MEMORIE VAN TOELICHTING

ALGEMEEN DEEL

INHOUDSOPGAVE

1. Inleiding

Dit wetsvoorstel strekt tot de uitvoering van de Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148.[1] Deze richtlijn wordt hierna aangeduid als de NIS2-richtlijn. De lidstaten van de Europese Unie (hierna: lidstaten) moeten uiterlijk op 17 oktober 2024 aan de NIS2-richtlijn voldoen door deze richtlijn waar nodig in hun nationale regelgeving om te zetten. Aan het eind van het algemeen deel van deze memorie van toelichting is een transponeringstabel opgenomen.

2. De NIS2-richtlijn

2.1 Kern van de richtlijn

De NIS2-richtlijn is de opvolger van de zogeheten NIB1-richtlijn.[2] Voor de duidelijkheid wordt in het verdere vervolg van deze toelichting de NIB1-richtlijn aangeduid als de NIS1-richtlijn, naar de Engelse afkorting van die richtlijn.

Het doel van de richtlijn is om, ter ondersteuning van het functioneren van onze samenleving en economie, eenheid en samenhang te brengen in Europees beleid voor netwerk- en informatiebeveiliging, door de digitale paraatheid te vergroten en de gevolgen van cyberincidenten te verkleinen. De NIS1-richtlijn laat veel discretionaire ruimte over aan lidstaten bij de uitvoering van de richtlijn. Door die geboden ruimte zijn er tussen lidstaten aanzienlijke verschillen ten aanzien van de implementatie van de richtlijn in de lidstaten. Zo zijn er aanzienlijke verschillen op het gebied van de afbakening van het toepassingsgebied van de richtlijn. Dat verschil betekent concreet dat een aanbieder in de ene lidstaat wel onder de werking van de richtlijn valt, terwijl een nagenoeg identieke aanbieder (dezelfde sector, met een soortgelijke dienstverlening, werkzaam in een soortgelijke context) uit een andere lidstaat niet onder de werking van de richtlijn valt. Ook bestaan er aanzienlijke verschillen ten aanzien van de uitvoering van de verplichtingen op nationaal niveau, zoals het soort cyberbeveiligingseisen en de mate van gedetailleerdheid, en het toezicht op de naleving van de verplichtingen die uit de richtlijn volgen. Deze verschillen kunnen nadelige effecten hebben op de werking van de interne markt en kunnen sommige lidstaten meer kwetsbaar maken voor cyberdreigingen, met mogelijke overloopeffecten in de hele Europese Unie. Daarom wordt de NIS1-richtlijn ingetrokken en vervangen door de NIS2-richtlijn. Daarmee wordt beoogd om de hiervoor benoemde verschillen weg te nemen.[3]

De NIS2-richtlijn heeft tot doel om een hoog gemeenschappelijk niveau van cyberbeveiliging in de Europese Unie te bereiken, teneinde de werking van de interne markt te verbeteren. Deze richtlijn beoogt dit doel te bereiken door de verschillen weg te nemen die tussen lidstaten bestaan op het gebied van de cyberbeveiligingseisen die worden gesteld aan entiteiten die economisch belangrijke activiteiten of diensten verrichten. De richtlijn tracht dit doel te bereiken door onder meer regels vast te stellen over entiteiten die van rechtswege, zonder tussenkomst van een lidstaat, onder het toepassingsbereik van de richtlijn komen te vallen, en door te voorzien in doeltreffende voorzieningen ten aanzien van de cyberbeveiligingseisen waar entiteiten aan moeten voldoen en het toezicht op de naleving van de verplichtingen die voortvloeien uit de richtlijn.[4] De NIS2-richtlijn gaat uit van minimumharmonisatie. De richtlijn belet de lidstaten daarom niet om bepalingen vast te stellen of te handhaven die een hoger cyberbeveiligingsniveau waarborgen, mits dergelijke bepalingen stroken met de in het Unierecht vastgelegde verplichtingen van de lidstaten.[5]

---

[1] *PbEU* 2022, L 333.
[2] 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 (*PbEU* 2016, L 194).
[3] Overwegingen 2, 4 en 5 NIS2-richtlijn.
[4] Artikel 1, eerste lid, en de overwegingen 4 en 5 NIS2-richtlijn.
[5] Artikel 5 NIS2-richtlijn.

2.2 Belangrijkste onderdelen van de richtlijn

Hierna wordt kort ingegaan op de belangrijkste onderdelen van de NIS2-richtlijn:
a. reikwijdte;
b. toepasselijkheid richtlijn van rechtswege of na aanwijzing;
c. onderscheid essentiële entiteiten en belangrijke entiteiten;
d. verplichtingen;
e. toezicht en handhaving;
f. nationale cyberbeveiligingsstrategie;
g. aanwijzing CSIRT, centraal contactpunt en bevoegde autoriteiten;
h. samenwerking op nationaal, Europese Unie (hierna: EU)- en internationaal niveau.

a. reikwijdte
De NIS2-richtlijn bevat uitbreidingen ten opzichte van de NIS1-richtlijn. Allereerst is het aantal sectoren dat onder het bereik van de richtlijn valt uitgebreid naar onder meer de sectoren afvalwater, ruimtevaart, post- en koeriersdiensten, afvalstoffenbeheer, onderzoek met het oog op commerciële doeleinden en productie en verwerking en distributie van levensmiddelen. Ook is het aantal subsectoren binnen de sectoren, die in de NIS1-richtlijn worden genoemd, uitgebreid. Zo is de sector energie uitgebreid met de subsectoren waterstof en stadsverwarming en -koeling. Tot slot is ook het aantal soorten entiteiten, binnen de sectoren die in de NIS1-richtlijn worden genoemd, uitgebreid. Deze uitbreidingen hebben tot gevolg dat er meer entiteiten onder het toepassingsbereik van de NIS2-richtlijn komen te vallen in vergelijking met de NIS1-richtlijn.

b. toepasselijkheid richtlijn van rechtswege of na aanwijzing
Op grond van de NIS1-richtlijn zijn lidstaten zelf verantwoordelijk voor het identificeren van de entiteiten die voldoen aan de criteria om als aanbieders van essentiële diensten te worden aangemerkt en daarmee onder het toepassingsbereik van die richtlijn vallen. Alleen digitale dienstverleners vallen van rechtswege onder de NIS1-richtlijn. In de NIS2-richtlijn is de manier waarop wordt bepaald welke entiteiten binnen het toepassingsbereik van deze richtlijn vallen anders geregeld. Ten aanzien van een groot deel van de entiteiten is in de NIS2-richtlijn bepaald dat zij onder het toepassingsbereik van de richtlijn vallen indien zij voldoen aan bepaalde criteria. Ten aanzien van andere entiteiten is bepaald dat zij onder specifieke voorwaarden kunnen worden aangewezen als essentiële entiteit of belangrijke entiteit, waardoor zij onder het toepassingsbereik van de richtlijn komen te vallen.

c. onderscheid essentiële entiteiten en belangrijke entiteiten
De NIS1-richtlijn maakt een onderscheid tussen aanbieders van essentiële diensten en digitale dienstverleners. Met de NIS2-richtlijn is er een nieuw onderscheid, namelijk dat van essentiële entiteiten en belangrijke entiteiten. Dit onderscheid komt tot uiting in het toezichtsregime, dat voor essentiële entiteiten uitgebreider is dan het toezichtsregime op belangrijke entiteiten. Er is vanuit de richtlijn geen onderscheid in de verplichtingen die gelden voor essentiële entiteiten en belangrijke entiteiten.
De NIS2-richtlijn kent tot slot een derde categorie entiteiten, namelijk entiteiten die domeinnaamregistratiediensten verlenen. Op domeinregistratiediensten is een aantal verplichtingen, waaronder de zorgplicht en de meldplicht, niet van toepassing. Voor hen gelden andere, specifieke verplichtingen. Indien een aanbieder van domeinnaamregistratiediensten tevens een belangrijke of essentiële entiteit is, gelden de bijhorende verplichtingen uiteraard wel.

d. verplichtingen
De NIS2-richtlijn bevat verplichtingen voor essentiële entiteiten en belangrijke entiteiten op het gebied van onder meer het nemen van maatregelen voor het beheer van cyberbeveiligingsrisico's (zorgplicht), het melden van significante incidenten (meldplicht) en het verstrekken van informatie. Voor entiteiten die domeinnaamregistratiediensten verlenen, gelden de zorgplicht en de meldplicht niet, maar wel andere verplichtingen zoals de verplichting om informatie te verstrekken ten behoeve van het register van het Agentschap van de Europese Unie voor cyberbeveiliging (hierna: het Enisa-register).

e. toezicht en handhaving

Op de naleving van de verplichtingen die volgen uit de NIS2-richtlijn door essentiële entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen, wordt toezicht gehouden. De NIS2-richtlijn bevat enkele bevoegdheden voor de toezichthouder die nieuw zijn in het Nederlands (bestuurs-)recht. Paragraaf 5.7 gaat hier nader op in.

f. nationale cyberbeveiligingsstrategie
Elke lidstaat moet op grond van de NIS2-richtlijn een nationale cyberbeveiligingsstrategie vaststellen, die voorziet in de strategische doelstellingen, de middelen die nodig zijn om die doelstellingen te behalen en passende beleids- en regelgevingsmaatregelen.

g. aanwijzing CSIRT, centraal contactpunt en bevoegde autoriteiten
Elke lidstaat moet op grond van de NIS2-richtlijn overgaan tot het aanwijzen of instellen van:
- één of meer computer security incident response teams (hierna: CSIRT's), die onder meer de taak hebben om te waarschuwen voor cyberrisico's en te reageren op cyberincidenten;
- één centraal contactpunt, dat een verbindingsfunctie heeft in de nationale samenwerking en de samenwerking binnen de EU;
- één of meer bevoegde autoriteiten, die toezien op de naleving van de verplichtingen die voortvloeien uit de richtlijn; en
- een of meer bevoegde autoriteiten, die verantwoordelijk zijn voor het beheer van grootschalige cyberbeveiligingsincidenten en -crises en –wanneer er meer dan één autoriteit wordt aangewezen– de aanwijzing van een coördinerende cybercrisisbeheersautoriteit.

h. samenwerking op nationaal, EU- en internationaal niveau
De NIS2-richtlijn schrijft samenwerking op nationaal, EU- en internationaal niveau voor. Op nationaal niveau moeten de CSIRT's, het centrale contactpunt en de bevoegde autoriteiten binnen een lidstaat met elkaar samenwerken. Op EU-niveau geldt dat de bevoegde autoriteiten van de lidstaten met elkaar moeten samen werken, onder meer door elkaar bijstand te verlenen. Op EU-niveau wordt de reeds bestaande samenwerkingsgroep uitgebreid om de strategische samenwerking en de uitwisseling van informatie tussen de lidstaten te ondersteunen en te vergemakkelijken.[6] Ook wordt een netwerk van nationale CSIRT's (het CSIRT-netwerk) uitgebreid[7] en wordt met de NIS2-richtlijn het EU-netwerk van verbindingsorganisaties voor cybercrises (EU-CyCLONe) opgericht.[8]
Op het gebied van de samenwerking op internationaal niveau biedt de NIS2-richtlijn de mogelijkheid voor de EU om internationale overeenkomsten met derde landen of internationale organisaties te sluiten voor hun deelname aan en de organisatie van bepaalde activiteiten van de samenwerkingsgroep, het CSIRT-netwerk en EU-CyCLONe.[9]

2.3 Verhouding tot de NIS1-richtlijn en de Wet beveiliging netwerk- en informatiesystemen

De NIS1-richtlijn is de voorganger van de NIS2-richtlijn en heeft tot doel om, ter ondersteuning van het functioneren van de samenleving en economie, eenheid en samenhang te brengen in het Europees beleid voor netwerk- en informatiebeveiliging. Op grond van die richtlijn moeten lidstaten bepaalde aanbieders onder meer verplichten om maatregelen te nemen op het gebied van de beveiliging van hun netwerk- en informatiesystemen en om ernstige cyberincidenten te melden.

De NIS1-richtlijn is in 2018 geïmplementeerd in de Wet beveiliging netwerk- en informatiesystemen (Wbni). Bij de implementatie van de NIS1-richtlijn is de toenmalige Wet gegevensverwerking en

[6] De samenwerkingsgroep bestaat uit vertegenwoordigers van de lidstaten, de Europese Commissie en het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa).
[7] Het CSIRT-netwerk dient een snelle en doeltreffende operationele samenwerking tussen de lidstaten te bevorderen. Het netwerk bestaat uit vertegenwoordigers van de nationale CSIRT's en het computercrisisresponsteam voor de instellingen, organen en instanties van de Unie (CERT-EU).
[8] EU-CyCLONe ondersteunt het gecoördineerde beheer van grootschalige cyberbeveiligingsincidenten en crises op operationeel niveau en zorgt voor informatie-uitwisseling tussen de lidstaten en de instellingen, organen en agentschappen van de Europese Unie. Dit netwerk bestaat uit de vertegenwoordigers van de cybercrisisbeheerautoriteiten van de lidstaten. Wanneer een grootschalig cyberbeveiligingsincident plaatsvindt of mogelijk plaats zal vinden met een (mogelijk) aanzienlijke impact op diensten en activiteiten die binnen het toepassingsgebied van de richtlijn vallen, dan bestaat het netwerk ook uit de Europese Commissie.
[9] Artikel 17 NIS2-richtlijn.

meldplicht cybersecurity (Wgmc) beleidsneutraal, zonder materiële wijzigingen, geïncorporeerd in de Wbni en is de Wgmc ingetrokken. Daardoor bevat de Wbni ook onderdelen die niet uit de NIS1-richtlijn volgen, maar uit nationale wetgeving. De Wbni zal worden ingetrokken. Enkele onderdelen die afkomstig waren uit de Wgmc, zullen wederom beleidsneutraal worden overgezet naar de Cbw.

2.4 Verhouding tot de CER-richtlijn

Gelijktijdig aan de NIS2-richtlijn is de Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten en tot intrekking van Richtlijn 2008/114/EG van de Raad vastgesteld.[10] Die richtlijn wordt hierna aangeduid als de CER-richtlijn, ontleend aan de woorden *critical entities* en *resilience* die voorkomen in de titel van de Engelstalige naam van die richtlijn. Voor de CER-richtlijn geldt dezelfde eveneens als implementatiedeadline in de nationale regelgeving 17 oktober 2024. De CER-richtlijn wordt in Nederland geïmplementeerd in de Wet weerbaarheid kritieke entiteiten (hierna: Wwke).

De CER-richtlijn ziet op het verhogen van de weerbaarheid van kritieke entiteiten, dit zijn aanbieders van essentiële diensten. Die weerbaarheid ziet op natuurlijke en door de mens veroorzaakte risico's die negatieve gevolgen kunnen hebben voor de verlening van essentiële diensten. Voorbeelden van zulke risico’s zijn ongevallen, natuurrampen, noodsituaties op het gebied van de volksgezondheid (zoals pandemieën) en dreigingen (zoals terroristische misdrijven, criminele infiltratie en sabotage).

Gezien de onderlinge verbanden tussen cyberbeveiliging en de weerbaarheid van entiteiten, bevatten de NIS2-richtlijn en de CER-richtlijn waarborgen om te zorgen voor een coherente samenhang tussen de richtlijnen. Daartoe regelt de NIS2-richtlijn dat entiteiten die uit hoofde van de CER-richtlijn worden aangewezen als kritieke entiteit, ook onder het toepassingsbereik van de NIS2-richtlijn vallen en automatisch als essentiële entiteit in de zin van de NIS2-richtlijn kwalificeren.[11] Andersom geldt dat echter niet: een essentiële entiteit kwalificeert niet automatisch als kritieke entiteit, omdat kritieke entiteiten eerst als zodanig moeten worden aangewezen. De CER-richtlijn regelt verder dat deze niet van toepassing is op aangelegenheden die vallen onder de NIS2-richtlijn.[12] Verder voorzien de richtlijnen in bepalingen over onder meer de samenwerking en informatie-uitwisseling tussen de bevoegde NIS2- en CER-autoriteiten.

De Cyberbeveiligingswet (hierna: Cbw)*,* waarin de NIS2-richtlijn is geïmplementeerd, kent een benadering die alle gevaren omvat (*all hazard*) en heeft tot doel om netwerk- en informatiesystemen en de fysieke omgeving daarvan te beschermen tegen gebeurtenissen die de beveiliging van die systemen kunnen aantasten. Het gaat hierbij niet alleen om de enkele bescherming tegen gebeurtenissen met kwade wil, zoals digitale aanvallen, diefstal of ongeoorloofde fysieke toegang. Het gaat ook om de bescherming van die systemen tegen andersoortige gebeurtenissen, zoals natuurrampen. Om de risico’s voor netwerk- en informatiesystemen te beheersen moeten entiteiten maatregelen treffen voor zowel de digitale beveiliging van die systemen als voor de bescherming van de fysieke omgeving en componenten van die systemen, zoals gebouwen en ruimtes waar die systemen zich bevinden. Het kan voorkomen dat een incident of bijna-incident gevolgen heeft die zowel de netwerk- en informatiesystemen betreffen als een verstoring van andere fysieke aspecten die de essentiële dienstverlening raken. In dat geval gelden de verplichtingen van beide wetten. De Wwke beschrijft dan de verplichtingen van de kritieke entiteit en de respons van de bevoegde autoriteit daarop, die zich niet uitstrekt over de netwerk- en informatiesystemen of de fysieke omgeving daarvan. Voor die systemen en de omgeving daarvan is de Cbw van toepassing.

2.5 Verhouding tot de Verordening digitale operationele weerbaarheid

Gelijktijdig met de NIS2-richtlijn is de Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU)

[10] *PbEU* 2022, L 333.
[11] Artikel 2, derde lid, en artikel 3, eerste lid, onderdeel f, NIS2-richtlijn.
[12] Artikel 1, tweede lid, CER-richtlijn.

nr. 909/2014 en (EU) 2016/1011 vastgesteld.[13] Deze verordening, die op de financiële sector van toepassing is, wordt hierna aangeduid als de Verordening digitale operationele weerbaarheid of DORA.

De bepalingen van de Verordening digitale operationele weerbaarheid over risicobeheer op het gebied van informatie- en communicatietechnologie (ICT), het beheer van ICT-gerelateerde incidenten en met name de rapportage van grote ICT-gerelateerde incidenten, alsmede die over digitale operationele weerbaarheidstests, informatie-uitwisselingsregelingen en risico van derden op het gebied van ICT, zijn van toepassing op een groot gedeelte van de financiële sector in plaats van de bepalingen uit de NIS2-richtlijn. Dit betekent dat de bepalingen uit dit wetsvoorstel over de zorgplicht en de meldplicht en het toezicht en de handhaving daarop, niet van toepassing zijn op financiële entiteiten die onder de verordening vallen. Tegelijkertijd is het van belang om een sterke relatie en uitwisseling van informatie met de financiële sector uit hoofde van de NIS2-richtlijn in stand te houden. Dit is van belang om te zorgen voor samenhang met de door de lidstaten van de EU ingevoerde cyberbeveiligingsstrategieën en zodat financiële toezichthouders informatie kunnen uitwisselen over cyberincidenten die gevolgen hebben voor de andere sectoren die onder de NIS2-richtlijn vallen.

Om de uitwisseling van informatie te bevorderen biedt de Verordening digitale operationele weerbaarheid toezichthoudende autoriteiten en de uit hoofde van die verordening bevoegde autoriteiten de mogelijkheid deel te nemen aan de activiteiten van de samenwerkingsgroep en informatie uit te wisselen en samen te werken met de centrale contactpunten, de CSIRT's en de bevoegde NIS2-autoriteiten[14]. De uit hoofde van de Verordening digitale operationele weerbaarheid bevoegde autoriteiten moeten de details van ernstige ICT-gerelateerde incidenten en significante cyberdreigingen ook doorgeven aan de CSIRT's, de bevoegde NIS2-autoriteiten of de centrale contactpunten[15].

De Minister van Financiën wordt in dit wetsvoorstel aangewezen als sectorale bevoegde autoriteit binnen de sectoren bankwezen en infrastructuur voor de financiële markt. De reden voor het aanwijzen van de minister van Financiën als sectorale bevoegde autoriteit is dat met dit wetsvoorstel alle exploitanten van handelsplatformen (voor zover zij niet kwalificeren als micro- of kleine onderneming) onder deze wet worden gebracht. De Autoriteit Financiële Markten (AFM) is momenteel belast met het financieel toezicht op deze instellingen en zal worden belast met het toezicht op deze partijen in het kader van de Verordening digitale operationele weerbaarheid. Door de Minister van Financiën aan te wijzen als sectorale bevoegde autoriteit wordt het mogelijk om relevante bepalingen en samenwerkingsmogelijkheden die voortvloeien uit de NIS2-richtlijn te delegeren naar de AFM voor zover het exploitanten van handelsplatformen betreft. De Minister van Justitie en Veiligheid (in de praktijk: het NCSC) zal als CSIRT blijven fungeren voor deze sectoren.

2.6 Verhouding tot de eIDAS-verordening

Verordening (EU) Nr. 910/2014 (hierna: eIDAS-verordening) geeft het wettelijk kader voor vertrouwensdiensten. Vertrouwensdiensten vallen binnen de reikwijdte van de NIS2-richtlijn, voor zover deze ook onder de reikwijdte vallen van de eIDAS-verordening. Overweging 93 van de NIS2-richtlijn geeft aan dat deze richtlijn aanvullend is op de eIDAS-verordening wat betreft de veiligheidseisen voor vertrouwensdiensten in de eIDAS-verordening.

3. Nationale context

[13] *PbEU* 2022, L 333.
[14] Artikel 47 Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011.
[15] Artikel 19 lid 6c Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011.

De Nederlandse Cybersecurity Strategie (NLCS) beschrijft de acties en ambities van het kabinet voor de periode 2022-2028 voor een digitaal veilige samenleving.[16] De NLCS wordt door de Minister van Justitie en Veiligheid in overeenstemming met de betrokken ministers vastgesteld; de Minister van Justitie en Veiligheid voert regie op en coördineert de totstandkoming van de strategie en monitort eveneens dat er uitvoering en opvolging aan wordt gegeven. In deze strategie is eveneens een tussentijds evaluatieonderzoek opgenomen op basis waarvan een volgend kabinet eventueel een beslissing kan nemen over de uiteindelijke doorlooptijd en eventuele eindevaluatie van de NLCS. Vanuit de rol als centraal contactpunt stelt de minister van Justitie en Veiligheid de Commissie binnen drie maanden in kennis van de vaststelling van de strategie (artikel 7, derde lid, NIS2-richtlijn). Hiermee voldoet Nederland aan het vereiste van artikel 7 NIS2-richtlijn tot het hebben van een nationale cyberbeveiligingsstrategie die voorziet in de strategische doelstellingen, de middelen die nodig zijn om die doelstellingen te behalen, en passende beleids- en regelgevingsmaatregelen, om een hoog niveau van cyberbeveiliging te bereiken en te handhaven.

De Nederlandse Cybersecuritystrategie is het generieke kader. In het kader hiervan is er ruimte voor specifieke invulling onder andere door sectorale beleidskaders, strategieën, agenda's, routekaarten op deelonderwerpen of aanvullende normenkaders. Strategische of beleidsmatige onderwerpen danwel onderdelen van de onderwerpen die worden genoemd in artikel 7, tweede lid, onderdeel a tot en met j, NIS2-richtlijn kunnen dan ook onder verantwoordelijkheid van andere ministers dan de Minister van JenV tot stand komen. Hiermee wordt aansluiting gezocht bij de beleidsverantwoordelijkheden van ministers zoals die op dat moment gelden.

Nederland is één van de meest gedigitaliseerde landen ter wereld. Dat biedt kansen, maar brengt ook risico's met zich mee. Het digitale ecosysteem is inmiddels zo verknoopt en complex, dat het voor individuele organisaties en personen ingewikkeld, zo niet onmogelijk is, om het geheel te doorgronden. Het is ook juist dit ecosysteem dat het moderne leven, en economie en samenleving als geheel mogelijk maakt. Criminelen maar ook kwaadwillende staten misbruiken deze complexiteit door zich ongezien op te houden en via digitale kwetsbaarheden onze publieke waarden aan te tasten.

Het kabinet zet daarom in op het versterken en transformeren van het digitale ecosysteem waarbij één organisatie of één individu niet langer de zwakste schakel kan zijn. Overheden en organisaties binnen de vitale infrastructuur hebben een speciale verantwoordelijkheid binnen dit ecosysteem. Voor organisaties die volgens deze wet actief zijn in een sector van maatschappelijk belang mag het nemen van cybersecuritymaatregelen niet vrijblijvend zijn. Wetgeving is één van de instrumenten die het kabinet inzet om deze verantwoordelijkheden voor organisaties in deze sectoren te beleggen en bestendigen. Vanwege de verwevenheid van de interne markt neemt het kabinet dit soort maatregelen bij voorkeur in EU-verband. De implementatie van de NIS2-richtlijn levert daarmee een belangrijke bijdrage aan het doel uit de NLCS dat organisaties zicht hebben op cyberincidenten, -dreigingen en -risico's en dat zij daar op een adequate manier mee omgaan.

De implementatie van de NIS2-richtlijn hangt samen met de zogeheten Aanpak vitaal. De processen en diensten die samen de vitale infrastructuur vormen, zijn het fundament waarop de Nederlandse samenleving draait. Uitval, verstoring of manipulatie van de vitale infrastructuur schaadt het functioneren van de Nederlandse economie en maatschappij en kan een bedreiging vormen voor de nationale veiligheid, de economische veiligheid en de stabiliteit van de interne markt van de EU. Het is dan ook van belang de weerbaarheid van de vitale infrastructuur tegen bestaande en nieuwe bedreigingen en risico's te versterken. Het doel van de Aanpak vitaal is het voorkomen van maatschappelijke ontwrichting en verstoring van de samenleving door het verhogen van de weerbaarheid van vitale aanbieders. Dat wordt gedaan door het vermogen om uitval, verstoring of manipulatie te voorkomen te verhogen, de effecten daarvan te beheersen en ervan te herstellen. De NIS2-richtlijn biedt samen met de CER-richtlijn een wettelijk kader voor het versterken van de digitale en fysieke weerbaarheid van onder meer de vitale infrastructuur.

4. Gemaakte implementatiekeuzes op hoofdlijnen

[16] Kamerstukken II 2022-2023, 26643 nr. 925.

In dit wetsvoorstel zijn op hoofdlijnen de volgende implementatiekeuzes gemaakt:

1. **Implementatie in één centrale wet:** De NIS2-richtlijn wordt, evenals dat bij de NIS1-richtlijn het geval was, geïmplementeerd in één centrale wet en niet in sectorale wetten, zoals de Wet op het financieel toezicht, de Elektriciteitswet 1998 en de Gaswet. De titel van de wet luidt Cyberbeveiligingswet.

2. **Verantwoordelijkheid vakminister bij aanwijzing en vrijstelling van entiteiten, medeverantwoordelijkheid Minister van Justitie en Veiligheid:** De vakminister is verantwoordelijk voor de toepassing van dit wetsvoorstel binnen de sectoren die onder zijn beleidsverantwoordelijkheid vallen. De Minister van Justitie en Veiligheid is medeverantwoordelijk vanuit zijn rol als coördinerend bewindspersoon voor cybersecurity en de bescherming van de vitale infrastructuur. De aanwijzing van entiteiten als essentiële entiteit of belangrijke entiteit door de vakminister, voor zover zij niet al van rechtswege als zodanig zijn aangemerkt op grond van de artikelen 8 of 12 van dit wetsvoorstel, geschiedt daarom na overleg met de Minister van Justitie en Veiligheid (zie artikel 9 en 13 Cbw).

Overheidsinstanties die in hoofdzaak activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving, met inbegrip van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, zijn van rechtswege uitgesloten van het toepassingsgebied van de NIS2-richtlijn. Overheidsinstanties waarvan de activiteiten slechts zijdelings verband houden met die gebieden, zijn daarentegen niet uitgesloten van het toepassingsgebied van de richtlijn. De richtlijn biedt lidstaten echter wel de mogelijkheid om specifieke entiteiten die activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving, of die uitsluitend diensten verlenen aan overheidsinstanties die in hoofdzaak zulke activiteiten uitvoeren, met betrekking tot die activiteiten of diensten vrij te stellen van bepaalde verplichtingen, zoals de zorgplicht en de meldplicht. De bevoegdheid om zulke entiteiten vrij te stellen van verplichtingen wordt belegd bij de vakminister. De vakminister kan overgaan tot het verlenen van de vrijstelling, in overeenstemming met de Minister van Justitie en Veiligheid (zie artikel 25 Cbw).

3. **Aanwijzing gemeenten, provincies, waterschappen en gemeenschappelijke regelingen als essentiële entiteit:** In dit wetsvoorstel is gebruik gemaakt van de mogelijkheid uit artikel 2, vijfde lid, onderdeel a, NIS2-richtlijn om lokale overheden onder het toepassingsbereik van de voorgestelde wet te brengen. Zij worden aangewezen als essentiële entiteit (zie artikel 8, eerste lid, onder h, Cbw). Paragraaf 5.1.1.3 gaat hier nader op in.

4. **Bevoegdheid aanwijzing onderwijsinstellingen:** In dit wetsvoorstel is de in artikel 2, vijfde lid, onderdeel b, NIS2-richtlijn geboden mogelijkheid geïmplementeerd om onderwijsinstellingen aan te wijzen als essentiële entiteit of als belangrijke entiteit. De Minister van Onderwijs, Cultuur en Wetenschap kan hiertoe overgaan, na overleg met de Minister van Justitie en Veiligheid (zie artikel 25, tweede lid, Cbw). Paragraaf 5.1.1.4 gaat hier nader op in.

5. **Aanwijzing Minister van Justitie en Veiligheid als het centrale contactpunt:** De Minister van Justitie en Veiligheid wordt aangewezen als het centrale contactpunt voor Nederland (zie artikel 15 Cbw).

6. **Aanwijzing Minister van Justitie en Veiligheid als de cybercrisisbeheerautoriteit:** De Minister van Justitie en Veiligheid wordt aangewezen als de cybercrisisbeheerautoriteit voor Nederland (zie artikel 19 Cbw).

7. **Opstellen lijst van entiteiten door Minister van Justitie en Veiligheid via een registratiemechanisme:** De in artikel 3, derde lid, NIS2-richtlijn opgenomen verplichting voor lidstaten om een lijst op te stellen van essentiële entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen, wordt belegd bij de Minister van Justitie en Veiligheid. In dit wetsvoorstel wordt de lijst genoemd: het nationale register. Er wordt een registratiemechanisme ingericht waarmee essentiële entiteiten, belangrijke entiteiten en entiteiten die

domeinregistratiediensten verlenen informatie aan moeten leveren ten behoeve van deze lijst. Dit wordt verder toegelicht in paragraaf 5.8.

8. **Dubbele meldplicht:** Essentiële entiteiten en belangrijke entiteiten moeten significante incidenten zowel bij het CSIRT als bij de bevoegde autoriteit melden. Er wordt naar gestreefd deze dubbele meldplicht technisch zo in te richten dat het verspreiden van de benodigde informatie maar één handeling van entiteiten vergt. Paragraaf 5.5 gaat hier nader op in.

9. **Instantie voor vrijwillige meldingen van significante incidenten, incidenten, bijna-incidenten en cyberdreigingen:** Het CSIRT wordt aangewezen als de instantie waar een essentiële entiteit of belangrijke entiteit op vrijwillige basis een melding kan indienen over een incident, bijna-incident en cyberdreiging. Voor eenieder, dus ook individuen en entiteiten die geen essentiële entiteit of belangrijke entiteit zijn, geldt dat zij op vrijwillige basis meldingen kunnen indienen over een significant incident, incident, bijna-incident en cyberdreiging bij een CSIRT.[17]

10. **Aanwijzing bevoegde autoriteit:**
In dit wetsvoorstel is ervoor gekozen om de vakministers aan te wijzen als de bevoegde autoriteit voor de sectoren en subsectoren die onder hun beleidsverantwoordelijkheid vallen (zie artikel 16 Cbw). De NIS2-richtlijn bevat diverse taken voor de bevoegde autoriteit. Zo heeft zij taken in het kader van meldingen van incidenten, maar ook de taak om te zorgen voor de handhaving van verplichtingen. Voor zover het gaat om het toezicht op de verplichtingen uit dit wetsvoorstel, is gekozen voor sectoraal toezicht. In de praktijk worden de toezichtstaken van de bevoegde autoriteit uitgevoerd door daartoe door de bevoegde autoriteit aangewezen ambtenaren van een dienstonderdeel van het departement of van een andere overheidsdienst. De andere taken van de bevoegde autoriteit worden in de praktijk uitgevoerd door het vakdepartement. Voor de duidelijkheid van deze toelichting wordt gebruik gemaakt van de terminologie "toezichthoudende instantie" enerzijds (wanneer wordt gedoeld op de uitvoering van toezichtstaken van de bevoegde autoriteit) en "de vakminister" anderzijds (wanneer wordt gedoeld op de andere taken van de bevoegde autoriteit).

11. **Hoofdlijnen in de wet, nadere uitwerking in lagere (sectorale) regelgeving:** Diverse artikelen uit dit wetsvoorstel over verplichtingen bevatten een verplichting op hoofdlijnen, zoals de zorgplicht en de meldplicht. Die artikelen bevatten een delegatiegrondslag voor het bij of krachtens algemene maatregel van bestuur (amvb) stellen of kunnen stellen van regels. Die delegatiegrondslagen bieden de mogelijkheid om met sectorspecifieke regels te komen, zoals sectorspecifieke drempelwaarden voor het bepalen van incidenten die meldplichtig zijn.

5. Hoofdlijnen van het voorstel

In dit hoofdstuk wordt een nadere toelichting gegeven op de belangrijkste onderdelen van het wetsvoorstel. Daarbij wordt ook ingegaan op de beleidskeuzes die daar aan ten grondslag liggen.

5.1 Toepassingsbereik

5.1.1 Binnen toepassingsbereik

5.1.1.1 Inleiding

In artikel 2 NIS2-richtlijn is bepaald op welke entiteiten de richtlijn van toepassing is of van toepassing kan worden verklaard. Er zijn entiteiten die van rechtswege onder het toepassingsbereik vallen, bijvoorbeeld omdat zij voldoen aan bepaalde criteria. Er zijn ook entiteiten die onder het toepassingsbereik kunnen vallen voor zover een lidstaat dit bepaalt (artikel 2, vijfde lid, NIS2-richtlijn). Het gaat daarbij om onderwijsinstellingen en overheidsinstanties op lokaal niveau.

[17] Voor entiteiten, die geen essentiële entiteit of belangrijke entiteit zijn, geldt niet de verplichting om significante incidenten te melden. Zij kunnen wel op vrijwillige basis significante en niet-significante incidenten melden.

5.1.1.2 Entiteiten die binnen toepassingsbereik vallen

In artikel 2, eerste lid, NIS2-richtlijn is bepaald dat entiteiten onder het toepassingsbereik van de richtlijn vallen als zij voldoen aan de volgende criteria:

1. zij behoren tot een van de in bijlage I en II van de NIS2-richtlijn genoemde soorten publieke of particuliere entiteiten (zeer kritieke sectoren respectievelijk andere kritieke sectoren);
2. zij kwalificeren als middelgrote ondernemingen uit hoofde van artikel 2 van de bijlage bij de Aanbeveling 2003/361/EG[18], of overschrijden de in het eerste lid van dat artikel vastgestelde plafonds voor middelgrote ondernemingen (size cap)[19]; en
3. zij verlenen hun diensten of verrichten hun activiteiten in de Europese Unie.

In artikel 2, tweede lid, NIS2-richtlijn is bepaald dat verschillende entiteiten, behorende tot een van de soorten entiteiten in bijlage I of II van de richtlijn, ongeacht hun omvang ook onder het toepassingsbereik van deze richtlijn vallen. Dit betreft een aantal specifiek genoemde soorten entiteiten (bijvoorbeeld aanbieders van openbare elektronische communicatienetwerken, aanbieders van vertrouwensdiensten en overheidsinstanties van de centrale overheid). Het gaat ook om entiteiten die voldoen aan een of meer criteria, genoemd in artikel 2, tweede lid, onderdelen b tot en met e, NIS2-richtlijn. Die criteria zien onder meer op het zijn van de enige aanbieder van een dienst in de lidstaat die essentieel is voor de instandhouding van kritieke maatschappelijke of economische activiteiten.

De Cbw is ook van toepassing op entiteiten die op grond van artikel 7 van de Wwke worden aangemerkt als een kritieke entiteit. Artikel 7 Wwke maakt een onderscheid tussen enerzijds entiteiten die als kritieke entiteit worden aangewezen in sectoren die volgen uit de bijlage van de Wwke. Die bijlage correspondeert met de bijlage van de CER-richtlijn. Anderzijds kunnen entiteiten als kritieke entiteit worden aangewezen in eventuele aanvullende sectoren, subsectoren dan wel binnen type entiteiten die in een ministeriele regeling van de vakminister worden aangewezen op grond van artikel 7a Wwke. Voor die eerste categorie kritieke entiteiten geldt dat zij op grond van artikel 2, derde lid, en artikel 3, eerste lid, onderdeel f, NIS2-richtlijn van rechtswege essentiële entiteiten als bedoeld in het onderhavige wetsvoorstel zijn. Ten aanzien van die tweede categorie kritieke entiteiten is ervoor gekozen om ook die entiteiten van rechtswege te beschouwen als essentiële entiteit als bedoeld in het onderhavige wetsvoorstel. Om die reden is in artikel 4a Cbw bepaald dat de Cbw ook van toepassing is op die aanvullende sectoren, subsectoren dan wel type entiteiten van de Wwke. Entiteiten zullen in de beschikking, waarin zij worden aangewezen als kritieke entiteit in de zin van de Wwke, worden gewezen op de verplichting uit artikel 45 van dit wetsvoorstel om informatie te verstrekken in het kader van het nationale register van entiteiten.

De in deze paragraaf genoemde bepalingen uit de NIS2-richtlijn zijn geïmplementeerd in de artikelen 8, 9, 12 en 13 van dit wetsvoorstel.

5.1.1.3 Overheidsinstanties

Inleiding

De NIS2-richtlijn is van rechtswege van toepassing op overheidsinstanties van de centrale overheid, ongeacht hun omvang.[20] Daarnaast is de richtlijn ook van rechtswege van toepassing op overheidsinstanties op regionaal niveau, met dien verstande dat de richtlijn hiervoor een nadere voorwaarde bevat.[21] Op overheidsinstanties op lokaal niveau is de richtlijn slechts van toepassing voor zover een lidstaat dat heeft bepaald.[22] Het kabinet kiest er voor de Richtlijn ook van toepassing te laten zijn op lokale overheden. Onder lokale overheden moet in dit verband worden verstaan:

[18] Aanbeveling 2003/361/EG van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (*PbEU* 2003, L 124).
[19] Zie hiervoor de nadere toelichting op de Aanbeveling 2003/361/EG onder paragraaf 5.2.
[20] Artikel 2, tweede lid aanhef en onder f, onder i, NIS2-richtlijn.
[21] Artikel 2, tweede lid, onder f, onder ii, NIS2-richtlijn.
[22] Artikel 2, vijfde lid, onder a, NIS2-richtlijn.

aangewezen overheidsinstanties die onder de werkingssfeer van de richtlijn vallen en die niet tot de centrale overheid behoren.

In deze paragraaf zal achtereenvolgens worden ingegaan op wat een overheidsinstantie in de zin van de NIS2-richtlijn is, welke instanties van de Richtlijn zijn uitgezonderd, wat overheidsinstanties van de centrale overheid in de Nederlandse context zijn en tot slot zal de keuze om lokale overheden ook onder de toepassing van de Richtlijn te brengen worden toegelicht, evenals welke instanties het op lokaal niveau betreft.

Overheidsinstantie

Om een entiteit te kunnen aanmerken als een overheidsinstantie, moet het gaan om een overheidsinstantie als bedoeld in artikel 6, punt 35, NIS2-richtlijn. Voor de definitie van overheidsinstantie is in artikel 1 van dit wetsvoorstel dan ook verwezen naar dat onderdeel uit de Richtlijn. "Overheidsinstantie" wordt in de Richtlijn gedefinieerd als een entiteit die overeenkomstig het nationale recht als zodanig in een lidstaat is erkend en die aan de volgende criteria voldoet:

a. zij is opgericht om te voorzien in behoeften van algemeen belang en heeft geen industrieel of commercieel karakter;
b. zij heeft rechtspersoonlijkheid of mag volgens de wet namens een andere entiteit met rechtspersoonlijkheid optreden;
c. zij wordt grotendeels gefinancierd door de staat, regionale autoriteiten of andere publiekrechtelijke organen, is onderworpen aan beheerstoezicht door die autoriteiten of organen, of heeft een bestuurs-, leidinggevend of toezichthoudend orgaan waarvan de leden voor meer dan de helft door de staat, regionale autoriteiten of andere publiekrechtelijke organen worden benoemd; en
d. zij heeft de bevoegdheid om ten aanzien van natuurlijke of rechtspersonen administratieve of regelgevende besluiten te nemen die van invloed zijn op hun rechten op het grensoverschrijdende verkeer van personen, goederen, diensten of kapitaal.

Overheidsinstanties die in hoofdzaak activiteiten uitvoeren op het gebied van de nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving zijn uitgesloten van het toepassingsbereik van de NIS2-richtlijn (zie artikel 2, zevende lid, van de NIS2-richtlijn). De verplichtingen uit de NIS2-richtlijn zijn dan ook niet op hen van toepassing, zie artikel 6 Cbw. Dit geldt onder andere voor de veiligheidsregio's, het Ministerie van Defensie, het openbaar ministerie en de Nationale Politie. Verder vallen de rechterlijke macht, parlementen en centrale banken niet onder het begrip 'overheidsinstantie' op grond van de Richtlijn (zie artikel 6, punt 35, aanhef). Op de rechtspraak, de Tweede en Eerste Kamer en de Nederlandse Bank zijn de verplichtingen uit de NIS2-richtlijn dus evenmin van toepassing.

Omdat het kabinet er aan hecht dat de hiervoor genoemde, van de Richtlijn uitgezonderde, overheidsinstanties van de centrale overheid blijven voldoen aan een hoog cyberbeveiligingsniveau, zullen zij blijven voldoen aan verplichtingen zoals bij de Rijksdienst thans geregeld in het Voorschrift Informatiebeveiliging Rijksdienst 2007 (Vir 2007[23]), het Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie 2013 (Vir-bi 2013[24]), de Baseline Informatiebeveiliging Overheid (BIO) en in toepasselijke verplichtingen van internationale herkomst.

Centrale overheid

De NIS2-richtlijn is van rechtswege van toepassing op overheidsinstanties van de centrale overheid, ongeacht hun omvang.[25] Welke overheidsinstanties tot de centrale overheid behoren, wordt gedefinieerd door een lidstaat overeenkomstig het nationale recht. Op het niveau van de centrale overheid in Nederland is het de Staat die rechtspersoonlijkheid bezit (zie artikel 2:1 Burgerlijk Wetboek) alsmede de zelfstandige bestuursorganen mét rechtspersoonlijkheid. Omdat onder het begrip Staat ook een aantal overheidsinstanties valt, dat niet kwalificeert als overheidsinstantie in de

[23] Stcrt. 2007, 122, pagina 11.
[24] Stcrt. 2013, 15497
[25] Artikel 2, tweede lid aanhef en onder f, onder i, NIS2-richtlijn.

zin van Richtlijn, is er voor gekozen om in de Cbw de Ministeries aan te wijzen als essentiële entiteit (artikel 8, eerste lid, onder g, Cbw), omdat de Ministeries voldoen aan de criteria voor overheidsinstantie. Onder het Ministerie worden tevens de daartoe behorende dienstonderdelen begrepen. Gelet op hetgeen is bepaald in artikel 6 van de Cbw valt het Ministerie van Defensie daar overigens niet onder.

Voorts zijn zelfstandige bestuursorganen van de centrale overheid, voor zover zij kwalificeren als overheidsinstantie in de zin van artikel 6, punt 35, van de NIS2-Richtlijn, een essentiële entiteit (zie artikel 8, eerste lid, onder h, Cbw). Voor wat betreft zelfstandige bestuursorganen die vallen onder de Kaderwet zelfstandige bestuursorganen (hierna: Kaderwet zbo's) geldt dat deze zbo's vallen onder de centrale overheid. Artikel 1, onder a, Kaderwet zbo's bepaalt immers dat een zbo is een bestuursorgaan *van de centrale overheid* dat bij de wet, krachtens de wet bij algemene maatregel van bestuur of krachtens de wet bij ministeriële regeling met openbaar gezag is bekleed, en dat niet hiërarchisch ondergeschikt is aan een minister. Uiteraard zal wel moeten zijn voldaan aan de overige vereisten uit artikel 6, punt 35 van de Richtlijn. Als dat laatste niet het geval is, zijn de bepalingen van de NIS2-richtlijn op dat zbo niet van toepassing.

Zbo's waarop de Kaderwet zbo's niet van toepassing is, kunnen nog steeds onder het bereik van de NIS2-richtlijn vallen. Daarvoor zal moeten worden bezien of zij onderdeel zijn van de centrale overheid en of zij kwalificeren als overheidsinstantie. Als zij geen onderdeel van de centrale overheid zijn of geen overheidsinstantie, vallen zij buiten het bereik van de Richtlijn.

Lokale overheid - Provincies, gemeenten en waterschappen

Ten aanzien van lokale overheden geeft de richtlijn lidstaten in artikel 2, vijfde lid, onder a, de mogelijkheid ze onder het toepassingsbereik van de NIS2-richtlijn te brengen. Van die mogelijkheid maakt het kabinet gebruik. Per brief van 23 november 2023 zijn de lokale overheden via het IPO, de VNG en de Unie van Waterschappen reeds geïnformeerd over het voornemen om hen onder het bereik van de NIS2-richtlijn te brengen. De overheid zelf heeft de maatschappelijke taak om op een zorgvuldige manier om te gaan met gegevens van onze burgers en bedrijven. Burgers en bedrijven zijn bovendien veelal verplicht hun gegevens te delen met de overheid. Ook heeft de overheid simpelweg een voorbeeldfunctie. Het kabinet vindt het van belang dat overheidsinstanties op alle niveaus aan een hoog beveiligingsniveau voldoen. Het kiest er daarom voor om provincies, waterschappen en gemeenten onder dit wetsvoorstel te brengen als essentiële entiteit (zie artikel 8, eerste lid, onder h, Cbw). Deze drie rechtspersonen voldoen altijd aan de hierboven weergegeven definitie van overheidsinstantie uit de NIS2-richtlijn.

In de praktijk zijn veel verplichtingen als genoemd in de NIS2-richtlijn op dit moment al van toepassing op de overheid, met inbegrip van lokale overheden. Op dit moment geldt al de Baseline Informatiebeveiliging Overheid (BIO)[26]. Deze is juridisch gezien een vorm van zelfbinding. Daarnaast is er tal van sectorale wet- en regelgeving van kracht met ook informatiebeveiligingseisen die veelal overlappen met de eisen die in de BIO worden gesteld of daarmee vergelijkbaar zijn. Een van de redenen voor deze versnippering is de juridische status van de BIO. Het kabinet heeft daarom de ambitie uitgesproken om de informatiebeveiligingsregelgeving overheidsbreed te harmoniseren en onder meer de BIO wettelijk te verankeren.[27] De keuze om lokale overheden onder dit wetsvoorstel aan te wijzen geeft invulling aan dit beleid. De BIO wordt dan wettelijk verankerd via NIS2. Voorts geldt dat lokale overheden taken uitvoeren die onder de NIS2-richtlijn zijn ondergebracht bij de (sub)sectoren, zoals vervoer over de weg of afvalwater. Ook om die reden worden zij in dit wetsvoorstel aangewezen als essentiële entiteit.

Wellicht ten overvloede wordt opgemerkt dat de drie bijzondere gemeenten van Nederland Bonaire, Sint Eustatius en Saba buiten het bereik van de Richtlijn vallen, omdat de Richtlijn enkel van toepassing is op Europees Nederland.

Lokale overheid – gemeenschappelijke regelingen

[26] *Stcrt*. 2020, 7857.
[27] *Werkagenda "Waardengedreven Digitaliseren"*, bijlage bij Kamerstukken II 2022/23, 26643, nr. 940.

Ook gemeenschappelijke regelingen zijn op grond van artikel 8, eerste lid, onderdeel h, Cbw, aangewezen als essentiële entiteit, voor zover zij kwalificeren als entiteit van het in bijlage I of II van de NIS2-richtlijn bedoelde soort én als overheidsinstantie in de zin van artikel 6, punt 35, van de NIS2-richtlijn. Overheden kunnen immers via gemeenschappelijke regelingen taken in gezamenlijkheid uitvoeren. Hierbij valt te denken aan gemeenschappelijke regelingen die ten doel hebben om lokale belastingen en heffingen te innen of ten doel hebben. Evenals bij zelfstandige bestuursorganen is gelet op de uiteenlopende aard van deze groep entiteiten, van belang om telkens per entiteit te bezien of deze kwalificeert als overheidsinstantie in de zin van de NIS2 richtlijn.

Tot slot

Op grond van artikel 3, derde lid, van de Richtlijn dienen de lidstaten voor 17 oktober 2024 een lijst op te stellen van essentiële en belangrijke entiteiten en entiteiten die domeinregistratiediensten verlenen. Bovengenoemde overheidsinstanties van zowel de centrale als de lokale overheid dienen ook op die lijst te worden opgenomen.

5.1.1.4 Onderwijsinstellingen

Artikel 2, vijfde lid, onderdeel b, NIS2-richtlijn biedt lidstaten de mogelijkheid om te bepalen dat de richtlijn ook van toepassing is op onderwijsinstellingen, met name wanneer zij kritieke onderzoeksactiviteiten verrichten. Deze mogelijkheid is geïmplementeerd in de artikelen 11 en 14 van dit wetsvoorstel. Deze artikelen bieden de Minister van Onderwijs, Cultuur en Wetenschap de mogelijkheid om instellingen voor hoger onderwijs aan te wijzen als essentiële entiteit of belangrijke entiteit. Door die aanwijzing wordt het bepaalde bij of krachtens dit wetsvoorstel van toepassing op deze instellingen. Meer specifiek gaat het om instellingen voor hoger onderwijs als bedoeld in artikel 1.1, onder g, Wet op het hoger onderwijs en wetenschappelijke onderzoek. Dat zijn de bekostigde instellingen die genoemd staan op de bijlage bij die wet (de openbare, bijzondere, levensbeschouwelijke en open universiteit en de bijzondere hogescholen) en (niet-bekostigde) rechtspersonen voor hoger onderwijs.

Het kan van belang zijn om deze instellingen onder de reikwijdte van dit wetsvoorstel te brengen, omdat het verkrijgen van hoogwaardige kennis en technologie een belangrijk doel van statelijke actoren is. Daarvoor wordt gebruik gemaakt van uiteenlopende strategieën. Eén van deze middelen is digitale spionage, onder andere door (te proberen) op netwerken van bedrijven en kennisinstellingen in te breken.[28] Dit kan schadelijk zijn voor de Nederlandse belangen. Verschillende cyberincidenten in de afgelopen jaren (onder andere bij de Universiteit Maastricht)[29] hebben aangetoond dat de impact van incidenten aanzienlijk kan zijn voor een onderwijsinstelling, ketenpartners, haar medewerkers en studenten.

Onderwijsinstellingen hebben een belangrijke maatschappelijke functie. In 2021 zijn daarom met de onderwijskoepels afspraken gemaakt om de cyberweerbaarheid van de hoger onderwijsinstellingen te verhogen. Ten behoeve van het nader te nemen besluit over de eventuele aanwijzing van instellingen voor hoger onderwijs als essentiële entiteit of belangrijke entiteit in de zin van dit wetsvoorstel voert het Ministerie van Onderwijs, Cultuur en Wetenschap momenteel een impactanalyse uit onder de bekostigde hoger onderwijsinstellingen. De onderwijskoepels zijn hierbij betrokken. Naar verwachting zal in 2024 een nader besluit worden genomen of en welke hoger onderwijsinstellingen als essentiële entiteit of belangrijke entiteit worden aangewezen. Die aanwijzing geschiedt bij regeling of besluit van de Minister van Onderwijs, Cultuur en Wetenschap na overleg met de Minister van Justitie en Veiligheid.

5.1.1.5 Essentiële entiteit of belangrijke entiteit

In artikel 3, eerste en tweede lid, NIS2-richtlijn is bepaald welke entiteiten als essentiële entiteit moeten worden beschouwd en welke entiteiten als belangrijke entiteit moeten worden beschouwd. Zo is voor entiteiten, behorende tot een van de soorten entiteiten in bijlage I bij de richtlijn

[28] AIVD-jaarverslag 2021, p. 14-19.
[29] Kamerstukken II 2019/20, 26643, nr. 872.

(corresponderend aan bijlage 1 van dit wetsvoorstel), die het plafond voor middelgrote ondernemingen uit artikel 1 van de bijlage bij de Aanbeveling 2003/361/EG overschrijden, bepaald dat zij als essentiële entiteit aangemerkt worden. Ook is bepaald dat dezelfde soorten entiteiten, als zij een middelgrote onderneming in bovenbedoelde zin zijn én ten aanzien van hen de criteria van artikel 2, tweede lid, onderdelen b tot en met e, NIS2-richtlijn geen toepassing vinden, belangrijke entiteit zijn[30]. Welke entiteiten een belangrijke danwel essentiële entiteit zijn en welke criteria voor aanwijzing gelden, is geïmplementeerd in de artikelen 8 tot en met 14 van dit wetsvoorstel. Het onderscheid is met name van belang als het gaat om de vraag welk toezichtsregime op de entiteit van toepassing is. Paragraaf 5.7.3 gaat hier nader op in.

5.1.1.6 Sectorspecifieke rechtshandelingen

In artikel 4 NIS2-richtlijn is bepaald dat als sectorspecifieke rechtshandelingen van de EU voorschrijven dat essentiële entiteiten of belangrijke entiteiten risicobeheersmaatregelen op het gebied van cyberbeveiliging moeten nemen of significante incidenten moeten melden, en als deze eisen ten minste gelijkwaardig zijn aan de in de NIS2-richtlijn vastgestelde verplichtingen, de relevante bepalingen van de NIS2-richtlijn dan niet van toepassing zijn op die entiteiten. Meer concreet gaat het hierbij om de zorgplicht en de meldplicht. De andere bepalingen uit dit wetsvoorstel zijn dus wel van toepassing op die entiteiten. Artikel 4 NIS2-richtlijn is geïmplementeerd in de artikelen 24 en 33 van dit wetsvoorstel.

5.1.1.7 Ontheffingen van verplichtingen

Artikel 2, achtste lid, van de NIS2-richtlijn biedt lidstaten de mogelijkheid om entiteiten die activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving, of die uitsluitend diensten verlenen aan overheidsinstanties die in hoofdzaak zulke activiteiten uitvoeren, met betrekking tot die activiteiten of diensten vrij te stellen van bepaalde verplichtingen, waaronder de zorgplicht en de meldplicht. Dit is geïmplementeerd in de artikelen 25, 34, 46 en 49 van dit wetsvoorstel. In dit wetsvoorstel is de bevoegdheid om zulke entiteiten een ontheffing van verplichtingen te verlenen belegd bij de vakminister. De vakminister kan overgaan tot het verlenen van een ontheffing in overeenstemming met de Minister van Justitie en Veiligheid.

5.1.2 Buiten toepassingsbereik

In de artikelen 2, zevende tot en met tiende lid, en 6, onderdeel 35, NIS2-richtlijn is geregeld op welke entiteiten en organisaties (bepaalde delen van) de richtlijn niet van toepassing is en waarop (bepaalde delen van) dit wetsvoorstel dus ook niet van toepassing is. Dit wetsvoorstel is niet van toepassing op:

- overheidsinstanties die activiteiten uitvoeren op het gebied van, nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving met inbegrip van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten.[31] Daarbij wordt opgemerkt dat overheidsinstanties die activiteiten verrichten die daar slechts zijdelings verband mee houden wél onder het bereik van de Richtlijn en dus dit wetsvoorstel vallen. Voor de toepassing van de NIS2-richtlijn worden entiteiten met regelgevende bevoegdheden niet geacht activiteiten op het gebied van de rechtshandhaving uit te voeren en deze vallen daarmee onder het toepassingsbereik;
- overheidsinstanties die gezamenlijk met een derde land zijn opgericht bij een internationale overeenkomst;
- diplomatieke en consulaire missies in derde landen of op hun netwerk- en informatiesystemen, voor zover deze systemen zich in de lokalen van de missie bevinden of voor gebruikers in een derde land worden gebruikt;[32]
- de rechterlijke macht, parlementen en centrale banken;
- entiteiten die zijn uitgesloten van het toepassingsgebied van de Verordening digitale operationele weerbaarheid in overeenstemming met artikel 2, vierde lid, van die verordening. In

[30] Artikel 3, tweede lid, NIS2-richtlijn.
[31] Zie ook overweging 8 NIS2-richtlijn, waaruit volgt dat het gaat om het in hoofdzaak uitvoeren van deze activiteiten.
[32] Overweging 8 NIS2-richtlijn.

Nederland zijn dat de Nederlandse Investeringsbank voor Ontwikkelingslanden N.V., de N.V. Noordelijke Ontwikkelingsmaatschappij, de N.V. Limburgs Instituut voor Ontwikkeling en Financiering, de Ontwikkelingsmaatschappij Oost-Nederland N.V. en kredietunies.

Het voorgaande is geïmplementeerd in de artikelen 1, 4, 6 en 7 van dit wetsvoorstel.[33]

5.2 Entiteiten van rechtswege en aanwijzing van entiteiten

5.2.1 Essentiële entiteit of belangrijke entiteit van rechtswege

Van veel entiteiten is in de NIS2-richtlijn al bepaald dat zij onder het toepassingsbereik van de richtlijn vallen en dat zij als gevolg daarvan als essentiële entiteit of als belangrijke entiteit worden aangemerkt. Lidstaten hoeven ten aanzien van deze entiteiten dus niet meer te beoordelen of zij moeten of kunnen worden aangewezen, zoals dat in de NIS1-richtlijn wel was vereist. Voor deze entiteiten wordt in dit wetsvoorstel (direct) bepaald dat zij een essentiële entiteit of belangrijke entiteit zijn. Dit komt tot uiting in de artikelen 8 en 12 van dit wetsvoorstel.

Om te bepalen of een entiteit van rechtswege onder het toepassingsbereik van de NIS2-richtlijn valt, is het in de meeste gevallen noodzakelijk om de omvang van de entiteit te bepalen. Hiervoor maken de lidstaten gebruik van bestaande Europese kaders, namelijk de Aanbeveling 2003/361/EG van de Europese Commissie. Deze aanbeveling schrijft voor in welke gevallen een organisatie als micro-, kleine, middelgrote of grote onderneming wordt gekwalificeerd. Dit wordt bepaald op basis van het aantal werknemers en de jaaromzet en/of het balanstotaal. Deze gegevens worden jaarlijks berekend aan de hand van het laatste afgesloten boekjaar. Een onderneming verliest of verkrijgt de status van micro-, kleine of middelgrote entiteit als de omvang in twee opeenvolgende boekjaren boven of onder de vastgestelde drempels voor deze categorieën uitkomt. Deze gegevens worden vanaf de datum van afsluiting van de rekeningen in aanmerking genomen. Daarnaast schrijft de aanbeveling voor in welke gevallen er sprake is van partner- en verbonden ondernemingen. In de overheidscommunicatie over dit wetsvoorstel worden digitale hulpmiddelen ter beschikking gesteld om organisaties te helpen bij het bepalen van hun omvang.

5.2.2 Essentiële entiteit of belangrijke entiteit op basis van criteria

In de NIS2-richtlijn is bepaald dat andere entiteiten die behoren tot één van de in bijlage I en II van de richtlijn (die zijn geïmplementeerd in bijlage 1 en 2 van dit wetsvoorstel) worden aangewezen als essentiële entiteit of als belangrijke entiteit, wanneer zij voldoen aan één of meer criteria uit artikel 2, tweede lid, onderdelen b tot en met e, NIS2-richtlijn. Eén van die criteria is dat het gaat om een entiteit waarvan een verstoring van de door haar verleende dienst aanzienlijke gevolgen kan hebben voor de openbare veiligheid, de openbare beveiliging of de volksgezondheid. Voor deze entiteiten geldt dat zij niet direct in de wet worden aangewezen, omdat er eerst een beoordeling moet plaatsvinden aan de hand van de hiervoor bedoelde criteria. In dit wetsvoorstel is daarom in de artikelen 9 en 13 geregeld dat zij door de vakminister (in het wetsvoorstel aangeduid als de bevoegde autoriteit), na overleg met de Minister van Justitie en Veiligheid, worden aangewezen op basis van een beoordeling aan de hand van de criteria uit artikel 2, tweede lid, onderdelen b tot en met e, NIS2-richtlijn. Deze criteria zijn geïmplementeerd in de artikelen 9 en 13 van dit wetsvoorstel.

Om vast te stellen of entiteiten voldoen aan de criteria uit artikel 9 of artikel 13 zal gebruik worden gemaakt van de nationale vitaalbeoordeling.[34] Hier is voor gekozen omdat de aanmerking als vitale

---

[33] In artikel 1 van dit wetsvoorstel is bepaald dat voor de definitie van overheidsinstantie wordt aangesloten bij de definitie daarvan in artikel 6, onderdeel 35, NIS2-richtlijn. In de laatstgenoemde bepaling is bepaald dat de rechterlijke macht, parlementen en centrale banken niet vallen onder de definitie van overheidsinstantie. Door de verwijzing in artikel 1 van dit wetsvoorstel naar artikel 6, onderdeel 35, NIS2-richtlijn is geregeld dat dit wetsvoorstel niet van toepassing is op de rechterlijke macht, parlementen en centrale banken van Nederland.

34 Het doel van de vitaalbeoordeling is om inzichtelijk te maken welke processen en diensten zo essentieel zijn voor de Nederlandse samenleving, dat uitval, verstoring of manipulatie daarvan kan leiden tot ernstige maatschappelijke ontwrichting, ernstige economische schade of – in het uiterste geval – een bedreiging van de nationale veiligheid.

aanbieder plaatsvindt op basis van vergelijkbare criteria als die voor het aanwijzen van essentiële entiteiten en belangrijke entiteiten. Deze systematiek wordt ook toegepast voor het aanwijzen van kritieke entiteiten als bedoeld in de Wwke. Het uitvoeren van de vitaalbeoordeling en de aanwijzing van entiteiten is in de eerste plaats de verantwoordelijkheid van de vakminister. Een aanwijzing komt tot stand na overleg met de Minister van Justitie en Veiligheid als coördinerend minister voor cybersecurity en de vitale infrastructuur.

In artikel 3, tweede lid, NIS2-richtlijn is bepaald dat lidstaten op basis van de criteria uit artikel 2, tweede lid, onderdeel b tot en met e, NIS2-richtlijn zowel essentiële entiteiten als belangrijke entiteiten kunnen aanwijzen. Artikel 13 van dit wetsvoorstel, over de aanwijzing van entiteiten als belangrijke entiteit op basis van criteria, is opgenomen in dit wetsvoorstel omdat artikel 3, tweede lid, NIS2-richtlijn hiertoe dwingt. Het is echter onwenselijk dat entiteiten die voldoen aan dezelfde criteria op verschillende manieren behandeld zouden worden. Vanwege het belang van deze organisaties voor de nationale veiligheid worden entiteiten die voldoen aan de hiervoor bedoelde criteria altijd aangewezen als essentiële entiteit. In beginsel blijft artikel 13 van dit wetsvoorstel daarmee ongebruikt, tenzij dit op basis van voortschrijdend inzicht in de toekomst nodig wordt geacht.

5.2.3 Aanwijzing bij besluit of regeling

Bij de implementatie van de NIS1-richtlijn was ervoor gekozen om zogeheten aanbieders van essentiële diensten bij besluit van de vakminister of amvb aan te wijzen. Bij de implementatie van de NIS2-richtlijn is ervoor gekozen om essentiële entiteiten en belangrijke entiteiten aan te wijzen bij besluit of regeling van de vakminister. Er is namelijk gebleken dat aanwijzing bij amvb niet de benodigde flexibiliteit biedt om in te kunnen spelen op snel veranderende technologische, maatschappelijke en geopolitieke ontwikkelingen. Deze snelheid is wenselijk om entiteiten, waarvan is vastgesteld dat zij bijvoorbeeld de enige aanbieder zijn van een dienst die essentieel is voor de instandhouding van kritieke maatschappelijke of economische activiteiten, zo snel mogelijk te laten voldoen aan onder meer de zorgplicht én de meldplicht en zodoende ertoe bij te dragen dat nadelige maatschappelijke gevolgen worden voorkomen of beperkt. Andersom biedt een aanwijzing bij besluit of regeling ook de flexibiliteit en snelheid om entiteiten die onder het toepassingsbereik van de voorgestelde wet vallen, daar zo snel als mogelijk niet meer onder te laten vallen op het moment dat zij niet meer voldoen aan bovenbedoelde criteria. Dit kan bijvoorbeeld het geval zijn als een entiteit haar activiteiten afschaalt of stopzet en daarmee niet meer aan bepaalde criteria voldoet.

Een ministeriële regeling moet voor eenieder kenbaar worden gemaakt door middel van publicatie in de Staatscourant, dus ook een regeling waarin een entiteit wordt aangewezen als essentiële entiteit of belangrijke entiteit. Er zijn echter gevallen denkbaar waarin de openbaarheid van een aanwijzing als essentiële entiteit of belangrijke entiteit onaanvaardbare risico’s met zich mee kan brengen voor de desbetreffende entiteit en gelet daarop mogelijk ook voor de nationale veiligheid. Dit kan bijvoorbeeld het geval zijn bij entiteiten die ogenschijnlijk niet kwalificeren als essentiële entiteit of als belangrijke entiteit, maar waarvoor het door de aanwijzing bij ministeriële regeling voor eenieder, en dus ook voor kwaadwillenden, bekend wordt dat die entiteit dat wel is. Die algemene bekendheid kan er dan toe leiden dat die entiteit wordt blootgesteld aan een grotere (cyber)dreiging dan wanneer de aanwijzing niet bekend zou zijn geworden. In zulke gevallen kan de vakminister kiezen voor een aanwijzing bij besluit.

Hierbij wordt overigens opgemerkt dat de vakminister ook bij de aanwijzing bij regeling moet voldoen aan de in Algemene wet bestuursrecht (hierna: Awb) gestelde eisen aan besluitvorming door bestuursorganen en dat zij in lijn moet zijn met de algemene beginselen van behoorlijk bestuur.

5.2.4 Ondersteuning CSIRT ten behoeve van andere entiteiten

Zoals aangegeven in paragraaf 2.3 wordt de Wbni ingetrokken (zie artikel 91 Cbw). Een aantal entiteiten dat onder de Wbni recht op bijstand van het NCSC heeft, valt niet van rechtswege onder de

---

Deze geïdentificeerde processen worden vitale processen genoemd en gezamenlijk vormen deze vitale processen de vitale infrastructuur van Nederland.

Cbw of wordt hiervan uitgezonderd. Deze partijen verliezen het recht op bijstand van een CSIRT door intrekking van de Wbni en dat is ongewenst. Hoewel dit strikt genomen niet voortvloeit uit de NIS2-richtlijn is het is in het belang van de cyberveiligheid en nationale veiligheid dat daartoe aangewezen partijen hun recht op bijstand van een CSIRT behouden. In artikel 88a Cbw is daarom geregeld dat entiteiten die waren aangewezen als vitale aanbieder krachtens de Wbni, zoals die wet luidde op de dag voorafgaande aan de intrekking en waarop Cbw niet van toepassing is, recht op ondersteuning door en bij regeling of besluit van de Bevoegde Autoriteit, na overleg met onze Minister, aan te wijzen CSIRT.

5.3 Zorgplicht

5.3.1 Inleiding

Essentiële entiteiten en belangrijke entiteiten moeten passende en evenredige technische, operationele en organisatorische maatregelen nemen om de risico's voor de beveiliging van de netwerk- en informatiesystemen te beheersen. Ook moeten zij deze maatregelen nemen om incidenten te voorkomen of de gevolgen van incidenten voor de afnemers van hun diensten en voor andere diensten te beperken. Deze verplichting, ook wel de zorgplicht genoemd, volgt uit artikel 21 NIS2-richtlijn en is geïmplementeerd in artikel 23 van dit wetsvoorstel. De zorgplicht geldt alleen voor essentiële entiteiten en belangrijke entiteiten, en niet voor entiteiten die domeinnaamregistratiediensten verlenen en die niet tevens een essentiële of belangrijke entiteit zijn.

Essentiele entiteiten en belangrijke entiteiten zijn zelf verantwoordelijk voor het vaststellen van welke maatregelen passend en evenredig zijn om de risico's waarmee zij geconfronteerd kunnen worden, beheersbaar te houden. Entiteiten hebben immers zelf inzicht – op basis van een risicobeoordeling – in de risico's die hun dienstverlening kunnen raken en hebben de meeste kennis van hun eigen systemen en processen. Daarmee omvat de zorgplicht de plicht voor entiteiten om risico's voor de beveiliging van de netwerk- en informatiesystemen, die zij voor hun werkzaamheden of voor het verlenen van hun diensten gebruiken, in kaart te hebben, omdat zij anders niet in staat zijn om passende en evenredige maatregelen te kunnen nemen. Risicomanagement of een risicobeoordelingscyclus door de entiteit vormt hiervoor de basis.

Het is aan de toezichthouder om te beoordelen of de maatregelen die entiteiten hebben genomen om hun weerbaarheid te waarborgen voldoende zijn om de risico's te mitigeren.

5.3.2 Beveiliging van netwerk- en informatiesystemen

De zorgplicht uit artikel 23 van dit wetsvoorstel heeft enkel betrekking op de netwerk- en informatiesystemen en de bescherming van de fysieke omgeving van die systemen. Dit is vastgelegd in het derde lid van artikel 23 Cbw. Een zorgplicht ten aanzien van weerbaarheid in brede zin kan daarnaast op basis van de Wwke op entiteiten rusten indien zij op grond van de Wwke zijn aangemerkt als kritieke entiteit. De zorgplicht van artikel 23 van dit wetsvoorstel gaat voor op de zorgplicht uit artikel 16 Wwke ten aanzien van hetgeen artikel 23 van dit wetsvoorstel regelt, namelijk het beheersen van de risico's voor de beveiliging van netwerk- en informatiesystemen. In artikel 4 Wwke is bepaald dat die wet, en daarmee ook de in artikel 16 Wwke geregelde zorgplicht, niet van toepassing is voor zover het netwerk- en informatiesystemen en de fysieke componenten en omgevingen van die systemen betreft.

De zorgplicht ziet op de netwerk- en informatiesystemen die entiteiten gebruiken voor hun werkzaamheden of voor het verlenen van hun diensten. De definitie van netwerk- en informatiesystemen betreft die uit artikel 6, onderdeel 1, NIS2-richtlijn en is ruim en technologieneutraal geformuleerd. De reikwijdte van de zorgplicht is daarmee onafhankelijk van het toepassingsgebied waar de netwerk- en informatiesystemen worden ingezet en van de benaming van dergelijke systemen of categorieën van systemen binnen sectoren. Onder een netwerk- en informatiesysteem valt ook Operationele Technologie (OT), ook wel bekend als Industrial Automation & Control Systems (IACS). Deze meet- en regelsystemen kunnen van cruciaal belang zijn voor de

continuïteit van de infrastructuur van essentiële en belangrijke entiteiten. De uitval van die systemen kan leiden tot maatschappelijke ontwrichting. Aangezien steeds meer Operationele Technologie verbonden is met informatietechnologie, is het verhogen van de digitale weerbaarheid urgent.[35]

De beveiliging van netwerk- en informatiesystemen betreft het vermogen van netwerk- en informatiesystemen om op een bepaald niveau van betrouwbaarheid weerstand te bieden aan elke gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die door of via deze netwerk- en informatiesystemen worden aangeboden, in gevaar kan brengen. Daarnaast betreft de beveiliging van netwerk- en informatiesystemen ook het vermogen van die systemen om goed en snel diensten en processen te herstellen in het geval dat een incident of een crisis deze systemen raakt.

Essentiële entiteiten en belangrijke entiteiten moeten een benadering kiezen die alle dreigingen en gevaren omvat en tot doel heeft netwerk- en informatiesystemen en de fysieke omgeving van die systemen te beschermen tegen gebeurtenissen die de beveiliging van die systemen kunnen aantasten. Het gaat hierbij niet alleen om de enkele bescherming tegen gebeurtenissen met kwade wil als digitale aanvallen, diefstal, bedrijfsspionage, sabotage, ongeoorloofde fysieke toegang tot, beschadiging van of interferentie met de netwerk- en informatiesystemen. Het gaat ook om gebeurtenissen zonder kwade wil als brand, overstromingen, telecommunicatie- en stroomstoringen systeemstoringen, menselijke fouten en natuurverschijnselen. Bij het nemen van maatregelen om de risico's voor de beveiliging van netwerk- en informatiesystemen te beheersen dienen entiteiten een benadering te kiezen die zowel de fysieke als digitale beveiliging van de netwerk- en informatiesystemen evenals de fysieke omgeving van die systemen omvat. Bij de fysieke omgeving kan bijvoorbeeld gedacht worden aan gebouwen en ruimtes waar zich netwerk- en informatiesystemen bevinden en van daar aanwezige voorzieningen die noodzakelijk zijn voor het ongestoord functioneren van de netwerk- en informatiesystemen of het voorkomen of beperken van de gevolgen van incidenten.

5.3.3 Passende en evenredige maatregelen

De maatregelen die de essentiële entiteiten en belangrijke entiteiten op grond van dit wetsvoorstel moeten nemen, moeten passend en evenredig zijn in relatie tot de specifieke risico's waarmee de entiteiten ten aanzien van de beveiliging van netwerk- en informatiesystemen kunnen worden geconfronteerd.

Bij de beoordeling of een maatregel of combinatie van maatregelen passend is, wordt allereerst gekeken naar de effectiviteit van de maatregel om de betreffende risico's te beheersen. Hierbij gaat het erom dat de juiste maatregel op de juiste plek wordt ingezet. De effectiviteit van een maatregel kan onder andere worden afgeleid uit wat daarover beschreven staat in Europese en internationale standaarden, evenals de stand van de techniek en de door de entiteit uitgevoerde risicoanalyses. Europese of internationale standaarden kunnen een goede indicatie geven dat een maatregel passend is of zou kunnen zijn om een of meer van de genoemde doelen te bereiken. Dat geldt ook voor maatregelen die de actuele stand van de techniek benutten of toepassen.

Daarnaast geldt het vereiste van evenredigheid. Dit betekent dat een maatregel of coherente set van maatregelen in verhouding dient te staan tot het te beheersen risico. De entiteit dient daarbij naar behoren rekening te houden met de mate waarin de entiteit aan risico's is blootgesteld, evenals de kans dat zich incidenten voordoen en de ernst ervan, met inbegrip van de maatschappelijke en economische gevolgen. Ook de omvang van de entiteit kan een rol spelen bij de vraag of maatregelen proportioneel zijn. Wat ook een rol kan spelen bij de evenredigheid van maatregelen, zijn de nadelige effecten of risico's van die maatregelen, zoals de verstoring van de continuïteit van de kritieke processen van een entiteit. In beginsel kan de omvang van een entiteit of de hoogte van uitvoeringskosten van invloed zijn op de keuze van de te nemen maatregelen. Hierbij wordt benadrukt dat een beperkte financiële capaciteit of een beperkte omvang van een entiteit een entiteit niet algeheel kan ontslaan van de verplichting om - kort gezegd - de weerbaarheid op orde te hebben. De

[35] *Advies inzake digitale veiligheid van Industrial Automation & Control Systems (IACS) in de vitale infrastructuur van Nederland*, Cyber Security Raad, 2020, nr. 2.

evenredigheid houdt daarnaast in dat een maatregel of coherente set van maatregelen het minst belastend is voor de entiteit om het risico te beheersen. Ten slotte kan een maatregel niet evenredig zijn indien het nemen van een maatregel leidt tot onevenredig nadelige effecten of risico's, zoals verstoring van de continuïteit van de kritieke processen van een entiteit.

Als gevolg van de afweging of een maatregel passend en evenredig is, is er een bepaald niveau van risico dat aanvaardbaar is. Het volledig uitsluiten van risico's en het creëren van volledige bescherming is niet mogelijk. Essentiële entiteiten en belangrijke worden daarom geacht maatregelen te nemen om risico's te beheersen en de mogelijke gevolgen van restrisico's zoveel mogelijk tot een minimum te beperken.

5.3.4 Technische, operationele en organisatorische maatregelen

Het beheersen van de risico's voor de beveiliging van de netwerk- en informatiesystemen behoeft een integrale aanpak. Dit betekent dat maatregelen niet alleen technisch van aard zijn, maar ook operationeel en organisatorisch.

In artikel 21, tweede lid, NIS2-richtlijn is bepaald dat de door essentiële entiteiten en belangrijke entiteiten te nemen maatregelen ten minste het volgende moeten omvatten:

a. beleid inzake risicoanalyse en beveiliging van informatiesystemen;
b. behandeling van incidenten;
c. bedrijfscontinuïteit;
d. beveiliging van de toeleveringsketen;
e. beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen;
f. beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen;
g. basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging;
h. beleid en procedures inzake het gebruik van cryptografie en, in voorkomend geval, encryptie;
i. beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van activa;
j. in voorkomend geval: het gebruik van multifactor-authenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit.

De NIS2-richtlijn schrijft voor dat entiteiten ten minste deze maatregelen treffen, waardoor er voor entiteiten geen ruimte bestaat om op basis van een eigen afweging van passendheid en evenredigheid deze maatregelen niet te treffen. Wel zal de concrete invulling van deze maatregelen door entiteiten op passende en evenredige wijze moeten plaatsvinden.

Ten aanzien van de bedrijfscontinuïteit (punt c) benoemt artikel 21, tweede lid, onderdeel c, NIS2-richtlijn het hebben van back-upbeheer, noodvoorzieningenplannen en maatregelen op het gebied van crisisbeheer.

Ten aanzien van de beveiliging van de toeleveringsketen (punt d) wordt in artikel 21, tweede lid, onderdeel d, en derde lid, NIS2-richtlijn aangegeven dat dit met inbegrip is van beveiliging gerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners. Wanneer essentiële entiteiten en belangrijke entiteiten overwegen welke maatregelen in dit verband passend zijn, moeten zij rekening houden met de specifieke kwetsbaarheden van elke rechtstreekse leverancier en dienstverlener en met de algemene kwaliteit van de producten en de cyberbeveiligingspraktijken van hun leveranciers en dienstverleners, met inbegrip van hun veilige ontwikkelingsprocedures. Ook houden zij rekening met de resultaten van gecoördineerde risicobeoordelingen van kritieke toeleveringsketens als bedoeld in artikel 22 NIS2-richtlijn.

Ten aanzien van de beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen (punt e) is in artikel 21, tweede lid, onderdeel e, NIS2-richtlijn bepaald dat dit

met inbegrip is van de respons op en de bekendmaking van kwetsbaarheden.

5.3.5 Delegatie van regelgevende bevoegdheid

De maatregelen uit artikel 21, tweede lid, NIS2-richtlijn, hiervoor reeds genoemd in paragraaf 5.3.4, zullen worden opgenomen en nader worden geconcretiseerd in een amvb. Artikel 23, vierde lid, van dit wetsvoorstel biedt hiervoor de grondslag.

Artikel 5 van de NIS2-richtlijn biedt lidstaten de ruimte om bepalingen vast te stellen die een hoger cyberbeveiligingsniveau waarborgen. In de amvb wordt naar verwachting gebruik gemaakt van deze ruimte uit de richtlijn om maatregelen vast te stellen die een hoger cyberbeveiligingsniveau waarborgen.

Daarnaast biedt deze delegatiegrondslag ook de mogelijkheid om aan essentiële en belangrijke entiteiten op te leggen dat zij bepaalde ICT-producten, ICT-diensten en ICT-processen gebruiken die zijn gecertificeerd op grond van artikel 49 van de Cyberbeveiligingsverordening (EU) 2019/881 (Cybersecurity Act (CSA)). Dit ter implementatie van artikel 24, eerste lid van NIS2.
Op grond van artikel 24, tweede lid NIS2 heeft de Commissie een vergelijkbare bevoegdheid: de Commissie kan via gedelegeerde handelingen aan essentiële en belangrijke entiteiten opleggen dat zij gebruik maken van bepaalde ICT-producten, ICT-diensten en ICT-processen of een certificaat verkrijgen die ook op grond van artikel 49 van de Cyberbeveiligingsverordening (EU) 2019/881 is vastgesteld.
Mocht de wens bestaan om aan een bepaalde sector verplichte certificering op te leggen zal eveneens moeten worden beoordeeld of dit beter op nationaal niveau – via de delegatiegrondslag van artikel 23 van deze wet – of via de gedelegeerde handelingen van de Commissie kan worden geregeld, zoals bedoeld in artikel 24, tweede lid NIS2. Een belangrijke overweging om het op Europees niveau te regelen kan zijn het creëren van een gelijk speelveld voor sectoren die internationaal georiënteerd zijn. Voor sectoren die vooral nationaal zijn georganiseerd zal een nationale invulling van de verplichting meer voor de hand liggen. Bij de overweging om een certificeringsschema op grond van artikel 49 van de Cyberbeveiligingsverordening verplicht te stellen zou ook moeten worden beoordeeld of het schema geschikt is om de (vermoedelijke) conformiteit met bepaalde eisen van de zorgplicht uit deze wet aan te tonen. Tot slot, indien er wordt gekozen voor verplichte certificering zal onder andere ook rekening moeten worden houden met de gevolgen die de maatregelen hebben voor de fabrikanten of aanbieders van zulke ICT-producten, -diensten of -processen en voor de gebruikers in termen van de kosten van die maatregelen, evenals de maatschappelijke of economische voordelen die voortvloeien uit de verwachte betere beveiliging voor de beoogde ICT-producten, -diensten of -processen.

In de amvb wordt voorzien in een delegatiegrondslag om bij ministeriële regeling van de vakminister sectorspecifieke regels te kunnen stellen over de te nemen maatregelen in het kader van de zorgplicht. Deze sectorspecifieke regels kunnen bijvoorbeeld zien op de toepassing van NEN-normen zoals de NEN 7510 voor zorgaanbieders onder de sector gezondheidszorg. Ook kunnen de regels zien op (sectorale) normen van internationale, Europese of nationale standaardisatieorganisaties.

In deze amvb kunnen ook regels worden gesteld die nodig zijn ter implementatie van uitvoeringshandelingen van de Europese Commissie over technische en methodologische vereisten als bedoeld in artikel 21, vijfde lid, NIS2-richtlijn.

5.3.6 Europese en internationale normen

Essentiële entiteiten en belangrijke entiteiten kunnen hun eigen normenkader hanteren voor het beheersen van hun risico's ten aanzien van de beveiliging van netwerk- en informatiesystemen. Hiermee wordt de regeldruk beperkt. Een normenkader voor informatiebeveiliging is gewoonlijk gebaseerd op een Europese, internationale norm, nationale of sectorale norm (zoals de ISO/IEC 27000-serie) met een procesbeschrijving en eisen voor het beveiligen van netwerk- en informatiesystemen. Met een normenkader geeft een entiteit zichzelf houvast bij het beheersen van de risico's. Het voldoen aan een eigen normenkader betekent op zichzelf niet dat een entiteit aan de

zorgplicht van artikel 23 van dit wetsvoorstel voldoet. De entiteit dient te borgen dat de maatregelen uit de amvb in ieder geval onderdeel zijn van het maatregelenpakket.

5.4 Governance

Algemeen

Gelet op artikel 20, eerste lid, NIS2-richtlijn doet deze wet in hoge mate een beroep op de verantwoordelijkheid van het bestuur van essentiële entiteiten en belangrijke entiteiten voor het nemen van risicobeheersmaatregelen op het gebied van cyberbeveiliging. De leden van het bestuur van essentiële entiteiten en belangrijke entiteiten moeten de in artikel 23 van dit wetsvoorstel bedoelde risicobeheersmaatregelen op het gebied van cyberbeveiliging goedkeuren en toezicht houden op de uitvoering ervan. Dit is vastgelegd in artikel 26, eerste lid, van dit wetsvoorstel. In de Nederlandse vertaling van de Richtlijn wordt gesproken over de "bestuursorganen" van essentiële en belangrijke entiteiten. Uit de tekst van de Richtlijn en ook uit enkele andere vertalingen blijkt evenwel dat daarmee geen "bestuursorgaan" in de zin van de Awb wordt bedoeld, maar het bestuur van een organisatie.[36]

Opleiding

Om een goed oordeel te kunnen geven over de in artikel 23 van dit wetsvoorstel bedoelde risicobeheersmaatregelen op het gebied van cyberbeveiliging en de uitvoering ervan, moet het bestuur over voldoende kennis en vaardigheden beschikken om de risico's voor de beveiliging van de netwerk- en informatiesystemen van de entiteit te kunnen identificeren, de risicobeheerspraktijken te kunnen beoordelen en de gevolgen van die praktijken voor de door de entiteit aangeboden diensten te kunnen beoordelen. Dit is geregeld in artikel 26, tweede lid, Cbw en vormt de implementatie van artikel 20, tweede lid, NIS2-richtlijn.

Bestuursleden spelen een cruciale rol in het neerzetten van een sterke cyberweerbaarheidscultuur. Naast de beoordeling van de digitale gezondheid van essentiële entiteiten en belangrijke entiteiten is het ook daarom van belang dat bestuursleden een training volgen. Vanuit die voorbeeldfunctie dragen ze cyberbewustheid uit, en moedigen werknemers binnen hun organisatie aan soortgelijke trainingen te volgen.

Het moet aantoonbaar zijn dat de training door het bestuurslid gevolgd is. Dit kan door middel van een certificaat van de training. Nieuwe bestuursleden moeten kunnen aantonen dat de training binnen twee jaar na hun benoeming gevolgd is (artikel 26, derde lid, van dit wetsvoorstel). Voor zittende bestuursleden geldt dat zij een relevante training moeten hebben gevolgd binnen twee jaar nadat artikel 26, tweede lid, van dit wetsvoorstel in werking is getreden (artikel 26, derde lid, van dit wetsvoorstel). Wel rust op hen vanaf de inwerkingtredingsdatum de verplichting dat zij over voldoende kennis en vaardigheden beschikken. Het is aan het bestuurslid om aan te tonen dat hiervan sprake is. Te denken valt aan regelmatige interne of externe voorlichting.

Daarnaast moeten de kennis en vaardigheden actueel zijn (artikel 26, vierde lid, van dit wetsvoorstel). Dit past bij het uitgangspunt van deze wet dat cyberweerbaarheid een cyclisch en continue proces is. Dit betekent dat het bestuurslid zijn of haar kennis en kunde ververst en indien nodig aanvult, door bijvoorbeeld een opfriscursus. Ook dit moet aangetoond kunnen worden.

Bestuur overheidsorganisaties

In artikel 26, achtste lid, Cbw is bepaald dat de ambtelijke leiding van een ministerie, provincie, gemeente, waterschap of gemeenschappelijke regeling wordt aangemerkt als het bestuur van die overheidsinstanties. Bij ministeries is de ambtelijke leiding belegd bij de bestuursraad, waar in elk geval de secretaris-generaal toe behoort. Bij provincies, gemeenten, waterschappen en gemeenschappelijke regelingen verschilt de benaming van de ambtelijke leiding; veelal wordt dit aangeduid als directie of managementteam. Bij provincies, gemeenten en waterschappen maakt in elk

[36] In de Engelse versie wordt gesproken over 'management bodies', in de Duitse versie van "die Leitungsorgane" en in de Franse vertaling over "les organes de direction".

geval de secretaris deel uit van de ambtelijke leiding. Een duidelijke keuze op dit punt was noodzakelijk omdat duidelijk moet zijn op wie binnen die overheidsinstanties de verplichtingen uit deze wet rusten. Het kabinet is van oordeel dat genoemde verplichtingen het beste kunnen worden belegd bij de ambtelijke leiding van die organisaties, omdat die verantwoordelijk is voor de uitvoering van de dagelijkse werkzaamheden. De NIS2-richtlijn gaat er bovendien van uit dat het bestuur dat de risicobeheersmaatregelen goedkeurt en toeziet op de uitvoering ervan, ook een opleiding volgt om voldoende kennis en vaardigheden te hebben met betrekking tot cyberbeveiliging. Die kennis en vaardigheden moet het bestuur daarnaast blijvend actueel houden. Dergelijke verplichtingen passen niet goed bij politiek benoemde ambtsdragers zoals een Minister of wethouder. Bovendien past het sanctioneren van hen bij het niet voldoen aan de verplichtingen uit de Richtlijn niet bij de aard van hun benoeming.

In artikel 20, eerste lid, tweede alinea van de NIS2-richtlijn is overigens geregeld dat de toezichtsverplichting uit dat artikel van de Richtlijn geen afbreuk doet aan het nationale recht met betrekking tot de aansprakelijkheidsregels die gelden voor overheidsinstanties en voor de aansprakelijkheid van ambtenaren en verkozen of benoemde overheidsfunctionarissen. Het feit dat deze organen zijn aangemerkt als het bestuur van die overheidsinstanties, brengt dus geen wijziging in het aansprakelijkheidsregime voor die organen. Voor zover deze organen onder het huidige recht al aansprakelijk kunnen worden gesteld, blijft dat het geval. De NIS2-richtlijn breidt de aansprakelijkheid van deze organen echter niet uit.

5.5 Meldplicht en vrijwillige meldingen

5.5.1 Melding van significante incidenten

Algemeen
Essentiële entiteiten en belangrijke entiteiten moeten elk significant incident melden bij hun CSIRT en de toezichthoudende instantie (meldplicht). Deze meldplicht volgt uit artikel 23 NIS2-richtlijn en is geïmplementeerd in de artikelen 27 tot en met 31 van dit wetsvoorstel. De meldplicht geldt niet voor entiteiten die domeinnaamregistratiediensten verlenen en niet tevens een essentiële of belangrijke entiteit zijn. Overigens leidt een melding niet tot blootstelling van de entiteit aan een verhoogde aansprakelijkheid.[37]

Significante incidenten
De meldplicht ziet alleen op significante incidenten. De meldplicht ziet niet op bijna-incidenten of dreigingen. Een incident is significant als het een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken of als het andere natuurlijke of rechtspersonen heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken (zie artikel 23, derde lid, NIS2-richtlijn). Het gaat derhalve ook om incidenten waarbij de hiervoor genoemde mogelijke aanzienlijke gevolgen zich nog niet hebben voorgedaan, maar mogelijk wel gaan plaatsvinden. Ook ten aanzien van zulke incidenten is het van belang dat deze worden gemeld bij het CSIRT en de toezichthoudende instantie.

Delegatiegrondslagen en drempelwaarden
Om te bepalen of een incident significant is, zijn in artikel 23, derde lid, NIS2-richtlijn drie parameters opgenomen. Deze parameters zien op een (mogelijke) ernstige operationele verstoring van de diensten, (mogelijke) financiële verliezen voor de betrokken entiteit en het (mogelijk) treffen van andere natuurlijke of rechtspersonen door aanzienlijke materiële of immateriële schade.
In artikel 37 van dit wetsvoorstel is een delegatiegrondslag opgenomen om bij of krachtens amvb nadere regels te kunnen stellen ter uitwerking van de meldplicht. Deze grondslag biedt de mogelijkheid om de hiervoor bedoelde parameters nader in te vullen en regels vast te stellen over aanvullende parameters. Van deze delegatiegrondslag zal gebruik worden gemaakt. Ook wordt in de amvb voorzien in de grondslag om bij ministeriële regeling van de vakminister, na overleg met de Minister van Justitie en Veiligheid en met de sector, regels te stellen over meldplichtige incidenten per

[37] Artikel 23, eerste lid, NIS2-richtlijn.

sector, subsector of soort entiteit. De nadere invulling en aanvulling van deze parameters wordt ook wel de drempelwaarde genoemd.

In de amvb zal tevens uitvoering worden gegeven aan de uitvoeringshandelingen die de Europese Commissie vaststelt op grond van artikel 23, elfde lid, NIS2-richtlijn over de meldplicht.

Dubbele meldplicht
Voor essentiële entiteiten en belangrijke entiteiten geldt een dubbele meldplicht overeenkomstig artikel 28 lid 1 Cbw: zij moeten significante incidenten melden bij zowel hun CSIRT als de toezichthoudende instantie. Met de meldingen kunnen het CSIRT en de toezichthoudende instantie invulling geven aan hun taken en blijven hun functies daarbij gescheiden. Het CSIRT heeft als taak om advies te geven en bijstand te verlenen aan de entiteit indien nodig, om overloopeffecten naar andere sectoren te kunnen identificeren en de betreffende entiteiten in die sectoren te waarschuwen en om trends te analyseren. De toezichthoudende instantie heeft een melding nodig om invulling te kunnen geven aan het toezicht op naleving van de wet door de entiteit. Het CSIRT en de toezichthoudende instantie hebben dus verschillende taken en daarom is het belangrijk dat de meldingen bij het CSIRT én de toezichthoudende instantie worden gedaan. Er wordt naar gestreefd deze dubbele meldplicht technisch zo in te richten dat het verspreiden van de benodigde informatie maar één handeling voor de entiteit vergt.

Dubbele meldplicht vertrouwensdiensten
Niet-gekwalificeerde en gekwalificeerde vertrouwensdiensten hebben op grond van de eIDAS-verordening (artikel 19bis, eerste lid, onderdeel b, respectievelijk artikel 24, tweede lid, onderdeel fter) een meldplicht voor beveiligingsinbreuken of verstoringen in de verlening van de dienst of de uitvoering van bepaalde maatregelen die een aanzienlijk effect hebben op de verleende vertrouwensdienst of op de daarin bijgehouden persoonsgegevens. Deze meldingen moeten gedaan worden bij het toezichthoudend orgaan volgens de eIDAS-verordening, de identificeerbare getroffen personen en andere relevante bevoegde organen. De meldplicht in artikel 23 NIS-richtlijn is aanvullend op de meldplicht uit de eIDAS-verordening. Voor een goede uitvoering van de dubbele meldplicht voor vertrouwensdienstverleners is een enkel loket waar beide meldingen tegelijkertijd kunnen worden gedaan wenselijk en is nauwe samenwerking en uitwisseling van informatie van meldingen tussen de toezichthouders noodzakelijk, conform overweging 94 van de NIS2-richtlijn.

5.5.2 De fasen van een melding

De melding bestaat uit meerdere fasen, te beginnen met een vroegtijdige waarschuwing en eindigend met een eindverslag. Deze fasen zijn opgenomen in de artikelen 28 tot en met 31 van dit wetsvoorstel en worden hierna beschreven.[38]

1. Vroegtijdige waarschuwing
Wanneer een essentiële entiteit of belangrijke entiteit zich bewust wordt van een significant incident, moet zij onverwijld of, als dat niet mogelijk is, binnen 24 uur een vroegtijdige waarschuwing geven over het incident aan haar CSIRT en de toezichthoudende instantie. Bij de vroegtijdige waarschuwing is het voldoende om alleen informatie te geven die noodzakelijk is om het CSIRT en de toezichthoudende instantie op de hoogte te brengen van het significante incident en om de betrokken entiteit in staat te stellen om indien nodig bijstand te vragen. Wel moet de entiteit daarbij aangeven of het significante incident vermoedelijk door onrechtmatige of kwaadwillige handelingen is veroorzaakt en of het waarschijnlijk grensoverschrijdende gevolgen heeft. Ransomware en criminele afpersing door een hack zijn voorbeelden van zulke onrechtmatige of kwaadwillige handelingen die significante incidenten kunnen veroorzaken.

[38] Artikel 23 NIS2-richtlijn

2. Melding met update en initiële beoordeling
De vroegtijdige waarschuwing moet worden gevolgd door de melding van het incident met een update van de gegeven informatie in het kader van de vroegtijdige waarschuwing, een initiële beoordeling van het significante incident, de ernst en de gevolgen ervan en, indien beschikbaar, de indicatoren voor aantasting. De melding is dus met name om de informatie bij te werken die bij de vroegtijdige waarschuwing is ingediend en om een initiële beoordeling door de entiteit van het significante incident kenbaar te maken. Bij de initiële beoordeling moet rekening worden gehouden met onder meer de getroffen netwerk- en informatiesystemen, het belang daarvan voor de door de entiteit verleende diensten, de ernst en technische kenmerken van een cyberdreiging en eventuele onderliggende kwetsbaarheden die worden uitgebuit, en de ervaring van de entiteit met soortgelijke incidenten.

3. Tussentijds verslag (alleen na verzoek van CSIRT of toezichthoudende instantie)
Het CSIRT en de toezichthoudende instantie kunnen naar aanleiding van de melding een essentiële entiteit of een belangrijke entiteit verzoeken om een tussentijds verslag over relevante updates van de situatie.

4. Eindverslag
Uiterlijk een maand na de melding van het incident moet een eindverslag worden ingediend. Als het incident nog aan de gang is op het moment dat het eindverslag wordt ingediend, moet de betrokken entiteit op dat moment een voortgangsverslag indienen (in plaats van een eindverslag) en binnen één maand nadat het significante incident is afgehandeld, een eindverslag indienen. Het voortgangsverslag is qua inhoud vergelijkbaar met het tussentijds verslag.
Het eindverslag moet een gedetailleerde beschrijving van het incident, inclusief technische details, de ernst en de gevolgen ervan bevatten. Ook moet hierin het soort bedreiging of grondoorzaak van het significante incident worden gemeld.

Informeren van ontvangers van diensten
De essentiële entiteit respectievelijk de belangrijke entiteit stelt in voorkomend geval zo snel mogelijk de ontvangers van haar diensten in kennis van significante incidenten die een nadelige invloed kunnen hebben op de verlening van die diensten. Ook deelt de entiteit alle maatregelen of voorzieningen die de ontvanger van de dienst ter beschikking staan om de risico's die uit een cyberdreiging voortvloeien te beperken. Vooral wanneer de cyberdreigingen waarschijnlijk tot incidenten zullen leiden, moeten die entiteiten de ontvangers van hun dienst ook op de hoogte brengen van de dreiging zelf. Dit doen zij naar hun beste vermogen, maar het ontslaat hen niet van de verplichting om op eigen kosten passende en onmiddellijke maatregelen te nemen om dergelijke dreigingen te voorkomen of te verhelpen en het normale beveiligingsniveau van de dienst te herstellen. Dergelijke informatie over cyberdreigingen aan de ontvangers van de dienst moet zonder kosten worden verstrekt en in gemakkelijk te begrijpen taal worden opgesteld.

Meer in het bijzonder geldt voor aanbieders van openbare elektronische communicatienetwerken en van openbare elektronische communicatiediensten dat zij security (en privacy) *by default* en *by design* moeten bieden. Ook moeten zij hun dienstontvangers op de hoogte brengen van significante cyberdreigingen en van de maatregelen die zij kunnen nemen om de beveiliging van hun apparaten en communicatie te beschermen, bijvoorbeeld door gebruik te maken van specifieke soorten software of encryptietechnologieën.[39]

5.5.3 Vrijwillige meldingen

Essentiële entiteiten en belangrijke entiteiten moeten significante incidenten melden. Maar zij kunnen, naast significante incidenten, ook te maken hebben met incidenten (die niet worden gekwalificeerd als significant), bijna-incidenten en cyberdreigingen. Deze termen zijn gedefinieerd in artikel 6 NIS 2 richtlijn. Om te voorkomen dat incidenten (die niet significant zijn), bijna-incidenten en cyberdreigingen tot incidenten kunnen leiden die aanzienlijke schade kunnen veroorzaken, is het belangrijk dat deze ook worden gemeld overeenkomstig artikel 27 Cbw en artikel 30 NIS 2 richtlijn. Dit wetsvoorstel regelt daarom dat essentiële entiteiten en belangrijke entiteiten op vrijwillige basis

[39] Zie ook overweging 104 NIS2-richtlijn.

hiervan melding kunnen maken. Dit kunnen zij doen bij hun CSIRT. Hiermee kan onder meer worden voorkomen dat cyberdreigingen tot incidenten kunnen leiden die aanzienlijke materiële of immateriële schade kunnen veroorzaken.

Niet alleen essentiële entiteiten en belangrijke entiteiten kunnen te maken hebben met significante incidenten, incidenten, bijna-incidenten en cyberdreigingen, maar ook entiteiten die geen essentiële entiteit of belangrijke entiteit zijn. Dit wetsvoorstel regelt ook dat iedereen, ongeacht of degene een essentiële entiteit of belangrijke entiteit is, op vrijwillige basis een melding kan doen van significante incidenten, incidenten, bijna-incidenten en cyberdreigingen bij een CSIRT.

Het CSIRT kan de vrijwillige melding ter behandeling doorsturen naar een ander CSIRT. Hier wordt de melder van op de hoogte gesteld.

Onverminderd de voorkoming van, het onderzoek naar en de opsporing en de vervolging van strafbare feiten, leidt een vrijwillige melding er niet toe dat de melder bijkomende verplichtingen worden opgelegd waaraan zij niet onderworpen zou zijn geweest als zij de melding niet had ingediend.[40]

5.6 Informatiedeling

In dit wetsvoorstel zijn verschillende bepalingen opgenomen over samenwerking en informatiedeling om de doeltreffende uitvoering van deze wet te vergemakkelijken met als doel de cyberbeveiliging in de gehele Unie te verstreken, de bedreigingen voor netwerk- en informatiesystemen die worden gebruikt om essentiële diensten in belangrijke sectoren aan te bieden te beperken en op die wijze bij te dragen aan de veiligheid van de Europese Unie, en tot doeltreffende werking van de economie en de samenleving. Het is essentieel dat partijen voor wie dit relevant is, worden geïnformeerd en geadviseerd over dreigingen en incidenten met betrekking tot hun netwerk- en informatiesystemen. CSIRT's hebben de wettelijke taak om partijen te informeren over dreigingen en incidenten die relevant zijn voor die partijen. Door bijvoorbeeld de Tweede Kamer en de Cyber Security Raad is eerder al aangegeven dat het delen van informatie over digitale dreigingen en incidenten met relevante partijen noodzakelijk is om die partijen in staat te stellen om maatregelen te treffen om de continuïteit van hun dienstverlening te waarborgen en daarmee nadelige maatschappelijke gevolgen in sterkere mate te voorkomen, te beperken of te verhelpen. [Brief Cyber Security Raad inzake CSR Adviesbrief inzake het versneld delen van incidentinformatie 22 februari 2021]

Hoofdstuk 14 van dit wetsvoorstel bevat bepalingen die betrekking hebben op informatie-uitwisseling tussen verschillende partijen. Hoofdstuk 15 bevat een wettelijke grondslag voor het verwerken van bijzondere persoonsgegevens en het uitwisselen van vertrouwelijke gegevens tussen een aantal specifieke partijen nader uitgewerkt.

5.6.1 CSIRT

Artikel 10 NIS2-richtlijn verplicht lidstaten tot het aanwijzen of instellen van één of meer CSIRT's. Een CSIRT is een organisatie die zich bezighoudt met cybersecurity-gerelateerde incidenten. Een hoofddoel van een CSIRT is om snel en efficiënt te reageren op cyberincidenten, het adequaat afhandelen ervan en het minimaliseren van schade. Een tweede belangrijk doel richt zich op de fase voorafgaand aan incidenten, namelijk het bieden van ondersteuning bij het voorkomen van incidenten. De taken van het CSIRT zijn opgenomen in artikel 11, derde lid, NIS2-richtlijn. Deze richtlijnbepaling is geïmplementeerd in artikel 17 van dit wetsvoorstel. Een deel van de taken gaat over operationele activiteiten. Deze activiteiten zien op monitoring, analyse, meldingen, incident response en regie en coördinatie.

Artikel 12 NIS2-richtlijn verplicht lidstaten tot het aanwijzen van één van de CSIRT's als coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden. De coördinator heeft onder meer de taak om op te treden als tussenpersoon tussen de natuurlijke persoon of rechtspersoon die

[40] Zie ook artikel 30, tweede lid, en overweging 105 NIS2-richtlijn.

een kwetsbaarheid heeft gemeld en de fabrikant of aanbieder van de mogelijk kwetsbare ICT-producten of -diensten.

Het CSIRT en de coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden worden aangewezen bij amvb. Naar verwachting zullen de taken van het CSIRT in ieder geval worden uitgevoerd door het NCSC, Z-CERT, CERT Watermanagement (onderdeel van het openbaar lichaam Het Waterschapshuis) en Informatiebeveiligingsdienst (IBD, onderdeel van VNG Realisatie B.V.) voor de daarbij bepaalde entiteiten. Deze organisaties hebben geïnvesteerd in het opbouwen van kennis over de eigen sector, met name over binnen de sector gebruikte systemen en processen, en sluiten goed aan op de eigen doelgroep. Het uitvoeren van de CSIRT-taak door deze organisaties past ook bij de uitkomsten van het rapport dat het Ministerie van Justitie en Veiligheid namens de vakdepartementen heeft laten opstellen over de (her)inrichting van het CSIRT-stelsel in Nederland.[41]

5.6.2. Verwerking van gegevens door het CSIRT

Bij de uitvoering van zijn taken, zoals opgesomd in artikel 17 Cbw, verwerkt het CSIRT gegevens. Deze gegevens kunnen in beperkte mate ook persoonsgegevens bevatten. Bij de verwerking van die persoonsgegevens gaat het in beginsel alleen om die gegevens die noodzakelijk zijn voor het uitoefenen van zijn CSIRT-taken, zoals IP-adressen[42], e-mailadressen en domeinnamen. Tevens kan dit ook informatie omvatten over een entiteit of organisatie, alsook de contactgegevens. Voor zover het gaat om vertrouwelijke gegevens, voorziet artikel 65 Cbw in een grondslag. Zie voor een nadere toelichting hierop ook de artikelsgewijze toelichting. Op de verwerking van deze persoonsgegevens is de Avg van toepassing. De Autoriteit Persoonsgegevens en de departementale functionaris gegevensbescherming houden toezicht op de verwerking van persoonsgegevens door het CSIRT.

Een belangrijk doel van CSIRT-taken is om de uitval van netwerk- en informatiesystemen te voorkomen en hiermee de digitale weerbaarheid van organisaties te verhogen. Ten behoeve hiervan heeft een CSIRT verschillende taken waarbij er gegevens worden verwerkt, zoals het monitoren en analyseren van cyberdreigingen, het verzamelen en analyseren van forensische gegevens, het verlenen van bijstand en het verstrekken van informatie (artikel 17 Cbw). Essentiele entiteiten en belangrijke entiteiten zijn zelf verantwoordelijk voor het vaststellen van welke maatregelen passend en evenredig zijn om de risico's waarmee zij geconfronteerd kunnen worden, beheersbaar te houden zoals ook eerder beschreven onder paragraaf 5.3 Zorgplicht.

Door het verzamelen en analyseren van cyberdreigingen, kwetsbaarheden en incidenten is het CSIRT in staat de aard en ernst van dreigingen en incidenten te bepalen. Op basis hiervan kan het CSIRT essentiële en belangrijke entiteiten en andere relevante partijen waarschuwen en adviseren. Een CSIRT krijgt bijvoorbeeld informatie van een CSIRT uit een ander land. In deze informatie bevinden zich kenmerken van een digitale aanval, zoals ransomware en de betrokken IP-adressen. Door deze informatie te analyseren en vervolgens te delen met essentiële entiteiten, belangrijke entiteiten en relevante partijen, worden deze organisaties in staat gesteld om passende maatregelen te nemen om digitale incidenten te voorkomen en/of te verhelpen. Hiermee wordt ook de continuïteit van de dienstverlening zo goed mogelijk gewaarborgd.

5.6.3. Verwerking strafrechtelijke persoonsgegevens

Zoals reeds aangegeven verwerkt het CSIRT een veelheid aan gegevens, waaronder IP-adressen. Naar aanleiding van op de wetswijziging van de Wbni[43] is opnieuw beoordeeld of IP-adressen kunnen worden aangemerkt als strafrechtelijke persoonsgegevens in de zin van artikel 10 Avg bij de

---

[41] *CSIRT-Stelsel - Een beleidskader voor het herinrichten van het stelsel met een nationale en sectorale CSIRT's in Nederland*, Petra Oldengarm, 2023.

[42] IP-adressen zijn alleen dan aan te merken als persoonsgegevens, wanneer de verwerkingsverantwoordelijke beschikt over de (rechts)middelen waarvan redelijkerwijs valt te verwachten, dat zij worden ingezet om een natuurlijke persoon te identificeren. Zie hiervoor: overweging nr. 26, AVG. Zie ook: HvJ EU 19 oktober 2016, ECLI:EU:C:2016:779 (Breyer); HvJ EU 21 juni 2021, ECLI:EU:C:2021:492 (Mircom); HvJ EU 9 november 2023, ECLI:EU:C:2023:837 (Scania); ABRvS 13 juli 2022, ECLI:NL:RVS:2022:1993.

[43] *Kamerstukken II* 2021/22, 36 084, nr. 3, pag. 12-13.

verwerking onder de NIS2-richtlijn. Daarbij is om de hiernavolgende redenen geconcludeerd dat een IP-adres niet als zodanig kan worden aangemerkt. Hierbij is het van belang of sprake is van zodanige concrete feiten en omstandigheden d een persoonsgegevens als een strafbaar feit te kwalificeren bewezenverklaring – in de zin van artikel 350 Wetboek van Strafvordering – kunnen dragen.[44] Hieruit volgt de maatstaf of vastgestelde gedragingen een zwaardere verdenking dan een redelijk vermoeden van schuld opleveren, in die zin dat te verwerken strafrechtelijke persoonsgegevens in voldoende mate moeten vaststaan Daarnaast speelt attributie – de mate waarin een strafbaar feit daadwerkelijk aan een persoon kan worden toegerekend – een rol in de vraag of een persoonsgegeven kan worden gekwalificeerd als een strafrechtelijk persoonsgegeven.

De verstrekking van dreigings- en incidentinformatie, met inbegrip van persoonsgegevens, door het CSIRT aan essentiële en belangrijke entiteiten of andere relevante partijen heeft tot doel om hen in de gelegenheid te brengen om maatregelen te nemen om digitale incidenten te voorkomen of te verhelpen en daarmee de digitale weerbaarheid van deze organisaties te vergroten, en bijvoorbeeld niet tot doel om handhavend op te treden tegen partijen die verantwoordelijk zijn voor genoemde incidenten. De IP-adressen dienen niet als strafrechtelijke persoonsgegevens in de zin van artikel 10 AVG te worden beschouwd, omdat niet kan worden afgeleid dat sprake is van een gedraging die een zwaardere verdenking dan een redelijk vermoeden van schuld oplevert. Om te constateren dat sprake is van een zwaardere verdenking dan een redelijk vermoeden van schuld zullen naast IP-adressen namelijk meer concrete feiten en omstandigheden nodig zijn. Bovendien zullen de te verwerken IP-adressen alleen in combinatie met andere tot een persoon herleidbare gegevens kunnen leiden tot attributie. Aan de bovengenoemde twee criteria wordt niet voldaan.

5.6.4. Informatiedeling met relevante partijen

Zoals reeds aangegeven kan het CSIRT, ter uitvoering van zijn taken, informatie delen met relevante partijen. Zogenoemde relevante partijen zijn relevant omdat de informatie die het CSIRT heeft voor hun cyberweerbaarheid relevant is of voor hun achterban. Door deze informatie met hen te delen weten deze relevante partijen dat ze kwetsbaar zijn en kunnen zij de benodigde maatregelen treffen. Partijen die in het concrete geval door het CSIRT worden aangemerkt als relevante partij voor het ontvangen van bepaalde informatie worden geacht eventuele in die informatie opgenomen persoonsgegevens te verwerken conform de Avg, voor zover de Avg op de betreffende partij van toepassing is. Daarnaast worden relevante partijen geacht de van het CSIRT ontvangen informatie zorgvuldig te verwerken en de vertrouwelijkheid van deze informatie voldoende te waarborgen. Daarmee wordt ervoor gezorgd dat het CSIRT beschikt over een passende, veilige en weerbare communicatie- en informatie-infrastructuur voor informatie-uitwisseling tussen het CSIRT en – in dit geval- relevante partijen (artikel 10, derde lid, NIS2-richtlijn).

5.6.5. Schakelorganisaties

Een aantal organisaties zijn op grond van de Wbni aangewezen als OKTT (‘objectief kenbaar tot taak’ heeft om andere organisaties of het publiek te informeren over dreigingen en incidenten met betrekking tot andere netwerk- en informatiesystemen) [45] of CSIRT’s.[46] Met het intrekken van de Wbni komen die aanwijzingen te vervallen. Wat genoemde organisaties gemeen hebben, is dat zij ten behoeve van een achterban informatie verspreiden, welke zij ontvangen van het NCSC. Deze voormalige Organisaties die fungeren als schakelorganisatie voor een achterban van aanbieders (hierna: schakelorganisaties) kunnen onder het regime van de Cbw onder omstandigheden worden gekwalificeerd als een relevante partij als bedoeld in artikel 17, tweede lid, onderdeel b, Cbw. In dat geval heeft het CSIRT tot taak bepaalde informatie als bedoeld in genoemd artikellid ook te verstrekken aan die organisatie ten behoeve van de achterban. Voor het antwoord op de vraag of een schakelorganisatie ook in de toekomst in het concrete geval als relevante partij voor het ontvangen van bepaalde informatie kan worden aangemerkt, is bepalend of de achterban van aanbieders bestaat uit essentiële entiteiten, belangrijke entiteiten dan wel relevante partijen. Ten aanzien van

[44] Zie het arrest van de Hoge Raad van 29 mei 2009, ECLI:NL:HR:2009:BH4720.
[45] Het gaat om het Digital Trust Center voor zover paragraaf 7.2 nog niet geldt, de Vereniging Abuse Information Exchange, de Stichting Nationale Beheersorganisatie Internet Providers, de Stichting Cyber Weerbaarheidscentrum Brainport, de Vereniging Cyberveilig Nederland, de Stichting Connect2Trust, de Stichting FERM, de Stichting NL CISO Circle of Trust.
[46] Surfcert is hier een voorbeeld van.

schakelorganisaties zal het CSIRT uiteraard de in de vorige alinea aangehaalde vertrouwelijkheid en zorgvuldigheid van informatie-uitwisseling meewegen om te bepalen of en welke informatie met een dergelijke partij kan worden uitgewisseld.

5.6.6. Nederlandse Inlichtingen- en veiligheidsdiensten

De Nederlandse inlichtingen-en veiligheidsdiensten hebben op grond van artikel 8 lid 2 sub a t/m f en artikel 10 lid 2 sub a t/m g van de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017) de taak om, waar de nationale veiligheid in het geding is, onder meer onderzoek te verrichten naar organisaties die een gevaar vormen voor de democratische rechtsorde, het bevorderen van maatregelen ter bescherming van (vitale) belangen of het opstellen van dreigings- en risicoanalyses. De informatie waarover het CSIRT vanwege haar taakuitoefening beschikt, kan daarbij relevant zijn voor de taakuitoefening van de inlichtingen- en veiligheidsdiensten. De inlichtingen- en veiligheidsdiensten zijn hiermee beter in staat om onderzoek te doen naar actoren die achter een incident zitten bij een belangrijke of essentiële entiteit. Dit vergroot het zicht op de dreiging richting Nederlandse belangen en de democratische rechtsorde en stelt zowel de inlichtingen- en veiligheidsdiensten als het CSIRT beter in staat om mitigerende maatregelen te treffen. Indien de diensten daarom bij het CSIRT-verzoeken, zullen zij een relevante partij zijn voor het CSIRT om informatie mee te delen.

5.6.7. Rol NCSC

Naar verwachting wordt in de amvb het NCSC aangewezen als één van de CSIRT's met de taken uit artikel 17 Cbw en als coördinator met het oog op het gecoördineerd bekendmaken van kwetsbaarheden (zie artikel 18 Cbw). Ook neemt het NCSC-taken op zich die volgen uit de NIS2 richtlijn zoals het fungeren als het centrale contactpunt, het nationale register en het beheren van een meld- en registratiefunctionaliteit (artikel 22 Cbw). Het fungeert als centraal contactpunt voor zowel nationale incident-response stakeholders alsook binnen de Europese Unie en voor andere CSIRT's wereldwijd. Het NCSC gaat de sterke positie die zij inmiddels heeft op het gebied van de digitale weerbaarheid na inwerkingtreding van de Cbw derhalve nog verder consolideren. Dit zijn niet allemaal rollen en taken die volgens de NIS2 kwalificeren als een CSIRT-taak. In internationaal verband zijn het vaak CSIRT's die al deze taken vervullen en veel landen hebben die organisatie gedefinieerd als hun "nationale CSIRT".
In de Nationale Cybersecurity Strategie (NLCS) is de ambitie uitgesproken om zo'n nationale CSIRT in Nederland aan te wijzen. De NIS2-richtlijn kent die term formeel niet, er wordt immers alleen CSIRT's aangewezen met de taken volgend uit artikel 17 Cbw. In de praktijk zal het NCSC in binnen- en buitenland als "nationale CSIRT" opereren. Ook gelet op de overige taken die het NCSC op grond van dit wetsvoorstel vervult en de cruciale positie die het NCSC inneemt in het versterken van de digitale weerbaarheid.

5.7 Handhaving

Dit wetsvoorstel voorziet in de handhaving van de verplichtingen uit dit wetsvoorstel die gelden voor essentiële entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen. Hiertoe verplicht artikel 31 NIS2-richtlijn. De artikelen 32 en 33 NIS2-richtlijn bevatten specifieke bepalingen over de handhaving van de verplichtingen ten aanzien van essentiële entiteiten en belangrijke entiteiten.

5.7.1 Bestuursrechtelijke handhaving

Dit wetsvoorstel voorziet in bestuursrechtelijke handhaving, die zowel reparatoir als punitief kan zijn (herstelsancties en bestraffende sancties). De handhaving heeft betrekking op verplichtingen voor essentiële entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen, waarvan de meesten op verschillende terreinen al te maken hebben met bestuursrechtelijke handhaving. Bij de implementatie van de NIS1-richtlijn werd het wenselijk geacht om aan te sluiten bij al bestaande bevoegdheden en instrumenten van de sectorale toezichthoudende instanties. Toen is ervoor gekozen in nationale wet- en regelgeving te kiezen voor bestuursrechtelijke handhaving en niet voor strafrechtelijke handhaving. Die lijn wordt bij de implementatie van de NIS2-richtlijn voortgezet.

Het toezicht op de naleving van het bepaalde bij of krachtens dit wetsvoorstel betreft bestuursrechtelijk toezicht. Dit betreft niet het interbestuurlijk toezicht als bedoeld in de Wet revitalisering generiek toezicht.

5.7.2 Toezichthouders

Het toezicht op de naleving van het bepaalde bij of krachtens dit wetsvoorstel wordt opgedragen aan door de toezichthoudende instantie aangewezen ambtenaren. Die aangewezen ambtenaren zijn toezichthouders in de zin van artikel 5:11 van de Awb. Dit zijn personen die bij of krachtens wettelijk voorschrift belast zijn met het houden van toezicht op de naleving van het bepaalde bij of krachtens enig wettelijk voorschrift. Daarmee beschikken zij over de bevoegdheden die titel 5.2 Awb aan hen toekent. Het gaat meer in het bijzonder om de bevoegdheden geregeld in de artikelen 5:15 tot en met 5:19 Awb en de verplichting om mee te werken van artikel 5:20 Awb. De ambtenaren die zijn aangewezen voor het toezicht op de naleving van het bepaalde bij of krachtens dit wetsvoorstel beschikken daarmee onder meer over de bevoegdheid om plaatsen te betreden (met uitzondering van woningen zonder toestemming van de bewoner), om identificatie van personen te vorderen, om inzage te vorderen van zakelijke gegevens en bescheiden en om daarvan kopieën te maken.

5.7.3 Differentiatie toezicht op essentiële entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen

Dit wetsvoorstel maakt, zoals voorgeschreven door de NIS2-richtlijn, onderscheid tussen enerzijds het toezicht op essentiële entiteiten en belangrijke entiteiten en anderzijds het toezicht op entiteiten die domeinnaamregistratiediensten verlenen.

Essentiële entiteiten en belangrijke entiteiten
De richtlijn schrijft voor dat essentiële entiteiten moeten worden onderworpen aan een alomvattende regeling voor toezicht vooraf en achteraf. Belangrijke entiteiten moeten worden onderworpen aan een regeling voor toezicht, uitsluitend achteraf. Hierover is in de NIS2-richtlijn toegelicht dat deze differentiatie zorgt voor een billijk evenwicht tussen op risico gebaseerde eisen en verplichtingen enerzijds en de administratieve lasten die voortvloeien uit het toezicht op de naleving anderzijds. Het toezicht achteraf ten aanzien van belangrijke entiteiten kan worden ingezet wanneer bewijzen, aanwijzingen of informatie onder de aandacht van de bevoegde autoriteiten zijn gekomen en deze door die autoriteiten worden geacht te wijzen op mogelijke inbreuken op de richtlijn. Dergelijke bewijzen, aanwijzingen of informatie kunnen bijvoorbeeld van het type zijn dat door andere autoriteiten, entiteiten, burgers, media of andere bronnen aan de bevoegde autoriteiten wordt verstrekt, kan openbaar beschikbare informatie zijn, of kan voortkomen uit andere werkzaamheden die de bevoegde autoriteiten in het kader van de uitvoering van hun taken verrichten.[47]
Omdat in de NIS2-richtlijn het toezicht op belangrijke entiteiten wordt omschreven als het "toezicht achteraf" dat kan worden "geactiveerd" wanneer de bevoegde autoriteiten op de hoogte zijn gekomen van mogelijke inbreuken op de richtlijn, wordt in dit wetsvoorstel voorzien in afzonderlijke artikelen ten aanzien van het toezicht op essentiële entiteiten en het toezicht op belangrijke entiteiten. Een belangrijk verschil in die artikelen ziet op het moment waarop de toezichthouder de hierin opgenomen bevoegdheden kan inzetten ten aanzien van belangrijke entiteiten.

Entiteiten die domeinnaamregistratiediensten aanbieden
De NIS2-richtlijn bevat geen specifieke bepalingen over het toezicht op de naleving van de verplichtingen die gelden voor entiteiten die domeinnaamregistratiediensten verlenen, anders dan de algemene bepaling dat lidstaten ervoor moeten zorgen dat hun bevoegde autoriteiten effectief toezicht houden op en de noodzakelijke maatregelen nemen om te zorgen voor de naleving van de richtlijn (artikel 31, eerste lid, NIS2-richtlijn). Dit betekent dat het aan de lidstaten is om te komen tot een passende invulling van het toezicht op deze entiteiten. Voor het toezicht op entiteiten die domeinnaamregistratiediensten verlenen is gekozen voor de bevoegdheid van de toezichthouder tot het opleggen van een aanwijzing, last onder dwangsom en bestuurlijke boete. Er is gekozen om niet te voorzien in de bevoegdheid tot het opleggen van een last onder bestuursdwang. De reden daarvoor

[47] Overweging 15 en 122 NIS2-richtlijn.

is gelegen in de aard van de verplichtingen die op grond van dit wetsvoorstel gelden voor entiteiten die domeinnaamregistratiediensten verlenen. Indien deze entiteiten de voor hen geldende verplichtingen niet nakomen, zoals de verplichting tot het verstrekken van informatie aan de Minister van Justitie en Veiligheid ten behoeve van het nationale register van entiteiten (artikel 45 Cbw) en het register van Enisa (artikel 48 Cbw), dan is het niet denkbaar dat de toezichthouder zelf overgaat tot het herstel van deze overtreding door de last door feitelijk handelen ten uitvoer te leggen.
Het voorgaande is van toepassing op entiteiten die domeinnaamregistratiediensten verlenen voor zover zij niet al op grond van dit wetsvoorstel worden aangemerkt of zijn aangewezen als essentiële entiteit of belangrijke entiteit. Indien een entiteit die domeinnaamregistratiediensten verleent ook op grond van dit wetsvoorstel een essentiële entiteit of belangrijke entiteit is, dan gelden de bepalingen over het toezicht en de handhaving op essentiële entiteiten respectievelijk belangrijke entiteiten.

5.7.4 Handhavingsinstrumentarium

Dit wetsvoorstel voorziet, ter implementatie van hetgeen de NIS2-richtlijn hierover bepaalt, in verschillende instrumenten van de toezichthoudende instantie voor het toezicht op de naleving van de verplichtingen uit dit wetsvoorstel. Dit instrumentarium verschilt tussen essentiële entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen, omdat de richtlijn dit verlangt. De afzonderlijke instrumenten worden in de hiernavolgende paragrafen uiteengezet.

Het handhavingsinstrumentarium ten aanzien van essentiële entiteiten omvat het volgende:
- het aanwijzen van een controlefunctionaris (paragraaf 5.7.5);
- het uitvoeren of laten uitvoeren van een beveiligingsscan; (paragraaf 5.7.6)
- het verplichten van een beveiligingsaudit;(paragraaf 5.7.7)
- het verplichten van de openbaarmaking van een overtreding;(5.7.8)
- het opleggen van een aanwijzing;(5.7.9)
- het opleggen van een last onder bestuursdwang;(5.7.10)
- het bepalen van een einddatum, het verzoeken van een tijdelijke opschorting van een certificering of vergunning en het verzoeken van een schorsing van een lid van het bestuur;(5.7.11)
- het opleggen van een bestuurlijke boete.(5.7.12)

Het handhavingsinstrumentarium ten aanzien van belangrijke entiteiten omvat het volgende:
- het uitvoeren of laten uitvoeren van een beveiligingsscan;
- het verplichten van een beveiligingsaudit;
- het verplichten van de openbaarmaking van een overtreding;
- het opleggen van een aanwijzing;
- het opleggen van een last onder bestuursdwang;
- het opleggen van een last onder dwangsom;
- het opleggen van een bestuurlijke boete.

Het handhavingsinstrumentarium ten aanzien van entiteiten die domeinnaamregistratiediensten verlenen, die op grond van het wetsvoorstel niet tevens essentiële entiteit of belangrijke entiteit zijn, omvat het volgende:
- het opleggen van een aanwijzing;
- het opleggen van een last onder dwangsom;
- het opleggen van een bestuurlijke boete.

5.7.5 Controlefunctionaris

Algemeen
Zoals bepaald in artikel 32, vierde lid, onderdeel g, NIS2-richtlijn kan de toezichthoudende instantie bij essentiële entiteiten een controlefunctionaris aanwijzen. Deze bepaling uit de richtlijn is geïmplementeerd in artikel 68 van dit wetsvoorstel. Deze bevoegdheid ziet alleen op essentiële entiteiten en niet op belangrijke entiteiten. Deze bevoegdheid ziet evenmin op entiteiten die domeinnaamregistratiediensten verlenen voor zover zij niet al op grond van dit wetsvoorstel worden aangemerkt of zijn aangewezen als essentiële entiteit.

De controlefunctionaris is niet een toezichthouder als bedoeld in de Awb. De aanwijzing van een controlefunctionaris betreft een besluit in de zin van de Awb waar bezwaar, beroep en hoger beroep tegen open staat.

Taken en doel van de controlefunctionaris
Een controlefunctionaris, zoals bedoeld in artikel 68, is een ter zake deskundige natuurlijk persoon die gedurende een bepaalde periode moet monitoren dat een essentiële entiteit voldoet aan de zorgplicht en de meldplicht. Ook moet de controlefunctionaris de toezichthoudende instantie en het bestuur van een essentiële entiteit informeren over de naleving van die verplichtingen door die entiteit. Voor de effectieve inzet van een controlefunctionaris dient deze een voldoende zelfstandige en onafhankelijke positie te hebben. Een controlefunctionaris kan een medewerker van de betrokken entiteit zijn of extern worden aangesteld. De controlefunctionaris mag geen conflict van belangen hebben die een goede taakoefening in de weg kunnen staan. Gezien de specifieke organisatiestructuur van elke organisatie moet dit van geval tot geval worden beoordeeld. In het algemeen kan het niet om een persoon van het hoger management van de betreffende entiteit gaan. De toezichthoudende instantie neemt deze factoren mee in haar besluit tot de aanwijzing van een controlefunctionaris. In artikel 68, tweede lid, Cbw staan de taken van de controlefunctionaris omschreven. Bij of krachtens amvb worden regels gesteld onder meer over de vereisten die gelden voor de aanwijzing van de controlefunctionaris (artikel 68, vierde lid) zoals professionele kwalificaties.

Voor de effectieve inzet van een controlefunctionaris is het ook noodzakelijk dat deze de middelen, faciliteiten en toegang tot informatie en andere organisatieonderdelen van de entiteit krijgt om zijn taak doeltreffend te kunnen uitoefenen. Dit vereist daarom actieve ondersteuning vanuit het bestuur van de entiteit. De controlefunctionaris dient dan ook naar behoren en tijdig te worden betrokken bij alle aangelegenheden van de betrokken entiteit die verband houden met zijn taken.

Het bestuur van de essentiële entiteit kan vervolgens op basis van de toegekomen informatie gepaste actie ondernemen om ervoor te zorgen dat de entiteit voldoet aan de zorgplicht en de meldplicht. Het doel van het aanwijzen van een controlefunctionaris is het bevorderen van de naleving van de zorgplicht en meldplicht door de betrokken essentiële entiteit. De controlefunctionaris neemt daarbij geen verantwoordelijkheden over van de betreffende entiteit. De betreffende entiteiten zijn en blijven verantwoordelijk voor de naleving van de zorgplicht en de meldplicht.

5.7.6 Beveiligingsscan

De toezichthoudende instantie is ten aanzien van essentiële entiteiten en belangrijke entiteiten bevoegd om zelf of middels een onafhankelijke deskundige beveiligingsscans uit te voeren op netwerk- en informatiesystemen van die entiteiten om kwetsbaarheden en risico’s voor de beveiliging van die netwerk- en informatiesystemen te identificeren. Deze bevoegdheid volgt uit de artikelen 32, tweede lid, onderdeel d, en 33, tweede lid, onderdeel c, NIS2-richtlijn en is geïmplementeerd in de artikelen 69 en 79 van dit wetsvoorstel.

Het doel van beveiligingsscans is het verkrijgen van nader inzicht in de effectiviteit van de door de entiteit genomen beheersmaatregelen en het beveiligingsniveau van hun netwerk- en informatiesystemen. Voorbeelden van beveiligingsscans zijn kwetsbaarheidsonderzoeken en penetratietesten. Beveiligingsscans kunnen zowel intern als op afstand worden uitgevoerd

De beveiligingsscans dienen plaats te vinden op basis van objectieve, niet-discriminerende, eerlijke en transparante risicobeoordelingscriteria, indien nodig in samenwerking met de betrokken entiteit. Hiermee wordt onder andere tot uiting gebracht dat van tevoren het doel van de beveiligingsscan, de daarbij in te zetten middelen, de wijze van uitvoering en te gebruiken criteria door de bevoegde autoriteit dienen te worden bepaald. Een belangrijk aandachtspunt daarbij is het beheersen van de risico’s die gepaard kunnen gaan met de inzet beveiligingsscans, zodat onbedoelde verstoringen worden voorkomen. Daarmee ligt het in de rede dat mogelijke meer risicovolle beveiligingsscans die bijvoorbeeld de continuïteit van de dienstverlening kunnen raken pas na consultatie van de betreffende entiteit en indien nodig in samenwerking met de entiteit door de toezichthoudende instantie worden ingezet.

Conform overweging 124 NIS2-richtlijn kan de toezichthoudende instantie bij essentiële entiteiten de verplichting tot het laten uitvoeren van beveiligingsscans ex-ante inzetten als onderdeel van een risico-gebaseerd toezichtregime, waarbij de toezichthouder het type en de frequentie van verplichte beveiligingsscans kan bepalen.

5.7.7 Beveiligingsaudit

De toezichthoudende instantie kan essentiële entiteiten en belangrijke entiteiten verplichten zich aan een beveiligingsaudit te onderwerpen. Deze bevoegdheid volgt uit de artikelen 32, tweede lid, onderdeel b, en 33, tweede lid, onderdeel b, NIS2-richtlijn en is geïmplementeerd in de artikelen 70 en 80 van dit wetsvoorstel.

Bij een beveiligingsaudit onderzoekt een onafhankelijke en gekwalificeerde deskundige de opzet en werking van de door de entiteit genomen beheers- of beveiligingsmaatrelen. De audit verschaft daarmee aanvullende inzichten voor de toezichthoudende instantie om te kunnen controleren in welke mate de entiteit voldoet aan de regelgeving. Ook geeft de audit de toezichthoudende instantie inzicht in welke mate de entiteit 'in control' is ten aanzien van het nemen van adequate beheers- of beveiligingsmaatregelen. De audit kan betrekking hebben op de gehele entiteit of specifieke processen binnen de entiteit.

Conform overweging 124 NIS2-richtlijn kan de toezichthoudende instantie bij essentiële entiteiten de verplichting tot het laten uitvoeren van audits ex-ante inzetten als onderdeel van een risico-gebaseerd toezichtregime, waarbij de toezichthouder het type en de frequentie van verplichte audits kan bepalen.

5.7.8 Het verplichten van de openbaarmaking van de overtreding

De toezichthoudende instantie kan essentiële en belangrijke entiteiten verplichten om door de entiteit begane overtredingen (gedeeltelijk) openbaar te maken.

5.7.9 Bindende aanwijzing

De toezichthoudende instantie kan aan essentiële entiteiten en belangrijke entiteiten een bindende aanwijzing opleggen om binnen een daarbij gestelde redelijke termijn de daarin omschreven handelingen te verrichten of de daarin omschreven maatregelen te nemen ter naleving van het bepaalde bij of krachtens dit wetsvoorstel. Deze bevoegdheid volgt uit de artikelen 32, vierde lid, onderdeel b, en 33, vierde lid, onderdeel b, NIS2-richtlijn en is geïmplementeerd in de artikelen 72 en 82 van dit wetsvoorstel.

De aanwijzing kent een juridisch bindend karakter en is een beschikking in de zin van artikel 1:3 Awb waar bezwaar, beroep en hoger beroep tegen open staat. Een bindende aanwijzing is een enkele last tot het verrichten van bepaalde handelingen, bedoeld in artikel 5:2, tweede lid, Awb en geen bestuurlijke sanctie. De bindende aanwijzing wordt toegepast om te kunnen voldoen aan een wettelijke verplichting of norm. Daarmee wordt voor de entiteit die een aanwijzing krijgt opgelegd duidelijk waaraan moet worden voldaan en wat zij moet doen om aan die verplichting of norm te voldoen. Als niet aan de wettelijke verplichting of norm voldaan wordt, kan de toezichthoudende instantie vervolgens handhaven met bijvoorbeeld een last onder dwangsom of een bestuurlijke boete.

5.7.10 Last onder bestuursdwang

Op grond van de artikelen 73 en 83 van dit wetsvoorstel is de toezichthoudende instantie bevoegd tot het opleggen van een last onder bestuursdwang ten aanzien van een essentiële entiteit of een belangrijke entiteit. Er zijn situaties denkbaar waarin zij tot het oordeel komt dat deze herstelsanctie de meest passende maatregel betreft, bijvoorbeeld omdat het niet voldoen aan een last onder dwangsom enkel het gevolg heeft dat de dwangsom wordt verbeurd maar de overtreding door de overtreder niet ongedaan kan worden gemaakt Zo is de situatie denkbaar waarin als gevolg van de

overtreding van de zorgplicht de continuïteit van de dienstverlening in het geding is en er daardoor aanzienlijke gevolgen zijn voor dienstverlening van de entiteit, met mogelijk maatschappelijke ontwrichting tot gevolg. Een last onder bestuursdwang waarbij de bevoegde autoriteit zelf zorgt voor herstel, kan dan ervoor zorgen dat deze aanzienlijke negatieve gevolgen worden beperkt of voorkomen. Ook kunnen zich situaties voordoen waarin een last onder bestuursdwang de mogelijkheid biedt om de risico's voor derden als gevolg van een overtreding van bijvoorbeeld de zorgplicht af te wenden.

Op grond van artikel 5:32, eerste lid, Awb is de toezichthoudende instantie bevoegd om in plaats van een last onder bestuursdwang een last onder dwangsom op te leggen.

5.7.11 Bepalen einddatum, verzoek tot schorsing certificering of vergunning en verzoek tot schorsing leden van het bestuur

5.7.11.1 Implementatie van artikel 32, vijfde lid, NIS2-richtlijn

Dit wetsvoorstel bevat ter implementatie van artikel 32, vijfde lid, NIS2-richtlijn bevoegdheden voor de toezichthoudende instantie die nieuw zijn in het Nederlands bestuursrecht. Die bepaling uit de richtlijn ziet op de gevallen waarin een essentiële entiteit in overtreding is en de toezichthoudende instantie een of meerdere van de in artikel 32, vierde lid, onderdelen a tot en met d en f, NIS2-richtlijn genoemde handhavingsmaatregelen heeft genomen. Wanneer deze maatregelen ondoeltreffend zijn, moeten lidstaten ervoor zorgen dat de toezichthoudende instantie de bevoegdheid heeft om een termijn te stellen waarbinnen de essentiële entiteit wordt verzocht de noodzakelijke maatregelen te nemen om de tekortkomingen te verhelpen of aan de eisen van de toezichthoudende instantie te voldoen. Deze onderdelen zien op een waarschuwing over een inbreuk door de betrokken essentiële entiteit, een verplichting over de uitvoering van de aanbevelingen naar aanleiding van een beveiligingsaudit, een bindende aanwijzing of een last. Om verwarring te voorkomen met de in het bestuursrecht gehanteerde term van een begunstigingstermijn, wordt in dit kader in plaats van "het stellen van een termijn" in dit wetsvoorstel en de bijbehorende toelichting het volgende begrip gehanteerd: "het bepalen van een einddatum".

Op grond van artikel 32, vijfde lid, NIS2-richtlijn moeten lidstaten ervoor zorgen dat indien de verzochte actie niet uiterlijk op de bepaalde einddatum is uitgevoerd, de toezichthoudende instantie de bevoegdheid heeft om:
a. een certificering of vergunning tijdelijk op te schorten of een certificerings- of vergunningsinstantie of een rechterlijke instantie overeenkomstig het nationale recht te verzoeken deze tijdelijk op te schorten met betrekking tot alle of een deel van de relevante door de essentiële entiteit verleende diensten of verrichte activiteiten;
b. te verzoeken dat de bevoegde organen of rechterlijke instanties overeenkomstig het nationale recht een natuurlijke persoon met leidinggevende verantwoordelijkheden op het niveau van de algemeen directeur of de wettelijke vertegenwoordiger in de essentiële entiteit tijdelijk verbieden leidinggevende functies in die entiteit uit te oefenen.

Deze bevoegdheid is geïmplementeerd in de artikelen 74 tot en met 76 van dit wetsvoorstel.
Deze bevoegdheid ziet alleen op essentiële entiteiten en kan niet worden toegepast op belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen, voor zover deze laatstgenoemde niet tevens een essentiële entiteit zijn. Deze bevoegdheden zijn niet van toepassing is op overheidsinstanties om zo te voorkomen dat overheidsinstanties hun taken niet langer kunnen uitvoeren.

5.7.11.2 Bepaling einddatum door toezichthoudende instantie

Inleiding
Wanneer de in paragraaf 5.7.11.2 genoemde maatregelen ondoeltreffend zijn, kan de toezichthoudende instantie een einddatum bepalen waarop de betrokken essentiële entiteit uiterlijk de noodzakelijke maatregelen moet hebben genomen om tekortkomingen te verhelpen of aan de eisen van de toezichthoudende instantie moet hebben voldaan. Het bepalen van de einddatum is erop

gericht om die overtreding te stoppen. De maatregelen zijn ondoeltreffend zolang de overtreding gaande is.

Bepalen einddatum is Awb-besluit
Het bepalen van een einddatum is een besluit in de zin van de Awb. Ingevolge artikel 1:3, eerste lid, Awb wordt onder een besluit verstaan: een schriftelijke beslissing van een bestuursorgaan, inhoudende een publiekrechtelijke rechtshandeling. Een rechtshandeling is een handeling die is gericht op rechtsgevolg. Een beslissing heeft rechtsgevolg indien zij erop is gericht een bevoegdheid, recht of verplichting voor een of meer anderen te doen ontstaan of teniet te doen, dan wel de juridische status van een persoon of een zaak vast te stellen.
Het bepalen van een einddatum heeft weliswaar op het moment waarop dat gebeurt geen gevolgen voor de entiteit waar het aan is gericht, maar "activeert" wel bevoegdheden van de toezichthoudende instantie zodra niet uiterlijk op de bepaalde einddatum de noodzakelijke maatregelen zijn genomen of aan de eisen van de toezichthoudende instantie is voldaan. Het bepalen van een einddatum is dus erop gericht een bevoegdheid te doen ontstaan en is daarmee een handeling gericht op een rechtsgevolg. Aangezien in dit kader ook aan de andere elementen uit het besluitbegrip zal worden voldaan (schriftelijk, bestuursorgaan etc.) is het bepalen van een einddatum een besluit in de zin van de Awb. Daarmee is ook voldaan aan het vereiste van een doeltreffende voorziening in rechte: tegen een besluit in de zin van de Awb staan de mogelijkheden van bezwaar open bij het bestuursorgaan en beroep en hoger beroep bij de bestuursrechter open.

Evenredigheid en subsidiariteit
Zoals gezegd kan de toezichthoudende instantie een einddatum bepalen als de maatregelen genoemd in artikel 32, vierde lid, onderdelen a tot en met d en f, NIS2-richtlijn ondoeltreffend zijn. Onderdeel a ziet op een waarschuwing, onderdeel b ziet op een aanwijzing. De NIS2-richtlijn schrijft niet voor dat alle genoemde maatregelen eerst moeten zijn genomen voordat de toezichthoudende instantie de einddatum kan bepalen. Het gaat erom dat de genoemde maatregelen ondoeltreffend zijn gebleken of naar redelijke verwachting ondoeltreffend zullen zijn. De toezichthoudende instantie kan, na een overtreding van een verplichting uit dit wetsvoorstel, de termijn dus al stellen direct nadat een waarschuwing of aanwijzing is gegeven, die waarschuwing of aanwijzing ondoeltreffend is gebleken en volgens de toezichthoudende instantie de andere nog niet opgelegde maatregelen (zoals een last onder dwangsom) naar redelijke verwachting ondoeltreffend zullen zijn. Dit is echter alleen denkbaar in uitzonderlijke gevallen. In de meeste gevallen zal de toezichthoudende instantie eerst overgaan tot het opleggen van andere maatregelen. Een waarschuwing of bindende aanwijzing kan opgevolgd worden door bijvoorbeeld een last onder dwangsom. Als de toezichthoudende instantie wenst over te gaan tot het bepalen van de einddatum, moet zij motiveren waarom de eerdere genomen maatregel of maatregelen ondoeltreffend zijn en waarom andere maatregelen naar redelijke verwachting ondoeltreffend zullen zijn, en daarom niet eerst worden opgelegd voordat de termijn wordt gesteld.
Bij de bevoegdheid tot het bepalen van een einddatum differentieert de richtlijn niet in het soort overtreding. De bevoegdheid ziet dus niet alleen op overtredingen van de zorgplicht en de meldplicht, maar ook op overtredingen van andere verplichtingen, zoals de registratieverplichting. Dit betekent dat de toezichthoudende instantie ook bevoegd is tot het bepalen van de einddatum als een relatief lichte verplichting is geschonden. Gelet op de gevolgen van het bepalen van de einddatum en de aard van de verplichting is de toepassing van deze bevoegdheid na de overtreding van een "lichte" verplichting naar verwachting in de meeste gevallen niet in verhouding. Zowel de NIS2-richtlijn als de Awb eisen dat sancties evenredig moeten zijn. Dit betekent in de praktijk dat de toezichthoudende instantie telkens de aard van de verplichting en de gevolgen van het niet voldoen aan die verplichting naast het al dan niet stellen van de termijn en de gevolgen daarvan moet leggen. Als de toezichthoudende instantie bij de overtreding van een relatief lichte verplichting wil overgaan op het stellen van de termijn, zal zij met een zware motivering moeten komen.[48]

[48] Hierbij wordt ook verwezen naar overweging 133 NIS2-richtlijn: "Dergelijke tijdelijke opschortingen of verboden mogen alleen worden toegepast als ultiem middel, met name alleen nadat de andere in deze richtlijn neergelegde relevante handhavingsmaatregelen zijn uitgeput (...)".

Alleen bepaling einddatum na volledige verbeuring last onder dwangsom
Als de toezichthoudende instantie een last onder dwangsom heeft opgelegd, dan kan zij alleen een einddatum bepalen nadat de essentiële entiteit niet heeft voldaan aan die last en de dwangsom volledig is verbeurd (het maximum van de dwangsom is bereikt). Pas dan kan immers als regel geconcludeerd worden dat de handhavingsmaatregel van een last onder dwangsom ondoeltreffend is.

5.7.11.3 Verzoek tot schorsing certificering of vergunning en verzoek tot schorsing leden van het bestuur

Inleiding
Als niet uiterlijk op de bepaalde einddatum is voldaan aan de eisen van de toezichthoudende instantie, dan schrijft artikel 32, vijfde lid, NIS2-richtlijn voor dat de toezichthoudende instantie de bevoegdheid moet hebben om een certificering of vergunning tijdelijk op te schorten of een certificerings- of vergunningsinstantie of een rechterlijke instantie te verzoeken deze tijdelijk op te schorten met betrekking tot alle of een deel van de relevante door de essentiële entiteit verleende diensten of verrichte activiteiten. Ook heeft de toezichthoudende instantie de bevoegdheid om te verzoeken dat de bevoegde organen of rechterlijke instanties overeenkomstig het nationale recht een natuurlijke persoon met leidinggevende verantwoordelijkheden op het niveau van de algemeen directeur of de wettelijke vertegenwoordiger in de essentiële entiteit tijdelijk verbieden leidinggevende functies in die entiteit uit te oefenen. Deze bevoegdheden zijn geïmplementeerd in de artikelen 75 en 76 van dit wetsvoorstel.

Verzoek tot schorsing certificering of vergunning
Het verzoek van de toezichthoudende instantie aan de rechter of certificerings- of vergunningsinstantie tot het opschorten van een certificering of vergunning heeft als doel om te voorkomen dat zolang de essentiële entiteit niet voldoet aan de eisen van de toezichthoudende instantie, activiteiten van deze entiteit tot leiden tot onacceptabele schade en/of risico's voor derden. Het verzoek van de toezichthoudende instantie bevat onder meer een toelichting op het risico van het continueren van de dienstverlening van de entiteit. De certificerings- of vergunningsinstantie kan aanvullende bewijsstukken en informatie opvragen bij de toezichthoudende instantie. Het verzoek van de toezichthoudende instantie leidt niet tot een verplichting voor de certificerings- of vergunningsinstantie om het verzoek te honoreren. Het is aan het oordeel van de certificerings- of vergunningsinstantie of de certificering of vergunning voor bepaalde tijd dient te worden opgeschort. Dit geldt uiteraard ook voor wat betreft een dergelijk verzoek aan de rechter.

Verzoek tot schorsing leden van het bestuur
De bevoegdheid die ziet op natuurlijke personen met leidinggevende verantwoordelijkheden op het niveau van algemeen directeur of de wettelijke vertegenwoordiger in de essentiële entiteit, wordt geïmplementeerd als de bevoegdheid van de toezichthoudende instantie om een verzoek te doen bij de civiele rechter tot schorsing van één of meer leden van het bestuur van de essentiële entiteit. Het Nederlands ondernemingsrecht kent geen juridische status voor de in de richtlijn omschreven "natuurlijke persoon met leidinggevende verantwoordelijkheden op het niveau van de algemeen directeur". Het ondernemingsrecht kent alleen het bestuur als orgaan en de bestuurders als leden van dat orgaan. Zij zijn de enigen die juridisch aanspreekbaar zijn in de uitoefening van hun functie en hun handelen namens de rechtspersoon. Zij zijn de wettelijke vertegenwoordiger van de rechtspersoon en voldoen aan de omschrijving uit de richtlijn. Als het gaat om de in de richtlijn bedoelde algemeen directeur, betreft dat in het Nederlands recht de voorzitter van het bestuur. "Degenen op het niveau van wettelijke vertegenwoordiger" uit artikel 32, vijfde lid, NIS2-richtlijn betreffen de overige leden van het bestuur.

De in de richtlijn bedoelde "wettelijke vertegenwoordiger" betreft overigens niet degene die – naast het bestuur of de afzonderlijke leden van het bestuur – statutair bevoegd is de rechtspersoon te vertegenwoordigen. Die bevoegdheid volgt immers niet uit de wet, maar uit de statuten. Wanneer op verzoek van de toezichthoudende instantie alle leden van het bestuur door de rechter zijn geschorst, is er in theorie niemand meer bevoegd om de tekortkomingen op dit wetsvoorstel te herstellen. Het Burgerlijk Wetboek schrijft voor dat de statuten moeten voorzien in voorschriften over de wijze waarop de uitoefening van de taken en bevoegdheden voorlopig wordt voorzien bij

ontstentenis of belet van alle bestuurders (zoals artikel 2:134, vierde lid, van het Burgerlijk Wetboek). Voor de gevallen waarin geen "wettelijke vertegenwoordiger" kan worden aangewezen, is in dit wetsvoorstel geregeld dat de rechtbank zo nodig alle overige gevolgen van de door haar uitgesproken schorsing regelt.

De wet regelt dat de rechtbank haar vonnis naar de Kamer van Koophandel moet sturen voor het opnemen van het vonnis in het Handelsregister. De schorsing duurt zolang niet is voldaan aan het hiervoor bedoelde besluit van de toezichthoudende instantie waarin de termijn wordt gesteld. Zodra hieraan is voldaan (in de praktijk betekent dit: de overtreding is beëindigd), moet de toezichthoudende instantie de Kamer van Koophandel hiervan op de hoogte stellen vanwege het verwijderen van de schorsing uit het Handelsregister.

5.7.12 Bestuurlijke boete

Inleiding
Dit wetsvoorstel voorziet in de artikelen 77, 84 en 88 in de bevoegdheid voor de toezichthoudende instantie om een bestuurlijke boete op te leggen aan essentiële entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen die een verplichting uit dit wetsvoorstel overtreden.

Clausulering ten aanzien van essentiële entiteiten en belangrijke entiteiten
In artikel 34, tweede lid, NIS2-richtlijn is bepaald dat bestuurlijke boetes aan essentiële entiteiten en belangrijke entiteiten worden opgelegd bovenop de maatregelen die in dat artikel zijn genoemd. Het gaat hierbij om maatregelen zoals een waarschuwing, aanwijzing, last of verplichting om een overtreding openbaar te maken. De toezichthoudende instantie kan dus alleen een bestuurlijke boete opleggen aan een essentiële entiteit of belangrijke entiteit tezamen met of nadat één of meer van deze maatregelen zijn genomen. De richtlijn bevat niet zo'n bepaling ten aanzien van bestuurlijke boetes die worden opgelegd aan entiteiten die domeinnaamregistratiediensten verlenen.
De toezichthoudende instantie is altijd, en dus ook bij het opleggen van een bestuurlijke boete, gehouden aan de Awb en de algemene beginselen van behoorlijk bestuur. Zo dient de toezichthoudende instantie de beslissing om een bestuurlijke boete op te leggen te motiveren en toe te lichten waarom een bestuurlijke boete in het specifieke geval evenredig en subsidiair is. Op grond van de richtlijn (en daarmee ook in dit wetsvoorstel) is het dus in theorie mogelijk om direct na of gelijktijdig aan een waarschuwing een bestuurlijke boete op te leggen, maar dit is gelet op de voor de toezichthoudende instantie geldende juridische kaders slechts denkbaar in uitzonderlijke gevallen.

Boetemaximum overtreding zorgplicht en meldplicht
Alleen ten aanzien van de overtreding van de zorgplicht en de meldplicht bevat de NIS2-richtlijn regels over de maximale hoogte van een bestuurlijke boete voor de overtreding van die verplichtingen. Artikel 34, vierde lid, NIS2-richtlijn schrijft voor dat de maximale hoogte van een boete voor een overtreding van de zorgplicht of van de meldplicht door een essentiële entiteit betreft: 10 miljoen euro of 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar als dat laatste leidt tot een hoger bedrag. Artikel 34, vijfde lid, NIS2-richtlijn schrijft verder voor dat de maximale hoogte van een boete voor de overtreding van de zorgplicht of van de meldplicht door een belangrijke entiteit betreft: 7 miljoen euro of 1,4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar als dat laatste leidt tot een hoger bedrag.

Boetemaximum overtreding medewerkingsplicht
Voor alle entiteiten die onder het toepassingsbereik van dit wetsvoorstel vallen geldt dat zij op basis van artikel 5:20 Awb verplichting hebben aan een toezichthouder binnen de door hem gestelde redelijke termijn alle medewerking te verlenen die deze redelijkerwijs kan vorderen bij de uitoefening van zijn bevoegdheden. Voor het boetemaximum van een bestuurlijke boete voor de overtreding van deze verplichting is gekozen voor het bedrag van de tweede categorie, bedoeld in artikel 23, vierde lid, Wetboek van Strafrecht. De reden voor deze keuze is als volgt. Het opzettelijk niet voldoen aan een bevel of vordering van een ambtenaar is een overtreding van artikel 184 Wetboek van Strafrecht. De maximale geldboete voor een overtreding hiervan is een geldboete van de tweede categorie van artikel 23, vierde lid, Wetboek van Strafrecht. In 2015 heeft de Afdeling advisering van de Raad van

State een ongevraagd advies uitgebracht over de sanctiestelsels.[49] In het daarop volgend nader rapport heeft het kabinet aangegeven dat maxima van bestuurlijke boetes in nieuwe wetgeving in beginsel niet hoger zullen zijn dan de maximale boete die op grond van het strafrecht kan worden opgelegd voor eenzelfde overtreding.[50] In lijn met kabinetsbeleid wordt daarom in dit wetsvoorstel geregeld dat de maximale hoogte van een bestuurlijke boete voor de overtreding van artikel 5:20 Awb dezelfde is als de maximale hoogte van een geldboete voor een overtreding van artikel 184 Wetboek van Strafrecht.

Boetemaximum overtreding overige verplichtingen
Naast de zorgplicht en de meldplicht bevat dit wetsvoorstel ook andere verplichtingen, zoals de verplichting voor entiteiten om informatie te verstrekken ten behoeve van het nationale register van entiteiten (artikel 45 Cbw). Voor wat betreft een bestuurlijke boete voor de overtreding van verplichtingen anders dan de zorgplicht, de meldplicht en de verplichting uit artikel 5:20 Awb is gekozen voor een maximum van 1 miljoen euro. Dat betreft een voortzetting van de gekozen lijn in het kader van de implementatie van de NIS1-richtlijn in nationale wet- en regelgeving. Hierbij is toegelicht dat een boetemaximum van 1 miljoen euro de sectorale toezichthouder die uit hoofde van bestaande wetgeving al bevoegd is om een bestuurlijke boete op te leggen de ruimte biedt om voor de boetebedragen aan te sluiten bij de boetehoogtes die in die sector passend zijn.[51]Bij het maximeren van de boete voor dergelijke overtredingen speelt tevens mee dat het hoge boetemaximum dat geldt bij de overtreding van de zorgplicht en de meldplicht (10 miljoen euro of 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, of 7 miljoen of 1,4 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar) niet evenredig is in verhouding tot de aard van de overtreding.

Boetemaximum overtredingen door entiteiten die domeinnaamregistratiediensten verlenen
Bij het boetemaximum dat kan worden opgelegd aan entiteiten die domeinnaamregistratiediensten verlenen moet een onderscheid worden gemaakt tussen zulke entiteiten die op grond van dit wetsvoorstel ook zijn aangemerkt of aangewezen als essentiële of belangrijke entiteit en entiteiten die niet ook als zodanig zijn aangemerkt of aangewezen. Als een entiteit die domeinnaamregistratiediensten verleent ook een essentiële of belangrijke entiteit is, dan gelden voor die entiteit ook de zorgplicht en de meldplicht en de daarbij behorende boetemaxima. Als een entiteit die domeinnaamregistratiediensten verleent niet tevens een essentiële of belangrijke entiteit is, zijn deze verplichtingen niet op hen van toepassing en dus ook niet de daarbij behorende boetemaxima van 10 miljoen euro of 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, of 7 miljoen euro of 1,4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar. In dat geval geldt alleen het boetemaximum van het bedrag van de tweede categorie, bedoeld in artikel 23, vierde lid, Wetboek van Strafrecht voor een overtreding van artikel 5:20 Awb en een boetemaximum van 1 miljoen euro voor de overtreding van de overige verplichtingen.

Motivering bestuurlijke boete en hoogte daarvan
Voor de goede orde wordt benadrukt dat het gaat om maximale hoogten van de op te leggen bestuurlijke boeten; de toezichthoudende instantie kan uiteraard ook besluiten om over te gaan tot het opleggen van een bestuurlijke boete van een lager bedrag.
De toezichthoudende instantie moet de beslissing om over te gaan tot het opleggen van een bestuurlijke boete en de hoogte daarvan afstemmen op de ernst van de overtreding en de mate waarin deze aan de overtreder kan worden verweten en daarbij zo nodig rekening moeten houden met de omstandigheden waaronder de overtreding is gepleegd (artikel 5:46, tweede lid, Awb). Artikel 5:41 Awb bepaalt verder dat er geen bestuurlijke boete wordt opgelegd voor zover de overtreding niet aan de overtreder kan worden verweten. Artikel 3:4 van de Awb is onverkort van toepassing bij het opleggen van de bestuurlijke boete door de toezichthoudende instantie.

[49] Advies van de Afdeling advisering van de Raad van State van 13 juli 2015 met kenmerk W03.15.0138/II.
[50] Kamerstukken II 2015/16, 34300-VI, nr. 72
[51] Kamerstukken II 2017/18, 34 883, nr. 3, p. 14.

5.7.12 Overtrederschap

In artikel 5:1, eerste lid, Awb is bepaald dat in de Awb wordt verstaan onder overtreding: een gedraging die in strijd is met het bepaalde bij of krachtens enig wettelijk voorschrift. In artikel 5:1, tweede lid, Awb is bepaald dat onder overtreder wordt verstaan: degene die de overtreding pleegt of medepleegt. Artikel 5:1, derde lid, Awb bepaalt dat overtredingen kunnen worden begaan door natuurlijke personen en rechtspersonen en dat artikel 51, tweede en derde lid, Wetboek van Strafrecht van overeenkomstige toepassing is. Artikel 51, tweede lid, Wetboek van Strafrecht bepaalt dat indien een strafbaar feit wordt begaan door een rechtspersoon, de strafvervolging kan worden ingesteld en de in de wet voorziene straffen en maatregelen kunnen worden uitgesproken tegen die rechtspersoon, dan wel tegen de opdrachtgever of feitelijk leidinggevende, dan wel tegen de hiervoor genoemden tezamen. In artikel 51, derde lid, Wetboek van Strafrecht wordt voor de toepassing van het tweede lid met de rechtspersonen gelijkgesteld: de vennootschap zonder rechtspersoonlijkheid, de maatschap, de rederij en het doelvermogen.

Door de schakelbepaling in artikel 5:1, derde lid, Awb is het mogelijk om in het geval dat een overtreding is gepleegd of medegepleegd door een rechtspersoon, een bestuurlijke boete of een last onder bestuursdwang of dwangsom op te leggen aan degenen die tot de door de rechtspersoon begane overtreding opdracht hebben gegeven of daaraan feitelijk leiding hebben gegeven.
De toezichthoudende instantie kan bij een overtreding van een verplichting uit dit wetsvoorstel dus handhavend optreden tegen de entiteit die de overtreding begaat, maar ook tegen degenen die worden aangemerkt als opdrachtgever van de door de entiteit begane overtreding en degenen die feitelijke leiding hebben gegeven aan de verboden gedraging.

Het voorgaande brengt met zich mee dat de artikelen 20, eerste lid, 32, zesde lid, en 33, vijfde lid, (voor wat betreft de schakeling naar artikel 32, zesde lid) NIS2-richtlijn reeds zijn geïmplementeerd in het Nederlands recht. Artikel 20, eerste lid, NIS2-richtlijn schrijft onder meer voor dat lidstaten ervoor moeten zorgen dat de bestuursorganen van essentiële en belangrijke entiteiten aansprakelijk kunnen worden gesteld voor het overtreden van de zorgplicht door de entiteit. Hierbij wordt opgemerkt dat deze bepaling in de Nederlandse context niet verwijst naar bestuursorganen in de zin van de Awb, maar naar de leden van het bestuur als bedoeld in het Burgerlijk Wetboek. In artikel 32, zesde lid, NIS2-richtlijn is bepaald dat lidstaten ervoor moeten zorgen dat elke natuurlijke persoon die verantwoordelijk is voor of optreedt als wettelijke vertegenwoordiger van een essentiële entiteit op basis van de bevoegdheid om deze te vertegenwoordigen, de bevoegdheid om namens deze entiteit beslissingen te nemen of de bevoegdheid om controle uit te oefenen op deze entiteit, de bevoegdheid heeft om ervoor te zorgen dat deze entiteit deze richtlijn nakomt. De lidstaten moeten ervoor zorgen dat dergelijke natuurlijke personen aansprakelijk kunnen worden gesteld voor het niet nakomen van hun verplichtingen om te zorgen voor de naleving van deze richtlijn. Artikel 33, vijfde lid, NIS2-richtlijn verklaart artikel 32, zesde lid, NIS2-richtlijn van overeenkomstige toepassing ten aanzien van belangrijke entiteiten.

5.7.13 Samenwerking toezichthoudende instanties

In dit wetsvoorstel wordt het toezicht vormgegeven langs de lijnen van de ministeriële verantwoordelijkheden voor de respectievelijke NIS2-sectoren, zoals dit eerder onder de NIS1-richtlijn is vormgegeven. Dit leidt tot een uitbreiding in het aantal sectorale toezichthouders. Het is bij voorbaat niet uit te sluiten dat een essentiële entiteit of een belangrijke entiteit actief is binnen meerdere sectoren en daarmee mogelijk te maken kan krijgen met meerdere toezichthoudende instanties. Ook kan er overlap zijn met domeinnaamregistratiediensten. Mede in het licht van artikel 13 NIS2-richtlijn is het wenselijk dat deze toezichthouders met elkaar samenwerken in het belang van doelmatig en doeltreffend toezicht op deze voorgestelde wet.

Toezichthoudende instanties werken op grond van artikel 56 van deze wet zoveel mogelijk samen bij het (onderling gecoördineerd) toezicht houden op essentiële entiteiten, belangrijke entiteiten en domeinnaamregistratiediensten.

Om de doeltreffende en doelmatige uitvoering van deze wet te borgen, dienen de toezichthoudende instanties onderling afspraken te maken over gemeenschappelijke aangelegenheden. Hierbij wordt gedacht aan samenloop van toezicht op eenzelfde entiteit, het voorkomen van onevenredige toezichtslasten, de uitwisseling van gegevens en een consistente uitleg van begrippen en normen uit dit wetsvoorstel. Deze afspraken worden vastgelegd in een samenwerkingsprotocol. Dit zorgt voor transparantie over de gemaakte afspraken en maakt voor entiteiten die onder toezicht staan helder op welke wijze de toezichthouders invulling geven aan voorgenoemde aspecten. Na initiële publicatie dient het samenwerkingsprotocol voor zover nodig geactualiseerd te worden, bijvoorbeeld als er aanvullende toezichthouders actief worden in (sub)sectoren waar voorheen nog geen toezicht was ingericht.

5.8 Registratie

De richtlijn schrijft in artikel 3, derde lid, voor dat lidstaten een lijst dienen op te stellen van essentiële entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen. Ten behoeve van het opstellen van deze lijst zijn deze entiteiten verplicht om bepaalde gegevens te delen en actueel te houden, zoals hun contactgegevens en de sector(en) waarin zij actief zijn. Bevoegde autoriteiten, toezichthouders en CSIRT's moeten over deze gegevens kunnen beschikken voor het uitoefenen van hun taken op grond van deze richtlijn. Daarnaast zijn de lidstaten verplicht om het aantal entiteiten op de lijst, uitgesplitst naar sector en subsector, te delen met de Europese Commissie en de NIS Samenwerkingsgroep.

Om ervoor te zorgen dat entiteiten deze informatie laagdrempelig kunnen aanleveren en beheren heeft het kabinet ervoor gekozen om een registratiemechanisme in te richten bij de Minister van Justitie en Veiligheid. Deze taak zal namens de Minister van Justitie en Veiligheid worden uitgevoerd door het NCSC. Daar zal een loket worden ingericht waar essentiële entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen de gegevens die genoemd staan in artikel 3, derde lid, NIS2-richtlijn kunnen aanleveren en beheren. Er is gekozen om deze functionaliteit bij het NCSC te beleggen zodat alle entiteiten op dezelfde plek terecht kunnen. Daarnaast wordt hierdoor gewaarborgd dat de verschillende betrokken autoriteiten hun taken uitvoeren op basis van dezelfde informatie die op één plek opgeslagen en actueel gehouden wordt. Via een technische oplossing wordt gewaarborgd dat bevoegde autoriteiten, toezichthouders en CSIRT's uitsluitend toegang krijgen tot de gegevens uit het register voor zover zij deze nodig hebben voor het uitvoeren van hun wettelijke taken onder deze richtlijn. Op die manier wordt de groep die toegang heeft tot deze gegevens zo beperkt mogelijk gehouden.

Via het registratiemechanisme zal ook invulling worden gegeven aan artikel 27 van de richtlijn. Dit artikel schrijft voor dat DNS-dienstverleners, registers voor topleveldomeinnamen, entiteiten die domeinnaamregistratiediensten verlenen, aanbieders van cloudcomputingdiensten, aanbieders van datacentra, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, alsmede aanbieders van onlinemarktplaatsen, van onlinezoekmachines en van platforms voor socialenetwerkdiensten bepaalde informatie aanleveren ten behoeve van het register van Enisa. Deze informatie (die genoemd staat in artikel 27, tweede lid van de richtlijn) komt in grote mate overeen met de informatie die entiteiten moeten aanleveren als gevolg van artikel 3, derde lid van de richtlijn. In artikel 48 van dit wetsvoorstel is daarom opgenomen dat deze informatie verstrekt moet worden voor zover dit niet al is gedaan op grond van artikel 45.

5.9 Toepassing in Caribisch deel van het Koninkrijk

De NIS2-richtlijn is alleen van toepassing op Europees Nederland. De openbare lichamen Bonaire, Sint-Eustatius en Saba (BES) hebben de zogeheten LGO-status (landen en gebieden overzee, artikel 299, derde lid, en bijlage II van het Verdrag tot oprichting van de Europese Economische Gemeenschap) en maken geen deel uit van de Europese Unie. Nu deze richtlijn wordt geïmplementeerd via een voor Europees Nederland geldende implementatiewet dient in het kader van het principe van 'comply or explain' wel te worden bezien of en hoe dit wetsvoorstel van toepassing moet worden verklaard voor Caribisch Nederland. Hierna wordt toegelicht waarom er op dit moment nog geen wetgeving komt voor Caribisch Nederland vergelijkbaar met dit wetsvoorstel.

De onderwerpen die in de NIS2-richtlijn worden geregeld, zijn op dit moment nog niet uitvoerbaar in Caribisch Nederland voor onder meer de openbare lichamen. Er wordt op dit moment nog uitvoering gegeven aan een aantal randvoorwaarden voor het verhogen van de digitale weerbaarheid op de BES. Zo wordt in het kader van de Veiligheidsstrategie van het Koninkrijk gewerkt aan het in kaart brengen welke processen op de BES mogelijk maatschappelijk ontwrichtende effecten hebben, zodat duidelijk is welke processen betere bescherming behoeven. Daarnaast heeft het kabinet in de Nederlandse Cybersecuritystrategie aangekondigd om te verkennen welke stappen er nodig zijn om de digitale weerbaarheid van de vitale infrastructuur op de BES te verhogen. Het is denkbaar dat vanuit de uitvoering van deze randvoorwaarden in de toekomst (sectorale) wetgeving voortvloeit waarmee de bescherming van bepaalde infrastructuur in Caribisch Nederland tegen digitale risico's wordt gewaarborgd.

6. Verhouding tot hoger recht

6.1 Inleiding

Minister van Justitie en Veiligheid
De Minister van Justitie en Veiligheid is in dit wetsvoorstel aangewezen als:
- het centrale contactpunt;
- de cybercrisisbeheerautoriteit;
- de instantie voor het vaststellen van een nationale cyberbeveiligingsstrategie;
- de instantie voor het vaststellen van een nationaal plan voor grootschalige cyberbeveiligingsincidenten en crisisrespons; en
- de beheerder van een nationaal register van essentiële entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen;
- .

De Minister van Justitie en Veiligheid zal bij het uitoefenen van de taken persoonsgegevens verwerken. Hierbij gaat het bijvoorbeeld om de contactgegevens van de medewerkers van centrale contactpunten van andere lidstaten. Daarnaast kan het gaan om persoonsgegevens die door het CSIRT zijn gestuurd aan het centrale contactpunt in het kader van een bij het CSIRT gedane melding van een significant incident. Ook kan het gaan om het verstrekken van die gegevens aan de centrale contactpunten van andere lidstaten. Meer concreet kan hierbij worden gedacht aan de IP-adressen die zijn betrokken bij een incident.

CSIRT
Het CSIRT heeft krachtens dit wetsvoorstel diverse taken, waaronder het verstrekken van vroegtijdige waarschuwingen en meldingen en het verspreiden van informatie over cyberdreigingen, kwetsbaarheden en incidenten (zie artikel 17, tweede lid, onderdeel b, van dit wetsvoorstel). Ook heeft het CSIRT diverse taken in het kader van meldingen van significante incidenten. Zo moet het CSIRT zulke meldingen in ontvangst nemen, vervolgens een antwoord verstrekken aan de meldende entiteit en, als de entiteit hier om vraagt, ondersteuning bieden (zie artikel 38 van dit wetsvoorstel). Ook moet het CSIRT het centrale contactpunt in kennis stellen van deze meldingen (zie artikel 41, eerste lid, van dit wetsvoorstel). Verder fungeert één CSIRT als de coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden. Die coördinator heeft onder meer de taak om de bij gemelde kwetsbaarheden betrokken entiteiten te identificeren en om contact met hen op te nemen (zie artikel 18, tweede lid, onderdeel b, van dit wetsvoorstel). De werkzaamheden van het CSIRT houden niet op bij de landsgrenzen; het CSIRT kan in het kader van een samenwerkingsrelatie met een CSIRT van een derde land relevante informatie, met inbegrip van persoonsgegevens, uitwisselen (zie artikel 55, eerste lid, van dit wetsvoorstel).

Het CSIRT zal als gevolg van dit wetsvoorstel de beschikking krijgen over aanzienlijke hoeveelheden data, waaronder informatie die entiteiten verstrekken bij meldingen van significante incidenten. Meer concreet gaat het in elk geval om de contactgegevens van de medewerker die namens een entiteit een melding doet.

Bevoegde autoriteit
In dit wetsvoorstel worden de vakministers aangewezen als bevoegde autoriteit voor de onderscheidene sectoren (artikel 16). De bevoegde autoriteit heeft krachtens dit wetsvoorstel diverse taken. Naast de taak om te zorgen voor de bestuursrechtelijke handhaving van het bepaalde bij of krachtens deze wet, heeft de bevoegde autoriteit ook taken op het gebied van meldingen van significante incidenten, zoals het in ontvangst nemen daarvan (significante incidenten moeten zowel aan de bevoegde autoriteit als aan het CSIRT worden gemeld) en het daarover informeren van de bevoegde autoriteit, bedoeld in de Wwke. De bevoegde autoriteit zal bij de uitoefening van haar taken de beschikking krijgen over persoonsgegevens. Naar verwachting zal het daarbij in hoofdzaak gaan over de contactgegevens, zoals e-mailadressen, van medewerkers van essentiële entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen. Vooropgesteld wordt dat het voor de bevoegde autoriteit, met het oog op de uitoefening van de taken op grond van dit wetsvoorstel, niet nodig is om over bijzondere persoonsgegevens te beschikken. Mocht de bevoegde autoriteit deze desondanks ontvangen, dan zal zij die gegevens onmiddellijk vernietigen.

6.2 Inmenging door openbaar gezag in recht op respect voor de persoonlijke levenssfeer

De verwerking van persoonsgegevens door de Minister van Justitie en Veiligheid, het CSIRT en de bevoegde autoriteit is een inmenging door het openbaar gezag in het recht op respect voor de persoonlijke levenssfeer. Dit recht is gecodificeerd in de artikelen 10 van de Grondwet, 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM), 17 van het Internationaal Verdrag inzake burgerrechten en politieke rechten (IVBPR) en 7 van het Handvest van de grondrechten van de Europese Unie (Handvest). Artikel 8 van het Handvest ziet specifiek op het recht van eenieder op de bescherming van zijn persoonsgegevens.

Artikel 8, eerste lid, EVRM bepaalt dat eenieder recht heeft op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. Het tweede lid van dat artikel staat inmenging in dit recht alleen toe voor zover die inmenging bij wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen. Het noodzaakcriterium wordt in de jurisprudentie van het Europese Hof voor de rechten van de mens (EHRM) nader ingevuld met de vereisten van een dringende maatschappelijke behoefte, proportionaliteit en subsidiariteit. Dit wetsvoorstel is aan deze beginselen getoetst. Die toetsing wordt hieronder besproken. Dit wetsvoorstel is ook getoetst aan de artikelen 10 Grondwet, 17 IVBPR en 7 en 8 Handvest. Die toetsing leidt niet tot andere gezichtspunten.

6.2.1 Beperkende maatregel moet voorzien bij wet zijn

Dit wetsvoorstel bevat specifieke wettelijke grondslagen voor de verwerking van persoonsgegevens door de Minister van Justitie en Veiligheid (als het centrale contactpunt en beheerder van het nationale register), het CSIRT en de bevoegde autoriteit, zie onder meer de artikelen 52, 53, 56, 57 en 59 van dit wetsvoorstel. Daarnaast bevat dit wetsvoorstel een specifieke wettelijke grondslag voor de verwerking van bijzondere persoonsgegevens door het CSIRT (artikel 64a).

6.2.2 Beperking moet legitiem doel dienen en noodzakelijk zijn

Artikel 8, tweede lid, EVRM bepaalt dat inmenging in het recht op respect voor het privéleven uitsluitend is toegestaan binnen de kaders van de expliciet en limitatief in dat lid opgesomde belangen: de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

De verwerking van persoonsgegevens door de Minister van Justitie en Veiligheid (als het centrale contactpunt en beheerder van het nationale register), het CSIRT en de bevoegde autoriteit dient ter uitvoering van hun taken uit dit wetsvoorstel, die volgen uit de NIS2-richtlijn. Deze taken hebben primair tot doel om cyberrisico's te beheersen, incidenten te voorkomen, gevolgen van incidenten te

beperken en om informatie over incidenten, bijna-incidenten, cyberdreigingen en kwetsbaarheden te verkrijgen en te verstrekken. Door persoonsgegevens te verwerken, kunnen ernstige verstoringen van essentiële diensten, met als gevolg ernstige maatschappelijke ontwrichting, worden voorkomen. Deze verwerkingen dienen dus onder meer de nationale veiligheid, de openbare veiligheid en het economisch welzijn van het land. Deze belangen zijn genoemd in artikel 8, tweede lid, EVRM.

De beperking dient bovendien noodzakelijk te zijn in een democratische samenleving. Het noodzaakcriterium wordt in de jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM) nader ingevuld met de vereisten van: 1. een dringende maatschappelijke behoefte; 2. proportionaliteit; en 3. subsidiariteit. Deze vereisten worden in de hiernavolgende paragrafen nader behandeld. Staten moeten redenen aandragen die voldoende en relevant zijn en hebben daarbij een eigen beoordelingsruimte.

6.2.2.1 Dringende maatschappelijke behoefte

Inleiding
De dringende maatschappelijke behoefte van de verwerking van persoonsgegevens door de Minister van Justitie en Veiligheid, het CSIRT en de bevoegde autoriteit is gelegen in de grote afhankelijkheid van de samenleving van elektronische beveiligings- en informatiesystemen, die bovendien onderling verweven zijn en niet ophouden bij de landsgrenzen. Deze systemen spelen een grote rol in de verlening van essentiële diensten. Het waarborgen van de continuïteit van die essentiële dienstverlening is van groot belang om maatschappelijke ontwrichting te voorkomen. Door het verwerken van persoonsgegevens, waaronder de verwerking door het CSIRT die nodig is in het kader van cyberincidenten, kan grote maatschappelijke ontwrichting worden voorkomen.

Minister van Justitie en Veiligheid
Ter bevordering van de grensoverschrijdende samenwerking is het nodig dat iedere lidstaat een centraal contactpunt aanwijst dat verantwoordelijk is voor het leggen van verbindingen voor de samenwerking op het niveau van de Europese Unie, en meer in het bijzonder het informeren van andere lidstaten in geval van incidenten met grensoverschrijdende consequenties. In Nederland is de Minister van Justitie en Veiligheid aangewezen als het centrale contactpunt. Om de taken van het centrale contactpunt uit te kunnen voeren is het nodig dat het contactpunt persoonsgegevens verwerkt. Het kan hierbij gaan om informatie uit meldingen die worden doorgegeven aan andere lidstaten om hen in staat te stellen adequaat te reageren op grensoverschrijdende meldingen (denk bijvoorbeeld aan het IP-adres van een aanvaller) en het spiegelbeeld daarvan (informatie die het centrale contactpunt ontvangt van andere centrale contactpunten), maar ook om bijvoorbeeld contactgegevens van medewerkers van andere centrale contactpunten.

CSIRT
Zoals ook uit de huidige praktijk van het NCSC blijkt, zullen IP-adressen door het CSIRT worden verwerkt om de aard en ernst van digitale dreigingen en incidenten te kunnen beoordelen en om entiteiten te kunnen waarschuwen en bijstaan. Enerzijds zal het CSIRT de gegevens die deel uitmaken van een incidentmelding onderzoeken om te achterhalen vanaf welke IP-adressen een digitale aanval wordt uitgevoerd. Die IP-adressen worden binnen de kaders van dit wetsvoorstel verstrekt aan derden om hen in staat te stellen maatregelen te nemen tegen (mogelijke) aanvallen vanaf die adressen. Anderzijds zal het CSIRT onderzoeken of de bij het CSIRT bekende IP-adressen van entiteiten getroffen of kwetsbaar zijn en waarschuwt het CSIRT zo nodig de betrokken entiteiten.
E-mailadressen zullen door het CSIRT worden verwerkt om derden te kunnen waarschuwen. Zo kan het voorkomen dat een door het CSIRT ontvangen dataset e-mailadressen bevat die zijn buitgemaakt bij een ICT-inbreuk. Deze e-mailadressen kunnen voor malafide doeleinden gebruikt worden, zoals het versturen van spam, of kunnen – doordat zij betrokken zijn bij een ICT-inbreuk – een kwetsbaarheid vormen voor de organisatie waartoe zij behoren. Ook hierover kan het CSIRT relevante partijen binnen de kaders van dit wetsvoorstel informeren, opdat deze partijen maatregelen kunnen nemen om de beschikbaarheid of betrouwbaarheid van hun netwerk- en informatiesystemen te waarborgen. Verder zal het CSIRT de e-mailadressen van melders en andere contactpersonen van onder meer aanbieders van producten en diensten verwerken. Deze informatie is noodzakelijk om gevolg te

kunnen geven aan een melding, het waarschuwen van anderszins gebleken betrokkenheid bij een ICT-inbreuk, of het informeren en adviseren over gebleken digitale dreigingen of kwetsbaarheden. Domeinnamen kunnen door het CSIRT worden verwerkt als het bij een melding informatie krijgt over kwetsbaarheden in websites. Om de digitale weerbaarheid van de Nederlandse samenleving te verhogen en nadelige maatschappelijke gevolgen te beperken of voorkomen is het van belang dat het CSIRT ook deze informatie kan analyseren en binnen de kaders van dit wetsvoorstel kan delen met de juiste organisaties.

Bevoegde autoriteit
De verwerking van gegevens door de bevoegde autoriteit in het kader van de handhaving op de verplichtingen uit dit wetsvoorstel is van belang om de hiervoor genoemde effectieve maatregelen te verzekeren. Om te kunnen handhaven, zal de bevoegde autoriteit persoonsgegevens moeten verwerken. Het gaat hierbij in hoofdzaak om contactgegevens van de contactpersonen voor de bevoegde autoriteit bij de entiteiten waarop toezicht wordt gehouden.

6.2.2.2 Proportionaliteit

Minister van Justitie en Veiligheid
De Minister van Justitie en Veiligheid zal bij het uitoefenen van de taken van het centrale contactpunt en bij het beheer van het nationale register persoonsgegevens verwerken.
Voor wat betreft de taken van het centrale contactpunt kan het gaan om het *ontvangen* van persoonsgegevens. Bijvoorbeeld de persoonsgegevens die door het CSIRT zijn gestuurd aan het centrale contactpunt in het kader van een bij het CSIRT gedane melding van een significant incident. Een ander voorbeeld betreft de ontvangst van gegevens, waaronder persoonsgegevens, van de centrale contactpunten van andere lidstaten, zoals de contactgegevens van de medewerkers van die contactpunten. Bij die ontvangen persoonsgegevens zal de Minister van Justitie en Veiligheid telkens bekijken of het, met het oog op de voor het centrale contactpunt in dit wetsvoorstel opgenomen taken, nodig is die te bewaren, en zo ja, voor hoe lang.
Voor wat betreft de taken van het centrale contactpunt kan het ook gaan om het *verstrekken* van persoonsgegevens. Hierbij valt te denken aan het verstrekken van die gegevens aan de centrale contactpunten van andere lidstaten. Meer concreet kan hierbij worden gedacht aan de IP-adressen die zijn betrokken bij een incident. De Minister van Justitie en Veiligheid zal telkens de afweging maken of het nodig is om persoonsgegevens mee te sturen.
Voor wat betreft het nationale register van entiteiten gaat het om een dwingende verplichting uit de NIS2-richtlijn voor lidstaten om een dergelijk register (in de richtlijn genoemd: een lijst van entiteiten) tot stand te laten komen, te beheren, te evalueren en indien nodig aan te passen. Het nationale register bevat naast de naam van de entiteit ook het adres en de actuele contactgegevens van de entiteit, met inbegrip van e-mailadressen, IP-bereiken en telefoonnummers. De Minister van Justitie en Veiligheid zal deze gegevens alleen verwerken ten behoeve van (de opname in) het nationale register.

CSIRT
Het CSIRT zal naar verwachting persoonsgegevens verwerken. Deze verwachting is gebaseerd op de huidige praktijk van het NCSC. Gelet op de aard van die gegevens (bijvoorbeeld e-mailadressen en contactgegevens van melders), het doel waarvoor zij worden verwerkt en de overige waarborgen waarmee de verwerking van deze gegevens is omkleed, gaat het niet om een forse inmenging in het recht op respect voor iemands privéleven. Het CSIRT moet de betrokken gegevens verwerken met inachtneming van de Avg. Bovendien staat het CSIRT voor wat betreft de verwerking van persoonsgegevens onder intern toezicht van de functionaris gegevensbescherming en onder extern toezicht van de Autoriteit Persoonsgegevens.

Het CSIRT verwerkt slechts gegevens voor zover dat noodzakelijk is voor het uitvoeren van de in dit wetsvoorstel genoemde taken van het CSIRT. Het monitoren en analyseren van cyberdreigingen, kwetsbaarheden en incidenten (artikel 17, tweede lid, onderdeel a, van dit wetsvoorstel) behoren alleen tot de taken van het CSIRT als die werkzaamheden in dienst staan van de taken van het CSIRT om bijstand te verlenen aan betrokken entiteiten of om deze entiteiten te informeren en te adviseren. Het is dus geen taak van het CSIRT om onderzoek te doen naar personen of organisaties die

verantwoordelijk zijn voor die dreigingen en incidenten met het oog op het verzamelen van bewijsmiddelen tegen individuen of organisaties. Dergelijk onderzoek is voorbehouden aan de inlichtingen- en veiligheidsdiensten, die daartoe beschikken over wettelijk geregelde bijzondere inlichtingenmiddelen, en aan de politie en het Openbaar Ministerie, die daartoe beschikken over opsporingsbevoegdheden.

Persoonsgegevens die het CSIRT verwerkt ten behoeve van zijn taken worden bovendien niet langer door het CSIRT bewaard dan noodzakelijk. Zo worden contactgegevens van de melder van een significant incident, incident, bijna-incident of cyberdreiging na het afhandelen van de melding vernietigd en worden andere persoonsgegevens, die benodigd zijn voor de uitoefening van de taken van het CSIRT, na het afhandelen van een incident, bijna-incident of dreiging vernietigd. Dit is gebaseerd op hoeveel tijd het NCSC in de huidige praktijk nodig heeft om zijn taken naar behoren te kunnen vervullen. Zo moet ook na enige tijd nog contact kunnen worden gezocht met de melder, bijvoorbeeld voor opvolging of om de melder te waarschuwen voor kwetsbaarheden die zijn systeem opnieuw in gevaar kunnen brengen.

Andere persoonsgegevens kunnen van belang zijn als bijvoorbeeld blijkt dat een bepaald IP-adres opnieuw geraakt wordt of een digitale aanval steeds vanuit dezelfde hoek komt. Dit kan voor het CSIRT aanleiding zijn om te onderzoeken of de aanval ook relevant is voor andere recent getroffen IP-adressen. Ook kan uit nieuw onderzoek van een afgehandeld incident blijken dat relevante informatie, zoals een kwetsbaarheid van bepaalde IP-adressen of een bepaalde aanvalstechniek, over het hoofd is gezien. De bewaartermijnen zullen geregeld opnieuw worden beoordeeld en zullen dan zo mogelijk worden verkort en zo nodig worden verlengd. Overigens komen de huidige door het NCSC gehanteerde bewaartermijnen komen overeen met de internationaal door CERT's gehanteerde termijnen.

Bevoegde autoriteit
De bevoegde autoriteit zal bij de uitoefening van haar taken uit dit wetsvoorstel de beschikking krijgen over persoonsgegevens. Naar verwachting zal het daarbij in hoofdzaak gaan over de contactgegevens, zoals e-mailadressen, van medewerkers van essentiële entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen, die onder het toezicht van de bevoegde autoriteit staan en aldaar significante incidenten moeten melden. De bevoegde autoriteit verwerkt deze persoonsgegevens alleen voor zover dit noodzakelijk is voor het uitoefenen van de in dit wetsvoorstel genoemde taken. De persoonsgegevens die de bevoegde autoriteit verwerkt ten behoeve van haar taken worden niet langer bewaard dan noodzakelijk. Ook de bevoegde autoriteit staat voor wat betreft de verwerking van persoonsgegevens onder toezicht van de Autoriteit persoonsgegevens.

6.2.2.3 Subsidiariteit

Minister van Justitie en Veiligheid
De Minister van Justitie en Veiligheid kan de taken van het centrale contactpunt niet uitvoeren zonder de verwerking van de persoonsgegevens die nodig zijn om contact te leggen met de centrale contactpunten van andere lidstaten. Dit geldt ook voor het doorsturen van meldingen van incidenten, inclusief de daarvan deel uitmakende persoonsgegevens, aan de centrale contactpunten van andere getroffen lidstaten. Dit is gebleken in de huidige praktijk van het centrale contactpunt onder de Wbni. Voor wat betreft het nationale register van entiteiten gaat het om een dwingende verplichting uit artikel 3, derde en vierde lid, NIS2-richtlijn voor lidstaten om een dergelijk register (in de richtlijn genoemd: een lijst van entiteiten) tot stand te laten komen, te beheren, te evalueren en indien nodig aan te passen. Uit artikel 3, vierde lid, NIS2-richtlijn volgt uit welke gegevens het nationale register in elk geval moet bestaan. Het nationale register moet naast de naam van de entiteit ook het adres en de actuele contactgegevens van de entiteit bevatten, met inbegrip van e-mailadressen, IP-bereiken en telefoonnummers.

CSIRT
Het is de verwachting dat de verwerking van persoonsgegevens door andere CSIRT's dan het NCSC in belangrijke mate vergelijkbaar zal zijn met de huidige verwerkingen van persoonsgegevens door het NCSC. Zoals ook uit de huidige praktijk van het NCSC is gebleken, kan het CSIRT zijn taken niet

uitoefenen wanneer het niet zou beschikken over de persoonsgegevens die deel uitmaken van datasets die het CSIRT verkrijgt bij de melding van een incident. Het CSIRT kan niet op een andere wijze de informatie verkrijgen die noodzakelijk is voor het uitoefenen van zijn taken. Ook anonimiseren of pseudonimiseren (vervangen, met een bepaald algoritme, van identificerende gegevens door versleutelde gegevens) van de data is voor het CSIRT niet mogelijk: als de data niet individualiseerbaar zijn, dan kan het CSIRT niet onderzoeken welke partijen zijn geraakt en hen rechtstreeks informeren. Ook kan het CSIRT niet de herkomst en het verdere verloop van de dreiging of het incident onderzoeken.

Bevoegde autoriteit
Voor de bevoegde autoriteit geldt dat zij haar toezichtstaken niet kan uitoefenen zonder de verwerking van de persoonsgegevens die nodig zijn om contact te leggen met de entiteiten waarop zij toezicht houdt.

6.3 Algemene verordening gegevensbescherming

De verwerking van persoonsgegevens door de Minister van Justitie en Veiligheid, het CSIRT en de bevoegde autoriteit moet in overeenstemming zijn met de Avg, meer in het bijzonder de artikelen 5 (beginselen inzake verwerking van persoonsgegevens) en 6 (rechtmatigheid van de verwerking) van de Avg. In deze paragraaf volgt een toetsing aan deze artikelen uit de Avg.

6.3.1 Rechtmatigheid, behoorlijkheid en transparantie

In artikel 5, eerste lid, onderdeel a, Avg is bepaald dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is.

Rechtmatigheid
Artikel 6, eerste lid, Avg moet worden beschouwd als de uitwerking en nadere invulling van het beginsel van rechtmatigheid zoals genoemd in artikel 5, eerste lid, onderdeel a, Avg. Deze eerstgenoemde bepaling richt zich tot de verwerkingsverantwoordelijke en geeft de voorwaarden voor de rechtmatigheid van een verwerking. Voor de verwerkingen van persoonsgegevens door de Minister van Justitie en Veiligheid, het CSIRT en de bevoegde autoriteit kan de grondslag worden gevonden in artikel 6, eerste lid, onderdeel c, Avg. Die verwerkingen zijn immers noodzakelijk om te voldoen aan een wettelijke verplichting die op deze verwerkingsverantwoordelijken rust. Voorts kan ook de grondslag worden gevonden in artikel 6, eerste lid, onderdeel e, Avg, omdat deze verwerkingen noodzakelijk zijn voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen.

Behoorlijkheid/transparantie
Het vereiste van behoorlijkheid houdt in dat een betrokkene op de hoogte moet (kunnen) zijn van de verwerking van zijn persoonsgegevens, inclusief de wijze waarop deze gegevens worden verwerkt verzameld, bewaard en gebruikt. Hierop zijn een aantal uitzonderingen, zie de artikelen 13 en 14 Avg. Het CSIRT en de bevoegde autoriteit zullen – gelet op de dubbele meldplicht – vaak de gegevens rechtstreeks van betrokkene zelf ontvangen. Dit geldt ook voor de gegevens van de medewerkers van de centrale contactpunten van andere lidstaten, die door deze contactpunten worden verzonden aan het Nederlandse centrale contactpunt (de Minister van Justitie en Veiligheid). Daarmee zijn deze betrokkenen op de hoogte van de verwerking en wordt voldaan aan het beginsel van behoorlijkheid. Er kan ook sprake zijn van de verwerking van persoonsgegevens die niet door de betrokkene zelf zijn verstrekt. In dergelijke gevallen geldt dat de verwerkingen van persoonsgegevens uitdrukkelijk zijn voorgeschreven in het onderhavige wetsvoorstel en dat in het wetsvoorstel voldoende waarborgen zijn opgenomen ter bescherming van de belangen van de betrokkene.

Transparantie kent verschillende vormen. Enerzijds houdt dit in dat het verwerkingsproces transparant is. Anderzijds houdt dit principe verband met het eerder besproken element van behoorlijkheid waardoor mensen wiens persoonsgegevens worden verwerkt dit kunnen weten. Het proces van de verwerking van persoonsgegevens zal door de Minister van Justitie en Veiligheid (als centrale contactpunt en beheerder van het nationale register), het CSIRT en de bevoegde autoriteit in

samenspraak met de functionaris gegevensbescherming worden ingericht. Daarmee wordt voldaan aan het element van transparantie. Het wetsvoorstel voorziet in de wettelijke verplichting voor het CSIRT dan wel de bevoegde autoriteit om het publiek te (laten) informeren over significante incidenten, waardoor door dat incident getroffenen weten dat op hen betrekking hebbende persoonsgegevens kunnen zijn verwerkt.

6.3.2 Doelbinding

In artikel 5, eerste lid, onderdeel b, Avg is bepaald dat persoonsgegevens worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en vervolgens niet verder op een met die doeleinden onverenigbare wijze mogen worden verwerkt. Dit betreft het zogeheten doelbindingsbeginsel.

De verwerking van persoonsgegevens in het kader van dit wetsvoorstel geschiedt in het kader van de in dit wetsvoorstel opgenomen doelen. De algemene doelen van dit wetsvoorstel zijn opgenomen in artikel 2. In de diverse artikelen in dit wetsvoorstel waarin de grondslag is geregeld voor het centrale contactpunt, het CSIRT en de bevoegde autoriteit om gegevens, waaronder persoonsgegevens, uit te wisselen zijn ook de doelen van die gegevensverwerking omschreven. Zie bijvoorbeeld artikel 52 van dit wetsvoorstel, waarin is bepaald dat de bevoegde autoriteit, het CSIRT en het centrale contactpunt met elkaar samen werken voor de doeltreffende en doelmatige uitoefening van hun taken uit hoofde van dit wetsvoorstel en daartoe onderling alle daarvoor benodigde gegevens uitwisselen, waaronder persoonsgegevens.

6.3.3 Minimale gegevensverwerking

In artikel 5, eerste lid, onderdeel c, Avg is bepaald dat persoonsgegevens toereikend moeten zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Voor de bespreking hiervan wordt verwezen naar paragraaf 6.2.2, waarin is ingegaan op de dringende maatschappelijke behoefte voor de verwerking van persoonsgegevens en de noodzaak van die verwerking.

6.3.4 Juistheid

In artikel 5, eerste lid, onderdeel d, Avg is bepaald dat persoonsgegevens juist moeten zijn en zo nodig moeten worden geactualiseerd. Ook is hierin bepaald dat alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren.

Het CSIRT, de bevoegde autoriteit en de Minister van Justitie en Veiligheid (als centrale contactpunt en beheerder van het nationale register) moeten dus passende maatregelen nemen om de juistheid van de gegevens te borgen. Dit betekent dat er processen en procedures uitgewerkt moeten worden om fouten bij het verkrijgen van de gegevens te voorkomen en om de gegevens met enige regelmaat te controleren. Deze processen en procedures worden door de Minister van Justitie en Veiligheid, het CSIRT en de bevoegde autoriteit in samenspraak met de functionaris gegevensbescherming opgesteld.

6.3.5 Opslagbeperking

In artikel 5, eerste lid, onderdeel e, Avg is bepaald dat persoonsgegevens moeten worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan noodzakelijk is voor de doeleinden waarvoor de persoonsgegevens worden verwerkt. Ten aanzien van de bewaartermijnen wordt verwezen naar paragraaf 6.2.2.2.

6.3.6 Integriteit en vertrouwelijkheid

In artikel 5, eerste lid, onderdeel f, Avg is bepaald dat persoonsgegevens door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier moeten worden verwerkt dat een passende beveiliging ervan gewaarborgd is en dat zij onder meer beschermd moeten

zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. De Minister van Justitie en Veiligheid (als centrale contactpunt en beheerder van het nationale register), het CSIRT en de bevoegde autoriteit hebben allemaal een passend beveiligingsbeleid om de integriteit en vertrouwelijkheid van de persoonsgegevens te borgen. Voor de minister geldt in het bijzonder dat het ook een essentiële entiteit in de zin van dit wetsvoorstel is en als gevolg daarvan moet voldoen aan de in dit wetsvoorstel opgenomen zorgplicht.

6.3.7 Verantwoordingsplicht

In artikel 5, tweede lid, Avg is bepaald dat de verwerkingsverantwoordelijke verantwoordelijk is voor de naleving van artikel 5, eerste lid, Avg en deze kan aantonen. Voor de Minister van Justitie en Veiligheid (als centrale contactpunt en beheerder van het nationale register), het CSIRT en de bevoegde autoriteit betekent dit dat zij intern aan de functionaris gegevensbescherming en extern aan de Autoriteit persoonsgegevens moeten kunnen verantwoorden dat persoonsgegevens overeenkomstig de Avg zijn verwerkt.

6.4 Verwerking bijzondere persoonsgegevens

Dit wetsvoorstel bevat in artikel 64a ook een grondslag voor het CSIRT en de Bevoegde Autoriteit voor de verwerking van bijzondere persoonsgegevens. Dit is noodzakelijk gelet op de in artikel 9, tweede lid, onderdeel g, van de AVG genoemde redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene.

Verwerking bijzondere persoonsgegevens door het CSIRT

In dit geval volgen de redenen voor de verwerking van bijzondere persoonsgegevens door het CSIRT uit het Unierecht, namelijk de NIS2-richtlijn en de daarin genoemde taken voor het CSIRT. Het CSIRT zal bij de uitoefening van haar taken de beschikking krijgen over aanzienlijke hoeveelheden data. Het is niet op voorhand duidelijk welk soort informatie of wat voor soort gegevens onderdeel uitmaken van die data. In die data kunnen ook bijzondere persoonsgegevens zitten. Een dataset kan bijvoorbeeld inloggegevens (credentials) bevatten waarin ook mailadressen zitten waaruit het lidmaatschap van een vakbond of politieke partij blijkt. Daarnaast kan het bijvoorbeeld voorkomen dat een server van een zorginstelling of een gemeente op het internet staat die medische of andere bijzondere persoonsgegevens bevat. Een analyse van of onderzoek naar deze gegevens in geanonimiseerde of gepseudonimiseerde vorm is niet in alle gevallen mogelijk. Voor de uitoefening van haar taken op grond van deze wet is het in die gevallen noodzakelijk dat het CSIRT bijzondere persoonsgegevens kan verzamelen en dus verwerken als bedoeld in de Avg.

Voor de verwerking van bijzondere persoonsgegevens geldt dat indien verwerking op grond van de AVG is toegestaan, passende en specifieke maatregelen moeten worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene. Deze passende en specifieke maatregelen bestaan uit het opnemen van een bewaartermijn. Het CSIRT zal daarnaast bij de opslag van bijzondere persoonsgegevens beveiligingsmaatregelen zoals encryptie, need-to-know en een geheimhoudingsplicht in acht nemen. In het tweede lid van artikel 64a van deze wet is geregeld dat bij algemene maatregel van bestuur nadere regels kunnen worden gesteld over de verwerking van bijzondere persoonsgegevens. Daarbij zal onder meer aandacht worden besteed aan de bewaartermijn van deze gegevens.

Verwerking bijzondere persoonsgegevens door bevoegde autoriteit

De redenen voor de verwerking van bijzondere persoonsgegevens door de bevoegde autoriteit volgen eveneens uit het Unierecht, namelijk de NIS2-richtlijn en de daarin genoemde taken voor de bevoegde autoriteit. Bij het doen van bijvoorbeeld technisch onderzoek kan het voorkomen dat de bevoegde autoriteit de beschikking krijgt over bijzondere persoonsgegevens. Dit komt met name voor in de

zorgsector, omdat in deze sector vooral met gezondheidsgegevens van patiënten wordt gewerkt. Het is ook mogelijk dat de bevoegde autoriteit bijzondere persoonsgegevens verwerkt om vast te stellen welke gegevens in geval van een incidenten door onbevoegden zijn geraadpleegd en wat de aard van die gegevens was, en of hieruit eventuele schade zou kunnen volgen. Het is niet altijd mogelijk om deze taken uit te voeren als de desbetreffende bijzondere persoonsgegevens zijn geanonimiseerd of gepseudonimiseerd. In die gevallen moet de bevoegde autoriteit daarom bijzondere persoonsgegevens verder kunnen verwerken. Indien deze gegevens niet nodig zijn voor de uitvoering van de taken van de bevoegde autoriteit, dan worden deze gegevens vernietigd. Voor de verwerking van bijzondere persoonsgegevens geldt dat indien verwerking op grond van de Avg is toegestaan, passende en specifieke maatregelen moeten worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene. Deze passende en specifieke maatregelen bestaan uit het opnemen van een bewaartermijn. De bevoegde autoriteit zal daarnaast bij de opslag van bijzondere persoonsgegevens beveiligingsmaatregelen zoals encryptie, need-to-know en een geheimhoudingsplicht in acht nemen. In het tweede lid van artikel 64a van deze wet is geregeld dat bij algemene maatregel van bestuur nadere regels kunnen worden gesteld over de verwerking van bijzondere persoonsgegevens. Daarbij zal onder meer aandacht worden besteed aan de bewaartermijn van deze gegevens.

7. Verhouding tot nationale regelgeving

In deze paragraaf wordt beschreven welke verplichtingen er op grond van nationale wetgeving reeds gelden voor specifieke sectoren en wordt bezien hoe die verplichtingen zich verhouden tot de verplichtingen uit de NIS2-richtlijn. Daarbij wordt de wetgeving per ministerie bekeken.

7.1 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

De NIS-richtlijn (2016/1148) is geïmplementeerd in de Wbni. In artikel 20, zevende lid, Wbni is voor de implementatie van artikel 1, vierde lid, van de NIS-richtlijn (2016/1148) een uitzondering op de Woo opgenomen in verband met vertrouwelijke gegevens. Deze uitzondering komt ook terug in de implementatie van artikel 2, dertiende lid, NIS2-richtlijn. De Wbni komt te vervallen met de inwerkingtreding van de Cbw. Daarom wordt in de bijlage bij artikel 8.8 Woo in de plaats van een verwijzing naar de Wbni een verwijzing naar de Cbw opgenomen.

7.2 Ministerie van Economische Zaken en Klimaat

Wet bevordering digitale weerbaarheid van bedrijven
Het voorstel van wet, houdende regels ter bevordering van de digitale weerbaarheid van bedrijven is op 19 maart 2024 aangenomen door de Tweede Kamer (kamerstukken II 2022/23, 36 270). Dit wetsvoorstel legt de taken en bevoegdheden van de Minister van Economische Zaken en Klimaat (hierna: Minister van EZK) op het gebied van de verbetering van de digitale weerbaarheid van het niet-vitale bedrijfsleven in Nederland vast. De taken zijn onder meer: het verwerken en verspreiden van informatie over kwetsbaarheden, dreigingen en incidenten te aan bedrijven en het samenwerken met andere bestuursorganen en organisaties op het gebied van digitale weerbaarheid. Tevens regelt dit wetsvoorstel een rechtstreekse informatie-uitwisseling tussen overheidsorganisaties die zich bezighouden met digitale beveiliging bezighouden - namelijk het NCSC en het Computer Security Incident Response Team (CSIRT) voor digitale diensten op grond van de Wet beveiliging netwerk- en informatiesystemen met de minister van EZK op grond van dat wetsvoorstel. Ten slotte, voorziet het wetsvoorstel in de voorwaarden waaronder vertrouwelijke gegevens die bij de Minister van EZK berusten, verstrekt mogen worden aan derden.
Vanwege de verwevenheid van het bovengenoemd wetsvoorstel met de Wbni en de NIS2-richtlijn, dient het wetsvoorstel nadat het tot de wet is verheven te worden aangepast aan de NIS2-richtlijn. Daarbij zal het uitgangspunt zijn om zoveel mogelijk het bestaand beleid beleidsneutraal om te zetten en de informatiepositie van de Minister van EZK ter uitvoering van de taken en bevoegdheden die het wetsvoorstel bevordering digitale weerbaarheid bedrijven aan haar toekent, te behouden.

Post
Voor belangrijke entiteiten in de sector post zijn er in de op hen van toepassing zijnde wetgeving (Postwet 2009) geen zorgplicht, meldplicht of andere met dit wetsvoorstel soortgelijke verplichtingen geregeld. Er is dus geen sprake van botsende verplichtingen.

Energie
Dit wetsvoorstel voorziet in een meldplicht en beveiligingsverplichting op het gebied van cybersecurity. Op de entiteiten uit de sector energie, subsector elektriciteit en gas, zijn de Elektriciteitswet 1998 en de Gaswet van toepassing. De Elektriciteitswet 1998 (artikel 16, eerste lid, onderdeel q) en de Gaswet (artikel 10, negende lid) bevatten de taak voor netbeheerders om hun netten te beschermen tegen invloeden van buitenaf. Cybersecurity is daar onderdeel van. De zorgplicht die dit wetsvoorstel regelt en de uitwerking daarvan bij algemene maatregel van bestuur kunnen gezien worden als instructie aan de netbeheerders hoe zij op het gebied van cybersecurity invulling geven aan hun taak op grond van de Elektriciteitswet 1998 en de Gaswet. Een meldplicht op het punt van cybersecurity is niet geregeld in deze wetten. Er is dus geen sprake van botsende verplichtingen.

Voor de subsectoren olie en warmte zijn er op dit moment geen sectorspecifieke wetten.

Ruimtevaart
Dit wetsvoorstel voorziet in een meldplicht en zorgplicht op het gebied van cybersecurity. Entiteiten waarop de Wet ruimtevaartactiviteiten van toepassing is, zullen in principe ook onder de sector ruimtevaart van dit wetsvoorstel vallen. De Wet ruimtevaartactiviteiten (artikel 10, tweede lid) bevat de verplichting voor vergunninghouders om een voorval dat gevaar kan opleveren voor de veiligheid van personen en goederen, de bescherming van het milieu in de ruimte, de bescherming van de openbare orde of de veiligheid van de staat, of anderszins schade kan opleveren, te melden aan de minister. De meldplicht die dit wetsvoorstel regelt staat deze verplichting niet in de weg. Zij leidt er slechts toe dat in bepaalde gevallen zal moeten worden gemeld aan het CSIRT en de toezichthoudende instantie onder dit wetsvoorstel.

Een zorgplicht op het punt van cybersecurity is niet geregeld in de Wet ruimtevaartactiviteiten. Wel bepaalt artikel 3, derde lid, van de Wet ruimtevaartactiviteiten dat aan een vergunningvoorschriften en beperkingen kunnen worden verbonden met het oog op veiligheid van personen en goederen, bescherming van het milieu in de kosmetisch ruimte, financiële zekerheid, bescherming van de openbare orde, veiligheid van de staat en het kunnen voldoen aan de internationale verplichtingen van de staat. Deze aan een vergunning verbonden voorschriften en beperkingen kunnen entiteiten helpen in het voldoen aan de zorgplicht uit dit wetsvoorstel.

7.3 Ministerie van Financiën

Voor de financiële sector geldt een lex specialis: de Verordening digitale operationele weerbaarheid. Deze verordening is nader toegelicht in paragraaf 2.5.

7.4 Ministerie van Infrastructuur en Waterstaat

Luchtvaart, scheepvaart, spoor en weg
Voor de vervoerssector is er geen sprake van botsing van bestaande wetgeving met de uit de NIS2-richtlijn voortvloeiende verplichtingen.

Drinkwater
De EU-Drinkwaterrichtlijn (2020/2184/EU) verplicht tot een all hazard-risicoanalyse en tot risicobeheer, (herstel)maatregelen, meldingen bij verstoringen en informatieplichten aan het publiek. De NIS1-richtlijn bevatte een zorgplicht specifiek voor cybersecurity, met een (herstel)maatregelplicht en meldings- en informatieplichten. De samenloop van de NIS1-richtlijn en de Drinkwaterrichtlijn is niet verder geregeld in de nationale wet, omdat deze beperkt is tot cybersecurity en omdat aan de verplichtingen op uitvoeringsniveau op een geïntegreerde en samenhangende wijze uitvoering kon

worden gegeven (door toepassing van een eigen procesautomatiseringsnorm en integratie in het toezicht door de eigenaar, de verstoringsrisicoanalyse en de verstoringsparagraaf van het leveringsplan).

De NIS2-richtlijn kent een all hazard-karakter, en treedt naar de opvatting van de regering niet terug voor de Drinkwaterrichtlijn, omdat deze laatste geen specifieke eisen kent voor cyberbeveiliging. De verplichtingen uit de NIS2-richtlijn zijn dus van toepassing naast die van de Drinkwaterrichtlijn. Het is daarom zaak op nationaal niveau de samenloop te regelen op een wijze die recht doet aan de richtlijnverplichtingen en die een doelmatige en samenhangende uitvoering mogelijk maakt. De samenloop van de verplichtingen van de omzettingsregelgeving speelt echter op verschillende niveaus van regelgeving: bij de NIS2-richtlijn worden de verplichtingen vooral op het niveau van de wet in formele zin geregeld, terwijl de verplichtingen op grond van de Drinkwaterrichtlijn vooral op het niveau van een algemene maatregel van bestuur zijn geregeld (het Drinkwaterbesluit). Het is daarom van belang dat op wetsniveau afstemming mogelijk wordt gemaakt met soortgelijke verplichtingen van de Drinkwaterrichtlijn. Het wetsvoorstel voorziet in een daartoe strekkende grondslag (artikel 23, vierde lid).

Afvalwater
Voor de sector afvalwater is er op dit moment geen wetgeving op het gebied van cybersecurity van toepassing. Van botsende verplichtingen en van een noodzaak tot wijziging van de sectorale wetgeving is daarom geen sprake.

Chemie
Voor de chemiesector is er geen sprake van botsing van bestaande wetgeving met de uit de NIS2-richtlijn voortvloeiende verplichtingen.

Plaats- en tijdsbepaling
Voor wat betreft de sector plaats- en tijdsbepaling met behulp van satellieten vallen er geen entiteiten onder de beleidsverantwoordelijkheid van de minister van Infrastructuur en Waterstaat als bevoegde autoriteit in de zin van de NIS2-richtlijn. De instanties die zich in Nederland bezighouden met plaats- en tijdsbepaling (het Galileo Reference Center in Noordwijk en het Galileo Sensor Station op Bonaire) vallen qua operationele verantwoordelijkheid onder het EU-agentschap voor het ruimtevaartprogramma (EUSPA).

7.5 Ministerie van Landbouw, Natuur en Voedselkwaliteit

Artikel 19 van de Europese Algemene Levensmiddelen Verordening (verordening (EG) 178/2002) verplicht exploitanten van een levensmiddelenbedrijf melding te doen bij de bevoegde autoriteit (Nederlandse Voedsel- en Warenautoriteit) als hij van mening is of redenen heeft om aan te nemen dat een levensmiddel dat hij ingevoerd geproduceerd, verwerkt, vervaardigd of gedistribueerd heeft niet aan de voedselveiligheidsvoorschriften voldoet. Voor een deel van de entiteiten uit de levensmiddelenindustrie kan er daarom sprake zijn van een meldplicht aan de NVWA en aan het CSIRT wanneer deze verplichting het gevolg is van een meldplichtig incident dat voortkomt uit de NIS2-Richtlijn.

Bovendien verplicht de Verordening Levensmiddelenhygiëne (verordening (EG) 852/2004, artikel 5) exploitanten van levensmiddelenbedrijven zorg te dragen voor de invoering, uitvoering en handhaving van een of meer permanente procedures die gebaseerd zijn op de HACCP-beginselen. In de praktijk kunnen aangewezen kritieke entiteiten onder die verplichting al passende en evenredige technische, beveiligings-, en organisatorische maatregelen ten behoeve van een aantal processen hebben genomen die ook voortkomen uit de NIS2-richtlijn.

7.6 Ministerie van Onderwijs, Cultuur en Wetenschap

Het hoger onderwijs kent op het gebied van informatiebeveiliging geen sectorspecifieke wet- en regelgeving.

7.7 Ministerie van Volksgezondheid, Welzijn en Sport

Sector gezondheidszorg

Er zijn diverse sectorspecifieke wetgeving op de sector gezondheidszorg van toepassing die ziet op kwaliteit van diensten en producten (zorgplicht) en op het melden van incidenten of onvolkomenheden (meldplicht) aan de Inspectie Gezondheidszorg en Jeugd (IGJ). Daarnaast heeft de IGJ het toezicht op de naleving van wetgeving en is bevoegd tot inzage van gegevens over de gezondheid van proefpersonen of patiënten en het vorderen van inlichtingen ter zake, bij zorgaanbieder, de entiteit die het wetenschappelijk onderzoek uitvoert. De desbetreffende beroepsbeoefenaar uit hoofde van ambt, beroep of overeenkomst tot geheimhouding van het dossier en de daarin opgenomen persoonsgegevens verplicht is, kan deze verplichting (in afwijking van artikel 5:20, tweede lid, van de Algemene wet bestuursrecht) niet inroepen tegenover de toezichthouder.

Voorts geldt de meldplicht voor datalekken bij de Autoriteit Persoonsgegevens (AP). Met dit wetsvoorstel komt voor de entiteiten in de zorg ook een meldplicht die specifiek ziet op cyberincidenten.

Zorgaanbieder
Op het gebied van de informatiebeveiliging in de zorg is er sectorspecifieke wet- en regelgeving. Op grond van de Wet gelden er aanvullende bepalingen t.a.v. verwerking persoonsgegevens in de zorg (Wabvpz) en het Besluit elektronische gegevensuitwisseling door zorgaanbieders (Begz.) Op grond van de Wet kwaliteit, klachten en geschillen zorg[52] geldt voor zorgaanbieders een verplichting om kwalitatief goede zorg te leveren en om te en om te voldoen aan de beveiligingsvoorschriften NEN 7510.

Farmaceutische entiteiten
In de Geneesmiddelenwet[53] is vastgesteld wat onder een geneesmiddel wordt verstaan en staat hoe een medicijn mag worden geproduceerd en verhandeld. Hiervoor is een fabrikantenvergunning nodig. Geneesmiddelen worden door de fabrikant slechts afgeleverd aan andere fabrikanten, groothandelaren en aan de degenen die bevoegd zijn de desbetreffende geneesmiddelen ter hand te stellen.

Onder een geneesmiddel worden ook medische isotopen verstaan. Dit zijn radioactieve stoffen voor diagnose (PET scans) en behandeling. Isotopen voor medische toepassing kennen een complexe toeleveringsketen (waarbij de stappen goed op elkaar dienen te zijn afgestemd omdat het product als gevolg van radioactief verval kort houdbaar is). De IGJ houdt toezicht op het productieproces en de ANVS op de straling.

Onderzoek naar de ontwikkeling van geneesmiddelen
In de NIS2-richtlijn wordt de subsector onderzoek naar geneesmiddelen genoemd welke in Nederland voor het preklinische onderzoek is vastgelegd in de wet op de dierproeven en voor klinisch onderzoek geïmplementeerd in de wet medische wetenschappelijk onderzoek met mensen.

Medische hulpmiddelen
Voor entiteiten die medische hulpmiddelen vervaardigen geldt op dit moment sectorspecifieke regelgeving die ziet op kwaliteit en de werking van medische hulpmiddelen en het melden van incidenten. Dit is vastgelegd in Europese verordeningen, de Medical Device Regulation (MDR[54]) waarvan de Nederlandse implementatie is vastgelegd in de Wet medische hulpmiddelen[55]. Meldingen van incidenten met medische hulpmiddelen dienen door fabrikant gemeld te worden bij IGJ.

---

[52] https://wetten.overheid.nl/BWBR0037173/2022-01-01
[53] wetten.nl - Regeling - Geneesmiddelenwet - BWBR0021505 (overheid.nl)
[54] EUR-Lex - 32017R0745 - EN - EUR-Lex (europa.eu)
[55] wetten.nl - Regeling - Wet medische hulpmiddelen - BWBR0042755 (overheid.nl)

8. Gevolgen

8.1 Gevolgen voor burgers en bedrijven

8.1.1 Inleiding

De door dit wetsvoorstel veroorzaakte regeldruk bestaat uit een stijging van administratieve lasten en inhoudelijke nalevingskosten per organisatie. Dit wetsvoorstel brengt verplichtingen met zich mee voor organisaties die kwalificeren als essentiële entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen.

Dit wetsvoorstel heeft geen gevolgen voor de regeldruk voor burgers en bedrijven die ofwel niet binnen de genoemde sectoren of categorieën vallen, ofwel de drempelwaardes niet overschrijden, ofwel niet anderszins bij besluit of regeling aangewezen zijn.

Sommige organisaties die onder dit wetsvoorstel vallen, vallen op dit moment al onder de Wbni. Voor deze organisaties zal de toename in regeldruk als gevolg van dit wetsvoorstel beperkter zijn dan entiteiten die op dit moment niet onder de Wbni vallen. Het aantal organisaties dat onder dit wetsvoorstel valt is van significant grotere orde dan onder de Wbni. Momenteel wordt dit aantal geschat op ongeveer 8.100 entiteiten.

In deze paragraaf wordt de regeldruk nader besproken. Daarbij wordt achtereenvolgens ingegaan op de zorgplicht betreffende beveiligingseisen, de meldplicht voor significante incidenten, registratieplicht, toezichtlasten, governance, uitzonderingssituaties en eenmalige kennisnamekosten.

8.1.2 Zorgplicht

Op grond van dit wetsvoorstel moeten essentiële entiteiten en belangrijke entiteiten passende en evenredige technische, operationele en organisatorische maatregelen nemen om de risico’s voor de beveiliging van de netwerk- en informatiesystemen te beheersen.

Ook zonder wetgeving zullen deze entiteiten veelal al beveiligingsmaatregelen hebben getroffen, zijnde een combinatie van technische, operationele en organisatorische maatregelen. Voor de continuïteit van hun eigen bedrijfsvoering is het immers cruciaal dat maatregelen worden getroffen op het gebied van netwerk- en informatiebeveiliging. Zonder maatregelen zijn entiteiten kwetsbaar voor dreigingen, zoals cybercrime, stroomstoringen en menselijke fouten. Daarbij zouden entiteiten een risico kunnen lopen waarbij hun eigen (cruciale) werkprocessen in gevaar komen.

Een deel van de entiteiten zal reeds in meer of mindere mate investeringen hebben gedaan op het gebied van beveiliging van hun systemen om zodoende incidenten en – als gevolg daarvan – mogelijk grote schadeposten zoveel mogelijk proberen te voorkomen. In de nota van toelichting bij de op grond van dit wetsvoorstel op te stellen amvb zal worden ingegaan op de nalevingskosten die voortvloeien uit de nadere wettelijke beveiligingseisen. Dit zal afhankelijk zijn van de mate waarin de beveiligingseisen overeenkomen met wat reeds wordt toegepast. In de *impact assessment* opgesteld door de Europese Commissie, wordt geschat dat nieuwe entiteiten een toename van maximaal 22% aan ICT-beveiligingskosten benodigd hebben om aan de eisen te voldoen. Voor entiteiten die reeds onder de Wbni vielen, is de schatting maximaal een toename van 12%. Hierbij dient wel vermeld te worden dat de impact assessment is geschreven op basis van het originele voorstel, dat op sommige punten afwijkt van de uiteindelijk aangenomen richtlijn.

Inzake regeldruk kan verwacht worden dat entiteiten die reeds passende en evenredige maatregelen hebben genomen, minder inhoudelijke nalevingskosten zullen ervaren. Entiteiten die deze maatregelen nog niet hebben genomen, kunnen een aanzienlijke regeldruk ervaren bij het implementeren van de zorgplichtmaatregelen.

8.1.3 Meldplicht

De meldplicht is een informatieverplichting en daarmee een administratieve last.
Uit dit wetsvoorstel volgt een meldplicht van significante incidenten voor essentiële entiteiten en belangrijke entiteiten bij zowel het CSIRT als de toezichthoudende instantie. Uitgangspunt is de meldplicht in te richten op een lastenluwe manier. Er wordt naar gestreefd deze dubbele meldplicht technisch zó in te richten dat het verspreiden van de benodigde informatie maar één handeling vergt, hetgeen de administratieve lasten reduceert. Naast de lasten heeft het doen van een melding ook voordelen voor de meldende entiteit. Zo kan er bijstand geleverd worden door het CSIRT in de vorm van informatieverstrekking of technische ondersteuning.

Per sector kan nadere invulling worden gegeven aan de parameters die bepalen wanneer incidenten meldplichtig zijn. Daarmee beïnvloeden deze parameters ook de regeldruk voor entiteiten. Naar verwachting zal deze meldplicht niet leiden tot een groot aantal meldingen voor entiteiten, daar alleen significante incidenten dienen te worden gemeld. Entiteiten dienen incidenten te melden die een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken, of aanzienlijke materiële of immateriële schade veroorzaakt dat andere natuurlijke of rechtspersonen heeft getroffen of kan treffen. Op basis van een inschatting van het NCSC op basis van de huidige aantal incidenten is de verwachting dat er circa 1.000 incidenten per jaar onder de meldplicht zullen vallen, onder voorbehoud van de nader te bepalen parameters.

Voor het verrichten van een melding zal het veelal gaan om handelingen als het verzamelen van informatie, het schriftelijk en eventueel telefonisch doen van een (voorlopige) melding en het eventueel verstrekken van nadere informatie aan het CSIRT en/of de toezichthoudende instantie. Deze meldingen dienen binnen de door de wet bepaalde termijnen gedaan te worden. Achteraf dient de entiteit ook een eindverslag in te dienen. De tijd die het entiteiten zal kosten om een melding en vervolghandelingen te doen onder de meldplicht zal verschillen per incident en zal onder andere afhankelijk zijn van hoe ernstig en complex het incident is. De meldplicht geldt alleen voor significante incidenten, daarom wordt uitgegaan van grootschalige of complexe incidenten en zullen de melding en extra vervolghandelingen naar schatting gemiddeld 480 minuten betreffen per incident. Vanwege de toename in handelingen ten opzichte van de meldplicht in de Wbni, omvat deze schatting 380 minuten voor het maken van de (voorlopige) melding en eindverslag en 100 minuten voor extra handelingen op het verzoek van het CSIRT en/of de toezichthoudende instantie. Deze inschatting is op basis van de huidige Wbni gemaakt en afgestemd met NCSC.

Als uurtarief wordt € 60 gehanteerd, een gangbaar tarief voor hoogopgeleide kenniswerkers[56]. Voor een groot aantal entiteiten is de meldplicht bij incidenten nieuw. Enkele entiteiten vielen daarentegen via de Wbni reeds onder de meldplicht. Daarom bedragen de nieuwe administratieve lasten per melding 480 minuten voor deze nieuwe entiteiten (€ 480 per melding), en is er voor entiteiten die thans onder de Wbni vallen een kleinere toename in verwachte regeldrukkosten van 180 minuten per melding (€ 180). Als rekenvoorbeeld, wanneer uitgegaan wordt van 1.000 meldingen per jaar, waaronder 900 meldingen vanuit nieuwe entiteiten en 100 vanuit entiteiten die nu al onder de Wbni vallen, zou dit neerkomen op structurele jaarlijkse regeldrukkosten van (900 x € 480) + (100 x € 180) = € 450.000.

Aanvullend op het voorgaande zijn entiteiten ook verplicht de ontvangers van hun diensten in kennis te stellen van significante incidenten die deze diensten kunnen verstoren. De regeldrukkosten hiervan kunnen afhankelijk zijn van het aantal ontvangers.

8.1.4 Registratieplicht

Entiteiten die onder de reikwijdte van dit wetsvoorstel vallen dienen zich te registreren bij het centrale contactpunt. Dit betreft een administratieve last. Hierbij moeten contactgegevens en IP-bereiken worden opgegeven, alsmede de sector en lidstaten waarin de entiteit opereert. Ook dienen wijzigingen op het bovenstaande binnen twee weken te worden doorgegeven.

[56] Handboek Meting Regeldrukkosten, versie 2.0 (2023), p. 14.

Het uitgangspunt is dat de registratieprocedure zo wordt ingericht, dat de regeldruk geminimaliseerd is. Voor de eerste registratie wordt ingeschat dat entiteiten maximaal 2 uur nodig hebben (€ 120). Latere wijzigingen worden geschat op 30 minuten per wijziging (€ 30).

Uitgaande van 8.100 eerste registraties van entiteiten, betekent dit eenmalige regeldrukkosten van 8.100 x € 120 = € 972.000. Een schatting van de coördinerende beleidsafdeling is gezet op 1.000 wijzigingen per jaar, dit geeft nog structurele jaarlijkse regeldrukkosten van 1.000 x € 30 = € 30.000.

8.1.5 Governance

Dit wetsvoorstel schrijft twee verplichtingen voor in het kader van governance die regeldruk kunnen veroorzaken. Allereerst zijn besturen van entiteiten verplicht de beveiligingsmaatregelen die in het kader van de zorgplicht genomen worden, goed te keuren en toe te zien op de uitvoering van die maatregelen. Aanvullend op de regeldruk beschreven bij zorgplicht, zal dit nog een administratieve last voor de besturen van entiteiten zijn.

Ten tweede dienen de leden van het bestuur van de entiteiten te beschikken over kennis en vaardigheden om tot een goed besluit betreffende de beveiligingsmaatregelen te komen. Dit kan bijvoorbeeld worden aangetoond door middel van een certificaat van deelname aan een relevante training.

8.1.6 Overige verplichtingen

Tenslotte zijn er nog enkele andere verplichtingen in dit wetsvoorstel die voor specifieke entiteiten tot extra regeldruk kunnen leiden, welke hieronder uitgewerkt worden.

Voor entiteiten die vallen onder sectoren genoemd in artikel 44 en die niet in de Europese Unie zijn gevestigd, maar daarin wel diensten aanbieden, geldt een verplichting om een vertegenwoordiger in de Europese Unie aan te wijzen. Indien zij een vertegenwoordiger in Nederland aanwijzen, dan vallen zij onder Nederlandse jurisdictie. De regeldrukkosten hiervan zijn afhankelijk van de overeenkomst die deze entiteiten met een vertegenwoordiger sluiten. Er kan geen inschatting worden gemaakt hoeveel bedrijven deze constructie nodig zullen hebben omdat zij geen vestiging hebben.

Voor registers van topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen, bestaat een aanvullende verplichting in de vorm van het bijhouden van een database met domeinnaamregistratiegegevens. De uit deze wet voortkomende verplichtingen dienen te worden opgenomen in de werkprocessen van deze entiteiten. Het aanpassen van de werkprocessen zal voornamelijk eenmalige regeldrukkosten veroorzaken. Aanvullend zullen deze entiteiten toegang moeten verschaffen aan partijen die daar een rechtmatig verzoek toe doen, wat structurele regeldrukkosten op zal leveren, afhankelijk van het aantal verzoeken dat wordt ingediend.

Belangrijke en essentiële entiteiten kunnen in het geval van niet-significante (bijna)incidenten of cyberdreigingen alsnog besluiten een vrijwillige melding te maken. Ook entiteiten die niet onder de reikwijdte van dit wetvoorstel vallen kunnen een vrijwillige melding doen. In deze gevallen is er dus sprake van een vrijwillige regeldruk, vergelijkbaar met de eerder beschreven regeldrukkosten voor het doen van meldingen. Na het doen van een dergelijke melding kan een CSIRT op verzoek besluiten bijstand te verlenen. Daarmee zal in de meeste gevallen de voordelen van een vrijwillige melding groter zijn dan de lasten.

8.1.7 Toezichtslasten

Op de naleving van het bepaalde bij of krachtens dit wetsvoorstel wordt toegezien door de toezichthoudende instantie. Voor essentiële entiteiten en belangrijke entiteiten betekent dit dat zij toezichtslasten krijgen. Deze toezichtslasten zijn voor essentiële entiteiten zwaarder dan voor belangrijke entiteiten.

Voor alle entiteiten geldt dat de toezichthoudende instanties bij de uitoefening van hun taak gebruik kunnen maken van een gerichte beveiligingsaudit of een beveiligingsscan, met als doel om kwetsbaarheden en risico's voor de beveiliging van de netwerk- en informatiesystemen te identificeren en inzicht te krijgen in de effectiviteit van genomen beheersmaatregelen. De regeldrukkosten van de inzet van dergelijke instrumenten hangen af van de omvang en reikwijdte waarmee het instrument wordt ingezet.

De toezichthoudende instantie kan daarnaast bij essentiële entiteiten een controlefunctionaris aanstellen en de entiteit onderwerpen aan (steekproefsgewijze) inspecties en ad-hoc audits en verzoeken om informatie, gegevens, documenten en bewijzen van uitvoering van het cyberbeveiligingsbeleid. Het is niet vast te stellen hoe vaak de toezichthoudende instantie deze instrumenten zal inzetten. De regeldrukkosten van deze inzet hangt ook af van de omvang van die inzet.

Voor belangrijke entiteiten gelden vergelijkbare verplichtingen, echter kunnen de verplichtingen alleen achteraf worden toegepast. Achteraf wil zeggen dat de toezichthoudende instantie informatie moet hebben dat een belangrijke entiteit zich mogelijk niet aan de uit deze wet voortkomende verplichtingen houdt, alvorens deze instrumenten worden ingezet.

8.1.8 Eenmalige kennisnamekosten

Entiteiten zullen eenmalig tijd besteden aan het verdiepen in en kennisnemen van de Cbw. Entiteiten zullen hier naar schatting 16 uur (2 werkdagen) voor nodig hebben. Uitgaande van een uurtarief van € 60 komt dit uit op € 960 eenmalige kennisnamekosten per organisatie.

8.2 Gevolgen voor de uitvoering

HUF

8.3 Financiële gevolgen voor de overheid

Het onderhavige wetsvoorstel ziet op een significante uitbreiding van zowel taken als scope van doelgroepen. Dit zal leiden tot extra financiële uitgaven. Een van de belangrijkste taken voor de Rijksoverheid houdt verband met de verplichting om essentiële entiteiten en belangrijke entiteiten te ondersteunen, waaronder middels het aanwijzen van een CSIRT. Hiervoor moet specifieke kennis worden uitgebreid en in termen van capaciteit worden versterkt. Zowel bij de Rijksoverheid als bij de CSIRT's Deze specialistische kennis is nu al schaars en duur, en zal met de komst van deze wet nog schaarser en duurder worden. Ook op het gebied van toezicht worden er veranderingen doorgevoerd met financiële gevolgen. Zo moet de capaciteit voor toezicht groeien vanwege de toename aan entiteiten. Ook is er voor essentiële entiteiten straks sprake van toezicht vooraf. Het vervullen van deze verplichtingen zal veelal een intensivering zijn van het huidige beleid ter bescherming van de vitale infrastructuur.

De kosten vallen grotendeels neer bij de verantwoordelijke departementen. Zij hebben op basis van hun sectorverantwoordelijkheid een coördinerende rol richting entiteiten om samenwerking, informatiedeling, de identificatie van risico's en de handhaving van de voorschriften van de NIS-richtlijn te bevorderen. Hier zijn consequenties aan verbonden met betrekking tot capaciteit en middelen, zowel voor de departementen, CSIRT's, als de sectorale toezichthouders. Wegens variatie in sectorale omvang en diepgang, wisselende specificiteit van complementaire sectorale wetgeving en uiteenlopende kosten voor capaciteitsvergroting verschillen de budgettaire gevolgen sterk per departement.

Conform de regels van de budgetdiscipline dienen de budgettaire gevolgen te worden ingepast op de begrotingen van de verantwoordelijke departementen. In onderstaande tabel zijn de budgettaire gevolgen geraamd. Daarin kunnen nog wijzigingen plaatsvinden. De afspraak is dat er over de bedragen uiterlijk bij Miljoenennota 2025 duidelijkheid en overeenstemming is; dat is een noodzakelijke voorwaarde om na de internetconsultatie verder te kunnen met het

implementatieproces. Deze bedragen zijn inclusief de budgettaire gevolgen horende bij de Wet weerbaarheid kritieke entiteiten.

Tabel 1: budgettaire gevolgen per departement

(in mln. €)	2024	2025	2026	2027	2028	Structureel
EZK	7,30	16,58	22,17	22,17	22,17	22,17
IenW	0,00	11,90	13,40	15,00	16,50	18,00
VWS	5,07	8,11	8,11	8,04	8,04	8,04
BZK	2,54	5,26	7,26	7,46	7,56	7,56
OCW	2,14	PM	PM	PM	PM	PM
LNV	0,70	5,10	5,80	6,80	6,80	6,80
JenV	3,64	6,37	9,00	10,68	13,92	15,17
Fin	0,00	1,20	1,30	1,40	1,50	1,50
Totaal	**21,39**	**54,52**	**67,04**	**71,55**	**76,49**	**79,24**

De kosten voor het ministerie van IenW worden bij Miljoenennota 2025 binnen de begroting verwerkt. Voor het ministerie van OCW geldt dat nader onderzocht wordt wat de kosten na 2024 zijn. Het streven is om de budgettaire gevolgen bij Miljoenennota 2025 in te passen binnen de OCW-begroting. Voor BZK geldt dat de kosten van NIS2 en van de BZK-gerelateerde kosten voor CER worden gedekt binnen de artikelen 6 en 7 van Hoofdstuk 7.

Hierbij dient opgemerkt te worden dat de ingeschatte uitgaven voor de uitvoering van het wetsvoorstel gebaseerd zijn op het op dit moment verwachte aantal entiteiten dat onder de reikwijdte van de richtlijn komt te vallen. Op basis hiervan hebben de verantwoordelijke departementen een raming opgenomen in hun begrotingen. Naar gelang de implementatie van het wetsvoorstel vordert kunnen meer betrouwbare ramingen worden gemaakt en bijstellingen nodig blijken te zijn. Bijvoorbeeld door voorgestelde wijzingen vanuit de consultatie of een uitvoeringstoets.

9. Advies en consultatie

PM

10. Overgangsrecht en inwerkingtreding

PM

11. Transponeringstabel

Bepaling EU-regelgeving	**Bepaling in implementatieregeling of bestaande regeling**	**Omschrijving beleidsruimte**	**Toelichting op de keuze(n) bij de invulling van de beleidsruimte**
Artikel 1	Artikel 2 van het wetsvoorstel		
Artikel 2, lid 1	Artikel 1 en artikel 8, lid 1, aanhef en onderdeel f, van het wetsvoorstel		
Artikel 2, lid 2, aanhef en onder a	Artikel 8, lid 1, aanhef en onderdeel a, b, c en d van het wetsvoorstel		
Artikel 2, lid 2, aanhef en onder b	Artikel 9, aanhef en onderdeel a, van het wetsvoorstel		
Artikel 2, lid 2, aanhef en onder c	Artikel 9, aanhef en onderdeel b, van het wetsvoorstel		
Artikel 2, lid 2, aanhef en onder d	Artikel 9, aanhef en onderdeel c, van het wetsvoorstel		
Artikel 2, lid 2, aanhef en onder e	Artikel 9, aanhef en onderdeel d, van het wetsvoorstel		
Artikel 2, lid 2, aanhef, onder f en subonderdeel i	Artikel 8, lid 1, aanhef en onderdeel g, van het wetsvoorstel		

Artikel 2, lid 2, aanhef, onder f en subonderdeel ii	Artikel 8, lid 1, aanhef en onderdeel g van het wetsvoorstel		
Artikel 2, lid 3	Artikel 8, lid 1, aanhef en onderdeel h, van het wetsvoorstel		
Artikel 2, lid 4	Artikel 8, lid 1, aanhef en onderdeel c, van het wetsvoorstel		
Artikel 2, lid 5, aanhef en onder a	Artikel 8, lid 1, aanhef en onderdeel g, van het wetsvoorstel		
Artikel 2, lid 5, aanhef en onder b	Artikel 11 en 14 van het wetsvoorstel		
Artikel 2, lid 6	Artikel 6, lid 1, van het wetsvoorstel		
Artikel 2, lid 7	Artikel 6, lid 1, van het wetsvoorstel		
Artikel 2, lid 8	Artikel 25, lid 1; artikel 34, lid 1; artikel 46 lid 1; en artikel 49, lid 1, van het wetsvoorstel	De mogelijkheid voor de lidstaat om specifieke entiteiten die activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving, met inbegrip van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, of die uitsluitend diensten verlenen aan de in lid 7 van dit artikel bedoelde overheidsinstanties vrij te stellen van de in artikel 21 of artikel 23 vastgestelde verplichtingen.	
Artikel 2, lid 9	Artikel 6, lid 2; artikel 25, lid 1; artikel 34, lid 2; artikel 46, lid 2; artikel 49 lid 2, van het wetsvoorstel		
Artikel 2, lid 10	Behoeft geen implementatie		
Artikel 2, lid 11	Artikel 66 van het wetsvoorstel		
Artikel 2, lid 12	Behoeft geen implementatie.		
Artikel 2, lid 13	Artikel 65 van het wetsvoorstel		
Artikel 2, lid 14	Artikel 64 van het wetsvoorstel		
Artikel 3, lid 1, aanhef en onder a	Artikel 8, lid 1, aanhef en onderdeel f, van het wetsvoorstel		
Artikel 3, lid 1, aanhef en onder b	Artikel 8, lid 1, aanhef en onderdeel a, b en c van het wetsvoorstel		
Artikel 3, lid 1, aanhef en onder c	Artikel 8, lid 1, aanhef en onderdeel d en e, van het wetsvoorstel		
Artikel 3, lid 1, aanhef en onder d	Artikel 8, lid 1, aanhef en onderdeel g van het wetsvoorstel		
Artikel 3, lid 1, aanhef en onder e	Artikel 9, aanhef en onderdeel a, b, c en d, van het wetsvoorstel		
Artikel 3, lid 1, aanhef en onder f	Artikel 8, lid 1, aanhef en onderdeel h, van het wetsvoorstel		
Artikel 3, lid 1, aanhef en onder g	Artikel 10 van het wetsvoorstel		

Artikel 3, lid 2	Artikel 12 en 13 van het wetsvoorstel		
Artikel 3, lid 3	Artikel 22 van het wetsvoorstel	De mogelijkheid voor de lidstaten om vaker dan in ieder geval twee jaar de lijst te evalueren van essentiële en belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen.	
Artikel 3, lid 4	Artikel 45 van het wetsvoorstel	De mogelijkheid voor de lidstaten om te bepalen dat de in artikel 3, derde lid, van de NIS2-richtlijn bedoelde entiteiten voor het opstellen van de lijst zoals vereist in artikel 3, derde lid van de NIS2-richtlijn meer informatie moeten aanleveren dan in artikel 3, vierde lid, van de NIS2-richtlijn worden genoemd. De lidstaten kunnen ook nationale mechanismen instellen waarmee entiteiten zichzelf kunnen registreren.	
Artikel 3, lid 5	Feitelijke uitvoering		
Artikel 3, lid 6	Feitelijke uitvoering		
Artikel 4, lid 1	Artikel 24, lid 1, van het wetsvoorstel		
Artikel 4, lid 2	Artikel 24, lid 2, van het wetsvoorstel		
Artikel 4, lid 3	Artikel 24, lid 3, van het wetsvoorstel		
Artikel 5	Behoeft geen implementatie	De mogelijkheid voor lidstaten om nationale bepalingen te treffen of te handhaven teneinde een hoger cyberbeveiligingsniveau te waarborgen, mits dergelijke bepalingen stroken met de plichten van de lidstaten die zijn vastgelegd in het Unierecht.	
Artikel 6, lid 1	Artikel 1 van het wetsvoorstel		
Artikel 6, lid 2	Artikel 1 van het wetsvoorstel		
Artikel 6, lid 3	Artikel 1 van het wetsvoorstel		
Artikel 6, lid 4	Rechtstreekse werking		
Artikel 6, lid 5	Artikel 1 van het wetsvoorstel		
Artikel 6, lid 6	Artikel 1 van het wetsvoorstel		
Artikel 6, lid 7	Rechtstreekse werking		
Artikel 6, lid 8	Rechtstreekse werking		
Artikel 6, lid 9	Rechtstreekse werking		
Artikel 6, lid 10	Artikel 1 van het wetsvoorstel		
Artikel 6, lid 11	Artikel 1 van het wetsvoorstel		
Artikel 6, lid 12	Artikel 1 van het wetsvoorstel		
Artikel 6, lid 13	Artikel 1 van het wetsvoorstel		
Artikel 6, lid 14	Rechtstreekse werking		
Artikel 6, lid 15	Artikel 1 van het wetsvoorstel		
Artikel 6, lid 16	Artikel 1 van het wetsvoorstel		
Artikel 6, lid 17	Rechtstreekse werking		
Artikel 6, lid 18	Rechtstreekse werking		
Artikel 6, lid 19	Rechtstreekse werking		
Artikel 6, lid 20	Artikel 1 van het wetsvoorstel		

Artikel 6, lid 21	Artikel 1 van het wetsvoorstel		
Artikel 6, lid 22	Artikel 1 van het wetsvoorstel		
Artikel 6, lid 23	-		
Artikel 6, lid 24	Artikel 1 van het wetsvoorstel		
Artikel 6, lid 25	Artikel 1 van het wetsvoorstel		
Artikel 6, lid 26	Rechtstreekse werking		
Artikel 6, lid 27	Artikel 1 van het wetsvoorstel		
Artikel 6, lid 28	Artikel 1 van het wetsvoorstel		
Artikel 6, lid 29	Artikel 1 van het wetsvoorstel		
Artikel 6, lid 30	Artikel 1 van het wetsvoorstel		
Artikel 6, lid 31	Artikel 1 van het wetsvoorstel		
Artikel 6, lid 32	Artikel 1 van het wetsvoorstel		
Artikel 6, lid 33	Artikel 1 van het wetsvoorstel		
Artikel 6, lid 34	Artikel 1 van het wetsvoorstel		
Artikel 6, lid 35	Artikel 1 van het wetsvoorstel		
Artikel 6, lid 36	Artikel 1 van het wetsvoorstel		
Artikel 6, lid 37	Artikel 1 van het wetsvoorstel		
Artikel 6, lid 38	Artikel 1 van het wetsvoorstel		
Artikel 6, lid 39	Artikel 1 van het wetsvoorstel		
Artikel 6, lid 40	Artikel 1 van het wetsvoorstel		
Artikel 6, lid 41	Artikel 1 van het wetsvoorstel		
Artikel 7, lid 1	Artikel 20, lid 1, van het wetsvoorstel		
Artikel 7, lid 2	Artikel 20, lid 2, van het wetsvoorstel	De mogelijkheid voor lidstaten om in het kader van de nationale cyberbeveiligingsstrategie meeromvattend beleid vast te stellen dan vereist in artikel 7, tweede lid, van de NIS2-richtlijn.	
Artikel 7, lid 3	Feitelijke uitvoering		
Artikel 7, lid 4	Artikel 20, lid 3, van het wetsvoorstel		
Artikel 8, lid 1	Artikel 16, lid 1, van het wetsvoorstel		
Artikel 8, lid 2	Bepaling richt zich tot de bevoegde autoriteiten		
Artikel 8, lid 3	Artikel 15, lid 1 en aanhef, van het wetsvoorstel		
Artikel 8, lid 4	Artikel 15, lid 1, aanhef en onderdeel a en b, van het wetsvoorstel		
Artikel 8, lid 5	-		
Artikel 8, lid 6	Feitelijke uitvoering		
Artikel 9, lid 1	Artikel 19 van het wetsvoorstel	De mogelijkheid voor de lidstaat om meer dan één cybercrisisbeheerautoriteiten aan te wijzen of in te stellen.	
Artikel 9, lid 2	Van de mogelijkheid is geen gebruik gemaakt		
Artikel 9, lid 3	-		
Artikel 9, lid 4	Artikel 21 van het wetsvoorstel	De mogelijkheid voor de lidstaat om in het nationale plan voor grootschalige cyberbeveiligingsincidenten en crisisrespons meer elementen te laten behelzen dan die genoemd in artikel 9, vierde lid, van de NIS2-richtlijn.	
Artikel 9, lid 5	Feitelijke uitvoering	De mogelijkheid voor de lidstaten om bij de kennisgeving	

		aan de Europese Commissie van de aanwijzing of instelling van cybercrisisbeheerautoriteiten informatie weg te laten indien en voor zover noodzakelijk voor hun nationale veiligheid.	
Artikel 10, lid 1	Artikel 17 van het wetsvoorstel	De mogelijkheid voor de lidstaat om binnen de cybercrisisbeheerautoriteiten computer security incident response teams (CSIRT's) aan te wijzen of in te stellen.	
Artikel 10, lid 2	-		
Artikel 10, lid 3	Artikel 17, lid 2, aanhef en onderdeel f, van het wetsvoorstel		
Artikel 10, lid 4	Artikel 17, lid 2, aanhef en onderdeel a, b, c, d en e, van het wetsvoorstel		
Artikel 10, lid 5	Feitelijke uitvoering		
Artikel 10, lid 6	Artikel 17, lid 2, aanhef en onderdeel f, van het wetsvoorstel		
Artikel 10, lid 7	Artikel 55 van het wetsvoorstel	De CSIRT's kunnen samenwerkingsrelaties aangaan en informatie uitwisselen met CSIRT's van derde landen.	
Artikel 10, lid 8	-	De CSIRT's kunnen ook met organen van derde landen die gelijkwaardig zijn aan een CSIRT samenwerken.	
Artikel 10, lid 9	Feitelijke uitvoering		
Artikel 10, lid 10	Feitelijke uitvoering		
Artikel 11, lid 1	Rechtstreekse werking volstaat.	De CSIRT's kunnen deelnemen aan internationale samenwerkingsnetwerken.	
Artikel 11, lid 2	Rechtstreekse werking volstaat.		
Artikel 11, lid 3	Rechtstreekse werking volstaat.	De CSIRT's kunnen overgaan tot het proactief en niet-intrusief scannen van openbaar toegankelijke netwerk- en informatiesystemen van essentiële en belangrijke entiteiten	
Artikel 11, lid 4	Rechtstreekse werking volstaat.		
Artikel 11, lid 5	Rechtstreekse werking volstaat.		
Artikel 12, lid 1	Artikel 19 van het wetsvoorstel		
Artikel 12, lid 2	Bepaling richt zich tot Enisa		
Artikel 13, lid 1	Artikel 52, lid 1, van het wetsvoorstel		
Artikel 13, lid 2	Artikel 27 en 35 van het wetsvoorstel	De mogelijkheid voor de lidstaten om te kiezen of hun CSIRT's of cybercrisisbeheerautoriteiten als meldpunt aan te wijzen voor significante incidenten op grond van artikel 23 van de NIS2-richtlijn en van incidenten, cyberdreigingen en bijna-incidenten.	

Artikel 13, lid 3	Artikel 41 van het wetsvoorstel		
Artikel 13, lid 4	Artikel 52 van het wetsvoorstel		
Artikel 13, lid 5	Artikel 42; artikel 52, lid 2, aanhef en onderdeel g; en artikel 57 van het wetsvoorstel		
Artikel 13, lid 6	-		
Artikel 14, lid 1	-		
Artikel 14, lid 2	-		
Artikel 14, lid 3	-		
Artikel 14, lid 4	-		
Artikel 14, lid 5	Rechtstreekse werking volstaat.		
Artikel 14, lid 6	Rechtstreekse werking volstaat.		
Artikel 14, lid 7	Bepaling richt zich tot de samenwerkingsgroep		
Artikel 14, lid 8	Bepaling richt zich tot de Europese Commissie		
Artikel 14, lid 9	-		
Artikel 15, lid 1	-		
Artikel 15, lid 2	-		
Artikel 15, lid 3	-		
Artikel 15, lid 4	Bepaling richt zich tot het CSIRT-netwerk		
Artikel 15, lid 5	Bepaling richt zich tot CSIRT-netwerk		
Artikel 15, lid 6	Bepaling richt zich tot CSIRT-netwerk en EU-CyCLONe		
Artikel 16, lid 1	-		
Artikel 16, lid 2	-		
Artikel 16, lid 3	-		
Artikel 16, lid 4	Bepaling richt zich tot EU-CyCLONe		
Artikel 16, lid 5	Bepaling richt zich tot EU-CyCLONe		
Artikel 16, lid 6	Bepaling richt zich tot EU-CyCLONe		
Artikel 16, lid 7	Bepaling richt zich tot EU-CyCLONe		
Artikel 17	Bepaling richt zich tot de Europese Unie		
Artikel 18, lid 1	Bepaling richt zich tot Enisa		
Artikel 18, lid 2	Bepaling richt zich tot Enisa		
Artikel 18, lid 3	Bepaling richt zich tot Enisa		
Artikel 19, lid 1	Bepaling richt zich tot de samenwerkingsgroep		
Artikel 19, lid 2	Bepaling richt zich tot de samenwerkingsgroep		
Artikel 19, lid 3	Artikel 17, lid 2, aanhef en onderdeel g, van het wetsvoorstel		
Artikel 19, lid 4	Artikel 17, lid 2, aanhef en onderdeel g, van het wetsvoorstel		
Artikel 19, lid 5	Artikel 17, lid 2, aanhef en onderdeel g, van het wetsvoorstel		
Artikel 19, lid 6	-		
Artikel 19, lid 7	-		
Artikel 19, lid 8	Artikel 17, lid 2, aanhef en onderdeel g, van het wetsvoorstel		

Artikel 19, lid 9	Bepaling richt zich tot cyberbeveiligingsdeskundigen die deelnemen aan collegiale toetsingen		
Artikel 20, lid 1	Artikel 26, lid 1, van het wetsvoorstel		
Artikel 20, lid 2	Artikel 26, lid 2, 3, 4, 5, 6 en 7, van het wetsvoorstel	De mogelijkheid voor de lidstaten om meer dan alleen de in artikel 21, eerste lid, van de NIS2-richtlijn maatregelen te nemen om de risico's voor de beveiliging van de netwerk- en informatiesystemen die deze entiteiten voor hun werkzaamheden of voor het verlenen van hun diensten gebruiken, te beheren en om incidenten te voorkomen of de gevolgen van incidenten voor de afnemers van hun diensten en voor andere diensten te beperken.	
Artikel 21, lid 1	Artikel 23, lid 1 en 2, van het wetsvoorstel		
Artikel 21, lid 2	Artikel 23, lid 3, van het wetsvoorstel		
Artikel 21, lid 3	Artikel 23, lid 4, van het wetsvoorstel		
Artikel 21, lid 4	Artikel 72 en 73 van het wetsvoorstel		
Artikel 21, lid 5	Bepaling richt zich tot de Europese Commissie		
Artikel 22, lid 1	Bepaling richt zich tot de samenwerkingsgroep		
Artikel 22, lid 2	Bepaling richt zich tot de Europese Commissie		
Artikel 23, lid 1	Artikel 27, lid 1; artikel 29; en artikel 32, lid 1, van het wetsvoorstel		
Artikel 23, lid 2	Artikel 32, lid 2, van het wetsvoorstel		
Artikel 23, lid 3	Artikel 27, lid 2, van het wetsvoorstel		
Artikel 23, lid 4 en onder a	Artikel 28 van het wetsvoorstel		
Artikel 23, lid 4 en onder b	Artikel 29, lid 1, van het wetsvoorstel		
Artikel 23, lid 4 en onder c	Artikel 30 van het wetsvoorstel		
Artikel 23, lid 4 en onder d	Artikel 31, lid 1, van het wetsvoorstel		
Artikel 23, lid 4 en onder e	Artikel 31, lid 2, van het wetsvoorstel		
Artikel 23, lid 1 en slotzin	Artikel 29, lid 2, van het wetsvoorstel		
Artikel 23, lid 5	Artikel 38 van het wetsvoorstel		
Artikel 23, lid 6	Artikel 41, lid 1 en 2, van het wetsvoorstel		
Artikel 23, lid 7	Artikel 39 van het wetsvoorstel		
Artikel 23, lid 8	Artikel 41, lid 3, van het wetsvoorstel		
Artikel 23, lid 9	Artikel 41, lid 5, van het wetsvoorstel		

Artikel 23, lid 10	Artikel 42, lid 1, van het wetsvoorstel		
Artikel 23, lid 11	Bepaling richt zich tot de Europese Commissie		
Artikel 24, lid 1	Van de mogelijkheid is (nog) geen gebruik gemaakt.	De mogelijkheid voor de lidstaten om essentiële en belangrijke entiteiten te verplichten bepaalde ICT-producten, -diensten en -processen te gebruiken.	
Artikel 24, lid 2	Bepaling richt zich tot de Europese Commissie		
Artikel 24, lid 3	Bepaling richt zich tot de Europese Commissie		
Artikel 25, lid 1	Feitelijke uitvoering		
Artikel 25, lid 2	Bepaling richt zich tot Enisa		
Artikel 26, lid 1 en aanhef	Artikel 4, lid 1 en aanhef, van het wetsvoorstel		
Artikel 26, lid 1, aanhef en onder a	Artikel 4, lid 2, van het wetsvoorstel		
Artikel 26, lid 1, aanhef en onder b	Artikel 4, lid 3 j° lid 5, van het wetsvoorstel		
Artikel 26, lid 1, aanhef en onder c	…		
Artikel 26, lid 2	Artikel 4, lid 5, van het wetsvoorstel		
Artikel 26, lid 3	Artikel 6, lid 6, en artikel 44 van het wetsvoorstel		
Artikel 26, lid 4	Rechtstreekse werking		
Artikel 26, lid 5	Artikel 61, lid 2, van het wetsvoorstel	De mogelijkheid voor lidstaten om voor te schrijven dat passende toezichts- en handhavingsmaatregelen moeten worden genomen bij een verzoek om wederzijdse bijstand.	
Artikel 27, lid 1	Bepaling richt zicht tot Enisa		
Artikel 27, lid 2	Artikel 48, lid 2 en 3, van het wetsvoorstel		
Artikel 27, lid 3	Artikel 48, lid 4, van het wetsvoorstel		
Artikel 27, lid 4	Feitelijke uitvoering		
Artikel 27, lid 5	Artikel 48, lid 1, aanhef, van het wetsvoorstel		
Artikel 28, lid 1	Artikel 50, lid 1, van het wetsvoorstel		
Artikel 28, lid 2	Artikel 50, lid 2, van het wetsvoorstel		
Artikel 28, lid 3	Artikel 50, lid 3, van het wetsvoorstel		
Artikel 28, lid 4	Artikel 50, lid 4, van het wetsvoorstel		
Artikel 28, lid 5	Artikel 51, lid 1, 2 en 3, van het wetsvoorstel		
Artikel 28, lid 6	Artikel 50, lid 5, van het wetsvoorstel		
Artikel 29, lid 1	Bepaling behoeft geen implementatie		
Artikel 29, lid 2	Idem		
Artikel 29, lid 3	Idem		
Artikel 29, lid 4	Idem		
Artikel 29, lid 5	Bepaling richt zich tot Enisa		

Artikel 30, lid 1	Artikel 35, lid 1, van het wetsvoorstel		
Artikel 30, lid 2	Artikel 35, lid 1 (en tweede volzin) en lid 2; artikel 41, lid 1 en 2, van het wetsvoorstel		
Artikel 31, lid 1	Artikel 72, 73, 74, 75, 76, 77, 78, 81, 82, 83, 84, 85, 86, 87 en 88 van het wetsvoorstel	De mogelijkheid voor lidstaten om binnen de kaders zoals omschreven in artikel 31, eerste lid, van de NIS2-richtlijn aan de cybercrisisbeheerautoriteiten zelf welke toezichtstaken geprioriteerd worden.	
Artikel 31, lid 2	Feitelijke uitvoering		
Artikel 31, lid 3	Artikel 59 van het wetsvoorstel		
Artikel 31, lid 4	Artikel 68, 69, 70, 71, 78, 79 en 80 van het wetsvoorstel	De mogelijkheid voor lidstaten om bij het vormgeven van het handhavings- en toezichtstelsel in het kader van de NIS2-richtlijn aan te sluiten bij hun nationale stelsels.	
Artikel 32, lid 1	-		
Artikel 32, lid 2 en onder a	Van de mogelijkheid is (nog) geen gebruik gemaakt.	De mogelijkheid voor lidstaten om meer dan die in artikel 31, tweede lid, van de NIS2-richtlijn genoemde toezichthoudende taken op te dragen aan de cybercrisisbeheerautoriteiten. De lidstaten kunnen verder gemotiveerd de gevallen geven waarin de kosten van een beveiligingsaudit wordt vergoed.	
Artikel 32, lid 2 en onder b	Artikel 70, lid 1, van het wetsvoorstel		
Artikel 32, lid 2 en onder c	Artikel 70, lid 2, van het wetsvoorstel		
Artikel 32, lid 2, aanhef en onder d	Artikel 69 van het wetsvoorstel	De mogelijkheid voor lidstaten om meer handhavingsbevoegdheden toe te kennen aan cybercrisisbeheerautoriteiten dan in artikel 32, tweede lid, van de NIS2-richtlijn worden genoemd.	
Artikel 32, lid 2, aanhef en onder e	Van de mogelijkheid is (nog) geen gebruik gemaakt.		
Artikel 32, lid 2, aanhef en onder f	Van de mogelijkheid is (nog) geen gebruik gemaakt.		
Artikel 32, lid 2, aanhef en onder g	Artikel 70, lid 1, aanhef en onder b, van het wetsvoorstel		
Artikel 32, lid 2, tweede volzin	Artikel 70, lid 3, van het wetsvoorstel		
Artikel 32, lid 2, derde volzin	Artikel 70, lid 1, aanhef en onderdeel b, van het wetsvoorstel		
Artikel 32, lid 2, vierde volzin	Artikel 70, lid 5, van het wetsvoorstel		
Artikel 32, lid 3	…		
Artikel 32, lid 4, aanhef en onder a	Artikel 74, lid 3, aanhef en onderdeel a, van het wetsvoorstel		
Artikel 32, lid 4, aanhef en onder b	Artikel 72 van het wetsvoorstel		

Artikel 32, lid 4, aanhef en onder c	Artikel 73 van het wetsvoorstel		
Artikel 32, lid 4, aanhef en onder d	Artikel 72 van het wetsvoorstel		
Artikel 32, lid 4, aanhef en onder e	Artikel 71 van het wetsvoorstel		
Artikel 32, lid 4, aanhef en onder f	Artikel 74, lid 3, aanhef en onderdeel b, van het wetsvoorstel		
Artikel 32, lid 4, aanhef en onder g	Artikel 68 van het wetsvoorstel		
Artikel 32, lid 4, aanhef en onder h	Artikel 71 van het wetsvoorstel		
Artikel 32, lid 4, aanhef en onder i	Artikel 77 van het wetsvoorstel		
Artikel 32, lid 5 en aanhef	Artikel 74, lid 1, van het wetsvoorstel		
Artikel 32, lid 5, aanhef en onder a	Artikel 75 van het wetsvoorstel		
Artikel 32, lid 5, aanhef en onder b	Artikel 76 van het wetsvoorstel		
Artikel 32, lid 6	Artikel 1 en 44 van het wetsvoorstel		
Artikel 32, lid 7	Behoeft geen implementatie.	De mogelijkheid voor lidstaten om te bepalen dat andere dan in artikel 32, zevende lid, van de NIS2-richtlijn opgesomde omstandigheden van het geval worden meegenomen in de afweging om handhavingsmaatregelen te nemen.	
Artikel 32, lid 8	-Behoeft geen implementatie.		
Artikel 32, lid 9	Artikel 57, lid 2, van het wetsvoorstel		
Artikel 32, lid 10	Artikel 58 van het wetsvoorstel		
Artikel 33, lid 1	Artikel 78 van het wetsvoorstel	De mogelijkheid voor lidstaten om zelf te bepalen wanneer het noodzakelijk is om toezichtmaatregelen achteraf te op te leggen.	
Artikel 33, lid 2, aanhef en onder a	-		
Artikel 33, lid 2, aanhef en onder b	Artikel 80 van het wetsvoorstel		
Artikel 33, lid 2, aanhef en onder c	Artikel 79 van het wetsvoorstel		
Artikel 33, lid 2, aanhef en onder d	-		
Artikel 33, lid 2, aanhef en onder e	-		
Artikel 33, lid 2, aanhef en onder f	-		
Artikel 33, lid 3	-		
Artikel 33, lid 4, aanhef en onder a	Artikel 74, aanhef, lid 3 en onder a; artikel 77, aanhef, lid 1 en onder a; artikel 84, aanhef, lid 1 en onder a, van het wetsvoorstel	De mogelijkheid voor lidstaten om meer handhavingsbevoegdheden te doen toekomen de cybercrisisbeheerautoriteiten dan die genoemd in artikel 33, vierde lid, van de NIS2-richtlijn.	
Artikel 33, lid 4, aanhef en onder b	Artikel 82 van het wetsvoorstel		

Artikel 33, lid 4, aanhef en onder c	Artikel 83 van het wetsvoorstel		
Artikel 33, lid 4, aanhef en onder d	Artikel 82 van het wetsvoorstel		
Artikel 33, lid 4, aanhef en onder e	Artikel 81 van het wetsvoorstel		
Artikel 33, lid 4, aanhef en onder f	Artikel 70, aanhef, lid 1, onder c; artikel 74, aanhef, lid 3 en onder b; artikel 80, aanhef, lid 1 en onder c, van het wetsvoorstel		
Artikel 33, lid 4, aanhef en onder g	Artikel 81 van het wetsvoorstel		
Artikel 33, lid 4, aanhef en onder h	Artikel 84 van het wetsvoorstel		
Artikel 33, lid 5	Artikel 1, artikel 44 en artikel 57, lid 2, van het wetsvoorstel		
Artikel 33, lid 6	Artikel 58 van het wetsvoorstel		
Artikel 34, lid 1	-		
Artikel 34, lid 2	Artikel 77, lid 1, en artikel 84, lid 1, van het wetsvoorstel		
Artikel 34, lid 3	-Behoeft geen implementatie.		
Artikel 34, lid 4	Artikel 74, lid 3, van het wetsvoorstel	De mogelijkheid voor lidstaten om de boetebedragen hoger vast te stellen dan het in artikel 34, vierde lid, van de NIS2-richtlijn maximumbedragen.	
Artikel 34, lid 5	Artikel 84, lid 3, van het wetsvoorstel	De mogelijkheid voor lidstaten om de boetebedragen hoger vast te stellen dan het in artikel 34, vijfde lid, van de NIS2-richtlijn maximumbedragen.	
Artikel 34, lid 6	Artikel 76, lid 3, en artikel 87 van het wetsvoorstel	De mogelijkheid voor lidstaten om te voorzien in de bevoegdheid tot oplegging van dwangsommen.	
Artikel 34, lid 7	Artikel 77, lid 7, van het wetsvoorstel		
Artikel 34, lid 8	Behoeft geen implementatie.		
Artikel 35, lid 1	Artikel 56 van het wetsvoorstel		
Artikel 35, lid 2	Artikel 52, lid 2, aanhef en onder b, van het wetsvoorstel		
Artikel 35, lid 3	Artikel 52, lid 2, aanhef en onder b, van het wetsvoorstel		
Artikel 36	Artikel 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87 en 88 van het wetsvoorstel		
Artikel 37, lid 1	Artikel 58 van het wetsvoorstel		
Artikel 38	Behoeft geen implementatie.		
Artikel 39 (Comitéprocedure)	Behoeft geen implementatie.		
Artikel 40 (Evaluatie)	Behoeft geen implementatie.		
Artikel 41 (Omzetting)	Behoeft geen implementatie.		
Artikel 42 (Wijziging van Verordening (EU) nr. 910/2014)	Behoeft geen implementatie.		
Artikel 43 (Wijziging van Richtlijn (EU) 2018/1972)	Behoeft geen implementatie.		
Artikel 44 (Intrekking)	Behoeft geen implementatie.		

Artikel 45 (Inwerkingtreding)	Behoeft geen implementatie.		
Artikel 46 (Adressaten)	Behoeft geen implementatie.		

ARTIKELSGEWIJZE TOELICHTING

Artikel 1 (begripsbepaling)

Bij de meeste definities wordt verwezen naar artikel 6 NIS2-richtlijn, waarin de begrippen uit de richtlijn worden gedefinieerd.

Overheidsinstantie
De definitie van overheidsinstantie betreft die uit artikel 6, onderdeel 35, NIS2-richtlijn. Het betreft een overheidsinstantie die overeenkomstig het nationale recht als zodanig is erkend, met uitzondering van de rechterlijke macht, parlementen en centrale banken, en die aan de volgende criteria voldoet:
a. zij is opgericht om te voorzien in behoeften van algemeen belang en heeft geen industrieel of commercieel karakter;
b. zij heeft rechtspersoonlijkheid of mag volgens de wet namens een andere entiteit met rechtspersoonlijkheid optreden;
c. zij wordt grotendeels gefinancierd door de staat, regionale autoriteiten of andere publiekrechtelijke organen, is onderworpen aan beheerstoezicht door die autoriteiten of organen, of heeft een bestuurs-, leidinggevend of toezichthoudend orgaan waarvan de leden voor meer dan de helft door de staat, regionale autoriteiten of andere publiekrechtelijke organen worden benoemd;
d. zij heeft de bevoegdheid om ten aanzien van natuurlijke of rechtspersonen administratieve of regelgevende besluiten te nemen die van invloed zijn op hun rechten op het grensoverschrijdende verkeer van personen, goederen, diensten of kapitaal.

Voor onderdeel b geldt dat de betreffende instantie niet per se zelf rechtspersoonlijkheid hoeft te hebben, maar in dat geval wel bevoegd moet zijn namens een andere rechtspersoon op te treden. Bijvoorbeeld een gemeenschappelijke regeling die gemandateerd is om namens een gemeente bepaalde besluiten te nemen voldoet aan dit vereiste voor overheidsinstantie.

Ten aanzien van onderdeel c wordt opgemerkt dat bijvoorbeeld een erkenninghouder van een erkenning APK (het uitvoeren van een Apk-keuring), veelal een garagehouder, als zelfstandig bestuursorgaan niet aan de in dat onderdeel gestelde vereisten voldoet waardoor de richtlijn daarop niet van toepassing is.

Onderdeel d stelt dat het moet gaan om de bevoegdheid om ten aanzien van natuurlijke of rechtspersonen besluiten te nemen of regelgeving vast te stellen die ook van invloed kunnen zijn op natuurlijke of rechtspersonen uit andere lidstaten. Hierbij kan bijvoorbeeld gedacht worden aan een beslissing op een vergunningaanvraag die door iemand uit een andere lidstaat is aangevraagd. De rijksoverheid, provincies, gemeenten en waterschappen voldoen hier in ieder geval aan.

Entiteit die domeinnaamregistratiediensten verleent
Bij de definitie van entiteit die domeinnaamregistratiediensten verleent is nader verduidelijkt dat het gaat om hetgeen in artikel 6, onderdeel 22, NIS 2-richtlijn wordt verstaan onder entiteit die domeinnaamregistratiediensten aanbiedt. In dit wetsvoorstel is gekozen voor de aanduiding "entiteit die domeinnaamregistratiediensten verleent" in plaats van "entiteit die domeinnaamregistratiediensten aanbiedt", omdat zulke entiteiten in de richtlijn telkens worden aangeduid als entiteiten die domeinnaamregistratiediensten verlenen en deze groep alleen in de definitiebepaling anders wordt aangeduid (artikel 6 van de NIS 2-richtlijn).

Aanbieders van openbare elektronische communicatienetwerken - & diensten
Indien een aanbieder van een openbaar elektronisch communicatienetwerk of –dienst een openbare recursieve DNS-dienst (publicly available recursive DNS service) zoals bedoeld in artikel 6 onderdeel 20, onder a NIS2-richtlijn verricht als onderdeel van de internettoegangsdienst, moet de entiteit worden geacht te vallen onder de jurisdictie zoals die voor telecom is geregeld.

Aanbieder van vertrouwensdiensten
Bij de definitie van aanbieder van vertrouwensdiensten is nader verduidelijkt dat het gaat om hetgeen in artikel 6, onderdeel 25, NIS2-richtlijn wordt verstaan onder verlener van vertrouwensdiensten.

Hierin wordt verwezen naar de definitie van vertrouwensdiensten, opgenomen in artikel 3, punt 19, van de eIDAS-verordening.

Gekwalificeerde aanbieder van vertrouwensdiensten
Bij de definitie van gekwalificeerde aanbieder van vertrouwensdiensten is nader verduidelijkt dat het gaat om hetgeen in artikel 6, onderdeel 27, NIS2-richtlijn wordt verstaan onder gekwalificeerde verlener van vertrouwensdiensten. Hierin wordt verwezen naar de definitie van gekwalificeerde vertrouwensdiensten opgenomen in artikel 3, punt 17 van de eIDAS-verordening. In de NIS2-richtlijn wordt namelijk zowel de term "aanbieder" als "verlener" gebruikt. In het kader van de consistentie is in dit wetsvoorstel gekozen om telkens te spreken van "aanbieder".

Artikel 2 (doel van deze wet)

In artikel 2 van dit wetsvoorstel is het doel van deze wet omschreven. Hetgeen hierin is opgenomen, is ontleend aan artikel 1, eerste lid, en de overwegingen 4 en 5 NIS2-richtlijn.

Artikel 3 (uitvoering uitvoeringshandelingen, gedelegeerde handelingen en richtsnoeren)

Artikel 3 van dit wetsvoorstel bevat een delegatiegrondslag om bij of krachtens amvb regels te stellen ter uitvoering van de op grond van de NIS2-richtlijn vastgestelde uitvoeringshandelingen, gedelegeerde handelingen en richtsnoeren.

Artikel 4 (jurisdictie en territorialiteit)

Artikel 4 van dit wetsvoorstel bevat bepalingen over jurisdictie en territorialiteit en betreft de implementatie van artikel 26 NIS2-richtlijn. Dit wetsvoorstel is van toepassing op essentiële entiteiten en belangrijke entiteiten die in Nederland zijn gevestigd en hun diensten verlenen of hun activiteiten verrichten in Nederland of een andere lidstaat van de Europese Unie. Tevens is in artikel 4, eerste lid, geregeld dat deze wet van toepassing is op entiteiten die domeinnaamregistratiediensten verlenen.

In het tweede en derde lid worden uitzonderingen geformuleerd voor specifieke soorten van entiteiten. In de praktijk kan het voorkomen dat een belangrijke entiteit of essentiële entiteit behoort tot meerdere van de in bijlage 1 en bijlage 2 genoemde soorten, of tegelijkertijd ook domeinnaamregistratiediensten verleent. In dat geval moeten voor de belangrijke entiteit en essentiële entiteit per soort de regels uit artikel 4 toegepast worden en zo worden bepaald of dit wetsvoorstel van toepassing is. Daarbij kunnen meerdere jurisdictieregels naast elkaar bestaan. Zo zal een elektriciteitsbedrijf dat gevestigd is in Nederland dat tegelijkertijd beheerde diensten aanbiedt met een hoofdvestiging in Duitsland, onder het toepassingsbereik van deze wet vallen. Hetzelfde geldt voor een aanbieder van cloudcomputingdiensten dat zijn hoofdvestiging in Frankrijk heeft en die in Nederland een aanbieder van openbare telecommunicatienetwerken – of diensten is. Ook op deze entiteit is dit wetsvoorstel van toepassing.

In het vierde lid wordt geregeld hoe wordt bepaald waar een entiteit zijn hoofdvestiging heeft.

Het vijfde lid regelt dat deze wet van toepassing is op de in het derde lid onder a tot en met k genoemde entiteiten, indien zij niet in de Europese Unie zijn gevestigd, maar wel hun diensten in Nederland aanbieden.

Het zesde lid regelt dat wederzijdse bijstand onder artikel 61 door bevoegde autoriteiten ook geleverd kan worden wanneer volgens de regeling van artikel 4, derde lid, Nederland geen jurisdictie zou hebben. Dit betreft een implementatie van artikel 26, vijfde lid, jo. Artikel 37 NIS2-richtlijn en maakt het mogelijk dat de bevoegde autoriteit wederzijdse bijstand verleent, ook in de gevallen dat een andere lidstaat van de Europese Unie op basis van artikel 26, eerste lid, onderdeel b, NIS2-richtlijn in beginsel jurisdictie heeft. Dit voorkomt dat de bevoegde autoriteit in Nederland ten aanzien van de in artikel 26, eerste lid, onderdeel b, NIS2-richtlijn genoemde entiteiten niet bevoegd zou zijn om in het kader van wederzijdse bijstand toezichts- en handhavingsmaatregelen te nemen wanneer die

entiteiten in Nederland diensten verlenen of waarvan een netwerk- en informatiesysteem zich in Nederland bevindt.**Artikel 4a (toepasselijkheid op sector of subsector, of type entiteit Wwke)**

Zoals al is toegelicht in het algemeen deel van deze memorie van toelichting is er een relatie tussen het onderhavige wetsvoorstel en de Wwke. Meer specifiek geldt dat entiteiten die op grond van artikel 7 Wwke zijn aangewezen als kritieke entiteit, van rechtswege worden beschouwd als essentiële entiteit als bedoeld in het onderhavige wetsvoorstel. Daarbij kan het ook gaan om kritieke entiteiten in sectoren, subsectoren dan wel binnen type entiteiten die *niet* volgen uit de bijlage van de CER-richtlijn (welke correspondeert met de bijlage van de Wwke), maar in aanvulling op de in die bijlage genoemde sectoren op grond van artikel 7a Wwke door de vakminister onder het toepassingsbereik van de Wwke zijn gebracht. Voor kritieke entiteiten in die aanvullende sectoren, subsectoren, dan wel binnen dat type entiteiten gelden de CER- en NIS2-richtlijn niet van rechtswege en geldt meer specifiek niet op grond van de NIS2-richtlijn dat die entiteiten van rechtswege essentiële entiteit zijn. Er is echter voor gekozen om ook die kritieke entiteiten van rechtswege als essentiële entiteit te beschouwen. Het is dan noodzakelijk dat de Cbw van toepassing is op die aanvullende sectoren, subsectoren dan wel type entiteiten van de Wwke. Artikel 4a voorziet hierin.

Artikel 5 (Nederlandse exclusieve economische zone)

Nederland heeft een exclusieve economische zone (EEZ) ingesteld krachtens de Rijkswet instelling exclusieve economische zone door middel van het Besluit van grenzen Nederlandse exclusieve economische zone. Deze zone wordt begrensd door de grens van de territoriale zee van Nederland (12 mijl uit de kust) enerzijds en de grenzen van het aan Nederland toekomende deel van het continentaal plat anderzijds (artikel 2 Besluit grenzen Nederlandse exclusieve economische zone).

Het gaat bij de EEZ om soevereine rechten ten behoeve van de exploratie, exploitatie, het behoud en het beheer van de levende en niet-levende natuurlijke rijkdommen van de zee, van de zeebodem en de ondergrond daarvan en ten behoeve van andere activiteiten zoals de opwekking van energie uit het water en wind. Rechtsmacht kan worden uitgeoefend ten aanzien van de bouw en het gebruik van kunstmatige eilanden, installaties en inrichtingen, het wetenschappelijk zeeonderzoek en de bescherming en het behoud van het mariene milieu. Ook Nederland oefent dergelijke soevereine rechten en rechtsmacht uit, bijvoorbeeld in het kader van olie- en gaswinning. Voor zover het kritieke infrastructuur betreft ten aanzien van dergelijke activiteiten in de Nederlandse EEZ heeft Nederland rechtsmacht.

Als het gaat om kabelverbindingen tussen landen – dus kabels die niet verbonden zijn met de uitoefening van soevereine rechten in de EEZ, zoals telecomkabels – dan is bij de aanleg van dergelijke kabels in de EEZ geen sprake van soevereine rechten, maar van de vrijheid voor alle landen om kabels te leggen.[57] In die gevallen volgt uit het VN-zeerechtverdrag een aanknopingspunt voor rechtsmacht in de EEZ voor het land van de nationaliteit van de eigenaar (en mogelijk ook de beheerder) van de kabel. Daarnaast kan het land waar de kabel aanlandt voorwaarden stellen ten aanzien van de kabel (bijvoorbeeld aanleg en gebruik) of bepaalde vormen van rechtsmacht uitoefenen ingeval van een interferentie (bijvoorbeeld verstoring of sabotage) met die kabel. In geval van soevereine rechten en uitoefening van rechtsmacht is de desbetreffende Nederlandse wet- en regelgeving ook in dat gebied van toepassing verklaard. Daarbij geldt dat de staten bij de uitoefening van deze soevereine rechten en rechtsmacht gehouden zijn het gemeenschapsrecht na te leven.[58] De toepasselijkheid van het gemeenschapsrecht volgt dus de toepasselijkheid van het nationale recht. Daarom is in artikel 5 van dit wetsvoorstel bepaald dat dit wetsvoorstel mede van toepassing is in de Nederlandse EEZ. Dit is uiteraard alleen relevant voor entiteiten die essentiële diensten aanbieden waarvan (een deel van) de infrastructuur zich in de Nederlandse EEZ bevindt.

[57] De artikelen 58 en 87 Verdrag van de Verenigde Naties inzake het recht van de zee (VN-zeerechtverdrag).
[58] Zie HvJ EG 20 oktober 2005, C-6/04, ECLI:EU:C:2005:626 (*Commissie/Verenigd Koninkrijk*), overwegingen 115 tot en met 120 en HvJ EG 29 maart 2007, C-111/05, ECLI:EU:C:2007:195 (*Aktiebolaget NN/Skatteverket*), overweging 59.

Artikel 6 (overheidsinstanties die activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving)

In artikel 6 van dit wetsvoorstel is geregeld op welke overheidsinstanties deze wet niet van toepassing is. Paragraaf 5.1.2 gaat hier nader op in.

Het eerste lid betreft de implementatie van artikel 2, zevende lid, NIS2-richtlijn. Overheidsinstanties die activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving vallen niet onder het toepassingsbereik van de NIS2-richtlijn en worden daarom uitgezonderd van het toepassingsbereik van dit wetsvoorstel. Dit geldt alleen voor overheidsinstanties die in hoofdzaak deze activiteiten uitvoeren. In overweging 8 NIS2-richtlijn is namelijk verduidelijkt dat overheidsinstanties, waarvan de activiteiten slechts zijdelings verband houden met deze gebieden, niet zouden moeten worden uitgesloten van het toepassingsgebied van de richtlijn.

Het tweede lid betreft de implementatie van artikel 2, zevende jo. Negende lid, jo. Artikel 6, onderdeel 35, jo. Overweging 11 NIS2-richtlijn.

Artikel 7 (instellingen uitgezonderd van Verordening 2022/2554)

Artikel 7 van dit wetsvoorstel strekt tot de implementatie van artikel 2, tiende lid, NIS2-richtlijn. In de laatstgenoemde bepaling is geregeld dat de NIS2-richtlijn niet van toepassing is op entiteiten die zijn uitgesloten van het toepassingsgebied van de Verordening digitale operationele weerbaarheid, in overeenstemming met artikel 2, vierde lid, van die verordening. In Nederland gaat het om de Nederlandse Investeringsbank voor Ontwikkelingslanden N.V., de N.V. Noordelijke Ontwikkelingsmaatschappij, de N.V. Limburgs Instituut voor Ontwikkeling en Financiering, de Ontwikkelingsmaatschappij Oost-Nederland N.V. en kredietunies.

Artikel 8 (essentiële entiteit van rechtswege)

Artikel 8, eerste lid, van dit wetsvoorstel strekt tot de implementatie van de artikelen 2, eerste en tweede lid, en 3, eerste lid, NIS 2-richtlijn. Voor een uitgebreide toelichting wordt verwezen naar paragraaf 5.1.1.

Artikel 8, tweede lid, van dit wetsvoorstel strekt tot de implementatie van artikel 2, eerste lid, tweede volzin, NIS2-richtlijn. Hierin is bepaald dat artikel 3, vierde lid, van de bijlage bij de Aanbeveling 2003/361/EG niet geldt voor de toepassing van de NIS2-richtlijn. Dat betekent concreet dat ondernemingen waarvan 25% of meer van het kapitaal of de stemrechten in handen is van overheidsinstanties alsnog kunnen kwalificeren als micro, kleine of middelgrote onderneming.

Artikel 9 (essentiële entiteit op basis van criteria)

Artikel 9 van dit wetsvoorstel strekt tot de implementatie van de artikelen 2, tweede lid, onderdelen b tot en met e, en 3, eerste lid, NIS2-richtlijn. Voor een uitgebreide toelichting wordt verwezen naar paragraaf 5.2.2.

Artikel 10 (essentiële entiteit die aanbieder van een essentiële dienst was)

Artikel 10 van dit wetsvoorstel strekt tot de implementatie van artikel 3, eerste lid, onderdeel g, NIS2-richtlijn. Overweging 17 NIS2-richtlijn gaat hier ook nader op in. In artikel 10 van dit wetsvoorstel is geregeld dat entiteiten die op grond van de Wet beveiliging netwerk- en informatiesystemen zijn aangewezen als aanbieder van een essentiële dienst, kunnen worden aangewezen als essentiële entiteit. Deze bevoegdheid is belegd bij de vakminister, die onder de NIS1-richtlijn ook verantwoordelijk was voor de aanwijzing van aanbieders als aanbieder van een essentiële dienst.

Artikel 11 (essentiële entiteit na aanwijzing)

Artikel 2, vijfde lid, onderdeel b, NIS2-richtlijn biedt lidstaten de mogelijkheid om te bepalen dat de richtlijn ook van toepassing is op onderwijsinstellingen, met name wanneer zij kritieke onderzoeksactiviteiten verrichten. Deze mogelijkheid is geïmplementeerd in de artikelen 11 en 14 van dit wetsvoorstel. Artikel 11 van dit wetsvoorstel biedt de Minister van Onderwijs, Cultuur en Wetenschap de mogelijkheid om instellingen voor hoger onderwijs aan te wijzen als essentiële entiteit. Paragraaf 5.1.1.4 gaat hier nader op in.

Artikel 12 (belangrijke entiteit van rechtswege)

Artikel 12, eerste lid, van dit wetsvoorstel strekt tot de implementatie van artikel 3, tweede lid, NIS2-richtlijn. Voor een uitgebreide toelichting wordt verwezen naar paragraaf 5.1.1.

Artikel 12, tweede lid, van dit wetsvoorstel strekt tot de implementatie van artikel 2, eerste lid, tweede volzin, NIS2-richtlijn. Hierin is bepaald dat artikel 3, vierde lid, van de bijlage bij de Aanbeveling 2003/361/EG niet geldt voor de toepassing van de NIS2-richtlijn. Dat betekent concreet dat ondernemingen waarvan 25% of meer van het kapitaal of de stemrechten in handen is van overheidsinstanties alsnog kunnen kwalificeren als micro, kleine of middelgrote onderneming.

Artikel 13 (belangrijke entiteit op basis van criteria)

Artikel 13 van dit wetsvoorstel strekt tot de implementatie van artikel 3, tweede lid, NIS2-richtlijn. Voor een uitgebreide toelichting wordt verwezen naar paragraaf 5.2.2.

Artikel 14 (belangrijke entiteit na aanwijzing)

Artikel 2, vijfde lid, onderdeel b, NIS2-richtlijn biedt lidstaten de mogelijkheid om te bepalen dat de richtlijn ook van toepassing is op onderwijsinstellingen, met name wanneer zij kritieke onderzoeksactiviteiten verrichten. Deze mogelijkheid is geïmplementeerd in de artikelen 11 en 14 van dit wetsvoorstel. Artikel 14 van dit wetsvoorstel biedt de Minister van Onderwijs, Cultuur en Wetenschap de mogelijkheid om instellingen voor hoger onderwijs aan te wijzen als belangrijke entiteit. Paragraaf 5.1.1.4 gaat hier nader op in.

Artikel 15 (aanwijzing en taken centrale contactpunt)

Artikel 15 van dit wetsvoorstel strekt tot de implementatie van artikel 8, derde en vierde lid, NIS2-richtlijn. In dit artikel wordt de Minister van Justitie en Veiligheid aangewezen als het centrale contactpunt als bedoeld in artikel 8, vierde lid, NIS2-richtlijn. Deze minister heeft als centrale contactpunt de in artikel 15 van dit wetsvoorstel opgenomen taken, die volgen uit de NIS2-richtlijn. Deze taken worden feitelijk vervuld door het Nationaal Cyber Security Centrum (NCSC). Dit sluit aan bij de huidige praktijk, waarin de Minister van Justitie en Veiligheid onder de Wet beveiliging netwerk- en informatiesystemen ook al is aangewezen als het centrale contactpunt en waarvan de taken van het centrale contactpunt in de praktijk worden uitgevoerd door het NCSC.

Het centrale contactpunt is verantwoordelijk voor de coördinatie van kwesties in verband met de beveiliging van netwerk- en informatiesystemen en de grensoverschrijdende samenwerking op het niveau van de Europese Unie. Dit om de grensoverschrijdende samenwerking en communicatie tussen de autoriteiten te vergemakkelijken en een doeltreffende uitvoering van de NIS2-richtlijn mogelijk te maken.[59]

[59] Overweging 39 NIS2-richtlijn.

Artikel 16 (aanwijzing en taken bevoegde autoriteit)

In artikel 16, eerste lid, van dit wetsvoorstel worden de vakministers aangewezen als de in artikel 8, eerste lid, NIS2-richtlijn bedoelde bevoegde autoriteiten voor de sectoren en subsectoren, genoemd in bijlage 1 en 2 van dit wetsvoorstel.

In artikel 16, tweede lid, van dit wetsvoorstel wordt de Minister van Economische Zaken en Klimaat aangewezen als de bevoegde autoriteit voor de entiteiten die domeinnaamregistratiediensten verlenen.

Dit wetsvoorstel biedt de mogelijkheid om instellingen voor hoger onderwijs als essentiële entiteit (artikel 11) of als belangrijke entiteit (artikel 14) onder de reikwijdte van de wet te brengen. In artikel 16, derde lid, van dit wetsvoorstel wordt daarom de Minister van Onderwijs, Cultuur en Wetenschap aangewezen als de bevoegde autoriteit voor die instellingen.

In het vierde lid van artikel 16 is geregeld dat voor de sector onderzoek de bevoegde autoriteit is de Minister die reeds is aangewezen als bevoegde autoriteit voor de sector of subsector waarin die onderzoeksorganisatie zijn of haar onderzoeksactiviteiten verricht. Voor bijvoorbeeld een onderzoeksorganisatie die onderzoek doet in de sector levensmiddelen is de Minister van Landbouw, Natuur en Voedselkwaliteit de bevoegde autoriteit en voor een onderzoeksorganisatie die onderzoek doet naar ruimtevaart de Minister van Economische Zaken en Klimaat. Voor onderzoeksorganisaties die onderzoek doen in een sector waarvoor op grond van deze wet nog geen bevoegde autoriteit is aangewezen, is de bevoegde autoriteit de Minister die het aangaat. Dat betekent dat voor een onderzoeksorganisatie die bijvoorbeeld onderzoek op onderwerpen die onder beleidsverantwoordelijkheid van het Ministerie van Defensie vallen, de Minister van Defensie de bevoegde autoriteit is.

Zoals reeds is toegelicht in paragraaf 5.1.12 van het algemeen deel van deze memorie van toelichting is ervoor gekozen om entiteiten die op grond van de Wwke (artikel 7 in samenhang met artikel 7a) zijn aangewezen als kritieke entiteit in sectoren, subsectoren dan wel binnen type entiteiten die niet uit de bijlage van de CER-richtlijn/Wwke volgen, onder het toepassingsbereik van het onderhavige wetsvoorstel te brengen (artikel 4a). De hier bedoelde kritieke entiteiten zijn daarmee van rechtswege essentiële entiteit als bedoeld in het onderhavige wetsvoorstel (artikel 8, eerste lid, onderdeel i). Voor de hier bedoelde kritieke entiteiten zal er een bevoegde autoriteit (toezichthoudende instantie) aangewezen moeten worden nu het sectoren, subsectoren dan wel type entiteiten betreft die niet in het onderhavige wetsvoorstel voorkomen. Artikel 16, vijfde lid, bepaalt dat de Wwke-bevoegde autoriteit voor de hier bedoelde entiteiten ook de bevoegde autoriteit als bedoeld in het onderhavige wetsvoorstel is.

In het zesde lid van artikel 16 is geregeld welke taken de bevoegde autoriteit heeft.

Artikel 17 (aanwijzing en taken CSIRT)

In artikel 17, eerste lid, van dit wetsvoorstel is geregeld dat het CSIRT wordt aangewezen bij amvb voor de in artikel 17 onder a tot en met e Cbw genoemde sectoren, subsectoren en entiteiten. Dit betreft de implementatie van artikel 10, eerste lid, NIS2-richtlijn.

In de overige leden van artikel 17 van dit wetsvoorstel zijn de taken van het CSIRT opgenomen. Dit betreft de implementatie van artikel 11, derde, vierde en vijfde lid, NIS2-richtlijn. Hierbij is de in artikel 11, derde lid, onderdeel b, NIS2-richtlijn gebruikte terminologie "relevante belanghebbenden" niet overgenomen in dit wetsvoorstel, omdat het in dit verband niet de belanghebbenden in de zin van artikel 1:2 Awb betreft. Om die reden is in artikel 17, tweede lid, onderdeel b, van dit wetsvoorstel gekozen voor de terminologie "andere relevante partijen".

Artikel 18 (aanwijzing en taken coördinator bekendmaking kwetsbaarheden)

In artikel 18 van dit wetsvoorstel is bepaald dat de CSIRT-coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden als bedoeld in artikel 12 NIS2-richtlijn bij amvb zal worden aangewezen.

Artikel 19 (aanwijzing en taken cybercrisisbeheerautoriteit)

In artikel 19 van dit wetsvoorstel wordt de Minister van Justitie en Veiligheid aangewezen als de cybercrisisbeheerautoriteit als bedoeld in artikel 9, eerste lid, NIS2-richtlijn. Deze rol wordt feitelijk vervuld door onderdelen die werken onder de verantwoordelijkheid van de minister, te weten de NCTV en het NCSC. Beide organisatieonderdelen hebben een rol bij een grootschalige cybercrisis, zoals vastgelegd in het Landelijk Crisisplan Digitaal.[60] Het beleggen van de taken en verantwoordelijkheid rondom het beheer van grootschalige cyberbeveiligingsincidenten en crises bij de Minister van Justitie en Veiligheid in deze wet, sluit aan op de huidige uitvoering. Daarnaast geeft het gevolg aan de operationele noodzaak van de onderdelen om bij de tenuitvoerlegging van deze taken effectief op te kunnen treden gedurende grootschalige cyberbeveiligingsincidenten en -crises.

Artikel 20 (nationale cyberbeveiligingsstrategie)

Artikel 20 van dit wetsvoorstel strekt tot de implementatie van artikel 7 NIS2-richtlijn en verplicht de Minister van Justitie en Veiligheid in overeenstemming met de Minister die het aangaat tot het opstellen van een nationale cyberbeveiligingsstrategie en uitvoerend beleid.

Artikel 21 (nationaal plan voor grootschalige cyberbeveiligingsincidenten en crisisrespons)

Artikel 21 van dit wetsvoorstel strekt tot de implementatie van artikel 9, vierde lid, NIS2-richtlijn.

Artikel 22 (nationaal register van entiteiten)

Artikel 22 van dit wetsvoorstel implementeert artikel 3, derde lid, NIS2-richtlijn. Die richtlijnbepaling verplicht lidstaten om een lijst van essentiële entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen bij te houden. Artikel 3, derde lid, NIS2-richtlijn wordt in dit wetsvoorstel geïmplementeerd als een verplichting van de Minister van Justitie en Veiligheid om een nationaal register van entiteiten tot stand te laten komen en te beheren. In artikel 45 van dit wetsvoorstel is opgenomen welke informatie entiteiten moeten aanleveren bij de Minister van Justitie en Veiligheid ten behoeve van dat register.

Artikel 23 (zorgplicht)

Artikel 23 van dit wetsvoorstel ziet op de zorgplicht en betreft de implementatie van artikel 21 NIS2-richtlijn. Voor een uitgebreide toelichting wordt verwezen naar paragraaf 5.3.

Artikel 24 (sectorspecifieke rechtshandelingen)

Artikel 24 van dit wetsvoorstel ziet op sectorspecifieke rechtshandelingen van de Europese Unie over een zorgplicht en strekt tot de implementatie van artikel 4 NIS2-richtlijn.

Artikel 25 (ontheffing zorgplicht)

Artikel 25 van dit wetsvoorstel strekt tot de implementatie van artikel 2, achtste lid, NIS2-richtlijn en ziet op een ontheffing van de zorgplicht. Zie paragraaf 5.1.1.7 voor een nadere toelichting op ontheffing van verplichtingen uit dit wetsvoorstel.

Artikel 26 (governance)

Artikel 26 van dit wetsvoorstel strekt tot de implementatie van artikel 20 NIS2-richtlijn. Zie paragraaf 5.4 voor een nadere toelichting op het bepaalde in dit artikel.

[60] Kamerstukken II 2022-2023, 26643, nr. 955.

De artikelen 27 tot en met 31 (meldplicht significante incidenten en de fases van de melding)

In de artikelen 27 tot en met 31 van dit wetsvoorstel is artikel 23, eerste, derde en vierde lid, NIS2-richtlijn geïmplementeerd. Artikel 27 van dit wetsvoorstel ziet op de meldplicht voor essentiële entiteiten en belangrijke entiteiten van significante incidenten. De artikelen 28 tot en met 31 zien op de verschillende fases van de melding. De paragrafen 5.5.1 en 5.5.2 gaan hier uitgebreid op in.

Artikel 32 (informeren van ontvangers van diensten)

Artikel 32 van dit wetsvoorstel strekt tot de implementatie van artikel 23, eerste en tweede lid, NIS2-richtlijn.

Artikel 33 (sectorspecifieke rechtshandelingen)

Artikel 33 van dit wetsvoorstel ziet op sectorspecifieke rechtshandelingen van de Europese Unie over een meldplicht en strekt tot de implementatie van artikel 4 NIS2-richtlijn.

Artikel 34 (ontheffing meldplicht)

Artikel 34 van dit wetsvoorstel strekt tot de implementatie van artikel 2, achtste lid, NIS2-richtlijn en ziet op een ontheffing van de meldplicht. Zie paragraaf 5.1.1.7 voor een nadere toelichting op vrijstellingen van verplichtingen uit dit wetsvoorstel.

Artikel 35 (vrijwillige meldingen van significante incidenten, incidenten, bijna-incidenten en cyberdreigingen)

Artikel 35 van dit wetsvoorstel strekt tot de implementatie van artikel 30, eerste en tweede lid, NIS2-richtlijn en gaat over vrijwillige meldingen van significante incidenten, incidenten, bijna-incidenten en cyberdreigingen. Zie hierover meer in paragraaf 5.5.3.

Artikel 36 (vrijwillige meldingen van kwetsbaarheden)

Artikel 36 van dit wetsvoorstel strekt tot de implementatie van artikel 12, eerste lid, NIS2-richtlijn en biedt natuurlijke personen en rechtspersonen de mogelijkheid om op vrijwillige basis melding te maken van een kwetsbaarheid bij de coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden, genoemd in artikel 18 van dit wetsvoorstel.

Artikel 37 (nadere regels over meldingen van significante incidenten)

De delegatiegrondslag in artikel 37 van dit wetsvoorstel biedt de mogelijkheid om bij amvb nadere regels te stellen ter uitwerking van de artikelen 27 tot en met 32, 35 en 36. Deze delegatiegrondslag wordt besproken in paragraaf 5.5.1.

Artikel 38 (taken CSIRT na melding significant incident)

Artikel 38 van dit wetsvoorstel strekt tot de implementatie van artikel 23, vijfde lid, NIS2-richtlijn. Dit artikel verplicht het CSIRT om een terugkoppeling te geven aan een entiteit als reactie op de door de entiteit gegeven vroegtijdige waarschuwing. Ook verleent het CSIRT indien gewenst technische ondersteuning en biedt het richtsnoeren om het incident te melden bij rechtshandhavingsinstanties indien het significante incident van criminele aard is.

Artikel 39 (openbaarmaking significant incident door CSIRT of bevoegde autoriteit)

Artikel 39 van dit wetsvoorstel strekt tot de implementatie van artikel 23, zevende lid, NIS2-richtlijn en ziet op het informeren van het publiek over een significant incident.

Artikel 40 (in kennis stelling natuurlijke personen of rechtspersonen door entiteit)

Artikel 40 van dit wetsvoorstel ziet op de bevoegdheid van de toezichthouder om een essentiële entiteit of belangrijke entiteit te verplichten om de natuurlijke personen of rechtspersonen aan wie de entiteit diensten verleent of voor wie de entiteit activiteiten uitvoert, die mogelijkerwijs door een significante cyberdreiging worden beïnvloed, in kennis te stellen van de aard van de dreiging en alle mogelijke beschermings- of herstelmaatregelen die deze natuurlijke personen of rechtspersonen kunnen nemen als reactie op die dreiging. Dit artikel betreft de implementatie van de artikelen 32, vierde lid, onderdeel e, en 33, vierde lid, onderdeel e, NIS2-richtlijn.

Artikel 41 (informatieverstrekking over gemelde significante incidenten, incidenten, bijna-incidenten en cyberdreigingen)

Artikel 41 van dit wetsvoorstel strekt tot de implementatie van de artikelen 13, eerste en derde lid, en 23, eerste lid (laatste volzin), zesde, achtste en negende lid, NIS2-richtlijn.

Dit artikel gaat over de verstrekking van informatie over significante incidenten, incidenten, cyberdreigingen en bijna-incidenten die in Nederland en in andere lidstaten zijn gemeld. Die informatie moet aan, via en door het centrale contactpunt worden verstrekt. Ten aanzien van het eerste lid wordt opgemerkt dat dit strekt ter uitvoering van artikel 13, derde lid, NIS2-richtlijn. De in dit lid genoemde meldingen van significante incidenten moeten op grond van artikel 27 van dit wetsvoorstel worden gedaan bij het CSIRT en de bevoegde autoriteit. De vrijwillige meldingen van incidenten, bijna-incidenten en cyberdreigingen als bedoeld in artikel 35, eerste lid, onderdeel a, moeten door essentiële entiteiten en belangrijke entiteiten worden gedaan bij het CSIRT. Hoewel het voor veel essentiële en belangrijke entiteiten de verwachting is dat de CSIRT-taak in de praktijk door het NCSC zal worden vervuld. Er zullen er ook sectoren zijn met een eigen sectoraal CSIRT, zoals de sector gezondheidszorg waar Z-CERT op dit moment soortgelijke taken vervuld. Dit artikel zorgt ervoor dat de Minister van Justitie als het centrale contactpunt het overzicht heeft van alle meldingen die zijn gedaan op grond van de artikelen 27 en 35, eerste lid, onderdeel a, van dit wetsvoorstel.

Dit artikel schrijft niet voor dat ook de toezichthouder (in het wetsvoorstel genoemd: de bevoegde autoriteit) de in dit artikel bedoelde incidentinformatie moet verstrekken aan het centrale contactpunt. Ten aanzien van de meldplicht voor significante incidenten geldt immers dat essentiële entiteiten en belangrijke entiteiten deze incidenten moeten melden bij zowel het CSIRT als bij de bevoegde autoriteit. Het gaat hierbij om een melding van hetzelfde incident bij twee instanties. Omdat het gaat om hetzelfde incident volstaat het om te regelen dat alleen het CSIRT de incidentgegevens moet verstrekken aan het centrale contactpunt.

Artikel 42 (informatieverstrekking over gemelde significante incidenten, incidenten, bijna-incidenten en cyberdreigingen door essentiële entiteiten die tevens kritieke entiteiten zijn)

Artikel 42 van dit wetsvoorstel strekt tot de implementatie van artikel 23, tiende lid, NIS2-richtlijn. Het artikel ziet op het verstrekken van informatie aan de bevoegde autoriteit, bedoeld in artikel 8 Wwke over gemelde significante incidenten door essentiële entiteiten die tevens kritieke entiteiten als bedoeld in de Wwke zijn. De Wwke betreft de nationale wet waarin de CER-richtlijn is geïmplementeerd. Over de verhouding tussen die richtlijn en de NIS2-richtlijn is in de NIS2-richtlijn onder meer toegelicht dat er een coherente aanpak moet worden gewaarborgd tussen beide richtlijnen, gezien de onderlinge verbanden tussen cyberbeveiliging en de fysieke beveiliging van entiteiten. Daartoe moeten entiteiten die uit hoofde van de CER-richtlijn als kritieke entiteiten worden aangemerkt, als essentiële entiteiten uit hoofde van de NIS2-richtlijn worden beschouwd. Bovendien moeten lidstaten ervoor zorgen dat de bevoegde autoriteiten van beide richtlijnen met elkaar samen werken en informatie uitwisselen over onder meer cyberdreigingen en incidenten die kritieke entiteiten treffen.[61]

[61] Overweging 30 NIS2-richtlijn.

Artikel 43 (informatieverstrekking in verband met incidenten met betrekking tot financiële entiteiten)

Artikel 43 van dit wetsvoorstel strekt tot de implementatie van hetgeen in overweging 40 NIS2-richtlijn is opgenomen over het doorsturen van informatie over incidenten met betrekking tot financiële entiteiten aan de CSIRT's en de bevoegde autoriteiten als bedoeld in deze wet. Het centrale contactpunt kan zulke informatie ontvangen van de bevoegde autoriteiten uit hoofde van de Verordening digitale operationele weerbaarheid. In dat geval kan hij die informatie doorsturen naar de CSIRT's en de bevoegde autoriteiten.

Artikel 44 (aanwijzing vertegenwoordiger)

Artikel 44 van dit wetsvoorstel bevat de verplichting voor bepaalde entiteiten om een vertegenwoordiger aan te wijzen. Wat onder vertegenwoordiger wordt verstaan, is gedefinieerd in artikel 1 van dit wetsvoorstel. Artikel 44 van dit wetsvoorstel betreft de implementatie van artikel 26, derde lid, NIS2-richtlijn.

Artikel 45 (informatieverstrekking ten behoeve van nationale register)

Artikel 45 van dit wetsvoorstel strekt tot de implementatie van artikel 3, vierde lid, NIS2-richtlijn. Die richtlijnbepaling schrijft voor dat lidstaten ervoor moeten zorgen dat entiteiten informatie aanleveren ten behoeve van een door lidstaten op te stellen lijst van entiteiten. Die lijst wordt in dit wetsvoorstel het nationale register genoemd en de taak van het tot stand brengen van het nationale register wordt belegd bij de Minister van Justitie en Veiligheid.

In artikel 45, eerste lid, onderdeel c, van dit wetsvoorstel is de zinsnede "indien van toepassing" opgenomen, omdat de nadere specificering van sector en subsector alleen kan worden gedaan door entiteiten die zijn genoemd in bijlage 1 en 2 van dit wetsvoorstel. Deze verplichting om de sector en subsector, bedoeld in bijlage 1 of 2 van deze wet, waartoe de entiteit behoort op te geven geldt dus bijvoorbeeld niet voor entiteiten die domeinnaamregistratiediensten verlenen, aangezien zij niet zijn opgenomen in bijlage 1 of 2 van dit wetsvoorstel.

De delegatiegrondslag in artikel 45, eerste lid, onderdeel e, van dit wetsvoorstel biedt de mogelijkheid om de opsomming van de verplicht te verstrekken informatie uit te breiden, bijvoorbeeld als in de toekomst blijkt dat er meer informatie nodig is om de taken uit de wet goed uit te kunnen voeren.

De delegatiegrondslag in artikel 45, derde lid, van dit wetsvoorstel maakt het mogelijk om bij of krachtens amvb nadere regels te stellen over de informatieverstrekking. Op basis hiervan kunnen nadere vereisten worden opgenomen over de manier waarop entiteiten de informatie dienen te verstrekken.

Artikel 46 (vrijstelling verplichting informatieverstrekking nationale register)

Artikel 46 van dit wetsvoorstel strekt tot de implementatie van artikel 2, achtste lid, NIS2-richtlijn en ziet op een vrijstelling van de verplichting om informatie te verstrekken ten behoeve van het nationale register. Zie paragraaf 5.1.1.7 voor een nadere toelichting op vrijstellingen van verplichtingen uit dit wetsvoorstel.

Artikel 47 (toegang tot nationale register)

Artikel 47 van dit wetsvoorstel bevat de verplichting voor de Minister van Justitie en Veiligheid om de bevoegde autoriteit en het CSIRT toegang te verlenen tot het nationale register van entiteiten, ten behoeve van de uitoefening van hun taken, alleen voor zover de toegang ziet op informatie over de entiteiten waarvoor zij zijn aangewezen als de bevoegde autoriteit respectievelijk het CSIRT.

Artikel 48 (informatieverstrekking ten behoeve van register van Enisa)

Artikel 48 van dit wetsvoorstel strekt tot de implementatie van artikel 27 NIS2-richtlijn. De in artikel 48, eerste lid, van dit wetsvoorstel genoemde entiteiten moeten de in het tweede lid genoemde informatie verstrekken aan het centrale contactpunt. De Minister van Justitie en Veiligheid is aangewezen als het centrale contactpunt en in de praktijk worden de taken van het centrale contactpunt uitgevoerd door het NCSC.

Na de ontvangst van de informatie zendt het NCSC die informatie door naar Enisa ten behoeve van het register van entiteiten dat Enisa onderhoudt. Hiermee wordt bewerkstelligd dat er een duidelijk overzicht is van de entiteiten die onder het toepassingsbereik van artikel 27, eerste lid, NIS2-richtlijn vallen.

Artikel 49 (vrijstelling verplichting informatieverstrekking register van Enisa)

Artikel 49 van dit wetsvoorstel strekt tot de implementatie van artikel 2, achtste lid, NIS2-richtlijn en ziet op een vrijstelling van de verplichting om informatie te verstrekken ten behoeve van het register van Enisa. Zie paragraaf 5.1.1.7 voor een nadere toelichting op vrijstellingen van verplichtingen uit dit wetsvoorstel.

Artikel 50 (database met domeinnaamregistratiegegevens)

Artikel 50 van dit wetsvoorstel betreft de implementatie van artikel 28, eerste tot en met vierde en zesde lid, NIS2-richtlijn. Dit artikel is alleen van toepassing op registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen. Deze entiteiten zijn gedefinieerd in artikel 1 van deze wet.

Artikel 50 van dit wetsvoorstel bevat de verplichting voor registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen om nauwkeurige en volledige domeinnaamregistratiegegevens te verzamelen in een database. Ook moeten zij die gegevens bijhouden. Deze verplichting is hen opgelegd om bij te dragen aan de beveiliging, stabiliteit en weerbaarheid van het domeinnaamsysteem.[62]

In het tweede lid van artikel 50 van dit wetsvoorstel is opgenomen welke gegevens de database moet bevatten. Dit betreffende de gegevens die noodzakelijk zijn om de houders van de domeinnamen en de contactpunten die de domeinnamen onder de topleveldomeinnamen te beheren, te identificeren en te contacteren.

Het derde lid van artikel 50 van dit wetsvoorstel bevat de verplichting voor registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen opgenomen om het beleid en de procedures, waaronder verificatieprocedures, vaststellen om ervoor te zorgen dat de database juiste en volledige informatie bevat. Dat beleid en die procedures ziet op het verzamelen en bijhouden van nauwkeurige en volledige domeinnaamregistratiegegevens en het voorkomen en corrigeren van onjuiste registratiegegevens. Voorbeelden van verificatieprocedures kunnen betrekking hebben op controles vooraf die worden uitgevoerd bij de registratie, en controles achteraf die worden uitgevoerd na de registratie. De registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen, moeten onder meer ten minste één van de manieren om met de domeinnaamhouder contact op te nemen, verifiëren.[63] Daarnaast zullen het hierboven genoemde beleid en procedures ook moeten ingaan op de bekendmaking en openbaarmaking van registratiegegevens, met inbegrip van overeenkomsten inzake het dienstverleningsniveau voor de behandeling van verzoeken om toegang van verzoekers om legitieme toegang. Bij het vaststellen van het beleid en procedures moet zoveel mogelijk rekening worden gehouden met richtsnoeren en normen die in internationaal verband zijn ontwikkeld.

[62] Artikel 28, eerste lid, en overweging 109 NIS2-richtlijn.
[63] Overweging 111 NIS2-richtlijn.

Het vierde lid van artikel 50 van dit wetsvoorstel bevat de verplichting voor registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen om domeinnaamregistratiegegevens die geen persoonsgegevens zijn, onverwijld na de registratie van een domeinnaam openbaar te maken. Uit de richtlijn volgt dat zij voor rechtspersonen ten minste de naam en het telefoonnummer van de domeinnaamhouder openbaar moeten maken. Ook het e-mailadres moet bekend worden gemaakt, op voorwaarde dat het geen persoonsgegevens bevat, zoals bij e-mailaliassen of functionele mailboxen.[64]

In het zesde lid van artikel 50 is een grondslag opgenomen voor het CSIRT om de gegevens uit de database te kunnen vorderen die noodzakelijk zijn voor haar taakuitoefening. De taken van het CSIRT zijn opgenomen in artikel 17 Cbw.

De grondslag in het zevende lid van artikel 50 van dit wetsvoorstel voor een ministeriële regeling van de Minister van Economische Zaken en Klimaat biedt de mogelijkheid om nadere regels te stellen over het bepaalde in dit artikel die van administratieve of uitvoeringstechnische aard zijn.

Artikel 51 (verzoeken om toegang tot gegevens over registratie van domeinnamen)

Artikel 51 van dit wetsvoorstel betreft de implementatie van artikel 28, vijfde lid, NIS2-richtlijn. Net als artikel 50 van dit wetsvoorstel is artikel 51 alleen van toepassing op registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen. Uit overweging 110 NIS2-richtlijn volgt dat onder verzoeker om legitieme toegang wordt verstaan elke natuurlijke en rechtspersoon die een verzoek indient krachtens het Unie- of nationale recht. Iedere natuurlijke of rechtspersoon die op basis van nationaal of Europees recht een grondslag heeft om (registratie)gegevens te vorderen/verzoeken en dat onderbouwd, heeft derhalve recht op die gegevens die voor de desbetreffende verzoeker nodig zijn voor de doeleinden van het toegangsverzoek. Het verzoek van verzoekers om legitieme toegang moet vergezeld gaan van een motivering aan de hand waarvan kan worden beoordeeld of toegang tot de gegevens noodzakelijk is. Onder verzoeker om legitieme toegang wordt verstaan elke natuurlijke of rechtspersoon die een verzoek indient krachtens het Unie- of nationale recht. Het kan gaan om de bevoegde autoriteit op grond van het onderhavige wetsvoorstel, om autoriteiten die krachtens het Unie- of nationale recht bevoegd zijn voor het voorkomen, onderzoeken, opsporen of vervolgen van strafbare feiten, evenals CSIRT's. De beschikbaarheid en tijdige toegankelijkheid van domeinnaamregistratiegegevens voor verzoekers, waaronder bevoegd autoriteiten en CSIRTS, om legitieme toegang is van essentieel belang om misbruik van het DNS te voorkomen en te bestrijden en om incidenten te voorkomen, op te sporen en erop te reageren. Reactie dient onverwijld doch uiterlijk binnen 72 uur te zijn.

De grondslag in het vierde lid van artikel 51 van dit wetsvoorstel voor een ministeriële regeling van de Minister van Economische Zaken en Klimaat biedt de mogelijkheid om nadere regels te stellen over het bepaalde in dit artikel die van administratieve of uitvoeringstechnische aard zijn.

Artikel 52 (samenwerking en informatie-uitwisseling tussen instanties)

Artikel 52 van dit wetsvoorstel strekt tot de implementatie van artikel 13, eerste, vierde en vijfde lid, NIS2-richtlijn. Om te garanderen dat het centrale contactpunt, de bevoegde autoriteiten en de CSIRT's hun taken uit deze wet doeltreffend en doelmatig uitvoeren, moeten zij niet alleen met elkaar samenwerken en relevante informatie uitwisselen, maar ook met diverse andere instanties, zoals de Autoriteit persoonsgegevens, de bevoegde autoriteiten van de Wwke en rechtshandhavingsautoriteiten.

Artikel 53 (samenwerking en informatie-uitwisseling tussen CSIRT's)

Artikel 53 van dit wetsvoorstel strekt tot de implementatie van artikel 10, vierde lid, NIS2-richtlijn.

[64] Overweging 112 NIS2-richtlijn.

Artikel 54 (informatie-uitwisseling met entiteiten en gemeenschappen van entiteiten)

Artikel 54 van dit wetsvoorstel implementeert artikel 10, vierde lid, jo. Artikel 29 NIS2-richtlijn.

Artikel 55 (samenwerking en informatie-uitwisseling met derde landen)

Artikel 55 van dit wetsvoorstel gaat over de samenwerking en informatie-uitwisseling met derde landen en betreft de implementatie van artikel 10, zevende en achtste lid, NIS2-richtlijn.

Het eerste lid van artikel 55 van dit wetsvoorstel strekt tot de implementatie van artikel 10, zevende lid, NIS2-richtlijn en ziet op het tot stand brengen van een samenwerkingsrelatie tussen het CSIRT en een nationaal computer security incident response team van een derde land. In de richtlijnbepaling is hierover opgenomen dat in het kader van dergelijke samenwerkingsrelaties de lidstaten de doeltreffende, efficiënte en veilige informatie-uitwisseling moeten vergemakkelijken met die nationale computer security incident response teams van derde landen, met gebruikmaking van relevante informatie-uitwisselingsprotocollen, waaronder het verkeerslichtprotocol ("traffic light protocol").
Het CSIRT kan binnen de samenwerkingsrelatie informatie uitwisselen voor zover dat noodzakelijk is voor de doeltreffende en doelmatige uitvoering van haar taken uit hoofde van deze wet. Te denken valt aan de situatie dat het CSIRT informatie verkrijgt over een server die door middel van malware gegevens uitwisselt met andere servers in landen binnen en buiten de Europese Unie: een zogenaamde *command-and-control server*, veelgebruikt bij datadiefstel, distributed-denial-of-serviceaanvallen (DdoS) en andere malware. Het CSIRT informeert dan Europese CSIRT's om hen in staat te stellen om essentiële entiteiten en belangrijke entiteiten binnen die lidstaten te informeren en maatregelen te treffen. Om echter dergelijke kwaadwillende infrastructuur duurzaam te bestrijden, is het noodzakelijk om ook nationale CSIRT's of CERT's van derde landen te informeren. Wanneer dat niet gebeurt, blijft daarmee het risico (het bestaan van die kwaadwillende infrastructuur) voor Nederlandse essentiële entiteiten en belangrijke entiteiten voortbestaan.
Ook kan worden gedacht aan de situatie dat het CSIRT beschikt over informatie over een nieuwe ransomwarevariant. Het kan noodzakelijk zijn om die informatie ook buiten de Europese Unie te delen, om te voorkomen dat partijen die zijn gevestigd buiten de Europese Unie, die in de keten een relatie hebben met een in Nederland gevestigde entiteit (bijvoorbeeld een dochteronderneming), besmet raken of blijven. Die ketens waaruit netwerk- en informatiesystemen bestaan zijn vaak EU-overstijgend. Hiervan was bijvoorbeeld sprake bij de Lockergoga-casus, waarbij uiteindelijk gegevens zijn gedeeld met partijen buiten de Europese Unie.
Indien het informatie betreft die ook persoonsgegevens bevatten moet het CSIRT hierbij uiteraard voldoen aan de nationale en internationale regels over de doorgifte van persoonsgegevens aan derde landen, waaronder die van artikel 49 van de Algemene verordening gegevensbescherming. De hierboven genoemde voorbeelden kunnen dan – wanneer het gaat om informatie die ook persoonsgegevens bevat, zoals bijvoorbeeld inloggegevens of mailbestanden– gelden als gewichtige redenen van algemeen belang. Immers, het algemeen belang van Nederland vergt dan, dat kwaadwillende infrastructuur wordt uitgeschakeld of dat ketens gevrijwaard worden van kwaadwillende besmettingen.

Het tweede lid van artikel 55 van dit wetsvoorstel strekt tot de implementatie van artikel 10, achtste lid, NIS2-richtlijn en ziet op de samenwerking tussen het CSIRT en een nationaal CSIRT of gelijkwaardig orgaan van een derde land.

Artikel 56 (samenwerking en informatie-uitwisseling tussen bevoegde autoriteiten van deze wet)

Artikel 56 van dit wetsvoorstel strekt tot de implementatie van artikel 13, vijfde lid, NIS2-richtlijn.
Zie paragraaf 5.7.13 Samenwerking toezichthouders voor een nadere toelichting.

Artikel 57 (samenwerking en informatie-uitwisseling met bevoegde autoriteiten Wet weerbaarheid kritieke entiteiten)

Artikel 57 van dit wetsvoorstel strekt tot de implementatie van artikel 13, vijfde lid, NIS2-richtlijn. Dit artikel ziet op de samenwerking en informatie-uitwisseling door de bevoegde autoriteit als bedoeld in deze wet met de bevoegde autoriteit als bedoeld in de Wwke. De Wwke betreft de nationale wet waarin de CER-richtlijn is geïmplementeerd. Over de verhouding tussen die richtlijn en de NIS2-richtlijn is in de NIS2-richtlijn onder meer toegelicht dat er een coherente aanpak moet worden gewaarborgd tussen beide richtlijnen, gezien de onderlinge verbanden tussen cyberbeveiliging en de fysieke beveiliging van entiteiten. Daartoe moeten entiteiten die uit hoofde van de CER-richtlijn als kritieke entiteiten worden aangemerkt, als essentiële entiteiten uit hoofde van de NIS2-richtlijn worden beschouwd. Bovendien moeten lidstaten ervoor zorgen dat de bevoegde autoriteiten van beide richtlijnen met elkaar samen werken en informatie uitwisselen over onder meer cyberdreigingen en incidenten die kritieke entiteiten treffen.[65]

Artikel 58 (samenwerking met bevoegde autoriteit Verordening (EU) 2022/2554)

Artikel 58 van dit wetsvoorstel strekt tot de implementatie van artikel 32, tiende lid, en artikel 33, zesde lid, NIS2-richtlijn. De bevoegde autoriteiten kunnen de lijst van kritieke derde aanbieders van ICT-diensten die op grond van artikel 31, negende lid, van de Verordening betreffende digitale operationele weerbaarheid voor de financiële sector door de ETA's wordt opgesteld en geactualiseerd gebruiken om dergelijke aanbieders ten behoeve van artikel 58, tweede lid, van dit wetsvoorstel te identificeren.

Artikel 59 (samenwerking met toezichthoudende autoriteiten in het kader van inbreuken in verband met persoonsgegevens)

Artikel 59 van dit wetsvoorstel strekt tot de implementatie van artikel 31, derde lid, en delen van artikel 35 NIS2-richtlijn.

Artikel 59, eerste lid, van dit wetsvoorstel ziet op de samenwerking tussen de bevoegde autoriteit met de toezichthoudende autoriteiten uit hoofde van de Algemene verordening gegevensbescherming (AVG).

Artikel 59, tweede lid, van dit wetsvoorstel gaat over overtredingen van de zorgplicht en van de meldplicht die een inbreuk in verband met persoonsgegevens kunnen inhouden. Hierin is bepaald dat wanneer de bevoegde autoriteit bij toezicht of handhaving er kennis van krijgt dat een overtreding van de zorgplicht of van de meldplicht een inbreuk in verband met persoonsgegevens kan inhouden die op grond van artikel 33 AVG gemeld zou moeten worden, zij de bevoegde toezichthoudende autoriteiten als bedoeld in de artikelen 55 en 56 van de AVG onverwijld daarvan in kennis moet stellen.

Artikel 59, derde lid, van dit wetsvoorstel ziet op de gevallen waarin de op grond van de AVG bevoegde toezichthoudende autoriteit in een andere lidstaat dan in Nederland is gevestigd. De bevoegde autoriteit moet dan de in Nederland gevestigde toezichthoudende autoriteit in kennis stellen van de potentiële inbreuk in verband met persoonsgegevens.

Artikel 60 (informatie-uitwisseling met andere bevoegde autoriteiten)

Artikel 60 van dit wetsvoorstel strekt tot de implementatie van artikel 13, vijfde lid, NIS2-richtlijn.

[65] Overweging 30 NIS2-richtlijn.

Artikel 61 (samenwerking met en bijstandsverzoek van de bevoegde autoriteit van de NIS2-richtlijn van een andere lidstaat)

Artikel 61 van dit wetsvoorstel betreft de implementatie van artikel 37 NIS2-richtlijn en ziet specifiek op de samenwerking van de Nederlandse bevoegde autoriteit met de bevoegde autoriteiten van de NIS2-richtlijn van andere lidstaten van de Europese Unie. De samenwerking houdt onder meer in dat de bevoegde autoriteiten elkaar via het centrale contactpunt informeren over genomen toezicht- en handhavingsmaatregelen met betrekking tot de in artikel 61, eerste lid, van dit wetsvoorstel genoemde entiteiten.

Verder schrijft de richtlijn voor dat deze bevoegde autoriteiten ook elkaar indien nodig bijstand moeten verlenen. Het doel hiervan om ervoor te zorgen dat de bevoegde autoriteiten in de verschillende lidstaten van de Europese Unie met elkaar samenwerken om zo tot effectief toezicht te komen, ook over grenzen heen. Het bijstandsverzoek van een bevoegde autoriteit van een andere lidstaat van de Europese Unie kan zien op het verstrekken van informatie of op het nemen van toezichtsmaatregelen, met inbegrip van inspecties ter plaatse, toezicht elders of beveiligingsaudits. Verder is in artikel 61 verduidelijkt dat de jurisdictieregeling van artikel 4 van dit wetsvoorstel er niet aan in de weg staat dat toezichthouders hun toezichtsbevoegdheden inzetten voor het verlenen van bijstand aan bevoegde autoriteiten uit andere lidstaten.

Wanneer de Nederlandse bevoegde autoriteit het vermoeden heeft van mogelijke gevolgen voor de wezenlijke belangen van de nationale veiligheid, de openbare veiligheid of de defensie, dan initieert die autoriteit de afstemming ter onderbouwing van de afwijzing. Om de eventuele gevolgen voor de nationale veiligheid, openbare veiligheid of defensie volledig in kaart te brengen en te onderbouwen consulteert de betreffende bevoegde autoriteit met de departementen die beleidsmatig verantwoordelijk zijn voor deze domeinen en, waar relevant, met andere betrokken bevoegde autoriteiten en de inlichtingen- en veiligheidsdiensten.

Als de netwerk- of informatiesystemen of vestigingen van een entiteit als bedoeld in artikel 61, tweede lid, van dit wetsvoorstel zich in Nederland bevinden, terwijl de hoofdvestiging van de entiteit zich in een andere lidstaat bevindt, dan is de bevoegde autoriteit bevoegd om in het kader van een aan haar gericht bijstandsverzoek toezichtsmaatregelen uit te voeren. Deze bevoegdheid omvat ook een aangewezen vertegenwoordiging, als bedoeld in artikel 44.

Deze bepaling betreft de implementatie van artikel 26, vijfde lid, NIS2-richtlijn. Hiermee wordt voorkomen dat een lidstaat door de jurisdictieregeling van artikel 26 NIS2-richtlijn onbevoegd zou zijn om bijstand te verlenen. In het geval de hoofdvestiging zich in Nederland bevindt en vestigingen of netwerk- en informatiesystemen zich in andere lidstaten bevinden, is het uiteraard voor de bevoegde autoriteit in Nederland om een wederzijds bijstandsverzoek te richten aan de betrokken bevoegde autoriteit(en) van de betreffende lidstaat.

Artikel 62 (bijstandsverzoek aan de bevoegde autoriteit van een andere lidstaat)

Artikel 62 van dit wetsvoorstel betreft de implementatie van artikel 37, meer in het bijzonder het eerste lid, onderdeel b, NIS2-richtlijn, en ziet op de bevoegdheid van de Nederlandse bevoegde autoriteit om een bijstandsverzoek te doen aan de bevoegde autoriteiten van de NIS2-richtlijn van andere lidstaten van de Europese Unie.

Artikel 64 (verwerkingsverantwoordelijkheid)

Artikel 64 van dit wetsvoorstel regelt de verwerkingsverantwoordelijkheid.

Artikel 64a (bijzondere persoonsgegevens)

In dit artikel is een grondslag opgenomen voor de verwerking van bijzondere persoonsgegevens door het CSIRT en de bevoegde autoriteit. Dit is uitgebreid toegelicht in paragraaf 6.4.

Artikel 65 (vertrouwelijke gegevens)

Dit artikel strekt tot de implementatie van artikel 2, dertiende lid, NIS2-richtlijn. Die bepaling uit de richtlijn ziet op de uitwisseling van vertrouwelijke informatie met de Europese Commissie en andere bevoegde autoriteiten.

Eerste lid

Artikel 65 Cbw bepaalt in het eerste lid wie vertrouwelijke gegevens met elkaar mogen uitwisselen. Het gaat om de Bevoegde Autoriteit, het centrale contactpunt, het CSIRT, de Minister van Justitie en Veiligheid, de bevoegde autoriteit als bedoeld in artikel 60 Cbw, de bevoegde NIS2-autoriteiten uit een andere lidstaat, een andere toezichthoudende autoriteiten die krachtens Unierecht of nationaal recht ter uitvoering van Unierecht is aangewezen of ingesteld en de Europese Commissie. Bij een andere toezichthoudende autoriteit die krachtens Unierecht of nationaal recht ter uitvoering van Unierecht is aangewezen of ingesteld, wordt in ieder geval gedacht aan de Autoriteit Persoonsgegevens. Omdat niet valt uit te sluiten dat er in de toekomst nog andere toezichthoudende autoriteiten krachtens Unierecht worden ingesteld of aangewezen met wie het eveneens noodzakelijke is vertrouwelijke gegevens te delen ter uitvoering van hun taken op grond van deze richtlijn, is voor deze ruimere formulering gekozen. Hoewel artikel 2, dertiende lid, NIS2-richtlijn het CSIRT niet expliciet noemt, is het noodzakelijk dat het CSIRT vertrouwelijke gegevens kan delen met de Bevoegde Autoriteit. Dat zich bijvoorbeeld een incident voordoet bij een essentiële of belangrijke entiteit is al een vertrouwelijk gegeven en het is van belang dat de Bevoegde Autoriteit daar ook van op de hoogte is.

In artikel 65, eerde lid, zijn verder opgesomd onder welke voorwaarden vertrouwelijke gegevens gedeeld mogen worden. Deze voorwaarden zijn overgenomen uit artikel 2, dertiende lid, NIS2-richtlijn.

Tweede lid

In het tweede lid is geregeld dat het CSIRT onder diezelfde voorwaarden vertrouwelijke gegevens mag delen met essentiële en belangrijke entiteiten en relevante partijen. Hoewel dit niet direct voortvloeit uit artikel 2, dertiende lid, NIS2-richtlijn, is het van belang dat het CSIRT genoemde partijen kan voorzien van vroegtijdige waarschuwingen, meldingen en aankondigingen en informatie over cyberdreigingen, kwetsbaarheden en incidenten, indien mogelijk in bijna-realtime, inclusief vertrouwelijke gegevens. Omdat het van belang is dat prudent met vertrouwelijke gegevens wordt omgegaan is voor de toe te passen voorwaarden aangesloten bij de voorwaarden van artikel 2, dertiende lid, NIS2-richtlijn. Relevant voor de uitoefening van de taken van het CSIRT is wat een dreiging of incident inhoudt en relevant kan zijn tot welke typen entiteiten die dreiging of dat incident zich richt, maar niet zonder meer bij wie die dreiging of dat incident zich specifiek voordoet. Dat het CSIRT vertrouwelijke gegevens als bedoeld in artikel 65, tweede lid, Cbw verstrekt aan een andere entiteit dan de entiteit zelf op wie de vertrouwelijke gegevens betrekking hebben, ligt daarom niet voor de hand.

Onder vertrouwelijke gegevens worden in beginsel die gegevens verstaan die door entiteiten vertrouwelijke aan het CSIRT zijn verstrekt. Daaronder vallen in ieder geval bedrijfsheimen. Bij bedrijfsgeheimen wordt gedacht aan technologische informatie, zoals gebruikte beveiligingsmethoden en algoritmes, maar ook aan handelsgegevens, zoals risicoanalyses of informatiebeveiligingsstrategieën. Deze vertrouwelijke gegevens kunnen ook zien op kwetsbaarheden in specifieke netwerk- en informatiesystemen (ongeacht of er sprake is van een concrete dreiging), of op specifieke informatie over dreigingen of incidenten met betrekking tot die specifieke, door die entiteit of entiteiten gebruikte systemen, voor zover dergelijke informatie niet reeds openbare informatie betreft, zoals een Autonomous System nummer (AS-nummer) of toegewezen of gebruikte IP-adressen. Ook kan worden gedacht aan concrete informatie over de entiteit die door een dreiging of incident is getroffen waarbij verdere verspreiding tot gevolg heeft dat die entiteit daarvan nadeel ondervindt (bijvoorbeeld omdat klanten weglopen, of omdat gegevens bekend worden waar

concurrenten of kwaadwillende actoren binnen het cyberdomein hun voordeel mee kunnen doen). In de praktijk zal het CSIRT met name over de hier bedoelde bedrijfsgeheimen komen te beschikken bij de uitvoering van de taken rondom de meldplicht of de taken als bedoeld in artikel 17, lid 2, aanhef en onder e en die als bedoeld in artikel 17, lid 3 Cbw.

Vertrouwelijke gegevens kunnen ook gegevens betreffen die krachtens Unie- of nationale voorschriften vertrouwelijk zijn. Hierbij wordt in elk geval gedacht aan bedrijfs- en fabricagegegevens die door natuurlijke personen of rechtspersonen vertrouwelijk aan de overheid zijn meegedeeld (artikel 5.1, eerste lid, onderdeel c, Woo). Het kan dan bijvoorbeeld gaan om gegevens die door een entiteit in het kader van de meldplicht van het onderhavige wetsvoorstel aan de overheid zijn verstrekt en daarbij zijn aangemerkt als vertrouwelijke bedrijfs- of fabricagegegevens. Het ligt voor de hand dat de hierboven bedoelde bedrijfsgeheimen veelal ook vertrouwelijk aan de overheid verstrekte bedrijfs- en fabricagegegevens zijn, maar dat is niet per definitie het geval.

Daarnaast wordt in elk geval gedacht aan persoonsgegevens (artikel 5.1, eerste lid, onderdeel d), Woo. Voor de uitwisseling van persoonsgegevens en de conformiteit hiervan met de AVG wordt verwezen naar hoofdstuk 6.

Wellicht ten overvloede wordt opgemerkt dat het bepaalde in artikel 65, tweede lid, Cbw er niet aan in de weg hoeft te staan voor het CSIRT om een getroffen essentiële of belangrijke entiteit op de hoogte te stellen van het feit dat zij bijvoorbeeld zijn gehackt.

Derde lid

Artikel 65, derde lid, kent een bijzondere openbaarheidsregeling voor vertrouwelijke gegevens. De bijzondere regeling geldt niet alleen zolang die gegevens bij de in het eerste en tweede lid genoemde overheidsinstanties berusten, maar ook nadat zij zijn verstrekt. De Wbni kende in relatie tot de Woo eenzelfde bijzondere openbaarmakingsregeling. Daardoor vallen onder andere incidentgegevens en ten behoeve van het toezicht verkregen onderzoeksgegevens volledig onder de uitzondering en hoeven zij dus niet openbaar te worden gemaakt. De vertrouwelijkheid van gegevens over bijvoorbeeld incidenten en kwetsbaarheden in de beveiliging van entiteiten moet zo veel mogelijk worden geborgd reputatieschade, benadeling van de concurrentiepositie en toegenomen kwetsbaarheid voor aanvallen kunnen worden voorkomen. Daarnaast moeten deze gegevens voor hulpverlening kunnen worden gebruikt zonder dat zij openbaar gemaakt worden. Denk daarbij aan een kwetsbaarheid in een systeem waarvoor nog geen "patch" bestaat. Datzelfde geldt voor de uitoefening van het toezicht. Met name als het gaat om niet verplicht te melden gegevens bestaat bij mogelijke openbaarmaking het risico dat entiteiten terughoudend worden met het delen van informatie aan CSIRT's en toezichthouders waardoor deze niet in staat zijn hun taken naar behoren uit te oefenen.

Deze bijzondere openbaarheidsregel zoals opgenomen in artikel 65, derde lid, Cbw, geldt echter niet voor milieu-informatie. De Woo kent (net als de Wob) aparte regels voor milieu-informatie, omdat dit voortvloeit uit het Verdrag van Aarhus EU en -richtlijn 2003/4/EG. Voor de definitie van 'milieu-informatie' wordt in de Woo (net als in de Wob) verwezen naar artikel 19.1a Wet milieubeheer. Zo geldt dat als e sprake is van een zwaarwegend belang, waaronder het belang van het milieu valt, dan mag een bestuursorgaan informatie actief openbaar maken, ook al zijn een of meer uitzonderingen op de openbaarmaking van toepassing (artikel 3.4 Woo). Voor de relatieve weigeringsgrond *economische of financiële belangen van de Staat, andere publiekrechtelijke lichamen of bestuursorganen* geldt dat in het geval van milieu-informatie enkel een beroep op deze grond kan worden gedaan als de informatie een vertrouwelijk karakter heeft (artikel 5,2, tweede lid, onderdeel b, Woo). Als relatieve weigeringsgrond is daarnaast opgenomen dat het belang van openbaarmaking van de desbetreffende informatie moet kunnen worden afgewogen tegenover het belang van het milieu waar de informatie op ziet (artikel 5,2, tweede lid, onderdeel g, Woo) Hoewel als hoofdregel geldt dat persoonlijke beleidsopvattingen niet (dan wel in niet-herleidbare vorm) openbaar worden gemaakt, geldt met betrekking tot milieu-informatie dat de openbaarmaking van de persoonlijke beleidsopvatting moet

worden afgewogen tegen het belang van de openbaarmaking van de milieu-informatie (artikel 5.2, vierde lid, Woo). Tenslotte wordt in dit verband opgemerkt dat milieu-informatie die betrekking heeft op emissies (schadelijke stoffen) in het milieu altijd openbaar gemaakt moet worden (artikel 5.1, zevende lid, Woo).

Artikel 66 (verstrekking van gegevens in relatie tot nationale veiligheid, openbare veiligheid en defensie)

In artikel 66 van dit wetsvoorstel is artikel 2, elfde lid, NIS2-richtlijn geïmplementeerd. Voor de informatie-uitwisseling bij of krachtens het onderhavige wetsvoorstel geldt op grond van dit artikel dat er geen informatie wordt verstrekt waarvan de bekendmaking strijdig is met de wezenlijke belangen van nationale veiligheid, openbare veiligheid of defensie. Het gaat hierbij in elk geval om overheidsinformatie welke is gerubriceerd op grond van het Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013). Te denken valt aan inlichtingenberichten van de Nederlandse inlichtingen- en veiligheidsdiensten.

Artikel 67 (toezichthouders)

Artikel 67 van dit wetsvoorstel ziet op de aanwijzing van natuurlijke personen die zijn belast met het toezicht op de naleving van het bepaalde bij of krachtens dit wetsvoorstel. Deze natuurlijke personen beschikken na de aanwijzing over de bevoegdheden uit titel 5.2 Awb en de toezichtsbevoegdheden in dit wetsvoorstel.

Artikel 68 (controlefunctionaris)

Artikel 68 van dit wetsvoorstel strekt tot de implementatie van artikel 32, vierde lid, onderdeel g, NIS2-richtlijn en ziet op de bevoegdheid van de toezichthouder om bij een essentiële entiteit een controlefunctionaris aan te wijzen. De taken en het doel van de controlefunctionaris zijn toegelicht in paragraaf 5.7.5.

In artikel 68, derde lid, van dit wetsvoorstel is de hoofdregel opgenomen dat in beginsel de essentiële entiteit de kosten van de controlefunctionaris draagt. Artikel 68, vierde lid, van dit wetsvoorstel betreft een grondslag om bij of krachtens amvb nadere regels te stellen, onder meer over de vereisten die gelden voor de aanwijzing van de controlefunctionaris.

Artikel 69 (beveiligingsscan)

Artikel 69 van dit wetsvoorstel betreft de implementatie van artikel 32, tweede lid, onderdeel d, NIS2-richtlijn en ziet op de bevoegdheid van de toezichthouder om een beveiligingsscan uit te voeren of uit te laten voeren bij een essentiële entiteit. Paragraaf 5.7.6 gaat hier nader op in.

Artikel 70 (beveiligingsaudit)

Artikel 70 van dit wetsvoorstel implementeert artikel 32, tweede lid, onderdelen b, en g, een na laatste en laatste alinea, en artikel 32, vierde lid, onderdeel f, NIS2-richtlijn. Artikel 70 van dit wetsvoorstel ziet op een beveiligingsaudit bij een essentiële entiteit. Paragraaf 5.7.7 gaat nader in op de beveiligingsaudit.

Artikel 70a (ad hoc beveiligingsaudit)
Artikel 70a van dit wetsvoorstel implementeert artikel 32, tweede lid, onderdelen, c een na laatste en laatste alinea, en artikel 32, vierde lid, onderdeel f, NIS2-richtlijn. Artikel 70 van dit wetsvoorstel ziet op een beveiligingsaudit bij een essentiële entiteit. Paragraaf 5.7.7 gaat nader in op de beveiligingsaudit.

Artikel 71 (openbaarmaking overtreding)

Artikel 71 van dit wetsvoorstel strekt tot de implementatie van artikel 32, vierde lid, onderdeel h, NIS2-richtlijn en ziet op de bevoegdheid van de toezichthouder om een essentiële entiteit de verplichting op te leggen om onderdelen van een door de entiteit begane overtreding van het bepaalde bij of krachtens deze wet, openbaar te maken.

Artikel 72 (aanwijzing)

Artikel 72 van dit wetsvoorstel ziet op de implementatie van artikel 32, vierde lid, onderdeel b, NIS2-richtlijn en ziet op de bevoegdheid van de toezichthouder tot het opleggen van een bindende aanwijzing aan een essentiële entiteit. Paragraaf 5.7.8 gaat hier nader op in.

Artikel 73 (last onder bestuursdwang)

Artikel 73 van dit wetsvoorstel strekt tot de implementatie van de artikelen 32, vierde lid, onderdeel c en d, en 34, zesde lid, NIS2-richtlijn en ziet op de bevoegdheid van de toezichthouder tot het opleggen van een last onder bestuursdwang aan een essentiële entiteit. Paragraaf 5.7.10 gaat nader in op deze bevoegdheid.

De artikelen 74 tot en met 76a (einddatum van de bevoegde autoriteit, beëindiging overtreding, of vergunning verzoek tot schorsing certificering of vergunning en verzoek tot schorsing leden van het bestuur uitzondering voor overheidsinstanties)

In de artikelen 74 tot en met 76a van dit wetsvoorstel is artikel 32, vijfde lid, NIS2-richtlijn geïmplementeerd. De hierin opgenomen bevoegdheden van de toezichthouder zijn alleen van toepassing ten aanzien van essentiële entiteiten. Voor een uitgebreide toelichting hierop wordt verwezen naar paragraaf 5.7.10.

Artikel 77 (bestuurlijke boete)

Artikel 77 van dit wetsvoorstel betreft de implementatie van de artikelen 32, vierde lid, onderdeel i, en 34, tweede en vierde lid, NIS2-richtlijn en ziet op de bevoegdheid van de toezichthouder om een bestuurlijke boete op te leggen aan een essentiële entiteit. Paragraaf 5.7.11 gaat uitgebreid in op deze bevoegdheid.

Artikel 78 (reikwijdte)

Artikel 78 van dit wetsvoorstel strekt tot de implementatie van artikel 33, eerste lid, NIS2-richtlijn en maakt een belangrijk verschil in het onderscheid tussen het toezicht op essentiële entiteit en dat op belangrijke entiteiten. Paragraaf 5.7.3 gaat hier nader op in.

Artikel 79 (beveiligingsscan)

Artikel 79 van dit wetsvoorstel strekt tot de implementatie van artikel 33, tweede lid, onderdeel c, NIS2-richtlijn en ziet op de bevoegdheid van de toezichthouder om een beveiligingsscan uit te voeren of uit te laten voeren bij een belangrijke entiteit. Paragraaf 5.7.6 gaat hier nader op in.

Artikel 80 (gerichte beveiligingsaudit)

Artikel 80 van dit wetsvoorstel implementeert artikel 33, tweede lid, onderdelen b en f, een na laatste en laatste alinea, en artikel 33, vierde lid, onderdeel f, NIS2-richtlijn. Artikel 80 van dit wetsvoorstel ziet op een beveiligingsaudit bij een belangrijke entiteit. Paragraaf 5.7.7 gaat nader in op de beveiligingsaudit.

Artikel 81 (openbaarmaking overtreding)

Artikel 81 van dit wetsvoorstel strekt tot de implementatie van artikel 33, vierde lid, onderdeel g, NIS2-richtlijn en ziet op de bevoegdheid van de toezichthouder om een belangrijke entiteit de verplichting op te leggen om onderdelen van een door de entiteit begane overtreding van het bepaalde bij of krachtens deze wet, openbaar te maken.

Artikel 82 (aanwijzing)

Artikel 82 van dit wetsvoorstel ziet op de implementatie van artikel 33, vierde lid, onderdeel b, NIS2-richtlijn en ziet op de bevoegdheid van de toezichthouder tot het opleggen van een bindende aanwijzing aan een belangrijke entiteit. Paragraaf 5.7.8 gaat hier nader op in.

Artikel 83 (last onder bestuursdwang)

Artikel 83 van dit wetsvoorstel strekt tot de implementatie van de artikelen 33, vierde lid, onderdeel c en d, en 34, zesde lid, NIS2-richtlijn en ziet op de bevoegdheid van de toezichthouder tot het opleggen van een last onder bestuursdwang aan een belangrijke entiteit. Paragraaf 5.7.10 gaat nader in op deze bevoegdheid.

Artikel 84 (bestuurlijke boete)

Artikel 84 van dit wetsvoorstel betreft de implementatie van de artikelen 33, vierde lid, onderdeel h, en 34, tweede en vijfde lid, NIS2-richtlijn en ziet op de bevoegdheid van de toezichthouder om een bestuurlijke boete op te leggen aan een belangrijke entiteit. Paragraaf 5.7.11 gaat uitgebreid in op deze bevoegdheid.

Artikel 85 (reikwijdte)

Artikel 85 van dit wetsvoorstel verduidelijkt dat de artikelen 86 tot en met 88 van dit wetsvoorstel alleen van toepassing zijn op de entiteit die domeinnaamregistratiediensten verleent, die op grond van dit wetsvoorstel niet tevens essentiële entiteit of belangrijke entiteit is. Indien een entiteit die domeinnaamregistratiediensten verleent ook op grond van dit wetsvoorstel een essentiële entiteit of belangrijke entiteit is, dan gelden de bepalingen over het toezicht en de handhaving op essentiële entiteiten respectievelijk belangrijke entiteiten.

De artikelen 86 tot en met 88 (aanwijzing, last onder dwangsom en bestuurlijke boete)

De NIS2-richtlijn bevat geen specifieke bepalingen over het toezicht op de naleving van de verplichtingen die gelden voor entiteiten die domeinnaamregistratiediensten verlenen, anders dan de algemene bepaling dat lidstaten ervoor moeten zorgen dat hun bevoegde autoriteiten effectief toezicht houden op en de noodzakelijke maatregelen nemen om te zorgen voor de naleving van de richtlijn (artikel 31, eerste lid, NIS2-richtlijn). Dit betekent dat het aan de lidstaten is om te komen tot een passende invulling van het toezicht op deze entiteiten.

Voor het toezicht op entiteiten die domeinnaamregistratiediensten verlenen is gekozen voor de bevoegdheid van de toezichthouder tot het opleggen van een aanwijzing, last onder dwangsom en bestuurlijke boete. Er is gekozen om niet te voorzien in de bevoegdheid tot het opleggen van een last onder bestuursdwang. Paragraaf 5.7.3 gaat hier nader op in.

Artikel 88a (ondersteuning CSIRT ten behoeve van andere entiteiten)

De Wbni zal worden ingetrokken (zie artikel 93 Cbw). Een aantal entiteiten dat onder de Wbni recht op bijstand van het NCSC heeft, valt niet van rechtswege onder de Cbw of wordt hiervan uitgezonderd. Deze partijen verliezen daardoor het recht op bijstand van een CSIRT met intrekking van de Wbni en dat is ongewenst. Hoewel dit strikt genomen niet voortvloeit uit de NIS2-richtlijn is het is in het belang van de cyberveiligheid en nationale veiligheid dat daartoe aangewezen partijen hun recht op bijstand

van het NCSC behouden. In artikel 88a Cbw is daarom geregeld dat die entiteiten die waren aangewezen als vitale aanbieder krachtens de Wbni, zoals die wet luidde op de dag voorafgaande aan de intrekking en waarop de Cbw niet van toepassing is, recht op ondersteuning door en bij regeling of besluit van de Bevoegde Autoriteit, na overleg met onze Minister, aan te wijzen CSIRT.
Het moet gaan om entiteiten waarop de Cbw niet krachtens artikel 4 van toepassing is. Omdat er op grond van de Wbni partijen zijn die recht hebben op bijstand van een CSIRT en die zullen verliezen vanwege de beperking in het toepassingsbereik zoals opgenomen in artikel 2, achtste lid, NIS2-richtlijn (en geïmplementeerd in artikel 6 van deze wet), wordt in artikel 88a expliciet geregeld dat artikel 6 hierop niet van toepassing is.
Het CSIRT zal op grond van artikel 88a ten aanzien van de betrokken entiteit de taken genoemd in artikel 17, tweede lid, onder a tot en met d, van deze wet verrichten alsmede bijstand verlenen in het geval zich een significant incident voordoet. Het betreft hier de taken die het CSIRT reeds op grond van de Wbni uitoefent jegens de betrokken entiteit.

Artikel 89 (wijziging Telecommunicatiewet)

Voor aanbieders van openbare elektronische communicatienetwerken en -diensten (telecomaanbieders) gold al – voor de komst van de NIS2-richtlijn – op grond van andere Europese regelgeving een meldplicht van incidenten en een zorgplicht. Deze zorg- en meldplicht was geregeld in de Europese richtlijn *European Electronic Communications Code (EECC oftewel Telecomcode)*[66] en is in Nederland geïmplementeerd in de Telecommunicatiewet (Tw). De NIS2-richtlijn brengt de telecomsector onder de werking van deze richtlijn door in artikel 43 van de NIS2-richtlijn de artikelen 40 en 41 van de Telecomcode te schrappen. De artikelen 40 en 41 van de Telecomcode gaan over de meldplicht, zorgplicht en het toezicht hierop.
Bij de nationale implementatie van de NIS2-richtlijn is bezien in hoeverre alle relevante bepalingen met betrekking tot de meldplicht, zorgplicht en toezicht uit de Telecommunicatiewet moeten worden gewijzigd omdat mogelijk de implementatiewet hierin zou kunnen voorzien.

Allereerst kan de meldplicht in de Telecommunicatiewet worden vervangen door de meldplicht zoals opgenomen in het onderhavige wetsvoorstel en kunnen de bestaande bepalingen inzake de meldplicht in de Telecommunicatiewet zoals bedoeld in artikel 11a.2 van die wet worden geschrapt.

Voor wat betreft de zorgplicht is deze – zoals geformuleerd in artikel 40, eerste lid, van de EECC en zoals geïmplementeerd in artikel 11a.1, eerste lid, van de Telecommunicatiewet – niet gelijkluidend aan de zorgplicht zoals bedoeld in artikel 21, eerste lid, van de NIS2-richtlijn en zoals bepaald in artikel 23 van dit wetsvoorstel. Daar waar de huidige sectorspecifieke wetgeving aangeeft dat aanbieders van openbare elektronische communicatienetwerken of openbare elektronische communicatiediensten passende en evenredige technische en organisatorische maatregelen moeten nemen om de risico's voor de beveiliging van hun netwerken of diensten te beheersen gaat de NIS2-richtlijn uit van essentiële respectievelijk de belangrijke entiteit die passende en evenredige technische, operationele en organisatorische maatregelen moet nemen om de risico's *voor de beveiliging van de netwerk- en informatiesystemen*, die zij voor haar werkzaamheden of voor het verlenen van haar diensten gebruikt, te beheersen. De reikwijdte van de zorgplicht uit de telecommunicatiewetgeving verschilt van die uit de NI2-richtlijn. De huidige zorgplicht uit de Telecommunicatiewet heeft een zeer brede reikwijdte die zowel op de totale beveiliging van de openbare elektronische communicatienetwerken als de openbare elektronische communicatiediensten ziet. De NIS2- richtlijn gaat over de beveiliging van netwerk- en informatiesystemen: hiertoe behoren in ieder geval de elektronische communicatienetwerken, aangezien in artikel 6, eerste lid, van de NIS2- richtlijn voor de definitie van "netwerk- en informatiesystemen" wordt verwezen naar de definitie van "elektronisch communicatienetwerk" zoals die in de Telecomcode is opgenomen. Voor wat betreft de veiligheid van diensten kan weliswaar worden gesteld dat een hoger niveau van beveiliging van netwerk– en informatiesystemen tot een hoger beveiligingsniveau zou moeten leiden van de

[66] https://eur-lex.europa.eu/eli/dir/2018/1972/oj.

diensten die via die netwerk- en informatiesystemen worden aangeboden. Echter, uit de "beveiliging van netwerk– en informatiesystemen" kan niet zonder meer worden afgeleid dat beveiligde netwerk- en informatiesystemen impliceren dat de openbare elektronische communicatiediensten die via deze systemen worden aangeboden daardoor ook in dezelfde mate veilig zijn. Derhalve behoudt de Telecommunicatiewet een bepaling – artikel 11a.1, eerste lid – die qua reikwijdte vergelijkbaar is met de huidige beveiliging van diensten zoals voorzien in de huidige artikel 11a.1, eerste lid.

Nederland heeft de afgelopen jaren ook maatregelen met betrekking tot de mobiele openbare elektronische communicatienetwerken genomen om de toenemende risico's en dreigingen vanuit statelijke actoren te adresseren, met name als het om de toeleveringsketen gaat. Hiervoor zijn in het kader van de nationale veiligheid noodzakelijke wettelijke maatregelen getroffen. Het gaat hierbij om het *Besluit veiligheid en integriteit telecommunicatie (Bvit)*[67] *en de Regeling veiligheid en integriteit telecommunicatie (Rvt)*[68]*.* In de amvb is de mogelijkheid gecreëerd om aan aanbieders de verplichting op te leggen om bepaalde leveranciers die apparatuur voor de telecommunicatienetwerken leveren te kunnen weren. In de regeling zijn meerdere, veelal technische beveiligingsmaatregelen opgenomen, onder andere op het gebied van toegangsbeheer, encryptie en configuratie van technische apparatuur. Met het oog op voortzetting van deze bestaande wetgeving wordt een delegatiegrondslag in de Telecommunicatiewet opgenomen. Dit is geregeld in het voorgestelde artikel 11a.1, tweede lid (nieuw), van de Telecommunicatiewet.

Met onderdeel E wordt het toezicht op de meldplicht in de Telecommunicatiewet geschrapt aangezien de meldplicht alsmede het toezicht hierop volledig wordt geregeld in dit wetsvoorstel.

Artikel 90 (wijziging Wet open overheid)

Voor wat betreft de uitzondering op de Wet open overheid, wordt de bijlage bij artikel 8.8. van de Woo overeenkomstig is bepaald in artikel 65, derde lid, aangepast. Tevens vervalt in genoemde bijlage de verwijzing naar de Telecommunicatiewet.

Artikel 91 (wijziging wet op economische delicten)
Ter implementatie van de NIS2-richtlijn wordt de Telecommunicatiewet gewijzigd, zie de artikelsgewijze toelichting bij artikel 90. Meer specifiek geldt dat artikel 11a1, Tw, zodanig wordt gewijzigd dat de verwijzing naar artikel 11a1, vijfde en zesde lid, Tw in de Wet op de economische delicten niet meer juist is. Om die reden wordt in artikel 1, onderdeel 1°, van de Wet op de economische delicten in de zinsnede met betrekking tot de Telecommunicatiewet "11a.1, vijfde en zesde lid," geschrapt.

Artikel 92 (intrekking Wet beveiliging netwerk- en informatiesystemen

De NIS1-richtlijn is in 2018 geïmplementeerd in de Wbni. Omdat de NIS2-richtlijn de NIS1-richtlijn intrekt en vervangt, zal de Wbni worden ingetrokken.
Artikel 93 (inwerkingtreding)

Dit artikel bevat de inwerkingtredingsbepaling.

Artikel 94 (citeertitel)

Dit artikel bevat de citeertitel van deze wet: Cyberbeveiligingswet.

[67] https://wetten.overheid.nl/BWBR0042843/2020-03-01
[68] https://wetten.overheid.nl/BWBR0045665/2021-10-06

Bijlagen

Bijlage 1 van dit wetsvoorstel correspondeert met bijlage I van de NIS2-richtlijn en bijlage 2 van dit wetsvoorstel correspondeert met bijlage II van de NIS2-richtlijn.

De Minister van Justitie en Veiligheid,