs dat een inventaris bevat, het informaticasysteem en de erin opgenomen gegevens in beslag nemen.
§ 7. Om de zoekactie in een informaticasysteem of een deel hiervan die op basis van paragraaf 6 werd opgestart, uit te breiden naar een informaticasysteem of een deel hiervan dat zich op een andere plaats bevindt dan die van de zoekactie, kan de inspectiedienst een onderzoeksrechter verzoeken op te treden.
Art. 45. § 1. Na elke inspectie stellen de leden van de inspectiedienst een verslag op en bezorgen ze een kopie daarvan aan de geïnspecteerde aanbieder van essentiële diensten en aan de bevoegde sectorale overheid.
§ 2. De autoriteit bedoeld in artikel 7, § 1, en de sectorale overheid kunnen de inspectiedienst, mits motivering, vragen om zijn inspectieverslagen te bezorgen.
Art. 46. § 1. De aanbieder van essentiële diensten verleent zijn volledige medewerking aan de leden van de inspectiedienst bij de uitoefening van hun functie en met name

om deze zo goed mogelijk te informeren over alle bestaande beveiligingsmaatregelen. Indien nodig stelt de aanbieder van essentiële diensten het nodige materiaal ter beschikking van de leden van de inspectiedienst of van de sectorale overheid zodat ze de veiligheidsvoorschriften kunnen naleven tijdens de inspecties.
§ 2. Voor iedere sector of deelsector kan de Koning, bij besluit vastgesteld na overleg in de Ministerraad en na advies van de sectorale overheid, retributies bepalen voor de inspectieprestaties. Deze retributies zijn ten laste van de aanbieders van essentiële diensten. De Koning bepaalt de nadere regels inzake berekening en betaling.
HOOFDSTUK 2. - Toezicht op de digitaledienstverleners
Art. 47. § 1. De Koning bepaalt de praktische nadere regels van het toezicht op de digitaledienstverleners.
§ 2. De digitaledienstverlener moet met name:
a) de bevoegde inspectiedienst binnen de gestelde termijn de informatie verstrekken die nodig is om de beveiliging van zijn netwerk- en informatiesystemen te beoordelen, met inbegrip van gedocumenteerde beleidsmaatregelen op het gebied van beveiliging;
b) elke niet-inachtneming van de beveiligingseisen en de eisen inzake het melden van incidenten rechtzetten binnen de gestelde termijn.
§ 3. Overeenkomstig de door de Koning bepaalde regels kan de inspectiedienst, indien nodig, door middel van toezichtmaatregelen achteraf, maatregelen nemen wanneer ze het bewijs in handen krijgt dat een digitaledienstverlener niet voldoet aan de beveiligingseisen of de eisen inzake het melden van incidenten. Dit bewijs kan worden voorgelegd door een bevoegde autoriteit van een andere lidstaat van de Europese Unie waar de dienst wordt verleend.
§ 4. In het kader van haar controles achteraf beschikt de inspectiedienst over dezelfde bevoegdheden als deze bedoeld in artikel 44.
§ 5. Wanneer een digitaledienstverlener zijn hoofdvestiging of een vertegenwoordiger in België heeft maar zijn netwerk- en informatiesystemen in een of meer andere landen, kan de inspectiedienst, in overleg met de autoriteit bedoeld in artikel 7, § 1, de bevoegde toezichthoudende autoriteiten van deze andere landen om samenwerking en bijstand verzoeken. Deze bijstand en samenwerking kunnen betrekking hebben op informatie-uitwisseling en verzoeken om toezicht-maatregelen.
§ 6. Overeenkomstig de door de Koning bepaalde regels kan de inspectiedienst de in dit artikel bedoelde bevoegdheden ook uitoefenen op verzoek van bevoegde autoriteiten van een andere lidstaat van de Europese Unie.
§ 7. De autoriteit bedoeld in artikel 7, § 1, kan de inspectiedienst vragen haar de inspectieverslagen van een digitaledienstverlener te bezorgen.
§ 8. De Koning kan, bij besluit vastgesteld na overleg in de Ministerraad en na advies van de sectorale overheid, retributies bepalen voor de controleprestaties. Deze retributies zijn ten laste van de digitale dienstverleners. De Koning bepaalt de nadere regels inzake berekening en betaling.
HOOFDSTUK 3. - De sancties
Afdeling 1. - Procedure
Art. 48. § 1. Wanneer een of meer inbreuken op de eisen van de wet, de uitvoeringsbesluiten ervan of de eraan verbonden individuele administratieve beslissingen worden vastgesteld, stelt de inspectiedienst de betrokken aanbieder van essentiële diensten of digitaledienstverlener in gebreke om zijn verplichtingen na te komen binnen een door hem vastgestelde termijn.
De termijn wordt bepaald rekening houdend met de werkings-voorwaarden van de

aanbieder van essentiële diensten of digitaledienstverlener en met de te nemen maatregelen.
§ 2. De inspectiedienst deelt de overtreder vooraf, op een met redenen omklede wijze, mee dat hij van plan is hem een ingebrekestelling te sturen en laat hem weten dat hij het recht heeft om, binnen de vijftien dagen na ontvangst van deze informatie, zijn verweermiddelen schriftelijk in te dienen of te vragen om te worden gehoord. De informatie wordt geacht te zijn ontvangen door de overtreder de zesde dag na de verzending ervan door de inspectiedienst.
§ 3. Op basis van de elementen waarover zij beschikt, kan de autoriteit bedoeld in artikel 7, § 1, mits motivering, de inspectiedienst ook aanbevelen om de aanbieder van essentiële diensten of digitaledienstverlener in gebreke te stellen.
Art. 49. § 1. Als de inspectiedienst vaststelt dat de aanbieder van essentiële diensten of digitaledienstverlener geen gevolg geeft aan de ingebrekestelling binnen de vastgestelde termijn, worden de feiten vastgesteld in een door de beëdigde leden van de inspectiedienst opgesteld proces-verbaal. Dat proces-verbaal wordt naar de bevoegde sectorale overheid gestuurd.
§ 2. Het feit dat iemand de uitvoering van een controle door de leden van de inspectiedienst vrijwillig verhindert of belemmert, de informatie die hem gevraagd wordt naar aanleiding van deze controle weigert mee te delen, of opzettelijk foutieve of onvolledige informatie meedeelt, wordt vastgesteld in een proces-verbaal door de beëdigde leden van de inspectiedienst.
§ 3. De paragrafen 1 en 2 zijn ook van toepassing op de potentiële aanbieder van essentiële diensten of op de exploitant van een kritieke infrastructuur die de informatieverplichtingen bedoeld in artikel 14 of in artikel 18, § 3, niet nakomt.
§ 4. De processen-verbaal opgesteld door de beëdigde leden van de inspectiedienst hebben bewijskracht tot het tegendeel is bewezen.
Art. 50. Inbreuken op deze wet of de uitvoeringsbesluiten ervan kunnen aanleiding geven tot strafrechtelijke of administratieve sancties.
Afdeling 2. - Strafrechtelijke sancties
Art. 51. § 1. Niet-naleving van een van de meldingsverplichtingen bedoeld in artikel 24 of 35 wordt bestraft met een gevangenisstraf van acht dagen tot een jaar en een geldboete van 26 euro tot 20 000 euro of met een van deze straffen alleen.
§ 2. Niet-naleving van een van de beveiligingsverplichtingen opgelegd door de Koning of de sectorale overheid krachtens artikel 21 of 33 wordt bestraft met een gevangenisstraf van acht dagen tot een jaar en een geldboete van 26 euro tot 30 000 euro of met een van deze straffen alleen.
§ 3. Niet-naleving van een van de toezichtverplichtingen bedoeld in hoofdstuk 1 en 2 van titel 4 wordt bestraft met een gevangenisstraf van acht dagen tot een jaar en een geldboete van 26 euro tot 50 000 euro of met een van deze straffen alleen.
§ 4. Niet-naleving van een van de informatieverplichtingen bedoeld in artikel 14 of in artikel 18, § 3, wordt bestraft met een gevangenisstraf van acht dagen tot een jaar en een geldboete van 26 euro tot 50 000 euro of met een van deze straffen alleen.
§ 5. Iedere vrijwillige verhindering of belemmering van de uitvoering van de controle door de leden van de inspectiedienst, weigering om de informatie mee te delen die naar aanleiding van deze controle is gevraagd, of opzettelijke mededeling van foutieve of onvolledige informatie wordt bestraft met een gevangenisstraf van acht dagen tot twee jaar en een geldboete van 26 euro tot 75 000 euro of met een van deze straffen alleen.
§ 6. In geval van herhaling van dezelfde feiten binnen een termijn van drie jaar wordt

de geldboete verdubbeld en de overtreder gestraft met een gevangenisstraf van vijftien dagen tot drie jaar.
§ 7. De bepalingen van Boek 1 van het Strafwetboek, met inbegrip van hoofdstuk VII en artikel 85, zijn van toepassing op de inbreuken bedoeld in dit artikel.
De artikelen 269 tot 274 en 276 van het Strafwetboek zijn van toepassing op de leden van de inspectiedienst die handelen in de uitoefening van hun functie.
§ 8. Inbreuken op artikel 9, §§ 2 en 3, van deze wet worden bestraft met de straffen bepaald in artikel 458 van het Strafwetboek.
Afdeling 3. - Administratieve sancties
Art. 52. § 1. Elke inbreuk op deze wet, op de uitvoeringsbesluiten ervan of op de administratieve beslissingen die krachtens deze wet genomen worden, kan aanleiding geven tot een administratieve sanctie.
§ 2. Niet-naleving van de meldingsverplichtingen bedoeld in artikel 24 of 35 wordt bestraft met een geldboete van 500 tot 75 000 euro.
§ 3. Niet-naleving van de beveiligingsverplichtingen opgelegd door de Koning of de sectorale overheid krachtens artikel 21 of 33 wordt bestraft met een geldboete van 500 tot 100 000 euro.
§ 4. Niet-naleving van de informatieverplichtingen bedoeld in artikel 14 of in artikel 18, § 3, wordt bestraft met een geldboete van 500 tot 125 000 euro.
§ 5. Niet-naleving van de toezichtverplichtingen bedoeld in hoofdstuk 1 en 2 van titel 4 wordt bestraft met een geldboete van 500 tot 200 000 euro.
§ 6. Iedere handeling waarbij een persoon die optreedt voor rekening van een aanbieder van essentiële diensten of digitaledienstverlener nadelige gevolgen ondervindt bij de uitvoering, te goeder trouw en in het kader van zijn functie, van de verplichtingen die voortvloeien uit deze wet, wordt bestraft met een geldboete van 500 tot 200 000 euro.
Art. 53. De inspectiedienst stuurt het origineel van het proces-verbaal naar de procureur des Konings.
Tegelijk wordt een kopie van het proces-verbaal naar de overtreder gestuurd.
Art. 54. De procureur des Konings beschikt over een termijn van twee maanden, te rekenen vanaf de dag van ontvangst van het proces-verbaal, om de sectorale overheid in te lichten dat strafrechtelijke vervolging is ingesteld.
De sectorale overheid mag de procedure voor het opleggen van een administratieve geldboete niet opstarten vóór het verstrijken van voormelde termijn, behalve wanneer de procureur des Konings vooraf meedeelt dat hij geen gevolg aan het feit wenst te geven.
Wanneer de procureur des Konings geen kennis geeft van zijn beslissing binnen de vastgestelde termijn of van strafvervolging afziet, kan de sectorale overheid beslissen de administratieve procedure op te starten.
Art. 55. § 1. De beslissing om een administratieve geldboete op te leggen wordt met redenen omkleed. Ze vermeldt ook het bedrag van de administratieve geldboete en de bedoelde inbreuken.
§ 2. De sectorale overheid bezorgt de overtreder op voorhand haar met redenen omkleed voorstel van administratieve sanctie en laat hem weten dat hij het recht heeft om, binnen de vijftien dagen na ontvangst van het voorstel, zijn verweermiddelen schriftelijk in te dienen of te vragen om te worden gehoord. Het voorstel wordt geacht te zijn ontvangen door de overtreder de zesde dag na de verzending ervan door de sectorale overheid.
§ 3. Rekening houdend met de aangevoerde verweermiddelen binnen de in paragraaf

2 bedoelde termijn of bij gebrek aan een antwoord van de overtreder binnen diezelfde termijn, kan de sectorale overheid een in artikel 52 bedoelde administratieve sanctie opleggen.
§ 4. De administratieve geldboete staat in verhouding tot de ernst, de duur, de gebruikte middelen, de veroorzaakte schade en de omstandigheden van de feiten.
De administratieve geldboete wordt verdubbeld in geval van herhaling van dezelfde feiten binnen een termijn van drie jaar.
§ 5. De samenloop van meerdere inbreuken kan aanleiding geven tot één enkele administratieve geldboete die in verhouding staat tot de ernst van het geheel van de feiten.
Art. 56. De beslissing wordt bij aangetekende zending ter kennis gebracht van de overtreder.
Een verzoek tot betaling van de geldboete binnen een maand wordt bij de beslissing gevoegd.
Art. 57. De overtreder kan de beslissing van de sectorale overheid betwisten bij het Marktenhof bedoeld in artikel 101 van het Gerechtelijk Wetboek.
De vordering wordt ingesteld bij verzoekschrift op tegenspraak dat, op straffe van verval, binnen zestig dagen na kennisgeving van de beslissing van de sectorale overheid wordt ingediend.
De zaak wordt behandeld zoals in kort geding overeenkomstig de artikelen 1035 tot 1038, 1040 en 1041 van het Gerechtelijk Wetboek.
Dit beroep schorst de uitvoering van de beslissing niet.
Art. 58. § 1. Als de overtreder de administratieve geldboete niet betaalt binnen de gestelde termijn, is de beslissing om een administratieve geldboete op te leggen uitvoerbaar en kan de sectorale overheid een dwangbevel uitvaardigen.
Het dwangbevel wordt uitgevaardigd door de wettelijke vertegenwoordiger van de sectorale overheid of door een daartoe gemachtigd personeelslid.
§ 2. Het dwangbevel wordt aan de overtreder bij gerechtsdeurwaarderexploot betekend. De betekening bevat een bevel om te betalen binnen vierentwintig uur op straffe van tenuitvoerlegging door beslag, alsook een boekhoudkundige verantwoording van de gevorderde bedragen en een afschrift van de uitvoerbaarverklaring.
§ 3. De overtreder kan tegen het dwangbevel verzet aantekenen bij de beslagrechter. Het verzet is, op straffe van nietigheid, met redenen omkleed. Het dient gedaan te worden door middel van een dagvaarding aan de sectorale overheid bij deurwaardersexploot binnen vijftien dagen te rekenen vanaf de betekening van het dwangbevel.
De bepalingen van hoofdstuk VIII van het eerste deel van het Gerechtelijk Wetboek zijn van toepassing op deze termijn, met inbegrip van de verlengingen bepaald in artikel 50, tweede lid, en artikel 55 van dit Wetboek.
De uitoefening van verzet tegen het dwangbevel schorst de tenuitvoerlegging van het dwangbevel, alsook de verjaring van de schuldvorderingen opgenomen in het dwangbevel, tot uitspraak is gedaan over de gegrondheid ervan. De reeds eerder gelegde beslagen behouden hun bewarend karakter.
§ 4. De sectorale overheid mag bewarend beslag laten leggen en het dwangbevel uitvoeren met gebruikmaking van de middelen tot tenuitvoerlegging bepaald in het vijfde deel van het Gerechtelijk Wetboek.
De gedeeltelijke betalingen gedaan ingevolge de betekening van een dwangbevel verhinderen de voortzetting van de vervolging niet.

§ 5. De betekeningskosten van het dwangbevel evenals de kosten van tenuitvoerlegging of van bewarende maatregelen zijn ten laste van de overtreder. Ze worden bepaald volgens de regels die gelden voor de akten van gerechtsdeurwaarders in burgerlijke zaken en handelszaken.

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

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

TITEL 5. - CSIRT

HOOFDSTUK 1. - Het nationale CSIRT

Afdeling 1. - Taken van het nationale CSIRT

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

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

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

c) reageren op incidenten;

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

e) computerbeveiligingsproblemen opsporen, observeren en analyseren;

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

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

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

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

Afdeling 2 - Voorschriften voor het nationale CSIRT

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

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

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

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

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

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

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

Art. 62. In het kader van de uitoefening van zijn bevoegdheden neemt het nationale CSIRT alle passende maatregelen om de in de artikelen 60 en 61 bepaalde

doelstellingen te verwezenlijken. Deze maatregelen moeten evenredig zijn met die doelstellingen en in overeenstemming met de beginselen van objectiviteit, transparantie en non-discriminatie.
Bij de verwezenlijking van die doelstellingen mag het nationale CSIRT alle beschikbare gegevens onder zich houden, aan een andere persoon onthullen of verspreiden, of er enig gebruik van maken, zelfs als die gegevens voortkomen uit een ongerechtigde toegang tot een informaticasysteem door een derde.
Het nationale CSIRT vervult zijn opdrachten met de nodige behoedzaamheid die verwacht mag worden van een overheid. Er moet steeds bij voorrang voor worden gezorgd dat de werking van het informaticasysteem niet wordt verstoord en alle redelijke voorzorgen moeten worden genomen om te voorkomen dat het informaticasysteem materiële schade oploopt.
De leidende ambtenaren van het nationale CSIRT zorgen voor de naleving van de in dit artikel vermelde voorwaarden. Daartoe werken zij interne procedures uit.
HOOFDSTUK 2. - Het sectoraal CSIRT
Afdeling 1. - Taken van het sectoraal CSIRT
Art. 63. De taken van een sectoraal CSIRT omvatten, in samenwerking met het nationale CSIRT, ten minste het volgende:
a) monitoren van sectorale incidenten;
b) ten behoeve van de betrokken belanghebbende partijen van de sector zorgen voor vroegtijdige waarschuwingen, alarmmeldingen, aankondigingen en verspreiding van informatie over risico's en incidenten;
c) reageren op sectorale incidenten;
d) zorgen voor een dynamische analyse van sectorale risico's en incidenten en situatiekennis;
e) zorgen voor op samenwerking gerichte contacten met de aanbieders van zijn sector;
f) kunnen deelnemen aan vergaderingen van het CSIRT-netwerk bedoeld in artikel 12 van de NIS-richtlijn, die gewijd zijn aan zijn sector.
Na advies van het sectorale CSIRT kan de Koning dit CSIRT bijkomende taken toevertrouwen.
Afdeling 2. - Voorschriften voor een sectoraal CSIRT
Art. 64. De voorschriften voor een sectoraal CSIRT omvatten het volgende:
a) een hoge mate van beschikbaarheid van zijn communicatiekanalen garanderen door zwakke punten (single points of failure) te voorkomen, en beschikken over diverse kanalen waarlangs te allen tijde contact met hen kan worden opgenomen en contact met anderen kan worden opgenomen.
b) beschikken over lokalen en informatiesystemen die zich op beveiligde locaties bevinden.
c) de bedrijfscontinuïteit garanderen met een adequaat systeem voor het beheren en routeren van verzoeken met het oog op vlotte overdrachten.
d) een beroep doen op infrastructuur waarvan de continuïteit gewaarborgd is. Hiertoe wordt voorzien in redundante systemen en reservewerkruimten.
f) ervoor zorgen dat zijn communicatiekanalen duidelijk worden gespecificeerd en bekend zijn bij zijn partners.
TITEL 6. - Verwerking van persoonsgegevens
HOOFDSTUK 1. - Beginselen inzake verwerking, wettelijke basis en doeleinden
Art. 65. § 1. Overeenkomstig artikel 5.1.c) van Verordening EU 2016/679 zorgt de verwerkingsverantwoordelijke, bij de verwerking van persoonsgegevens in het kader

van de uitvoering van deze wet, ervoor dat de verwerking tot het noodzakelijke minimum beperkt blijft en in verhouding staat tot het nagestreefde doeleinde.
§ 2. Overeenkomstig dat beginsel kunnen de verwerkte persoonsgegevens allerhande gegevens zijn in verband met de beveiliging van netwerk- en informatiesystemen, namelijk in voorkomend geval nominatieve informatie, gegevens over de medewerkers van een organisatie of externe personen, verbindingsgegevens of -identificatoren, locatie-gegevens, identificatie- of authenticatiegegevens, in voorkomend geval met behulp van beveiligde systemen.
§ 3. De belangrijkste verwerkingen van persoonsgegevens in het kader van deze wet kunnen als volgt worden ingedeeld:
- algemene informatie-uitwisseling tussen aanbieders van essentiële diensten en digitaledienstverleners, enerzijds, en de autoriteit bedoeld in artikel 7, anderzijds;
- de verwerking van specifieke informatie tussen de entiteiten bedoeld in het eerste streepje in het kader van incidentmeldingen of andere specifieke uitwisselingen;
- de verwerking door inspectiediensten overeenkomstig titel 4;
- de verwerking door hoven en rechtbanken of sectorale overheden in het kader van de uitvoering van de wet en met name de opsporing, vervolging en bestraffing van inbreuken;
- de uitwisseling en andere verwerking van informatie door het nationale en sectorale CSIRT voor hun opdrachten respectievelijk bedoeld in de artikelen 60 tot 62, 63 en 64.
Art. 66. § 1. Indien mogelijk worden de verwerkte gegevens gepseudonimiseerd of geaggregeerd om het risico te verkleinen dat persoonsgegevens worden gebruikt op een wijze die onverenigbaar is met de Verordening EU 2016/679 of de wetten en reglementen die ze aanvullen of verduidelijken.
§ 2. De bijzondere gegevenscategorieën in de zin van de artikelen 9 en 10 van Verordening EU 2016/679 worden verwerkt overeenkomstig deze verordening en de wetten en reglementen die ze aanvullen of verduidelijken.
§ 3. De verwerkingsverantwoordelijke kan ofwel een van de autoriteiten bedoeld in artikel 7 zijn, ofwel de aanbieders van essentiële diensten of de digitaledienstverleners, ofwel de politionele of gerechtelijke autoriteiten.
§ 4. De ontvangers van persoonsgegevens kunnen alle personen zijn die betrokken zijn bij de uitvoering van de bepalingen van de wet, voor zover noodzakelijk voor de informatie-uitwisseling waarin de wet voorziet.
Art. 67. Overeenkomstig de artikelen 6.1, c), en 6.1, e), van Verordening EU 2016/679, moeten de verwerkingen bedoeld in artikel 65, § 3, noodzakelijk blijven om te voldoen aan een wettelijke verplichting van de verwerkingsverantwoordelijke of voor de invulling van een taak van algemeen belang die aan deze laatste is opgedragen. Deze verwerkingen moeten noodzakelijk zijn enkel wat deze wettelijke basis betreft en beperkt blijven tot wat noodzakelijk is om eraan te voldoen.
Art. 68. § 1. De verwerkingen bedoeld in artikel 65, § 3, moeten beperkt zijn tot en verenigbaar blijven met de doeleinden bepaald door de verwerkingsverantwoordelijke.
§ 2. Deze doeleinden kunnen onder meer zijn: een betere bescherming van de netwerk- en informatiesystemen, een krachtiger preventie- en veiligheidsbeleid, de preventie van beveiligingsincidenten, de continuïteit van de in deze wet bedoelde essentiële of digitale diensten, het toezicht op aanbieders van essentiële diensten en digitaledienstverleners, nationale en internationale samenwerking, de evaluatie van de uitvoering van de wet, de voorbereiding, de organisatie, het beheer en de

opvolging van onderzoek of vervolging, alsook de andere opdrachten die bij wet zijn toegewezen aan de verschillende betrokken autoriteiten.
§ 3. Wat de relevante doeleinden en subdoeleinden betreft, bepaalt elke verwerkingsverantwoordelijke de betrokken gegevens- en persoonscategorieën, de ontvangers of categorieën van ontvangers van gegevens, de bewaartermijnen en de andere eventuele kenmerken van de verwerking, alsook de regels en praktijken voor de naleving van de toepasselijke regelgeving.
HOOFDSTUK 2. - Bewaartermijn
Art. 69. § 1. Onverminderd de bewaring die noodzakelijk is voor de verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden, bedoeld in artikel 89 van Verordening EU 2016/679, worden de in uitvoering van de wet verwerkte persoonsgegevens door de autoriteiten bedoeld in artikel 7 niet langer bewaard dan nodig is voor de doeleinden waarvoor ze worden verwerkt.
§ 2. Overeenkomstig de eerste paragraaf kan de Koning de maximale bewaartermijn van dezelfde gegevens bepalen bij besluit vastgesteld na overleg in de Ministerraad.
HOOFDSTUK 3. - Functionaris voor gegevensbescherming
Art. 70. Elke aanbieder van essentiële diensten, digitaledienstverlener en autoriteit bedoeld in artikel 7 van de wet die persoonsgegevens verwerkt, wijst een functionaris voor gegevensbescherming aan.
HOOFDSTUK 4. - Beperking van de rechten van de betrokken personen
Art. 71. § 1. Met toepassing van artikel 23.1, a), b), c), d), e), h), van Verordening EU 2016/679 worden bepaalde verplichtingen en rechten van deze verordening beperkt of uitgesloten, overeenkomstig de bepalingen van dit hoofdstuk. Deze beperkingen of uitsluitingen mogen geen afbreuk doen aan de wezenlijke inhoud van de grondrechten en fundamentele vrijheden en moeten worden toegepast voor zover dit strikt noodzakelijk is voor het nagestreefde doel.
§ 2. De artikelen 12 tot 22 van voormelde verordening zijn niet van toepassing op de verwerking van persoonsgegevens door een aanbieder van essentiële diensten, een digitaledienstverlener of een autoriteit bedoeld in artikel 7, overeenkomstig deze wet en om te voldoen aan de verplichtingen die deze oplegt inzake het melden van incidenten, als bedoeld in hoofdstuk 3 van titel 2 en hoofdstuk 3 van titel 3. Deze artikelen zijn evenmin van toepassing op het toezicht bedoeld in titel 4. De vrijstelling geldt enkel indien en voor zover deze verwerking noodzakelijk is voor de hierboven bepaalde doeleinden, met name voor zover de toepassing van de rechten bepaald in de voormelde verordening nadelig zou zijn voor de controle, het onderzoek of de voorbereidende werkzaamheden, of het geheim van het strafonderzoek of de veiligheid van personen zou kunnen schaden.
§ 3. De verwerkingsverantwoordelijke die de in paragraaf 2 bedoelde vrijstelling kan genieten, is ofwel de aanbieder van essentiële diensten, ofwel de digitaledienstverlener, ofwel de autoriteit bedoeld in artikel 7, elk voor de gegevens die hij of zij bezit in het kader van de opdrachten bedoeld in paragraaf 2.
§ 4. De vrijstelling geldt, onder voorbehoud van het evenredigheidsbeginsel en in voorkomend geval van het beginsel van minimale gegevensverwerking, voor alle categorieën van persoonsgegevens, voor zover de verwerking van deze gegevens in overeenstemming is met de doeleinden bedoeld in paragraaf 2. Deze vrijstelling geldt ook voor voorbereidende werkzaamheden of procedures met het oog op de eventuele toepassing van een administratieve sanctie.
§ 5. Persoonsgegevens die voortkomen uit de in paragraaf 2 bedoelde vrijstelling

worden niet langer bewaard dan nodig is voor de doeleinden waarvoor ze worden verwerkt, met een maximale bewaartermijn die de duur van de verjaringstermijn van eventuele inbreuken bedoeld in artikelen 51 en 52 niet mag overschrijden, overeenkomstig de toepasselijke wetgeving.
§ 6. De verwerkingsverantwoordelijke die niet alle bepalingen van de wet en met name van artikel 72 naleeft, kan de vrijstelling niet genieten.
§ 7. Bovendien moet elke verwerkingsverantwoordelijke de vertrouwelijkheid van de persoonsgegevens die het voorwerp uitmaken van de vrijstelling waarborgen, en ervoor zorgen dat ze enkel toegankelijk zijn voor personen die ze nodig hebben voor de uitvoering van de bepalingen van deze wet. Ook moet elke betrokken verwerkingsverant-woordelijke de Gegevensbeschermingsautoriteit minstens één keer per jaar schriftelijk een lijst bezorgen van de verzoeken tot uitoefening van de rechten bedoeld in de artikelen 12 tot 22 van de verordening die volgens deze verantwoordelijke onder de vrijstelling vallen. Onverminderd de bepalingen van deze wet moet elke betrokken verwerkingsverantwoordelijke daarenboven elke andere passende maatregel nemen om elke vorm van misbruik of onrechtmatige toegang of doorgifte van persoonsgegevens die onder de vrijstelling vallen te voorkomen, met name en zonder enige beperking de maatregelen van artikel 32 van Verordening EU 2016/679.
Art. 72. § 1. De betrokkenen kunnen een verzoek in verband met hun rechten bepaald in de artikelen 12 tot 22 van Verordening EU 2016/679 naar de functionaris voor gegevensbescherming sturen die de ontvangst ervan bevestigt.
§ 2. De functionaris voor gegevensbescherming van de verwerkings-verantwoordelijke informeert de betrokkene schriftelijk en dit onverwijld, en in ieder geval binnen een maand na ontvangst van het verzoek, over iedere weigering of beperking van zijn rechten bepaald in de artikelen 12 tot 22 van Verordening EU 2016/679, alsook over de redenen voor deze weigering of beperking. De informatie over de weigering of beperking kan achterwege worden gelaten wanneer de verstrekking ervan een van de doelstellingen vermeld in artikel 71, § 2, zou ondermijnen. Afhankelijk van de complexiteit van de verzoeken en van het aantal ervan kan die termijn indien nodig met twee maanden worden verlengd. De verwerkingsverantwoordelijke stelt de betrokkene binnen één maand na ontvangst van het verzoek in kennis van deze verlenging en van de redenen voor het uitstel.
§ 3. De functionaris voor gegevensbescherming van de verwerkings-verantwoordelijke 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 verwerkings-verantwoordelijke vermeldt de feitelijke of juridische redenen waarop zijn beslissing steunt. Deze inlichtingen worden ter beschikking gesteld van de Gegevensbeschermingsautoriteit.
§ 4. De betrokken verwerkingsverantwoordelijke verleent de betrokkene evenwel toegang tot beperkte informatie over de verwerking van zijn persoonsgegevens, voor zover deze kennisgeving de verwezenlijking van de doelstellingen van deze wet niet in het gedrang brengt. Hierbij is het voor betrokkene onmogelijk om na te gaan of hij al dan niet het voorwerp uitmaakt van een onderzoek, en kan hij in geen geval persoonsgegevens rechtzetten, wissen, beperken, meedelen, of aan derden overdragen, noch enige vorm van verwerking van voormelde gegevens die in het bovenvermelde kader noodzakelijk is, stopzetten.
§ 5. De maatregel van weigering of beperking van de rechten bepaald in de artikelen 12 tot 22 van Verordening EU 2016/679 moet worden opgeheven:

- voor maatregelen die gerechtvaardigd zijn door de verplichtingen inzake het melden van incidenten, bij het afsluiten van de verwerking van een incident door de autoriteiten bedoeld in artikel 24 of 34;
- voor maatregelen die gerechtvaardigd zijn door de verplichtingen krachtens titel 4, bij het afsluiten van de controle of het onderzoek of de voorbereidende werkzaamheden ervan door de inspectiedienst, alsook in de periode tijdens dewelke de sectorale overheid de stukken verwerkt die afkomstig zijn van de inspectiedienst met het oog op de vervolging;
- uiterlijk één jaar vanaf de ontvangst van het verzoek ingediend overeenkomstig de artikelen 12 tot 22 van Europese Verordening EU 2016/679, behalve indien een controle of onderzoek loopt.

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

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

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

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

TITEL 7. - Slotbepalingen

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

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

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

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

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

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

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

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

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

f) voor de sector gezondheidszorg: de overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad;
g) voor de sector drinkwater: de overheid aangewezen door de Koning bij besluit vastgesteld na overleg in de Ministerraad;";
3° het artikel wordt aangevuld met de bepalingen onder 13° tot 17°, luidende:
- "13° "de wet van 7 april 2019": de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid;
- 14° "beveiliging van netwerk- en informatiesystemen": de beveiliging van netwerk- en informatiesystemen als bedoeld in artikel 6, 8° en 9°, van de wet van 7 april 2019;
- 15° " de sector digitale infrastructuren": de sector bedoeld in punt 6 van bijlage 1 van de wet van 7 april 2019;
- 16° " de sector drinkwater": de sector bedoeld in punt 5 van bijlage 1 van de wet van 7 april 2019;
- 17° " de sector gezondheidszorg": de sector bedoeld in punt 4 van bijlage 1 van de wet van 7 april 2019.".

Art. 76. In artikel 4 van dezelfde wet, gewijzigd bij de wet van 15 juli 2018, wordt paragraaf 4 vervangen als volgt:
" § 4. Dit hoofdstuk is van toepassing op de sector financiën, met inbegrip van de exploitanten van een handelsplatform bedoeld in artikel 3, 3°, d), de sector elektronische communicatie, de sector digitale infrastructuren, de sector gezondheidszorg en de sector drinkwater, wat de beveiliging en de bescherming van de nationale kritieke infrastructuren betreft.".

Art. 77. Artikel 5 van dezelfde wet, gewijzigd bij de wet van 15 juli 2018, wordt aangevuld met een paragraaf 3, luidende:
" § 3. Tijdens het hele identificatieproces als bedoeld in deze afdeling wordt de autoriteit bedoeld in artikel 7, § 1, van de wet van 7 april 2019 betrokken bij het door de sectorale overheden en de ADCC gevoerde nationale en internationale overleg voor de identificatie van de kritieke infrastructuren met betrekking tot de beveiliging van netwerk- en informatiesystemen.".

Art. 78. In artikel 13 van dezelfde wet, gewijzigd bij de wetten van 25 april 2014 en 15 juli 2018 worden de volgende wijzigingen aangebracht:
1° in paragraaf 5bis worden de woorden "met uitzondering van die welke worden uitgebaat door een exploitant van een handelsplatform," ingevoegd tussen de woorden "vallen," en het woord "worden".
2° in paragraaf 6, eerste lid, worden de woorden ", met uitzondering van de kritieke infrastructuren die worden uitgebaat door een exploitant van een handelsplatform," ingevoegd tussen de woorden "de sector financiën" en de woorden "worden".

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

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

Art. 81. In artikel 19 van dezelfde wet worden de woorden "De exploitant, het beveiligingscontactpunt, de sectorale overheid, de ADCC, het OCAD en de

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

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

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

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

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

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

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

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

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

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

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

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

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

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

"Art. 15ter. Het Agentschap wordt aangewezen als inspectiedienst, in de zin van artikel 42 van de wet van 7 april 2019, en is belast met het controleren van de toepassing van de bepalingen van deze wet en de uitvoeringsbesluiten ervan door de aanbieders van essentiële diensten, die krachtens bovengenoemde wet geïdentificeerd zijn, wat betreft de elementen van een nucleaire installatie bestemd voor de industriële productie van elektriciteit die dienen voor de transmissie van de elektriciteit.
De Koning bepaalt de praktische inspectiemodaliteiten, na advies van het Agentschap.".
HOOFDSTUK 3. - Wijzigingen van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector
Art. 87. Artikel 1/1 van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector, ingevoegd bij de wet van 10 juli 2012, wordt aangevuld met een lid, luidende:
"Deze wet voorziet in de gedeeltelijke omzetting van Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie.".
Art. 88. In artikel 14, § 1, eerste lid, van dezelfde wet, gewijzigd bij de wetten van 13 december 2010, 10 juli 2012, 27 maart 2014, 18 april 2017, 5 mei 2017 en 31 juli 2017, worden de volgende wijzigingen aangebracht:
1° in het eerste lid worden de woorden ", met betrekking tot de sector digitale infrastructuren in de zin van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, met betrekking tot de sectoren elektronische communicatie en digitale infrastructuren in de zin van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren," ingevoegd tussen het woord "radioapparatuur" en de woorden "en met betrekking tot";
2° de bepaling onder 3° wordt vervangen als volgt:
"3° het toezicht op de naleving van de volgende normen en van de uitvoeringsbesluiten ervan:
a) de wet van 13 juni 2005 betreffende de elektronische communicatie;
b) Titel I, hoofdstuk X, en Titel III van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven;
c) de wet van 26 januari 2018 betreffende de postdiensten;
d) de artikelen 14, § 2, 2°, en 21, §§ 5 tot en met 7, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector;
e) de artikelen 4 en 4/1 van de wet van 17 januari 2003 betreffende de rechtsmiddelen en de geschillenbehandeling naar aanleiding van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector;
f) de wet van 5 mei 2017 betreffende de audiovisuele mediadiensten in het tweetalig gebied Brussel-Hoofdstad;
g) de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, wat de sectoren elektronische communicatie en digitale infrastructuren betreft;
h) de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid,

met betrekking tot de sector digitale infrastructuren;
i) de Verordening (EU) 611/2013 van de Commissie van 24 juni 2013 betreffende maatregelen voor het melden van inbreuken in verband met persoonsgegevens op grond van Richtlijn 2002/58/EG van het Europees Parlement en de Raad betreffende privacy en elektronische communicatie.
Voor de toepassing van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, wordt het Instituut aangewezen als sectorale overheid en inspectiedienst voor de sector digitale infrastructuren. De Koning kan de praktische inspectiemodaliteiten voor deze sector bepalen, na advies van het Instituut.".
Art. 89. In artikel 24, eerste lid, van dezelfde wet, gewijzigd bij de wetten van 27 maart 2014 en 26 januari 2018, worden de woorden ", de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, wat de sector elektronische communicatie en de sector digitale infrastructuren betreft, en de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, wat de sector digitale infrastructuren betreft", ingevoegd tussen de woorden "in het tweetalig gebied Brussel-Hoofdstad" en de woorden "en hun uitvoeringsbesluiten".
HOOFDSTUK 4. - Wijzigingen van de wet van 21 november 2017 over de infrastructuren voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU
Art. 90. Artikel 71 van de wet van 21 november 2017 over de infrastructuren voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU wordt aangevuld met de woorden "en van titel 2 van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid. Voor de uitvoering van de voormelde opdrachten betreffende de wet van 7 april 2019 kan de FSMA niettemin een gespecialiseerde externe dienstverlener belasten met de uitvoering van welbepaalde toezichtsopdrachten of de bijstand van een dergelijke dienstverlener verkrijgen.".
Art. 91. Artikel 79 van dezelfde wet wordt aangevuld met een paragraaf 4, luidende:
" § 4. In geval van schending van de toepasselijke bepalingen van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid kan de FSMA de in artikel 52 van voormelde wet bepaalde administratieve sancties opleggen.".
HOOFDSTUK 5. - Wijziging van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten
Art. 92. Artikel 75, § 1, 15°, van de wet van 2 augustus 2002 betreffende het toezicht op de financiële sector en de financiële diensten, opgeheven door de wet van 5 december 2017 houdende diverse financiële bepalingen, wordt hersteld in de volgende lezing:
"15° binnen de grenzen van het recht van de Europese Unie, aan de autoriteiten bedoeld in artikel 7 van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid voor de uitvoering van de bepalingen van deze wet en van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren;".
HOOFDSTUK 6. - Wijzigingen van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België

Art. 93. Artikel 36/1 van de wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België, ingevoegd bij het koninklijk besluit van 3 maart 2011, wordt aangevuld met de bepaling onder 28°, luidende:
"28° "de wet van 7 april 2019": de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.".
Art. 94. In artikel 36/14, § 1, van dezelfde wet, laatstelijk gewijzigd bij de wet van 30 juli 2018, worden de volgende wijzigingen aangebracht:
1° in de bepaling onder 20° worden de woorden "aan de autoriteit bedoeld in artikel 7, § 1, van de wet van 7 april 2019" ingevoegd tussen de woorden "de analyse van de dreiging," en de woorden "en aan de politiediensten";
2° de paragraaf wordt aangevuld met de bepaling onder 24°, luidende:
"24° binnen de grenzen van het recht van de Europese Unie, aan de autoriteiten bedoeld in artikel 7 van de wet van 7 april 2019 voor de uitvoering van de bepalingen van de wet van 7 april 2019 en van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren.".
Art. 95. In dezelfde wet wordt een hoofdstuk IV/4 ingevoegd, dat artikel 36/47 bevat, luidende:
"Hoofdstuk IV/4. Toezicht door de Bank in het kader van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.
Art. 36/47. "Voor de toepassing van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid wordt de Bank aangewezen als sectorale overheid en inspectiedienst voor de aanbieders van de sector financiën, met uitzondering van de exploitanten van een handelsplatform in de zin van artikel 3, 6°, van de wet van 21 november 2017 over de infrastructuren voor de markten voor financiële instrumenten en houdende omzetting van Richtlijn 2014/65/EU.
De artikelen 36/19 en 36/20 zijn van toepassing.
De Sanctiecommissie oordeelt over het opleggen van de administratieve geldboetes bedoeld in artikel 52 van voormelde wet van 7 april 2019. De artikelen 36/8 tot 36/12/3 en artikel 36/21 zijn van toepassing.
De Bank deelt relevante informatie over incidentmeldingen die zij ontvangt krachtens de wet van 7 april 2019 zo snel mogelijk met de ECB.".
HOOFDSTUK 7. - Inwerkingtreding
Art. 96. Deze wet treedt in werking de dag waarop ze in het Belgisch Staatsblad wordt bekendgemaakt.
Kondigen deze wet af, bevelen dat zij met 's Lands zegel zal worden bekleed en door het Belgisch Staatsblad zal worden bekendgemaakt.
Gegeven te Brussel, 7 april 2019.
FILIP
Van Koningswege :
De Eerste Minister,
Ch. MICHEL
De Minister van Veiligheid en Binnenlandse Zaken,
P. DE CREM
Met 's Lands zegel gezegeld :
De Minister van Justitie,
K. GEENS

Nota
(1) Kamer van volksvertegenwoordigers (www.dekamer.be):
Stukken: 54 3340
Integraal verslag: 21 maart 2019.

Bijlage 1 bij de wet van 7 april 2019 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid
Soorten aanbieders van essentiële diensten bedoeld in artikel 11, § 1

Sector	Deelsector	Soort entiteit
1. Energie	a) Elektriciteit	Elektriciteitsbedrijven in de zin van artikel 2, 15° ter, van de wet van 29 april 1999 betreffende de organisatie van de elektriciteitsmarkt.
		Distributienetbeheerders in de zin van artikel 2, 11°, van de wet van 29 april 1999 betreffende de organisatie van de elektriciteitsmarkt.
		Netbeheerders in de zin van artikel 2, 8°, van de wet van 29 april 1999 betreffende de organisatie van de elektriciteitsmarkt.
	b) Aardolie	Exploitanten van oliepijpleidingen.
		Exploitanten van installaties voor de productie, raffinage, verwerking, opslag en het vervoer van aardolie.
	c) Gas	Aardgasondernemingen in de zin van artikel 1, 5° bis, van de wet van 12 april 1965 betreffende het vervoer van gasachtige produkten en andere door middel van leidingen.
		Distributienetbeheerders in de zin van artikel 1, 13°, van de wet van 12 april 1965 betreffende het vervoer van gasachtige produkten en andere door middel van leidingen.
		Beheerders van het aardgasvervoersnet in de zin van artikel 1, 31°, van de wet van 12 april 1965 betreffende het vervoer van gasachtige produkten en andere door middel van leidingen.
		Beheerders van de opslag in de zin van artikel 1, 33°, van de wet van 12 april 1965 betreffende het vervoer van gasachtige produkten en andere door middel van leidingen.

		Beheerders van de LNG-installatie in de zin van artikel 1, 35°, van de wet van 12 april 1965 betreffende het vervoer van gasachtige produkten en andere door middel van leidingen.
		Exploitanten van raffinage- en verwerkingsinstallaties van aardgas.
2. Vervoer	a) Luchtvervoer	Luchtvaartmaatschappijen in de zin van artikel 3, punt 4) van de verordening (EG) nr. 300/2008 van het Europees Parlement en de Raad van 11 maart 2008 inzake gemeenschappelijke regels op het gebied van de beveiliging van de burgerluchtvaart en tot intrekking van verordening (EG) nr. 2320/2002.
		Luchthavenbeheerders in de zin van in artikel 2, punt 2), van het KB van 6 november 2010 betreffende de toegang tot de grondafhandelingsmarkt op de luchthaven Brussel-Nationaal, luchthavens in de zin van artikel 2, punt 1), van richtlijn 2009/12/EG van het Europees Parlement en de Raad, met inbegrip van de luchthavens die tot het kernnetwerk behoren, opgesomd in bijlage II, afdeling 2, van verordening (EU) nr. 1315/2013 van het Europees Parlement en de Raad, alsook entiteiten die bijbehorende installaties bedienen welke zich op luchthavens bevinden.
		Luchtvaartnavigatiediensten in de zin van artikel 2, punt 4), van de verordening (EG) nr. 549/2004 van het Europees Parlement en de Raad van 10 maart 2004 tot vaststelling van het kader voor de totstandbrenging van het gemeenschappelijke Europese luchtruim ("de kaderverordening").
		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 privé-klinieken)	Zorgverleners in de zin van artikel 3, punt g), van de richtlijn 2011/24/EU van het Europees Parlement en de Raad van 9 maart 2011 betreffende de toepassing van de rechten van patiënten bij grensoverschrijdende gezondheidszorg.
5. Drinkwater		Leveranciers en distributeurs van water bestemd voor menselijke consumptie in de zin van artikel 2, punt 1) a), van de richtlijn 98/83/EG van de Raad van 3 november 1998 betreffende de kwaliteit van voor menselijke consumptie bestemd water, behalve de distributeurs voor wie de distributie van water bestemd voor menselijke consumptie slechts een deel is van hun algemene distributieactiviteit van andere producten en goederen die niet worden beschouwd als essentiële diensten.
6.Digitale infrastructuren		IXP.
		Leveranciers van DNS-diensten.
		Registers van topleveldomeinnamen.

Gezien om te worden gevoegd bij de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.
FILIP
Van Koningswege :
De Eerste Minister,
Ch. MICHEL
De Minister van Veiligheid en Binnenlandse Zaken,
P. DE CREM

Bijlage 2 bij de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging

van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid
Soorten digitale diensten
1. Onlinemarktplaats
2. Onlinezoekmachines
3. Cloudcomputerdiensten
Gezien om te worden gevoegd bij de wet van 7 april 2019 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.
FILIP
Van Koningswege :
De Eerste Minister,
Ch. MICHEL
De Minister van Veiligheid en Binnenlandse Zaken,
P. DE CREM

begin

Publicatie : 2019-05-03
Numac : 2019011507