MEMORIE VAN TOELICHTING

ALGEMEEN DEEL

INHOUDSOPGAVE

1. Inleiding

Dit wetsvoorstel voor de Cyberbeveiligingswet (hierna: Cbw) 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 NIS1-richtlijn, die in 2018 is geïmplementeerd in de Wet beveiliging netwerk- en informatiesystemen.[2] Het doel van de NIS1-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 (hierna: EU). 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 EU 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). Voor deze richtlijn worden verschillende afkortingen gebruikt. Naast de afkorting NIS1-richtlijn (naar de Engelse benaming van deze richtlijn) wordt de richtlijn in Nederland soms ook wel aangeduid als de NIB-richtlijn of NIB1-richtlijn, waarbij voor die afkorting gebruik is gemaakt van de Nederlandse benaming van de richtlijn.
[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. domeinnaamregistratiegegevens;
f. toezicht en handhaving;
g. nationale cyberbeveiligingsstrategie;
h. aanwijzing CSIRT, centraal contactpunt en bevoegde autoriteiten;
i. samenwerking op nationaal, 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, 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. Deze uitbreidingen zijn nodig om de sectoren en diensten die van vitaal belang zijn voor belangrijke maatschappelijke en economische activiteiten in de interne markt, volledig te bestrijken.[6]

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 van rechtswege onder het toepassingsbereik van de richtlijn vallen indien zij voldoen aan bepaalde criteria, zoals omvang. Ten aanzien van entiteiten die niet van rechtswege onder het toepassingsbereik van de NIS2-richtlijn vallen, 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, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen
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 deze entiteiten is een aantal verplichtingen, waaronder de zorgplicht en de meldplicht, niet van toepassing, voor zover zij niet tevens een essentiële entiteit of belangrijke entiteit zijn. In dat geval gelden voor hen uitsluitend andere specifieke verplichtingen, zoals die over het verzamelen van domeinnaamregistratiegegevens in een database. Voor deze entiteiten gelden deze specifieke verplichtingen, vanwege hun belang voor de beveiliging,

[6] Overweging 6 NIS2-richtlijn.

weerbaarheid en stabiliteit van het domeinnaamsysteem (hierna: DNS).[7] Indien een aanbieder van domeinnaamregistratiediensten tevens een belangrijke entiteit of essentiële entiteit is, gelden de bijhorende verplichtingen, zoals de zorgplicht en de meldplicht, uiteraard wel.

d. verplichtingen
De NIS2-richtlijn bevat diverse verplichtingen, zoals die over het nemen van maatregelen voor het beheer van cyberbeveiligingsrisico's (zorgplicht), het melden van significante incidenten (meldplicht) en 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. domeinnaamregistratiegegevens
Het onderhouden van een nauwkeurige en volledige database van domeinnaamregistratiegegevens en het verlenen van rechtmatige toegang tot dergelijke gegevens is essentieel om de beveiliging, stabiliteit en weerbaarheid van het DNS te waarborgen. Voor dat specifieke doel volgt uit de NIS2-richtlijn dat registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen, verplicht worden bepaalde gegevens te verwerken die daartoe nodig zijn. Daarnaast zijn de beschikbaarheid en tijdige toegankelijkheid van domeinnaamregistratiegegevens voor verzoekers om legitieme toegang 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.

f. 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 5.6 gaat hier nader op in.

g. 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.

h. 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.

i. 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 samenwerken, 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.[8] Ook wordt een netwerk

[7] Overweging 109 NIS2-richtlijn.
[8] De samenwerkingsgroep bestaat uit vertegenwoordigers van de lidstaten, de Europese Commissie en het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa).

van nationale CSIRT's (het CSIRT-netwerk) uitgebreid[9] en wordt met de NIS2-richtlijn het EU-netwerk van verbindingsorganisaties voor cybercrises (EU-CyCLONe) opgericht.[10]
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.[11]

2.3 Verhouding tot de CER-richtlijn en de Wet weerbaarheid kritieke entiteiten

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.[12] 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 termijn waarbinnen de richtlijn moet zijn omgezet in nationale regelgeving als voor de NIS2-richtlijn. 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.[13] 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.[14] Verder voorzien de richtlijnen in bepalingen over onder meer de samenwerking en informatie-uitwisseling tussen de bevoegde NIS2- en CER-autoriteiten.

De Cbw 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 als andere fysieke aspecten van de

[9] 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).
[10] 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.
[11] Artikel 17 NIS2-richtlijn.
[12] *PbEU* 2022, L 333.
[13] Artikel 2, derde lid, en artikel 3, eerste lid, onderdeel f, NIS2-richtlijn.
[14] Artikel 1, tweede lid, CER-richtlijn.

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.

2.4 Verhouding tot de Verordening digitale operationele weerbaarheid

Gelijktijdig met de NIS2-richtlijn is de zogeheten Verordening digitale operationele weerbaarheid vastgesteld.[15] Deze verordening is van toepassing op de financiële sector.

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. In artikel 1, tweede lid, Verordening digitale operationele weerbaarheid is namelijk expliciet bepaald dat de verordening voor de toepassing van artikel 4 NIS2-richtlijn moet worden beschouwd als een sectorspecifieke rechtshandeling. Dit betekent dat de bepalingen uit de Cbw over de zorgplicht, governance en de meldplicht en het toezicht en de handhaving daarop, niet van toepassing zijn op financiële entiteiten die onder de verordening vallen, voor zover zij niet tevens kwalificeren als ander soort entiteit onder de Cbw. De verplichting uit artikel 44 Cbw (over het verstrekken van informatie ten behoeve van het nationale register) is wel van toepassing, voor zover deze entiteiten onder het toepassingsbereik van de Cbw vallen. De verplichtingen uit de artikelen 42 (over de aanwijzing van een vertegenwoordiger), 47 (over het verstrekken van informatie ten behoeve van het Enisa-register) en 49 (over een database met domeinnaamregistratiegegevens) Cbw zijn alleen van toepassing voor zover de betrokken financiële entiteit kwalificeert als één van de in die artikelen genoemde entiteiten en onder het toepassingsbereik van de Cbw valt.

Het is 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 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 om deel te nemen aan de activiteiten van de samenwerkingsgroep. Ook biedt de verordening de mogelijkheid om informatie uit te wisselen en samen te werken met de centrale contactpunten, de CSIRT's en de bevoegde NIS2-autoriteiten.[16] Zo moeten de uit hoofde van de Verordening digitale operationele weerbaarheid bevoegde autoriteiten de details van ernstige ICT-gerelateerde incidenten doorgeven aan de CSIRT's, de bevoegde NIS2-autoriteiten of de centrale contactpunten.[17] En voor wat betreft significante cyberdreigingen geldt dat financiële entiteiten deze op vrijwillige basis kunnen melden aan de uit hoofde van de Verordening digitale operationele weerbaarheid bevoegde autoriteit. Die bevoegde autoriteit kan vervolgens die informatie verstrekken aan onder meer de bevoegde NIS2-autoriteiten, de centrale contactpunten of de CSIRT's.[18]

De Minister van Financiën is als verantwoordelijke minister voor de financiële sector aangewezen als bevoegde autoriteit onder de Cbw.

---

[15] 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 (*PbEU* 2022, L 333).
[16] Artikel 47 Verordening digitale operationele weerbaarheid.
[17] Artikel 19, zesde lid, onderdeel c, Verordening digitale operationele weerbaarheid.
[18] Artikel 19, tweede lid, eerste alinea, jo. zesde lid, onderdeel c, Verordening digitale operationele weerbaarheid.

2.5 Verhouding tot de eIDAS-verordening

De zogeheten eIDAS-verordening geeft het wettelijk kader voor vertrouwensdiensten.[19] Vertrouwensdiensten vallen binnen de reikwijdte van de NIS2-richtlijn, voor zover deze ook onder de reikwijdte vallen van de eIDAS-verordening. In overweging 93 NIS2-richtlijn is benadrukt dat de NIS2-richtlijn aanvullend is op de eIDAS-verordening wat betreft de veiligheidseisen voor vertrouwensdiensten in de eIDAS-verordening. De eIDAS-verordening is laatstelijk gewijzigd bij Verordening (EU) 2024/1183.[20] Ten aanzien van verleners van vertrouwensdiensten en vertrouwensdiensten bevat de NIS2-richtlijn enkele bijzondere bepalingen, waaronder in artikel 2, negende lid, evenals artikel 23, vierde lid, NIS2-richtlijn.

3. Nationale context

Nederlandse Cybersecuritystrategie
De Nederlandse Cybersecuritystrategie (hierna: NLCS) beschrijft de acties en ambities van het kabinet voor de periode 2022-2028 voor een digitaal veilige samenleving.[21] 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 Europese Commissie binnen drie maanden in kennis van de vaststelling van de strategie. 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 NLCS is een generiek kader. In het kader hiervan is er ruimte voor een specifieke invulling, onder andere door sectorale beleidskaders, strategieën, agenda's, routekaarten op deelonderwerpen of aanvullende normenkaders. Strategische of beleidsmatige onderwerpen dan wel 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 Justitie en Veiligheid tot stand komen. Hiermee wordt aansluiting gezocht bij de beleidsverantwoordelijkheden van ministers zoals die op dat moment gelden.

Versterking en transformeren van het digitale ecosysteem
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

[19] Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (*PbEU* 2014, L 257).
[20] Verordening (EU) 2024/1183 van het Europees Parlement en de Raad van 11 april 2024 tot wijziging van Verordening (EU) nr. 910/2014, wat betreft de vaststelling van het Europees kader voor digitale identiteit (*PbEU* 2024, L 1183).
[21] *Kamerstukken II* 2022/23, 26643, nr. 925.

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.

Aanpak vitaal
Dit wetsvoorstel voor de Cbw en het voorstel voor de Wwke hangen 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 Cbw en de Wwke bieden een wettelijk kader voor het versterken van de digitale en fysieke weerbaarheid van onder meer de vitale infrastructuur.

4. Gemaakte implementatiekeuzes op hoofdlijnen

In de Cbw 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 (de Cyberbeveiligingswet) en niet in sectorale wetten, zoals de Wet op het financieel toezicht. Eén van de redenen hiervoor is dat de NIS2-richtlijn onder meer verplichtingen bevat waarvan het wenselijk is dat deze door de entiteiten uit de verschillende sectoren van de NIS2-richtlijn uniform worden toegepast. Bovendien bevat de NIS2-richtlijn onderwerpen waarvan de regeling per definitie alleen centraal kan worden geregeld (bijvoorbeeld het beheer van een nationaal register van essentiële entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen).

2. **Verantwoordelijkheid vakminister bij aanwijzing en ontheffing van entiteiten, medeverantwoordelijkheid Minister van Justitie en Veiligheid:** De vakminister is verantwoordelijk voor de toepassing van de Cbw 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. Dit is conform de werkwijze in de Wbni (waarin de voorganger van de NIS2-richtlijn, namelijk de NIS1-richtlijn, is geïmplementeerd) en in de Aanpak vitaal. 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 Cbw, geschiedt daarom na overleg met de Minister van Justitie en Veiligheid (zie artikel 9 Cbw).

3. **Aanwijzing gemeenten, provincies, waterschappen en gemeenschappelijke regelingen als essentiële entiteit:** In de Cbw 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). Er is gebruik gemaakt van de mogelijkheid, omdat het belangrijk is dat overheidsinstanties op alle niveaus aan een hoog beveiligingsniveau voldoen. Zij moeten op een zorgvuldige manier omgaan met gegevens van burgers en bedrijven. Burgers en bedrijven zijn bovendien vaak verplicht om hun gegevens te delen met de overheid. Paragraaf 5.1.2 gaat hier nader op in.

4. **Bevoegdheid aanwijzing onderwijsinstellingen:** In de Cbw is gebruik gemaakt van de mogelijkheid uit artikel 2, vijfde lid, onderdeel b, NIS2-richtlijn om onderwijsinstellingen aan te wijzen als essentiële entiteit of als belangrijke entiteit (zie de artikelen 11 en 13 Cbw). Het kan van belang zijn om deze instellingen onder de reikwijdte van de Cbw 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. Paragraaf 5.1.3 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 (artikel 14 Cbw). Dit is een voortzetting van het bestaande beleid onder de Wbni.

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 18 Cbw). Dit is conform staand beleid.

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. Zo wordt aangesloten bij de functie van de Minister van Justitie en Veiligheid van het centrale contactpunt. In de Cbw 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 5.7.

8. **Dubbele meldplicht:** Essentiële entiteiten en belangrijke entiteiten moeten significante incidenten zowel bij het CSIRT als bij de bevoegde autoriteit melden. Er komt een centraal meldloket zodat deze dubbele meldplicht technisch zo kan worden ingericht dat het verspreiden van de benodigde informatie maar één handeling van entiteiten vergt.

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. Daarnaast kan eenieder die geen essentiële entiteit of belangrijke entiteit is, dus ook een individu, op vrijwillige basis meldingen indienen over een significant incident, incident, bijna-incident en cyberdreiging bij een CSIRT.[22]

10. **Aanwijzing bevoegde autoriteit:** In de Cbw 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 15 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 de Cbw, 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).

5. Hoofdlijnen van de Cbw

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

[22] 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 Essentiële entiteiten en belangrijke entiteiten

De Cbw bevat diverse rechten en plichten voor essentiële entiteiten en belangrijke entiteiten. In deze paragraaf wordt ingegaan op het onderscheid tussen essentiële entiteiten en belangrijke entiteiten, de entiteiten die van rechtswege essentiële entiteit of belangrijke entiteit zijn, de entiteiten die op basis van criteria worden aangewezen als essentiële entiteit en de verhouding tot de Wwke. Daarnaast wordt ingegaan op de toepassing van de Cbw op overheidsinstanties en de lidstaatoptie om onderwijsinstellingen aan te wijzen als essentiële entiteit of belangrijke entiteit.

5.1.1 Essentiële entiteiten en belangrijke entiteiten

Onderscheid essentiële entiteit en belangrijke entiteit
De Cbw maakt een onderscheid tussen essentiële entiteiten en belangrijke entiteiten. Het onderscheid is met name van belang als het gaat om de vraag welk toezichtsregime op de entiteit van toepassing is. De NIS2-richtlijn veronderstelt dat het proportioneel is om belangrijke entiteiten minder te belasten met administratieve lasten die volgen uit toezicht dan essentiële entiteiten, vanwege hun omvang, de door hen verleende diensten en de sectoren waar zij in actief zijn. Welke entiteiten essentiële entiteit zijn en welke entiteiten belangrijke entiteit zijn, volgt uit de artikelen 8 tot en met 13 Cbw. Zo is voor entiteiten, behorende tot ten minste één van de soorten entiteiten in bijlage I bij de richtlijn (corresponderend aan bijlage 1 van de Cbw), die het plafond voor middelgrote ondernemingen uit artikel 1 van de bijlage bij de Aanbeveling 2003/361/EG[23] overschrijden, bepaald dat zij als essentiële entiteit aangemerkt worden.
Een entiteit kan onder de NIS2-richtlijn en de implementatie daarvan in de Cbw meerdere hoedanigheden bezitten. Een entiteit kan bijvoorbeeld van meerdere soorten zijn, genoemd in de laatste kolom van bijlagen 1 en 2 van de Cbw. Ook kan een entiteit zowel kwalificeren als belangrijke of essentiële entiteit en een entiteit die domeinnaamregistratiediensten verleent. In dergelijke gevallen cumuleren de verplichtingen uit de Cbw voor de betreffende entiteit. Dat is bijvoorbeeld het geval wanneer een entiteit binnen meerdere sectoren actief is. Dan rusten alle (sub)sectorale verplichtingen die op entiteiten binnen die (sub)sectoren van toepassing zijn bij of krachtens de Cbw op deze entiteit. De situatie kan ontstaan dat een entiteit volgens het ene soort als essentiële entiteit kwalificeert, maar als een ander soort als belangrijk kwalificeert. In dat geval geldt dat de gehele entiteit als essentieel kwalificeert. Als een entiteit onder de Cbw meerdere hoedanigheden bezit, zullen ook eventuele uitzonderingsregelingen per hoedanigheid toegepast moeten worden. Dit geldt ook voor de toepassing van artikel 4 Cbw over toepassingsbereik en jurisdictie, wat nader beschreven staat in de artikelsgewijze toelichting bij dat artikel.

Essentiële entiteit of belangrijke entiteit van rechtswege
Omdat de NIS2-richtlijn streeft naar harmonisatie tussen de lidstaten is in de richtlijn al voor de meeste entiteiten bepaald dat zij onder het toepassingsbereik vallen. Op basis van hun activiteiten in een bepaalde sector en hun omvang is het noodzakelijk dat zij maatregelen nemen om cyberrisico's te beheersen. Veel entiteiten zijn daarom van rechtswege essentiële entiteit (artikel 8 Cbw) of belangrijke entiteit (artikel 12 Cbw). Er hoeft dus geen beoordeling plaats te vinden van of zij worden aangewezen als essentiële entiteit of belangrijke entiteit in de zin van de Cbw. Op deze entiteiten zijn direct na de inwerkingtreding van de Cbw de daarin opgenomen rechten en plichten voor essentiële entiteiten en belangrijke entiteiten, van toepassing.
Om te bepalen of een entiteit van rechtswege essentiële entiteit of belangrijke entiteit is, is het in de meeste gevallen noodzakelijk om de omvang van de entiteit te bepalen. Hiervoor wordt gebruik gemaakt van 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. Hierbij moet worden gekeken naar het aantal werknemers, de jaaromzet en het balanstotaal. Aan de hand van de aanbeveling kan onder meer worden bepaald of een onderneming kwalificeert als een micro-, kleine, middelgrote of grote onderneming en wanneer een onderneming die kwalificatie verliest of verkrijgt. Daarnaast schrijft de aanbeveling voor in welke gevallen er sprake

[23] Aanbeveling 2003/361/EG van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (*PbEU* 2003, L 124).

is van partner- en verbonden ondernemingen. In de overheidscommunicatie over de Cbw worden digitale hulpmiddelen ter beschikking gesteld om organisaties te helpen bij het bepalen van hun omvang.

Essentiële entiteit op basis van criteria
Er zijn ook entiteiten die niet direct in de Cbw worden aangewezen als essentiële entiteit of belangrijke entiteit, omdat er eerst een beoordeling moet plaatsvinden aan de hand van criteria. Dit kan van belang zijn als een entiteit vanwege zijn omvang niet al van rechtswege onder de Cbw valt als essentiële entiteit, maar het wel noodzakelijk is dat zij maatregelen neemt om cyberrisico's te beheersen. Dit is geregeld in artikel 9, eerste lid, Cbw en betreft de implementatie van artikel 3, tweede lid, jo. artikel 2, tweede lid, onderdelen b tot en met e, NIS2-richtlijn. 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. Vanwege het belang van deze organisaties voor de nationale veiligheid worden entiteiten die voldoen aan de hiervoor bedoelde criteria altijd aangewezen als essentiële entiteit. Vanaf dat moment zijn op die entiteit de rechten en plichten die gelden voor essentiële entiteiten, van toepassing.
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. Een ander criterium is dat de entiteit in Nederland de enige aanbieder is van een dienst die essentieel is voor de instandhouding van maatschappelijke of economische activiteiten.
Om vast te stellen of een entiteit voldoet aan de criteria uit artikel 9 Cbw zal gebruik worden gemaakt van de nationale vitaalbeoordeling.[24] Hier is voor gekozen, omdat de aanmerking als vitale aanbieder plaatsvindt op basis van vergelijkbare criteria als die voor het aanwijzen van essentiële 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, in overleg met de minister van JenV als coördinerend bewindspersoon voor de bescherming van de vitale infrastructuur en cybersecurity.

Kritieke entiteit in de zin van Wwke is essentiële entiteit in de zin van Cbw
De Cbw is ook van toepassing op entiteiten die op grond van artikel 6 Wwke worden aangewezen als kritieke entiteit. Die entiteiten zijn op grond van artikel 8, eerste lid, onderdeel i, Cbw van rechtswege essentiële entiteit in de zin van de Cbw. Dit betekent dat een entiteit direct na de aanwijzing als kritieke entiteit in de zin van de Wwke, een essentiële entiteit is in de zin van de Cbw en dus ook vanaf dat moment de rechten en plichten uit de Cbw van toepassing zijn op die kritieke entiteit.

5.1.2 Overheidsinstanties

Inleiding

De NIS2-richtlijn is van toepassing op overheidsinstanties van de centrale overheid, ongeacht hun omvang. Daarnaast is de richtlijn ook van toepassing op overheidsinstanties op regionaal niveau, met dien verstande dat de richtlijn hiervoor een nadere voorwaarde bevat.[25] Op overheidsinstanties op lokaal niveau is de richtlijn slechts van toepassing voor zover een lidstaat dat heeft bepaald.[26] De regering kiest ervoor de NIS2-richtlijn ook van toepassing te laten zijn op lokale overheden. Onder lokale overheden moet in dit verband worden verstaan: in de Cbw aangewezen overheidsinstanties in de zin van de NIS2-richtlijn 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 NIS2-richtlijn zijn uitgezonderd (en daarmee dus ook van

[24] 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. Deze geïdentificeerde processen worden vitale processen genoemd en gezamenlijk vormen deze vitale processen de vitale infrastructuur van Nederland.
[25] Artikel 2, tweede lid, onderdeel f, onder ii, NIS2-richtlijn.
[26] Artikel 2, vijfde lid, onderdeel a, NIS2-richtlijn.

de Cbw) en wat overheidsinstanties van de centrale overheid in de Nederlandse context zijn. Tot slot zal de keuze om lokale overheden ook onder het toepassingsbereik van de NIS2-richtlijn te brengen worden toegelicht, evenals welke instanties het betreft.

Overheidsinstantie

Een entiteit is een overheidsinstantie als deze overeenkomstig het nationale recht als zodanig in een lidstaat is erkend en aan deze vier 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.

Criterium a betreft het doel waartoe een entiteit is opgericht. Bij een krachtens publiekrecht ingestelde entiteit zal dit doel blijken uit de wet waarbij de entiteit is ingesteld en de geschiedenis van de totstandkoming van die wet. Bij een privaatrechtelijke entiteit zal het doel blijken uit de statuten. Er zijn geen limitatieve criteria om te bepalen of een entiteit is opgericht om te voorzien in behoeften van algemeen belang en dat het voorzien in die behoefte van algemeen belang geen industrieel en commercieel karakter heeft. Relevante aanknopingspunten zijn of een entiteit onder normale marktomstandigheden opereert, of deze bestuurd wordt op basis van criteria van rendement, doelmatigheid en rentabiliteit, of de entiteit winstoogmerk als hoofddoel heeft of deze zelf de eigen verliezen draagt. Dergelijke omstandigheden wijzen in de richting van een commercieel of industrieel karakter.

Criterium b vereist dat de entiteit zelf rechtspersoonlijkheid heeft of volgens de wet mag optreden namens een andere entiteit met rechtspersoonlijkheid. Ingevolge artikel 2:1, eerste lid, Burgerlijk Wetboek (hierna: BW) bezitten de Staat, de provincies, de gemeenten, de waterschappen, alsmede alle lichamen waaraan krachtens de Grondwet verordenende bevoegdheid is verleend, rechtspersoonlijkheid. Ook kan rechtspersoonlijkheid aan een entiteit zijn toegekend in de wet waarbij de entiteit is opgericht. Verenigingen, coöperaties, onderlinge waarborgmaatschappijen, naamloze vennootschappen, besloten vennootschappen met beperkte aansprakelijkheid en stichtingen bezitten rechtspersoonlijkheid ingevolge artikel 2:3 BW. Aan criterium b wordt ook voldaan indien de entiteit zelf geen rechtspersoonlijkheid heeft, maar wel mag optreden namens een andere entiteit met rechtspersoonlijkheid. Hierbij kan worden gedacht aan zelfstandige bestuursorganen die namens de Staat mogen optreden. Ook ministers mogen namens de Staat handelen.

Criterium c ziet op de vereiste betrokkenheid van de overheid bij de entiteit. Die betrokkenheid kan verschillende vormen aannemen. Allereerst wordt aan dit criterium voldaan indien de entiteit grotendeels door de Staat, regionale autoriteiten of andere publiekrechtelijke organen wordt gefinancierd. De entiteit moet dus in hoofdzaak, dat wil zeggen voor meer dan 50%, worden gefinancierd door de overheid. Op welke manier deze financiering wordt vormgegeven, is in dat verband niet bepalend.
In de tweede plaats wordt aan dit criterium voldaan indien de entiteit onderworpen is aan beheerstoezicht door de Staat, regionale autoriteiten of andere publiekrechtelijke organen. Dit is het geval indien er een zekere afhankelijkheid bestaat van de entiteit ten opzichte van die autoriteiten of organen en indien zij de beslissingen van de entiteit kunnen beïnvloeden. Van beheerstoezicht is niet al sprake bij reguliere controle door de overheid op de naleving van regelgeving.
In de derde plaats wordt aan het criterium voldaan indien de entiteit een bestuursorgaan, leidinggevend of toezichthoudend orgaan heeft waarvan de leden voor meer dan de helft door de

Staat, regionale autoriteiten of andere publiekrechtelijke organen worden benoemd. Het begrip 'bestuursorgaan' moet niet worden gelezen als bestuursorgaan in de zin van artikel 1:1 Algemene wet bestuursrecht (hierna: Awb). Het gaat in dit kader om het bestuur van een organisatie.[27] Door middel van het benoemen van meer dan de helft van de leden van de genoemde organen, heeft de benoemende overheidsinstantie invloed op de beslissingen die de entiteit neemt.

Criterium d vereist allereerst dat de entiteit de bevoegdheid heeft om ten aanzien van natuurlijke personen of rechtspersonen administratieve of regelgevende besluiten te nemen. Het nemen van administratieve of regelgevende besluiten betreft in de Nederlandse context het nemen van besluiten in de zin van artikel 1:3 Awb. Belangrijk daarbij is dat de beslissingen een publiekrechtelijke rechtshandeling moeten inhouden. De beslissingen moeten dus onder meer rechtsgevolg hebben. Concreet betekent dit dat entiteiten die uitsluitend adviezen uitbrengen of feitelijke handelingen verrichten, niet aan dit criterium voldoen. Een entiteit heeft niet slechts een bevoegdheid om besluiten te nemen in de zin van dit criterium indien een bevoegdheid aan die entiteit is geattribueerd of gedelegeerd, maar ook indien een bevoegdheid aan die entiteit is gemandateerd. Het tweede deel van criterium d vereist dat de door de entiteit genomen besluiten van invloed zijn op de rechten van natuurlijke personen of rechtspersonen op het grensoverschrijdende verkeer van personen, goederen, diensten of kapitaal. Deze passage moet ruim worden uitgelegd. In het overgrote deel van de gevallen zal hiervan sprake zijn, ook indien sprake is van bevoegdheden met een meer nationaal karakter of gericht op nationale aangelegenheden. Slechts indien een entiteit niet het EU-recht (dat is gerelateerd aan een van de vier vrijheden) ten uitvoer brengt of indien het is uitgesloten dat besluiten van de entiteit gevolgen hebben voor natuurlijke personen of rechtspersonen buiten de lidstaat, is niet aan het tweede deel van het criterium voldaan.

Centrale overheid

De NIS2-richtlijn is van toepassing op overheidsinstanties van de centrale overheid, ongeacht hun omvang. 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 BW) alsmede de zelfstandige bestuursorganen van de centrale overheid mét rechtspersoonlijkheid. Omdat onder de Staat ook overheidsinstanties vallen die buiten het toepassingsbereik van de NIS2-richtlijn vallen, is ervoor gekozen om in de Cbw de ministeries aan te wijzen als essentiële entiteit (artikel 8, eerste lid, onder g, Cbw). Onder een ministerie worden tevens de daartoe behorende dienstonderdelen begrepen. Een ministerie heeft zelf geen rechtspersoonlijkheid, maar een minister mag wel namens de rechtspersoon de Staat optreden. Daarmee voldoet een ministerie aan het hiervoor genoemde criterium b. Ook voldoet een ministerie aan de overige criteria voor overheidsinstantie. Overigens valt het Ministerie van Defensie niet onder het toepassingsbereik van de NIS2-richtlijn en daarmee dus ook niet onder het toepassingsbereik van de Cbw, behoudens wanneer en voor zover het optreedt als verlener van vertrouwensdiensten die niet uitsluitend worden gebruikt binnen systemen die gesloten zijn als gevolg van een wettelijke regeling of een overeenkomst tussen een bepaalde groep deelnemers (zie artikel 5 Cbw).

Voorts zijn zelfstandige bestuursorganen van de centrale overheid, voor zover zij voldoen aan de vier hiervoor vermelde criteria die gelden voor het begrip overheidsinstantie, essentiële entiteit (zie artikel 8, eerste lid, onder g, Cbw). Voor wat betreft zelfstandige bestuursorganen die vallen onder de Kaderwet zelfstandige bestuursorganen geldt dat deze behoren tot de centrale overheid. Artikel 1, onder a, Kaderwet zelfstandige bestuursorganen bepaalt immers dat een zelfstandig bestuursorgaan 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 de definitie van het begrip overheidsinstantie. Als dit niet het geval is, zijn de bepalingen van de Cbw op dat zelfstandig bestuursorgaan niet van toepassing.

[27] In de Engelse versie van de NIS2-richtlijn wordt gesproken over "administrative board".

Zelfstandige bestuursorganen waarop de Kaderwet zelfstandige bestuursorganen 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 ook voor het overige voldoen aan de criteria uit de definitie van het begrip overheidsinstantie.

Lokale overheid - provincies, gemeenten en waterschappen

Ten aanzien van lokale overheden geeft de NIS2-richtlijn lidstaten in artikel 2, vijfde lid, onderdeel a, de mogelijkheid ze onder het toepassingsbereik van de NIS2-richtlijn te brengen. Van die mogelijkheid maakt de regering gebruik. De overheid zelf heeft de verplichting om op een zorgvuldige manier om te gaan met gegevens van burgers en bedrijven. Burgers en bedrijven zijn bovendien in allerlei gevallen verplicht hun gegevens te delen met de overheid. Ook heeft de overheid simpelweg een voorbeeldfunctie. De regering 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 de Cbw te brengen als essentiële entiteit (zie artikel 8, eerste lid, onder h, Cbw). 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).[28] Daarnaast zijn 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 het ontbreken van een juridische status van de BIO. Het kabinet heeft, bij monde van de Staatssecretaris van Digitale Zaken en Koninkrijksrelaties, de ambitie uitgesproken om de informatiebeveiligingsregelgeving overheidsbreed te harmoniseren en onder meer de BIO wettelijk te verankeren.[29] De keuze om lokale overheden onder het bereik van de Cbw te brengen, geeft invulling aan dit beleid.

Voor de decentrale overheden, uitgezonderd van de waterschappen, is de Minister van Binnenlandse Zaken en Koninkrijksrelaties de bevoegde autoriteit. Voor de waterschappen, ook voor hun diensten in de sector overheid, is de Minister van Infrastructuur en Waterstaat de bevoegde autoriteit, met het oog op zijn stelselverantwoordelijkheid uit de Waterschapswet en gelet op de primaire taken van de waterschappen.

De ministers die het aangaan (in het bijzonder de Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Infrastructuur en Waterstaat) stemmen de lagere regelgeving die geldt voor decentrale overheden met elkaar af.

Wellicht ten overvloede wordt opgemerkt dat de openbare lichamen 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

Gemeenschappelijke regelingen zijn op grond van artikel 8, eerste lid, onderdeel h, Cbw, aangewezen als essentiële entiteit, voor zover zij althans voldoen aan de definitie van het begrip overheidsinstantie. Specifieker gezegd betreft het openbare lichamen, bedrijfsvoeringsorganisaties en gemeenschappelijke organen als bedoeld in de Wet gemeenschappelijke regelingen. Gemeenten, provincies en waterschappen kunnen via gemeenschappelijke regelingen taken in gezamenlijkheid uitvoeren. Gemeenschappelijke regelingen zijn zo bezien als het ware een verlengstuk van decentrale overheden. Nu decentrale overheden zelf onder het toepassingsbereik van de Cbw zijn gebracht, is het wenselijk dat ook gemeenschappelijke regelingen onder het toepassingsbereik van de Cbw vallen. Het zou immers onwenselijk zijn indien het verplaatsen van decentrale taken en bevoegdheden naar een gemeenschappelijke regeling ertoe zou leiden dat de Cbw niet langer op de uitoefening van die taken en bevoegdheden van toepassing is. Evenals bij zelfstandige bestuursorganen is het, gelet op de

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

uiteenlopende aard van gemeenschappelijke regelingen, van belang om telkens per entiteit te bezien of deze voldoet aan de vier criteria uit de definitie van het begrip overheidsinstantie.
Uitgezonderde overheidsinstanties

Uitgezonderde overheidsinstanties

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 Cbw. Dit volgt uit artikel 2, zevende lid, NIS2-richtlijn. De verplichtingen uit de Cbw zijn dan ook niet op hen van toepassing. Dit geldt onder andere voor de veiligheidsregio's, het Ministerie van Defensie, het openbaar ministerie en de politie. Verder vallen de rechterlijke macht, parlementen en centrale banken niet onder het begrip overheidsinstantie (zie artikel 1 Cbw). Op rechtsprekende instanties, de Tweede en Eerste Kamer en De Nederlandsche Bank zijn de verplichtingen uit de Cbw dus evenmin van toepassing. Dit laat onverlet dat de regering eraan hecht dat deze instanties blijven voldoen aan een hoog cyberbeveiligingsniveau. Hierbij kan worden gedacht aan het blijven voldoen aan verplichtingen zoals die op dit moment zijn neergelegd in het Voorschrift Informatiebeveiliging Rijksdienst 2007 (Vir 2007[30]), het Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie 2013 (Vir-bi 2013[31]), de Baseline Informatiebeveiliging Overheid (BIO) en in toepasselijke verplichtingen van internationale herkomst.

5.1.3 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 13 Cbw. 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 de Cbw 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 de Cbw 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.[32] Dit kan schadelijk zijn voor de Nederlandse belangen. Verschillende cyberincidenten in de afgelopen jaren (onder andere bij de Universiteit Maastricht)[33] 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 de Cbw 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

[30] *Stcrt.* 2007, 122, p. 11.
[31] *Stcrt.* 2013, 15497.
[32] AIVD-jaarverslag 2021, p. 14-19.
[33] *Kamerstukken II* 2019/20, 26643, nr. 872.

de Minister van Onderwijs, Cultuur en Wetenschap na overleg met de Minister van Justitie en Veiligheid.

5.2 Zorgplicht

5.2.1 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 21 Cbw. 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 entiteit voldoende invulling heeft gegeven aan de eisen uit de Cbw.

5.2.2 Beveiliging van netwerk- en informatiesystemen

De zorgplicht uit artikel 21 Cbw heeft enkel betrekking op het beheersen van de risico's voor de beveiliging van netwerk- en informatiesystemen, het voorkomen en beperken van gevolgen van incidenten met betrekking tot deze systemen, evenals de bescherming van de fysieke omgeving van die systemen. Dit is vastgelegd in het derde lid van artikel 21 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 21 Cbw gaat voor op de zorgplicht uit artikel 15 Wwke ten aanzien van hetgeen artikel 21 Cbw regelt, namelijk het beheersen van de risico's voor de beveiliging van netwerk- en informatiesystemen, en het voorkomen of het beperken van de gevolgen van incidenten. In artikel 4 Wwke is bepaald dat die wet, en daarmee ook de in artikel 15 Wwke geregelde zorgplicht, niet van toepassing is op aangelegenheden waarop de Cyberbeveiligingswet van toepassing is.

De zorgplicht ziet op alle 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 entiteiten 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.[34]

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. Een incident betreft een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar brengt.

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.

5.2.3 De maatregelen

Passende en evenredige maatregelen
De maatregelen die de essentiële entiteiten en belangrijke entiteiten op grond van de Cbw 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 evenredig 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 evenredigheid houdt daarnaast in dat een maatregel of coherente set van maatregelen het minst belastend is voor de entiteit om het risico te beheersen.

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

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 entiteiten 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.

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, zowel gericht op preventie als detectie. Artikel 21, derde lid, Cbw bevat een opsomming van waar de maatregelen in ieder geval uit moeten bestaan. Voor entiteiten bestaat geen ruimte 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.

Bestaande normenkaders
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. Een normenkader geeft een entiteit 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 21 Cbw voldoet. De entiteit dient te borgen dat de maatregelen die zij moet nemen op grond van de Cbw in ieder geval onderdeel zijn van het maatregelenpakket.

5.3 Governance

Inleiding
Het bestuur van essentiële entiteiten en belangrijke entiteiten moet de zorgplichtmaatregelen goedkeuren en toezien op de uitvoering van die maatregelen. Daarnaast moeten de leden van het bestuur een opleiding volgen zodat zij voldoende kennis en vaardigheden verwerven om risico's te kunnen identificeren en risicobeheerspraktijken op het gebied van cyberbeveiliging en de gevolgen ervan voor de diensten die door de entiteit worden verleend, te kunnen beoordelen. Dit wordt voorgeschreven door artikel 20 NIS2-richtlijn. Dat artikel is geïmplementeerd in artikel 24 Cbw.

Training
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 daarom van belang dat bestuursleden een training volgen. Vanuit die voorbeeldfunctie dragen ze cyberbewustheid uit, in de eerste plaats naar hun werknemers die in het kader van de zorgplicht een soortgelijke training moeten volgen.
Elk lid van het bestuur van een essentiële entiteit en belangrijke entiteit moet over de kennis en vaardigheden beschikken om de risico's voor de beveiliging van netwerk- en informatiesystemen te kunnen identificeren, risicobeheersmaatregelen op het gebied van cyberbeveiliging te kunnen beoordelen en de gevolgen van de risico's en risicobeheersmaatregelen voor de diensten van de entiteit te kunnen beoordelen. Voor essentiële entiteiten en belangrijke entiteiten die naamloze vennootschappen of besloten vennootschappen zijn, en die statutair hebben bepaald dat bepaalde bestuurstaken worden verdeeld over één of meer niet-uitvoerende bestuurders en één of meer uitvoerende bestuurders, ligt dit overigens anders. In die gevallen rust de opleidingsverplichting enkel op de uitvoerende bestuursleden.
Het is aan het bestuurslid om aan te tonen dat sprake is van de hiervoor bedoelde kennis en vaardigheden. Dit kan door middel van een certificaat van een training. Bij algemene maatregel van bestuur (hierna: amvb) kunnen de vereisten van de training nader geconcretiseerd worden.
Elk lid van het bestuur moet de kennis en vaardigheden actueel houden. Dit past bij het uitgangspunt van de Cbw dat cyberweerbaarheid een cyclisch en continu 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
Voor zover het om overheidsinstanties gaat, is voor de invulling van het begrip bestuur zo veel mogelijk aangesloten bij de Grondwet en de verschillende organieke wetten. Dit betekent dat is bezien waar de verantwoordelijkheden en bevoegdheden voor de inrichting van de organisatie – en dus ook voor de cyberbeveiliging – berusten. Hoewel in de dagelijkse gang van zaken de werkzaamheden inzake cyberbeveiliging op ambtelijk niveau zullen worden uitgevoerd, liggen daar uiteindelijk niet de verantwoordelijkheden en bevoegdheden. Die berusten bij de formele, meer politieke bestuurslaag van overheidsinstanties. Het is aan deze bestuurslaag om ervoor te zorgen dat binnen de overheidsinstantie voldoende kennis en vaardigheden over cyberbeveiliging aanwezig zijn. Zonder deskundige medewerkers zal het bestuur immers in de regel niet in staat zijn om te voldoen aan de verplichtingen inzake cyberbeveiliging. Ook voor overheidsinstanties het eerdergenoemde uitgangspunt dat, voor zover er meerdere organen zijn, voor de toepassing van deze bepaling het dagelijks bestuur wordt aangewezen als het bestuur van de overheidsinstantie.
Ministeries staan ingevolge artikel 44, eerste lid, Grondwet onder leiding van een minister. Het betreft hier specifiek de zogenoemde 'minister van'. Een minister zonder portefeuille ('minister voor') is immers ingevolge artikel 44, tweede lid, Grondwet niet belast met de leiding van een ministerie. Het voorgaande laat onverlet dat de minister die aan het hoofd van een ministerie staat, een staatssecretaris van dat departement kan belasten met taken betreffende cyberbeveiliging.
Voor zelfstandige bestuursorganen van de centrale overheid geldt dat het zelfstandige bestuursorgaan zelf het bestuur vormt. Opgemerkt wordt dat het, voor zover van toepassing, niet gaat om de publiekrechtelijke rechtspersoon waarvan een zelfstandig bestuursorgaan deel uitmaakt. Het gaat in een dergelijk geval om het zelfstandige bestuursorgaan dat aan het hoofd staat van die rechtspersoon.
Bij veel decentrale overheidsinstanties bestaat het bestuur uit verschillende organen. Voor provincies betreft het op grond van de Grondwet en de Provinciewet provinciale staten, gedeputeerde staten en de commissaris van de koning.[35] In de Grondwet en de Gemeentewet is bepaald dat het bestuur van een gemeente wordt gevormd door de gemeenteraad, het college van burgemeester en wethouders en de burgemeester.[36] Voor waterschappen betreft het op grond van de Waterschapswet het algemeen bestuur, het dagelijks bestuur en de voorzitter.[37] Voor zover bij een gemeenschappelijke regeling een openbaar lichaam is ingesteld, bestaat het bestuur daarvan op grond van de Wet gemeenschappelijke regelingen uit een algemeen bestuur, een dagelijks bestuur en een voorzitter.[38]
Zoals hiervoor is uiteengezet, wordt voor de toepassing van deze bepaling het dagelijks bestuur aangewezen als bestuur van de overheidsinstantie. Bij provincies worden daarom gedeputeerde staten, bij gemeenten het college van burgemeester en wethouders en bij waterschappen het dagelijks bestuur aangewezen als bestuur van de overheidsinstantie. Voor gemeenschappelijke regelingen geldt dat, in lijn met de Wet gemeenschappelijke regelingen, het dagelijks bestuur van het openbaar lichaam, het bestuur van de bedrijfsvoeringsorganisatie onderscheidenlijk het gemeenschappelijk orgaan wordt aangewezen als bestuur van de overheidsinstantie.[39]
De verplichting om over voldoende kennis en vaardigheden te beschikken en daartoe een training te volgen, rust op ieder lid van het bestuur. Opgemerkt wordt dat ook hiervoor het in artikel 20, tweede lid, NIS2-richtlijn neergelegde uitgangspunt geldt dat 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.

5.4 Meldplicht

Inleiding

[35] Artikel 125 Grondwet en artikel 6 Provinciewet
[36] Artikel 125 Grondwet en artikel 6 Gemeentewet.
[37] Artikel 10, eerste lid, Waterschapswet.
[38] Artikel 12, eerste lid, Wet gemeenschappelijke regelingen.
[39] Artikelen 12, eerste lid, 14a, eerste lid, en 15 Wet gemeenschappelijke regelingen.

Essentiële entiteiten en belangrijke entiteiten moeten elk significant incident melden bij hun CSIRT en de toezichthoudende instantie. Deze meldplicht volgt uit artikel 23 NIS2-richtlijn en is geïmplementeerd in de artikelen 25 tot en met 29 Cbw. De melding leidt niet tot blootstelling van de entiteit aan een verhoogde aansprakelijkheid.[40] Naast de meldplicht aan het CSIRT en de toezichthoudende instantie hebben essentiële entiteiten en belangrijke entiteiten op grond van artikel 30 Cbw de verplichting om de ontvangers van hun diensten over significante incidenten en significante cyberdreigingen te informeren.
De hiervoor genoemde verplichtingen gelden niet voor entiteiten die domeinnaamregistratiediensten verlenen en niet tevens een essentiële entiteit of belangrijke entiteit zijn.

Meldplicht geldt alleen voor significante incidenten
De meldplicht geldt alleen voor significante incidenten. Een incident is een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar brengt. Een incident wordt als significant beschouwd (en is dus een significant incident) wanneer het: a) een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken; of b) als het andere natuurlijke of rechtspersonen heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken. Dit is opgenomen in artikel 25, tweede lid, Cbw en betreft de implementatie van artikel 23, derde lid, NIS2-richtlijn. Volgens deze definitie gaat het dus 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.
De Cbw bevat, ter implementatie van de NIS2-richtlijn, ook bepalingen die zien op significante cyberdreigingen, cyberdreigingen en bijna-incidenten. Een cyberdreiging is elke potentiële omstandigheid, gebeurtenis of actie die netwerk- en informatiesystemen, de gebruikers van dergelijke systemen en andere personen kan schaden, verstoren of op andere wijze negatief kan beïnvloeden. Een significante cyberdreiging is een cyberdreiging waarvan op basis van de technische kenmerken kan worden aangenomen dat zij ernstige gevolgen kan hebben voor de netwerk- en informatiesystemen van een entiteit of de gebruikers van de diensten van de entiteit door het veroorzaken van aanzienlijke materiële of immateriële schade. Een bijna-incident is een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar had kunnen brengen, maar die met succes is voorkomen of zich niet heeft voorgedaan. Deze begrippen zijn opgenomen in artikel 1 Cbw. Zoals gezegd ziet de meldplicht uit de Cbw aan het CSIRT en de toezichthoudende instantie alleen op significante incidenten.

De fasen van de melding
De melding bestaat uit de volgende fasen:
1. een vroegtijdige waarschuwing over het significante incident aan het CSIRT en de toezichthoudende instantie;
2. 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;
3. een tussentijds verslag (alleen na verzoek van CSIRT of toezichthoudende instantie); en
4. een eindverslag.

Drempelwaarden
Om te bepalen of een incident significant is, zijn in artikel 25, tweede lid, Cbw 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 35 Cbw 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

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

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, regels te stellen over meldplichtige incidenten per sector, subsector of soort entiteit. De nadere invulling en aanvulling van deze parameters worden ook wel de drempelwaarden genoemd.

Dubbele meldplicht aan het CSIRT en de toezichthoudende instantie
Voor essentiële entiteiten en belangrijke entiteiten geldt een dubbele meldplicht: 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 NIS2-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.

Informeren van ontvangers van diensten
Naast de hiervoor genoemde meldplicht aan het CSIRT en de toezichthoudende instantie dienen essentiële entiteiten en belangrijke entiteiten op grond van artikel 30 Cbw ook in voorkomend geval onverwijld de ontvangers van hun diensten in kennis te stellen van significante incidenten die een nadelige invloed kunnen hebben op de verlening van die diensten. Ook dienen zij de ontvangers van hun diensten, die mogelijkerwijs door een significante cyberdreiging in relatie tot het ontvangen van die diensten worden getroffen, onverwijld mee te delen welke maatregelen die ontvangers kunnen nemen in reactie op die dreiging. Indien nodig stelt de entiteit die ontvangers ook in kennis van de desbetreffende significante cyberdreiging.

5.5 CSIRT

5.5.1 Aanwijzing CSIRT's

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. Het 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 16 Cbw. 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 een kwetsbaarheid heeft gemeld en de fabrikant of aanbieder van de mogelijk kwetsbare ICT-producten of -diensten.

De CSIRT's 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 Nationaal Cyber Security Centrum (hierna: NCSC), Z-CERT, het CERT Watermanagement (onderdeel van het openbaar lichaam Het Waterschapshuis) en de Informatiebeveiligingsdienst (IBD, onderdeel van VNG Realisatie B.V.) voor de daarbij bepaalde entiteiten onder de Cbw. 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]

5.5.2 Verwerking van gegevens door het CSIRT

Een belangrijk doel van het CSIRT is het voorkomen van de uitval van netwerk- en informatiesystemen en hiermee de verhoging van de digitale weerbaarheid van organisaties. 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. 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 66 Cbw in nadere waarborgen.

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 entiteiten en belangrijke entiteiten en andere relevante partijen waarschuwen en adviseren. Een CSIRT krijgt bijvoorbeeld informatie van een CSIRT uit een ander land die kenmerken bevat 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 of te verhelpen. Hiermee wordt ook de continuïteit van de dienstverlening zo goed mogelijk gewaarborgd.

Naar aanleiding van de wijziging 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 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 dat 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

---

[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 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*,* 36084, nr. 3, p. 12-13.

[44] Zie het arrest van de Hoge Raad van 29 mei 2009, ECLI:NL:HR:2009:BH4720.

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 entiteiten 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.

5.5.3 Rol Nationaal Cyber Security Centrum

De CSIRT-taken ten aanzien van een groot deel van de entiteiten die onder het toepassingsbereik van de Cbw vallen zullen naar verwachting in de praktijk worden uitgevoerd door het NCSC. Dit is ook de verwachting voor wat betreft de taken van de coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden (artikel 17 Cbw), het centrale contactpunt, de beheerder van het nationale register en de beheerder van de meld- en registratiefunctionaliteit. In internationaal verband zijn het vaak CSIRT's die alle hiervoor genoemde taken vervullen en veel landen hebben die organisatie gedefinieerd als hun "nationale CSIRT". In de praktijk zal het NCSC in binnen- en buitenland, ook zonder formele aanwijzing, als "nationale CSIRT" opereren, ook gelet op de overige taken die het NCSC op grond van de Cbw vervult en de cruciale positie die het NCSC inneemt in het versterken van de digitale weerbaarheid.

5.5.4 Samenwerking tussen CSIRT's

In de Cbw worden de CSIRT-taken vormgegeven langs de lijnen van de ministeriële verantwoordelijkheden voor de respectievelijke sectoren. Het is niet uit te sluiten dat een essentiële entiteit of belangrijke entiteit actief is binnen meerdere sectoren en daarmee mogelijk te maken kan krijgen met meerdere CSIRT's. Mede in het licht van artikel 13 NIS2-richtlijn is het noodzakelijk dat deze CSIRT's met elkaar samenwerken in het belang van goede ondersteuning.

Om de doeltreffende en doelmatige uitvoering van de Cbw te borgen, moeten de CSIRT's onderling afspraken maken over gemeenschappelijke aangelegenheden. Deze afspraken worden vastgelegd in een samenwerkingsprotocol. Dit zorgt voor transparantie over de gemaakte afspraken en maakt voor de betrokken entiteiten helder op welke wijze de CSIRT's invulling geven aan voorgenoemde aspecten. Na de initiële publicatie wordt het samenwerkingsprotocol voor zover nodig geactualiseerd, bijvoorbeeld als er aanvullende CSIRT's actief worden in (sub)sectoren waar voorheen nog geen CSIRT-taken werden verricht.

5.6 Handhaving

De Cbw voorziet in de handhaving van de verplichtingen uit de Cbw die gelden voor essentiële entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen en van de verplichtingen die op grond van artikel 24, tweede tot en met zesde lid, Cbw gelden voor leden van het bestuur van een essentiële entiteit en belangrijke entiteit. 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.

5.6.1 Bestuursrechtelijke handhaving

De Cbw voorziet in bestuursrechtelijke handhaving, die zowel reparatoir als punitief kan zijn (herstelsancties en bestraffende sancties).[45] 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 de Cbw wordt opgedragen aan door de toezichthoudende instantie aangewezen ambtenaren. Die aangewezen ambtenaren zijn toezichthouders in de zin van artikel 5:11 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 de Cbw 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.

5.6.2 Differentiatie in het toezicht

De Cbw maakt, zoals voorgeschreven door de NIS2-richtlijn, onderscheid tussen het toezicht op essentiële entiteiten en belangrijke entiteiten, het toezicht op entiteiten die domeinnaamregistratiediensten verlenen en het toezicht op leden van het bestuur van essentiële entiteiten en belangrijke entiteiten (in verband met de verplichtingen, bedoeld in artikel 24, tweede tot en met zesde lid, Cbw).

Toezicht op essentiële entiteiten en belangrijke entiteiten
De NIS2-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.[46]
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 de Cbw 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.

[45] Het toezicht op de naleving van het bepaalde bij of krachtens de Cbw betreft bestuursrechtelijk toezicht. Deze vorm van toezicht geldt voor alle entiteiten die onder het toepassingsbereik van de Cbw vallen. Het bestuursrechtelijke toezicht geldt dus op gelijke wijze voor zowel private entiteiten als overheidsinstanties. Gelet op deze specifieke regeling van het toezicht in de Cbw, ligt het niet in de rede dat ten aanzien van provincies, gemeenten, waterschappen en gemeenschappelijke regelingen ook interbestuurlijk toezicht als bedoeld in onderscheidenlijk artikel 121 Provinciewet, artikel 124 Gemeentewet, artikel 60 Waterschapswet en artikel 32b Wet gemeenschappelijke regelingen wordt toegepast.
[46] Overweging 15 en 122 NIS2-richtlijn.

Toezicht op entiteiten die domeinnaamregistratiediensten verlenen
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 in de Cbw 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 hiervoor is dat de verplichtingen voor entiteiten die domeinnaamregistratiediensten aanbieden uitsluitend van administratieve aard zijn, waaronder het bijhouden van domeinnaamregistratiegegevens van geregistreerde domeinnamen, het verifiëren ervan, het publiceren van beleid en het op rechtmatig en gemotiveerd verzoek verstrekken daarvan aan legitieme toegangvragende partijen. Het ligt niet in de rede dat de toezichthouder zelf overgaat tot herstel van overtreding van deze verplichtingen 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 de Cbw worden aangemerkt of zijn aangewezen als essentiële entiteit of belangrijke entiteit. Indien een entiteit die domeinnaamregistratiediensten verleent ook op grond van de Cbw een essentiële entiteit of belangrijke entiteit is, dan gelden de bepalingen over het toezicht en de handhaving op essentiële entiteiten respectievelijk belangrijke entiteiten.

Toezicht op leden van het bestuur
De NIS2-richtlijn bevat geen specifieke bepalingen over het toezicht op de naleving van de verplichtingen die zijn geïmplementeerd artikel 24, tweede tot en met zesde lid, Cbw, die van toepassing zijn op leden van het bestuur van essentiële entiteiten en belangrijke entiteiten. De NIS2-richtlijn bevat alleen 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.
Nu het bestuur passende kennis en kunde moet hebben over informatiebeveiliging, is het belangrijk dat individuele leden van een bestuur kunnen worden aangesproken wanneer zij de verplichtingen uit artikel 24, tweede tot en met zesde lid, Cbw niet naleven. Voor het toezicht op de naleving hiervan door de hiervoor bedoelde leden van het bestuur is gekozen om in de Cbw te voorzien in de bevoegdheid van de toezichthouder tot het opleggen van een last onder dwangsom en bestuurlijke boete. Een last onder dwangsom kan een lid van het bestuur bewegen om alsnog een opleiding te volgen. Er is gekozen om niet te voorzien in de bevoegdheid tot het opleggen van een last onder bestuursdwang, omdat de inzet van een dergelijk instrument in de praktijk lastig voor te stellen is, aangezien artikel 24, tweede tot en met zesde lid, Cbw – kort gezegd – ziet op de verplichting om de kennis op peil te houden en een training te volgen.

5.6.3 Handhavingsinstrumentarium

De Cbw 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 de Cbw. Dit instrumentarium verschilt tussen essentiële entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen, omdat de richtlijn dit verlangt.

Het handhavingsinstrumentarium ten aanzien van essentiële entiteiten omvat het volgende:
- het aanwijzen van een controlefunctionaris;
- het uitvoeren of laten uitvoeren van een beveiligingsscan;
- het verplichten van een audit;
- het verplichten van de openbaarmaking van een overtreding;
- het opleggen van een aanwijzing;
- het opleggen van een last onder bestuursdwang;

- 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;
- het opleggen van een bestuurlijke boete.

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

Het handhavingsinstrumentarium ten aanzien van entiteiten die domeinnaamregistratiediensten verlenen, die op grond van de Cbw 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.

Het handhavingsinstrumentarium ten aanzien van leden van het bestuur van essentiële entiteiten en belangrijke entiteiten omvat het volgende:
- het opleggen van een last onder dwangsom;
- het opleggen van een bestuurlijke boete.

In de volgende paragrafen wordt specifiek ingegaan op 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. Ook wordt ingegaan op de bestuurlijke boete. In de artikelsgewijze toelichting wordt ingegaan op de controlefunctionaris, beveiligingsscan, audit, openbaarmaking van een overtreding, aanwijzing en last onder bestuursdwang.

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

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

De Cbw 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 audit, 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 de Cbw 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 75 tot en met 77 Cbw. 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.

5.6.4.2 Bepaling einddatum door toezichthoudende instantie

Inleiding
Wanneer de in paragraaf 5.6.4.1 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 de Cbw, 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, zoals de registratieverplichting, 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, zoals de registratieverplichting, 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.[47]

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.

5.6.4.3 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 76 en 77 Cbw.

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.

[47] 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 (...)".

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 de Cbw te herstellen. Het BW 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, BW). Voor de gevallen waarin geen "wettelijke vertegenwoordiger" kan worden aangewezen, is in de Cbw 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.

5.6.5 Bestuurlijke boete

Inleiding
De Cbw voorziet in de artikelen 79, 86, 90 en 92 in de bevoegdheid voor de toezichthoudende instantie om een bestuurlijke boete op te leggen

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. Ook dient zij een bestuurlijke boete aan te kondigen door middel van een voornemen van het opleggen van een bestuurlijke boete, waartegen een zienswijze kan worden ingediend. Op grond van de NIS2-richtlijn (en daarmee ook in de Cbw) is het dus in theorie mogelijk om direct na of gelijktijdig aan een waarschuwing een bestuurlijke boete op te leggen, maar daarbij is de toezichthoudende instantie uiteraard gebonden aan het in acht nemen van de eerder genoemde waarborgen.

Boetemaximum overtreding zorgplicht, meldplicht en verplichting tot het informeren van ontvangers van diensten
Alleen ten aanzien van de overtreding van de zorgplicht, de meldplicht en de verplichting tot het informeren van ontvangers van diensten 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 deze overtredingen door een essentiële entiteit betreft: € 10.000.000,- 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 deze overtredingen door een belangrijke entiteit betreft: € 7.000.000,- of 1,4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar als dat laatste leidt tot een hoger bedrag.

Boetemaximum overtreding overige verplichtingen door entiteiten
Naast de zorgplicht, de meldplicht en de verplichting tot het informeren van ontvangers van diensten bevat de Cbw ook andere verplichtingen voor entiteiten. Een voorbeeld hiervan is de verplichting voor entiteiten om informatie te verstrekken ten behoeve van het nationale register van entiteiten (artikel 44 Cbw). Voor wat betreft een bestuurlijke boete voor de overtreding van die andere verplichtingen, die gelden voor entiteiten, is gekozen voor een maximum van € 1.000.000,-. 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 € 1.000.000,- 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.[48] Bij het maximeren van de boete voor dergelijke overtredingen speelt tevens mee dat het hoge boetemaximum dat geldt bij de overtreding van de zorgplicht, de meldplicht en de verplichting tot het informeren van ontvangers van diensten (€ 10.000.000,- of 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, of € 7.000.000,- of 1,4 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar) niet evenredig is in verhouding tot de aard van de overige overtredingen.

Boetemaximum overtreding verplichtingen bij of krachtens artikel 24, tweede tot en met zesde lid, Cbw
Het boetemaximum voor een overtreding van het bepaalde bij of krachtens artikel 24, tweede tot en met zesde lid, Cbw is € 25.000,-. Bij het bepalen van dit maximum is gekeken naar de kosten van trainingen over cyberbeveiliging die nu worden aangeboden, waarbij ook een punitief element is meegenomen. Verder is meegewogen wat een individuele bestuurder zou moeten kunnen dragen.

Boetemaximum overtreding medewerkingsplicht
Een ieder is verplicht om een toezichthouder binnen de door hem gestelde redelijke termijn alle medewerking te verlenen die deze redelijkerwijs kan vorderen bij de uitoefening van zijn bevoegdheden. Deze verplichting is neergelegd in artikel 5:20 Awb. Voor het boetemaximum van een bestuurlijke boete voor de overtreding van deze verplichting is gekozen voor het bedrag van € 1.000.000,- voor zover het gaat om een essentiële entiteit, belangrijke entiteit of entiteit die domeinnaamregistratiediensten verleent. Voor zover het gaat om de niet-medewerking door een lid van het bestuur van een essentiële entiteit of belangrijke entiteit in verband met de in artikel 24, tweede tot en met zesde lid, Cbw opgenomen verplichtingen, is gekozen voor een boetemaximum van € 25.000,-.
De reden voor deze keuze is als volgt. Deze maximale hoogten zorgen ervoor dat de toezichthouder wegens overtreding van artikel 5:20 Awb een bestuurlijke boete kan opleggen die doeltreffend en afschrikkend is, en staan in verhouding tot de boetemaxima voor overtredingen van verplichtingen uit de Cbw. De gekozen boetemaxima (en dus niet lagere maxima) voorkomt dat de toezichthouder een bestuurlijke boete kan opleggen van slechts geringe hoogte, waardoor entiteiten of bestuursleden bewust kiezen voor het accepteren van de boete en niet meewerken aan een vordering van de toezichthouder.
Er wordt niet aangesloten bij de maximale hoogte van de geldboete die op grond van het strafrecht kan worden opgelegd voor eenzelfde overtreding. Dat betreft een overtreding van artikel 184 Wetboek van Strafrecht (over het opzettelijk niet voldoen aan een bevel of vordering van een ambtenaar), waarvoor per 1 januari 2024 het bedrag van € 5.150,- geldt als maximum van de geldboete die voor een overtreding daarvan kan worden opgelegd. Deze hoogte is in het kader van de Cbw niet doeltreffend, niet afschrikwekkend en staat ook niet in verhouding tot de boetemaxima voor overtredingen van verplichtingen uit de Cbw.

[48] *Kamerstukken II* 2017/18, 34883, nr. 3, p. 14.

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 de Cbw 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, de meldplicht en de verplichting tot het informeren van ontvangers van diensten 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 € 10.000.000,- of 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, of € 7.000.000,- of 1,4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar. In dat geval geldt alleen het boetemaximum van € 1.000.000,- voor de overtredingen.

Motivering bestuurlijke boete en hoogte daarvan
Voor de goede orde wordt benadrukt dat het gaat om maximale hoogten van de op te leggen bestuurlijke boetes; 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.

5.6.6 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 de Cbw 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 entiteiten 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 BW. 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.

Ten overvloede wordt nog opgemerkt dat naast het voorgaande ook civielrechtelijke aansprakelijkheid van het bestuur jegens de entiteit een rol kan spelen in het geval van niet-naleving van de Cbw, onder andere op grond van artikel 2:9 BW.

5.6.7 Samenwerking toezichthoudende instanties

In de Cbw 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 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 noodzakelijk 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 55 Cbw 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 de Cbw. 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 op cyberbeveiliging was ingericht.

5.7 Registratie

Artikel 3, derde lid, NIS2-richtlijn schrijft 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 samenwerkingsgroep.

Om ervoor te zorgen dat entiteiten deze informatie laagdrempelig kunnen aanleveren en beheren heeft de regering 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 NIS2-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, NIS2-richtlijn) komt in grote mate overeen met de informatie die entiteiten moeten aanleveren als gevolg van artikel 3, derde lid, NIS2-richtlijn. In artikel 47 Cbw is daarom opgenomen dat deze informatie verstrekt moet worden voor zover dit niet al is gedaan op grond van artikel 44 Cbw. Ten slotte zal via het registratiemechanisme tevens invulling worden gegeven aan artikel 29, vierde lid, NIS2-richtlijn, op grond waarvan essentiële entiteiten en belangrijke entiteiten de bevoegde autoriteiten in kennis dienen te stellen van hun deelname aan informatie-uitwisselingsregelingen op het gebied van cyberbeveiliging wanneer zij dergelijke regelingen aangaan, of, indien van toepassing, van hun terugtrekking uit dergelijke regelingen, zodra de terugtrekking van kracht wordt.

5.8 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 EU. 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 de Cbw 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 de Cbw.

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.

5.9 Rechtsbescherming en vereisten aan besluiten

De Cbw voorziet in de grondslag voor diverse besluiten in de zin van artikel 1:3 Awb. Een voorbeeld van een dergelijk besluit is de aanwijzing, bij regeling of besluit, van een entiteit als essentiële entiteit of belangrijke entiteit. Andere voorbeelden zijn de besluiten van de toezichthoudende instantie inhoudende een last onder bestuursdwang, last onder dwangsom of bestuurlijke boete. Ook de besluiten van de toezichthoudende instantie over de verplichting tot het uitvoeren van een audit of de

verplichting tot de openbaarmaking van (delen van) een overtreding van de Cbw, kwalificeren als besluit in de zin van artikel 1:3 Awb.

Bij de voorbereiding van besluiten gelden de regels hierover in de Awb en de algemene beginselen van behoorlijk bestuur. Zo moet bij de voorbereiding van een besluit de nodige kennis worden vergaard over de relevante feiten en de af te wegen belangen (artikel 3:2 Awb). De bij het besluit betrokken belangen moeten worden afgewogen (artikel 3:4, eerste lid, Awb). Verder mogen de voor één of meer belanghebbenden nadelige gevolgen van het besluit niet onevenredig zijn in verhouding tot de met het besluit te dienen doelen (artikel 3:4, tweede lid, Awb). Het besluit moet berusten op een deugdelijke motivering (motiveringsbeginsel, artikel 3:46 Awb). Het voorgaande is een niet-limitatief overzicht van enkele regels uit de Awb.

Tegen de op grond van de Cbw genomen besluiten in de zin van artikel 1:3 Awb staat bestuursrechtelijke rechtsbescherming open. Belanghebbenden in de zin van artikel 1:2 Awb (zoals entiteiten die op grond van de Cbw een bestuurlijke boete opgelegd hebben gekregen) kunnen tegen die besluiten achtereenvolgens in bezwaar bij het bestuursorgaan dat het besluit heeft genomen en in beroep en hoger beroep bij de bestuursrechter.

Het voorgaande levert de volgende voorbeelden op (niet-limitatief):
Als de toezichthoudende instantie overweegt om aan een entiteit de verplichting op te leggen om (delen van) een overtreding openbaar te maken, moet zij onder meer daarbij alle belangen afwegen, waaronder de eventuele schade als gevolg van de openbaarmaking. Als de toezichthoudende instantie na afweging toch overgaat tot het opleggen van een dergelijke verplichting, kan de betrokken entiteit daartegen in bezwaar bij de toezichthoudende instantie en in beroep en hoger beroep bij de bestuursrechter.
Als de toezichthoudende instantie overweegt om een last onder dwangsom op te leggen aan een entiteit, moet zij onder meer nagaan of de nadelige gevolgen van de last niet onevenredig zijn in verhouding tot de met het besluit te dienen doelen. Als wel sprake blijkt te zijn van onevenredigheid, moet de toezichthoudende instantie nagaan of een lichtere maatregel kan volstaan.

6. Verhouding tot hoger recht

6.1 Inleiding

De regels uit de Cbw kunnen raken aan in het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (hierna: EVRM), het Handvest van de grondrechten van de Europese Unie, het Internationaal Verdrag inzake burgerrechten en politieke rechten (IVBPR) en de Grondwet vastgelegde rechten en vrijheden. De gevolgen die de Cbw met zich meebrengt vloeien voort uit de NIS2-richtlijn waarbij de afwegingen ten aanzien van deze vrijheden door de Europese wetgever zijn gemaakt. Gelet op het belang van deze rechten en vrijheden wordt in dit hoofdstuk ingegaan op het in artikel 8 EVRM opgenomen recht op eerbiediging van de persoonlijke levenssfeer (paragraaf 6.3) en de verwerking van persoonsgegevens in het licht van de artikelen 5 (beginselen inzake verwerking van persoonsgegevens) en 6 (rechtmatigheid van de verwerking) van de Avg (paragraaf 6.4). Voordat die besprekingen plaatsvinden, volgt eerst in paragraaf 6.2 een overzicht van de gegevensverwerkingen door de Minister van Justitie en Veiligheid, het CSIRT en de bevoegde autoriteit.

6.2 Gegevensverwerkingen

Minister van Justitie en Veiligheid
De Minister van Justitie en Veiligheid is in de Cbw 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, maar ook aan e-mailadressen van in Nederland getroffen partijen.

CSIRT
Het CSIRT heeft krachtens de Cbw diverse taken, waaronder het verstrekken van vroegtijdige waarschuwingen en meldingen en het verspreiden van informatie over cyberdreigingen, kwetsbaarheden en incidenten (artikel 16, derde lid, onderdeel b, Cbw). 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 (artikel 36 Cbw). Ook moet het CSIRT het centrale contactpunt in kennis stellen van deze meldingen (artikel 39, eerste lid, Cbw). 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 (artikel 17, tweede lid, onderdeel b, Cbw). 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 (artikel 54, eerste lid, Cbw).
Het CSIRT zal als gevolg van de Cbw 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. Het CSIRT kan ook via andere wegen aan persoonsgegevens komen, bijvoorbeeld doordat een (ethische) hacker deze aanlevert. Benadrukt wordt dat de inlichtingentaak op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2017 is voorbehouden aan de inlichtingendiensten. Het CSIRT verleent geen inlichtingendiensten in de zin van de laatstgenoemde wet.

Bevoegde autoriteit
In de Cbw worden de vakministers aangewezen als bevoegde autoriteit voor de onderscheidene sectoren (artikel 15 Cbw). De bevoegde autoriteit heeft krachtens de Cbw diverse taken. Naast de taak om te zorgen voor de bestuursrechtelijke handhaving van het bepaalde bij of krachtens de Cbw, heeft de bevoegde autoriteit ook taken op het gebied van meldingen van significante incidenten, zoals het in ontvangst nemen daarvan 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.

6.3 Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden

6.3.1 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 niet alleen gecodificeerd in het EVRM (artikel 8), maar ook in de artikelen 10 van de Grondwet, 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, en specifiek proportionaliteit en subsidiariteit.[49]

6.3.2 Beperkende maatregel voorzien bij wet

In artikel 8, tweede lid, EVRM is bepaald dat inmenging in het recht op respect voor de persoonlijke levenssfeer alleen toegestaan is 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. In dit verband wordt opgemerkt dat in artikel 10 Grondwet is bepaald dat het recht op eerbiediging van de persoonlijke levenssfeer alleen kan worden beperkt bij of krachtens de wet. De Grondwet vereist dus een formeelwettelijke grondslag. Het EVRM vereist niet zozeer een formeelwettelijke grondslag, maar een voorziening bij wet.
Ten aanzien van de Grondwet wordt tevens opgemerkt dat in artikel 10, tweede lid, Grondwet is bepaald dat de wet regels stelt ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens. De vastlegging van persoonsgegevens wordt in vergaande mate gereguleerd door het Unierecht, in het bijzonder door de Avg. In paragraaf 6.4 wordt dit wetsvoorstel getoetst aan de Avg.
De Cbw 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 51, 52, 55, 56 en 58 Cbw. Daarnaast bevat de Cbw een specifieke wettelijke grondslag voor de verwerking van bijzondere persoonsgegevens door het CSIRT en de bevoegde autoriteit (artikel 64 Cbw). Hiermee wordt dus voldaan aan de door artikel 10, eerste lid, Grondwet vereiste formeelwettelijke grondslag voor de hiervoor bedoelde beperking en de door artikel 8, tweede lid, EVRM vereiste van bij wet voorziene inmenging.

6.3.3 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 de Cbw, 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 en om op de naleving van het bepaalde bij of krachtens de Cbw toe te zien. 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.

[49] EHRM 25 februari 1997, ECLI:CE:ECHR:1997:0225JUD002200993 (*Z./Finland*), punt 94.

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 (hierna: EHRM) nader ingevuld met de vereisten van een dringende maatschappelijke behoefte, proportionaliteit en 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.

6.3.3.1 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 netwerk–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 op het niveau van de EU, 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 de Cbw 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 de Cbw 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 betrokkenen 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 de Cbw 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 de Cbw is van belang om de hiervoor genoemde effectieve maatregelen te verzekeren. Om toezicht te kunnen houden en 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.

6.3.3.2 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 de Cbw opgenomen taken, nodig is die te bewaren, en zo ja, voor hoe lang. Dit is in lijn met het vereiste van opslagbeperking, waar het EHRM aan toetst in zijn rechtspraak.[50] Dit is ook een vereiste op grond van artikel 5, eerste lid, onderdeel e, Avg.
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. Dit is in lijn met het vereiste van minimale gegevensverwerking, waar het EHRM aan toetst in zijn rechtspraak.[51] Het vereiste van minimale gegevensverwerking is ook een vereiste op grond van artikel 5, eerste lid, onderdeel c, Avg.
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. Dit is in lijn met het doelbindingsbeginsel, waar het EHRM aan toetst in zijn rechtspraak.[52] Doelbinding is ook een vereiste op grond van artikel 5, eerste lid, onderdeel b, Avg.

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. 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 (hierna: AP).

Het CSIRT verwerkt slechts gegevens voor zover dat noodzakelijk is voor het uitvoeren van de in de Cbw genoemde taken van het CSIRT. Dit is in lijn met het doelbindingsbeginsel, waar het EHRM aan toetst in zijn rechtspraak.[53] Doelbinding is ook een vereiste op grond van artikel 5, eerste lid, onderdeel b, Avg.

---

[50] Zie bijvoorbeeld EHRM 4 december 2008, ECLI:CE:ECHR:2008:1204JUD003056204 (*S. en Marper/Verenigd Koninkrijk*).
[51] Zie bijvoorbeeld EHRM 6 november 2018, ECLI:CE:ECHR:2018:1106JUD002552713 (*Vicent Del Campo/Spanje*).
[52] Zie bijvoorbeeld EHRM 26 januari 2017, ECLI:CE:ECHR:2017:0126JUD004278806 (*Surikov/Oekraine*).
[53] Zie bijvoorbeeld EHRM 26 januari 2017, ECLI:CE:ECHR:2017:0126JUD004278806 (*Surikov/Oekraine*).

Het monitoren en analyseren van cyberdreigingen, kwetsbaarheden en incidenten (artikel 16, derde lid, onderdeel a, Cbw) 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. Dit is in lijn met het vereiste van opslagbeperking, waar het EHRM aan toetst in zijn rechtspraak.[54] Dit is ook een vereiste op grond van artikel 5, eerste lid, onderdeel e, Avg.
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 overeen met de internationaal door CERT's gehanteerde termijnen.

Bevoegde autoriteit
De bevoegde autoriteit zal bij de uitoefening van haar taken uit de Cbw 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 de Cbw genoemde taken. Ook de bevoegde autoriteit heeft zich te houden aan het doelbindingsbeginsel, waar het EHRM aan toetst in zijn rechtspraak.[55] Doelbinding is ook een vereiste op grond van artikel 5, eerste lid, onderdeel b, Avg.
De persoonsgegevens die de bevoegde autoriteit verwerkt ten behoeve van haar taken worden niet langer bewaard dan noodzakelijk. Dit is in lijn met het vereiste van opslagbeperking, waar het EHRM aan toetst in zijn rechtspraak.[56] Dit is ook een vereiste op grond van artikel 5, eerste lid, onderdeel e, Avg.
De bevoegde autoriteit staat voor wat betreft de verwerking van persoonsgegevens onder toezicht van de AP.

6.3.3.3 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,

[54] Zie bijvoorbeeld EHRM 4 december 2008, ECLI:CE:ECHR:2008:1204JUD003056204 (*S. en Marper/Verenigd Koninkrijk*).
[55] Zie bijvoorbeeld EHRM 26 januari 2017, ECLI:CE:ECHR:2017:0126JUD004278806 (*Surikov/Oekraine*).
[56] Zie bijvoorbeeld EHRM 4 december 2008, ECLI:CE:ECHR:2008:1204JUD003056204 (*S. en Marper/Verenigd Koninkrijk*).

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 alleen uitoefenen wanneer het beschikt 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.

6.3.4 Conclusie

De verwerking van persoonsgegevens door de Minister van Justitie en Veiligheid, het CSIRT en de bevoegde autoriteit is een gerechtvaardigde beperking van de persoonlijke levenssfeer met het oog op de cyberveiligheid van de entiteiten die onder het toepassingsbereik van de Cbw vallen. De voorgestelde bevoegdheden zijn omkleed met voldoende waarborgen, zoals hierboven is uiteengezet.

6.4 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. De elementen uit deze artikelen vertonen overlap met de rechtspraak van het EHRM.

6.4.1 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 voortvloeien uit een taak die uitdrukkelijk is voorgeschreven in de Cbw en dat in de Cbw 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. De Cbw 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.

6.4.2 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 de Cbw geschiedt in het kader van de in de Cbw opgenomen doelen. De algemene doelen van de Cbw zijn opgenomen in artikel 2 Cbw. In de diverse artikelen in de Cbw 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 51 Cbw, 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 de Cbw en daartoe onderling alle daarvoor benodigde gegevens uitwisselen, waaronder persoonsgegevens.

6.4.3 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 6.3.3.1, waarin is ingegaan op de dringende maatschappelijke behoefte voor de verwerking van persoonsgegevens en de noodzaak van die verwerking.

6.4.4 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.

6.4.5 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. Het CSIRT en de bevoegde autoriteit zullen voor verschillende processen, verschillende bewaartermijnen hanteren. Zo zal een CSIRT voor het proces rondom het melden van een incident een andere bewaartermijn hanteren dan voor het verzamelen en distribueren van dreigingsinformatie. Bij het bepalen van de bewaartermijnen zal enerzijds worden aangesloten bij de bestaande praktijk op grond van de Wbni en anderzijds bij de binnen een ministerie geldende uitgangspunten rondom selectie- en vernietiging van bescheiden. Ook zal naar de Archiefwet worden gekeken. De bewaartermijnen zullen periodiek worden geëvalueerd.

6.4.6 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. Ten aanzien van CSIRT's geldt tevens dat zij moeten voldoen aan de (beveiligings)eisen uit artikel 11, eerste lid, NIS2-richtlijn. Ten aanzien van de bevoegde autoriteit geldt dat de vakminister is aangewezen als de bevoegde autoriteit van de sector waar hij beleidsverantwoordelijk voor is. Alle ministeries, behalve het Ministerie van Defensie, zijn essentiële entiteit in de zin van de Cbw en moeten als gevolg daarvan voldoen aan de zorgplicht uit de Cbw.[57]

6.4.7 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 AP moeten kunnen verantwoorden dat persoonsgegevens overeenkomstig de Avg zijn verwerkt.

6.5 Verwerking bijzondere persoonsgegevens

De Cbw bevat in artikel 65 een grondslag voor het CSIRT en de bevoegde autoriteit voor de verwerking van bijzondere categorieën van persoonsgegevens (hierna: 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. De noodzaak voor de verwerking van bijzondere persoonsgegevens zal per geval worden beoordeeld in het licht van de zwaardere eisen die de Avg aan deze verwerking stelt.

Verwerking bijzondere persoonsgegevens door het CSIRT

[57] Het Ministerie van Defensie is uitgesloten van het toepassingsbereik van de Cbw.

Het CSIRT kan bij analyseren van informatie stuiten op bijzondere persoonsgegevens. Te denken valt aan een dataset die inloggegevens (credentials) bevat waarin ook e-mailadressen zitten waaruit het lidmaatschap van een vakbond, vereniging voor LHBTI-rechten of politieke partij blijkt. Daarnaast kan het bijvoorbeeld voorkomen dat een server van een zorginstelling op het internet staat die medische gegevens bevat of andere bijzondere persoonsgegevens, zoals de dieetwensen van cliënten of patiënten waaruit de geloofsovertuiging kan worden afgeleid. Ook dergelijke data moet het CSIRT in het kader van haar taakuitoefening moeten kunnen analyseren. Er zijn geen categorieën van bijzondere persoonsgegevens die in dit verband bij voorbaat uitgesloten kunnen worden wegens gebrek aan relevantie.
Het is niet altijd mogelijk om bijzondere persoonsgegevens in geanonimiseerde of gepseudonimiseerde vorm te analyseren, omdat zij dan haar taken op grond van de Cbw niet meer kan uitoefenen. Het anonimiseren of pseudonimiseren van bepaalde gegevens kan bijvoorbeeld ertoe leiden dat niet meer achterhaald kan worden bij welke entiteit dat gegeven hoort, waardoor een entiteit bijvoorbeeld niet kan worden gewaarschuwd bij een cyberdreiging of -incident (indien dat geval zich voordoet).

Verwerking bijzondere persoonsgegevens door bevoegde autoriteit
De bevoegde autoriteit kan bij het uitvoeren van bijvoorbeeld een audit of beveiligingsscan de beschikking krijgen over bijzondere persoonsgegevens. Dit kan met name voorkomen in de zorgsector, omdat in deze sector met medische gegevens 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 verkregen en wat de aard van die gegevens was, en of hieruit eventuele schade zou kunnen volgen. Het is niet altijd mogelijk om deze wettelijke taken uit te voeren als de desbetreffende bijzondere persoonsgegevens zijn geanonimiseerd of gepseudonimiseerd. Ook hier geldt dat er geen categorieën van bijzondere persoonsgegevens zijn die in dit verband bij voorbaat uitgesloten kunnen worden wegens gebrek aan relevantie.

7. Verhouding tot nationale regelgeving

7.1 Inleiding

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.

7.2 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Inleiding
In verschillende wetten op het terrein van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties zijn voor diverse vormen van (digitale) dienstverlening door de overheid verplichtingen opgenomen om maatregelen te nemen om de veiligheid en betrouwbaarheid van netwerk- en informatiesystemen te waarborgen. Dergelijke verplichtingen vertonen samenhang met de zorgplicht die de Cbw oplegt aan overheidsinstanties. In beginsel kunnen de specifieke verplichtingen uit de verschillende wetten naast de zorgplicht uit de Cbw functioneren. Deels kunnen zij als invulling van die zorgplicht worden gezien. Hierna zal kort op de Wet digitale overheid (hierna: Wdo), de Wet basisregistratie personen (hierna: Wet brp), de Wet algemene bepalingen burgerservicenummer (hierna: Wabb) en de Paspoortwet worden ingegaan.

Wet digitale overheid
Artikel 3, tweede lid, Wdo creëert de bevoegdheid om bij amvb een standaard aan te wijzen, indien die standaard noodzakelijk en proportioneel is gelet op onder andere de beveiliging van het elektronisch verkeer. Artikel 5 Wdo bepaalt dat de Minister van Binnenlandse Zaken en Koninkrijksrelaties zorgdraagt voor de inrichting, beschikbaarstelling, instandhouding, werking en beveiliging van de generieke digitale infrastructuur. Bij of krachtens amvb kunnen daarvoor regels worden gesteld.

Artikel 6 Wdo schrijft daarnaast voor dat bestuursorganen en aangewezen organisaties, volgens bij ministeriële regeling te stellen regels, bepalen voor welke door hen te verlenen elektronische diensten authenticatie of machtiging op een bepaald betrouwbaarheidsniveau vereist is. Bij elektronische dienstverlening waarvoor authenticatie op betrouwbaarheidsniveau substantieel of hoog vereist is, verlenen bestuursorganen en aangewezen organisaties uitsluitend toegang tot de dienstverlening indien gebruik wordt gemaakt van identificatiemiddelen die ten minste het voor de betreffende dienstverlening vereiste betrouwbaarheidsniveau hebben. Dit is uitgewerkt in de Regeling betrouwbaarheidsniveaus authenticatie elektronische dienstverlening.
In de toekomst zal ook artikel 4 Wdo in werking treden. Daarin is opgenomen dat bestuursorganen en aangewezen organisaties aan bij of krachtens amvb te stellen regels met betrekking tot onder de werking, betrouwbaarheid en beveiliging van de toegang tot elektronische diensten op verschillende betrouwbaarheidsniveaus moeten voldoen en dat ze een verklaring van een auditor moeten overleggen waaruit blijkt dat zij voldoen aan de genoemde vereisten. Bij of krachtens amvb worden regels gesteld over de wijze waarop bestuursorganen en aangewezen organisaties aantonen dat zij aan de regels voldoen.
Na inwerkingtreding van artikel 9 Wdo kan de Minister van BZK een publiek identificatiemiddel aanwijzen als toegelaten identificatiemiddel voor natuurlijke personen of een privaat identificatiemiddel door verlening van een erkenning toelaten indien wordt voldaan aan de bij of krachtens amvb gestelde eisen met betrekking tot de werking, beveiliging en betrouwbaarheid. Dit is uitgewerkt in het Besluit identificatiemiddelen voor natuurlijke personen Wdo.
De verplicht toe te passen standaarden, de verplichte betrouwbaarheidsniveaus en de eisen aan onder meer beveiliging van elektronische diensten en infrastructuur vertonen samenhang met de zorgplicht onder de Cbw. Zij kunnen gedeeltelijk worden gezien als specifieke invulling van die zorgplicht.

Wet basisregistratie personen
De Wet brp bepaalt dat bij amvb regels worden gesteld omtrent de technische en administratieve inrichting en werking en de beveiliging van de basisregistratie personen (artikel 1.10, eerste lid, onderdeel a, Wet brp). Deze regels zijn opgenomen in het Besluit basisregistratie personen (hierna: Besluit brp), waarin is bepaald dat zowel het college van burgemeester en wethouders als de minister verantwoordelijk zijn voor het nemen van passende technische en organisatorische maatregelen ter beveiliging van de in de basisregistratie opgenomen gegevens (artikel 6, eerste en tweede lid, Besluit brp). Daarnaast geldt de verplichting om periodiek een onderzoek te doen naar onder andere de beveiliging van de basisregistratie (artikel 4.3, eerste lid, Wet brp). Deze vereisten hebben raakvlakken met de zorgplicht die in de Cbw is opgenomen.

Wet algemene bepalingen burgerservicenummer
De Wet algemene bepalingen burgerservicenummer bepaalt dat de minister van BZK zorgdraagt voor de inrichting en instandhouding van een beheervoorziening en dat bij of krachtens amvb nadere regels gesteld worden met betrekking tot de inrichting, de instandhouding, de werking en de beveiliging van die beheervoorziening (artikel 3, eerste en derde lid, Wabb). Ook moeten bij of krachtens amvb regels worden gesteld betreffende de beveiliging van de technische voorzieningen waarmee de gebruikers kunnen aansluiten op de beheervoorziening (artikel 16, derde lid, Wabb). In artikel 5, eerste en tweede lid, Besluit burgerservicenummer is bepaald dat de Minister van Binnenlandse Zaken en Koninkrijksrelaties zorgdraagt voor de nodige maatregelen van technische en organisatorische aard ter beveiliging van de in het nummerregister opgenomen gegevens tegen verlies of aantasting van deze gegevens en tegen onbevoegde kennisneming, opneming, wijziging, verwijdering of verstrekking van deze gegevens, alsmede tegen onbevoegd gebruik en belemmering van de goede werking van de voorzieningen, bedoeld in artikel 3, eerste lid, Wabb.
Daarnaast bepaalt artikel 17, zesde lid, Wabb dat bij of krachtens amvb nadere regels worden gesteld met betrekking tot de inrichting, de instandhouding, de werking en de beveiliging van de sectorale berichtenvoorziening. De minister van BZK verricht eens per drie jaar een onderzoek naar de inrichting, de werking en de beveiliging van de beheervoorziening en de sectorale berichtenvoorziening (artikel 21, eerste en derde lid, Wabb).
Ook voor de Wabb en de daarop gebaseerde regelgeving wordt niet verwacht dat de Cbw tot botsende verplichtingen zal leiden.

Paspoortwet

De minister van BZK treft maatregelen voor het beheer en de beveiliging van het register vermiste of vervallen reisdocumenten en stelt regels met betrekking tot het beheer, de beveiliging en de betrouwbaarheid van het basisregister reisdocumenten (artikel 4a, negende lid, en artikel 4c, derde lid, Paspoortwet). Daarnaast worden bij of krachtens amvb regels gesteld over de beveiliging van het aanvraag- en uitgifteproces (artikel 28, vierde lid, Paspoortwet). Dit is nader uitgewerkt in het Paspoortbesluit, de Paspoortuitvoeringsregeling buitenland 2001, de Paspoortuitvoeringsregeling Marechaussee 2001, de Paspoortuitvoeringsregeling Nederland 2001 en de Paspoortuitvoeringsregeling Caribische landen. Ook hierbij zijn er raakvlakken met de zorgplicht in de Cbw.

7.3 Ministerie van Economische Zaken

Wet bevordering digitale weerbaarheid bedrijven
De Wet bevordering digitale weerbaarheid bedrijven (hierna: Wbdwb) legt de taken en bevoegdheden van de Minister van Economische Zaken vast op het gebied van de verbetering van de digitale weerbaarheid van het niet-vitale bedrijfsleven in Nederland. De taken zijn onder meer: het verwerken en verspreiden van informatie over kwetsbaarheden, dreigingen en incidenten aan bedrijven en het samenwerken met andere bestuursorganen en organisaties op het gebied van digitale weerbaarheid. Tevens regelt die wet de rechtstreekse informatie-uitwisseling tussen de Minister van Justitie en Veiligheid (in de praktijk: het NCSC) en het CSIRT voor digitale diensten. Ten slotte voorziet die wet in de voorwaarden waaronder vertrouwelijke gegevens die bij de Minister van Economische Zaken berusten, verstrekt mogen worden aan derden.
Vanwege de verwevenheid van de Wbdwb met de Wbni en het feit dat de laatstgenoemde wet met de komst van de Cbw komt te vervallen, dient de Wbdwb te worden aangepast aan de Cbw. Dit wordt geregeld in artikel 99 Cbw. Daarbij is het uitgangspunt dat het bestaand beleid beleidsneutraal wordt omgezet en dat de informatiepositie van de Minister van Economische Zaken die de Wbdwb aan hem toekent, wordt 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 de Cbw soortgelijke verplichtingen geregeld. Er is dus geen sprake van botsende verplichtingen.

Ruimtevaart
De Cbw voorziet in een meldplicht en zorgplicht op het gebied van cyberbeveiliging. Entiteiten waarop de Wet ruimtevaartactiviteiten van toepassing is, zullen ook onder de sector ruimtevaart van de Cbw vallen. Artikel 10, tweede lid, Wet ruimtevaartactiviteiten 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 van Economische Zaken. De meldplicht die de Cbw 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 de Cbw.
Een zorgplicht op het punt van cyberbeveiliging is niet geregeld in de Wet ruimtevaartactiviteiten. Wel bepaalt artikel 3, derde lid, Wet ruimtevaartactiviteiten dat aan een vergunning voorschriften en beperkingen kunnen worden verbonden met het oog op veiligheid van personen en goederen, bescherming van het milieu in de kosmische 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 de Cbw.

7.4 Ministerie van Financiën

Voor de financiële sector geldt een lex specialis: de Verordening digitale operationele weerbaarheid. Deze verordening is nader toegelicht in paragraaf 2.4.

7.5 Ministerie van Infrastructuur en Waterstaat

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

Drinkwater
De zogeheten Drinkwaterrichtlijn[58] 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 cyberbeveiliging, met een (herstel)maatregelplicht en meldings- en informatieplichten. De samenloop van de NIS1-richtlijn en de Drinkwaterrichtlijn is niet verder geregeld in nationale wetgeving, omdat de NIS1-richtlijn beperkt is tot cyberbeveiliging en omdat aan de verplichtingen op uitvoeringsniveau op een geïntegreerde en samenhangende wijze uitvoering kon worden gegeven. Dit laatste kon 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 om 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 amvb zijn geregeld (het Drinkwaterbesluit). Het is daarom van belang dat op wetsniveau afstemming mogelijk wordt gemaakt met soortgelijke verplichtingen van de Drinkwaterrichtlijn. De Cbw voorziet in een daartoe strekkende grondslag in artikel 21, vijfde lid.

Afvalwater
Voor de sector afvalwater is er op dit moment geen wetgeving op het gebied van cyberbeveiliging van toepassing. Er is voor wat betreft de uit de NIS2-richtlijn voortvloeiende verplichtingen dan ook geen sprake van botsing met bestaande verplichtingen.

Chemie
Voor de sector chemie is er geen sprake van botsing van bestaande wetgeving met de uit de NIS2-richtlijn voortvloeiende verplichtingen. Bestaande wetgeving, zoals de Omgevingswet waarin onder meer de zogeheten Seveso-richtlijn[59] is omgezet, ziet niet op de cyberbeveiliging van deze entiteiten. De NIS2-richtlijn kent een *all hazard*-karakter en treedt naar de opvatting van de regering niet terug voor de bedrijven waarop tevens de Seveso-richtlijn van toepassing is, omdat deze laatste geen specifieke eisen kent voor cyberbeveiliging. De verplichtingen uit de NIS2-richtlijn zijn dus van toepassing naast de Seveso-richtlijn en de Seveso toezichthouder is niet belast met het toezicht op de cyberbeveiliging.

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).

[58] Richtlijn (EU) 2020/2184 van het Europees Parlement en de Raad van 16 december 2020 betreffende de kwaliteit van voor menselijke consumptie bestemd water (*PbEU* 2020, L 435).
[59] Richtlijn 2012/18/EU van het Europees Parlement en de Raad van 4 juli 2012 betreffende de beheersing van de gevaren van zware ongevallen waarbij gevaarlijke stoffen zijn betrokken, houdende wijziging en vervolgens intrekking van Richtlijn 96/82/EG van de Raad (*PbEU* 2012, L 197).

Waterschappen
Waterschappen hebben verschillende verantwoordelijkheden. Eén van hun belangrijkste verantwoordelijkheden, het keren en het beheren van de waterkwantiteit, is niet als sector opgenomen in de NIS2-richtlijn. Het voornemen is om deze sector bij lagere regelgeving op grond van artikel 7 Wwke aan te wijzen, zodat waterschappen ook voor deze essentiële dienst als kritieke entiteiten en ook voor die taak als essentiële entiteiten worden beschouwd.

7.6 Ministerie van Klimaat en Groene Groei

Energie
De Cbw voorziet in een meldplicht en zorgplicht op het gebied van cyberbeveiliging. Op de entiteiten uit de sector energie, subsectoren elektriciteit en gas, zijn momenteel 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. Cyberbeveiliging is daar onderdeel van. De zorgplicht uit de Cbw en de uitwerking daarvan bij amvb kunnen gezien worden als instructie aan de netbeheerders hoe zij op het gebied van cyberbeveiliging invulling geven aan hun taak op grond van de Elektriciteitswet 1998 en de Gaswet. Een meldplicht op het punt van cyberbeveiliging is niet geregeld in deze wetten. Er is dus geen sprake van botsende verplichtingen.
In juni 2024 heeft de Tweede Kamer ingestemd met het wetsvoorstel houdende regels over energiemarkten en energiesystemen (Energiewet), die de huidige Elektriciteitswet 1998 en de Gaswet zal vervangen. In juli 2024 is de Eerste Kamer gestart met de behandeling; de verwachting is dat dit wetsvoorstel in de loop van 2025 in werking treedt.
De Energiewet bevat enkele (deels nieuwe) voorschriften die raken aan cyberbeveiliging. Ten eerste bevat artikel 3.18 Energiewet een nieuwe grondslag voor nadere regels ten behoeve van de bescherming van vitale processen. Dat artikel draagt onder andere bij aan het vergroten van de cyber weerbaarheid. Gedelegeerde regelgeving op grond van artikel 3.18 Energiewet bevat specifieke regels voor systeembeheerders en kan worden betrokken bij de invulling van de zorgplicht en de beoordeling of een essentiële entiteit aan de zorgplicht voldoet. Ten tweede regelt artikel 3.74 Energiewet de kwaliteitsborging en calamiteitenplannen van netbeheerders (in casu transmissie- en distributiesysteembeheerders). Het in kaart brengen van risico's voor de betrouwbaarheid van de uitvoering van de wettelijke taken is hier onderdeel van. Om dubbele lasten te voorkomen kunnen entiteiten documenten, opgesteld op grond van andere wet- en regelgeving zoals de concept Energiewet, tevens gebruiken voor de uitvoering van verplichtingen op grond van de Cbw, waarmee de administratieve lasten voor entiteiten tot het minimale worden beperkt. Deze exacte verhouding tussen de verplichting uit de Cbw en het kwaliteitsplan wordt bepaald door de toezichthoudende autoriteit. Ten derde besteedt de Energiewet ook expliciet aandacht aan de beveiliging en bescherming van gegevens die binnen het energiesysteem worden verzameld, gebruikt en verstrekt. Betrokken partijen moeten passende en evenredige technische en organisatorische maatregelen nemen om optredende risico's voor de beveiliging en bescherming van gegevens te beheersen (artikel 4.3 en 4.21) en daarnaast inbreuken op de beveiliging melden (artikel 4.4 en 4.22). Naast de netbeheerders vallen bijvoorbeeld ook meetbedrijven, gesloten distributiesysteembeheerders en de gegevensuitwisselingsentiteit onder deze verplichtingen. Hierbij bestaat enig risico op overlap in toezicht en onnodige regeldruk, omdat de Cbw ook cybersecurityrisico's en misbruik van gegevens beoogt tegen te gaan. In het wetsvoorstel Energiewet is daarom de keuze gemaakt om zowel het melden van inbreuken als het toezien op dit specifieke onderdeel bij de Minister van Klimaat en Groene Groei te beleggen. Dit heeft tot gevolg dat de Rijksinspectie Digitale Infrastructuur (hierna: RDI) toezicht zal houden op de genoemde wetsartikelen in het wetsvoorstel Energiewet. Op deze manier wordt beschikbare expertise inzake cybersecurity doelmatig en doeltreffend ingezet en komen meldingen binnen bij één toezichthouder, die de risico's en implicaties goed kan inschatten, zodat ook de regeldruk en toezichtlasten worden beperkt.

Netcode
Specifiek voor de elektriciteitssector wordt, naast de Cbw, verder gewerkt aan de implementatie van de Gedelegeerde Verordening van de Commissie van 11 maart 2024 tot aanvulling van Verordening (EU) 2019/943 van het Europees Parlement en de Raad door middel van de vaststelling van een

netcode inzake sectorspecifieke regels voor met cyberbeveiliging samenhangende aspecten van grensoverschrijdende elektriciteitsstromen (hierna: Netcode). De Netcode heeft tot doel de bescherming van kritieke infrastructuren in de elektriciteitssector te verbeteren tegen cyberaanvallen en -dreigingen. De Netcode bevordert tevens de internationale samenwerking en informatie-uitwisseling tussen lidstaten, nationale en Europese instanties, en overige stakeholders en entiteiten. Omzetting in nationaal recht is voor de werking niet nodig. Het is de verwachting dat de Netcode concreter is dan de Cbw. Zo is in overweging 3 van de Netcode aangegeven dat het de bepalingen van de NIS2-richtlijn aanvult en concretere bindende grensoverschrijdende cybersecurityvoorschriften vaststelt voor elektriciteitsentiteiten die, wanneer zij mikpunt worden van een cyberaanval, een risico vormen voor de stabiliteit van het Europese elektriciteitsnet. Aan de hand van vaste drempelwaarden worden kritieke en hoog impact entiteiten geïdentificeerd die gedigitaliseerde processen uitvoeren met een kritieke of grote impact op grensoverschrijdende elektriciteitsstromen. Naar verwachting zullen grote elektriciteitsproducenten en distributeurs onder de Netcode vallen. In lijn met de Cbw moeten deze entiteiten diverse maatregelen nemen op het gebied van cyberbeveiliging, moeten zij cyberincidenten melden en hebben zij recht op bijstand van een CSIRT.

Warmtewet
Op de entiteiten uit de sector energie, subsector stadsverwarming- en koeling, is de Warmtewet van toepassing. De Warmtewet is summier in het kader van een (cyber)weerbaarheidsverplichting. Op basis van artikel 2, eerste lid, Warmtewet zijn warmteleveranciers gehouden tot zorg voor een betrouwbare levering. De zorgplicht in de Cbw kan gezien worden als instructie aan de warmteleveranciers hoe zij op het gebied van cyberveiligheid invulling geven aan hun taak op grond van artikel 2, eerste lid, Warmtewet.

Wet collectieve warmtevoorziening
De Wet collectieve warmtevoorziening (Wcw) in voorbereiding is voor advies ingediend bij de Afdeling advisering van de Raad van State en zal naar verwachting op termijn de Warmtewet gaan vervangen. In die wet wordt een bepaling opgenomen die beheerders van collectieve warmtevoorzieningen verplicht de veiligheid van de collectieve warmtevoorziening op een doelmatige wijze te waarborgen. De meldplicht en zorgplicht uit de Cbw kunnen gezien worden als instructie aan de beheerders van collectieve warmtevoorzieningen hoe zij op het gebied van cyberveiligheid invulling geven aan hun taak op grond van de toekomstige Wcw. Een meldplicht ten behoeve van de cyberweerbaarheid is niet geregeld in de Wcw.

7.7 Ministerie van Landbouw, Visserij, Voedselzekerheid en Natuur

Artikel 19 van de Verordening (EG) Nr. 178/2002,[60] over levensmiddelen, verplicht exploitanten van een levensmiddelenbedrijf melding te doen bij de bevoegde autoriteit (de 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 dubbele meldplicht wanneer deze verplichting het gevolg is van een meldplichtig incident dat voortkomt uit de NIS2-richtlijn.

Artikel 5 van de Verordening (EG) Nr. 852/2004,[61] over levensmiddelenhygiëne, verplicht 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. HACCP staat voor *Hazard Analysis and Critical Control Points* en is een risico-inventarisatie voor voedingsmiddelen. In de praktijk kunnen entiteiten onder die verplichting al passende en evenredige technische, beveiligings-,

[60] Verordening (EG) Nr. 178/2002 van het Europees Parlement en de Raad van 28 januari 2002 tot vaststelling van de algemene beginselen en voorschriften van de levensmiddelenwetgeving, tot oprichting van een Europese Autoriteit voor voedselveiligheid en tot vaststelling van procedures voor voedselveiligheidsaangelegenheden (*PbEU* 2002, L 31).
[61] Verordening (EG) Nr. 852/2004 van het Europees Parlement en de Raad van 29 april 2004 inzake levensmiddelenhygiëne (*PbEU* 2004, L 139).

en organisatorische maatregelen ten behoeve van een aantal processen hebben genomen, die ook voortkomen uit de NIS2-richtlijn.

7.8 Ministerie van Onderwijs, Cultuur en Wetenschap

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

7.9 Ministerie van Volksgezondheid, Welzijn en Sport

Sector gezondheidszorg
Er is 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 de IGJ bevoegd tot inzage van gegevens over de gezondheid van proefpersonen of patiënten en het vorderen van inlichtingen ter zake. De desbetreffende beroepsbeoefenaar die 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, Awb) niet inroepen tegenover de toezichthouder.
Voorts geldt de meldplicht voor datalekken bij de AP. Met de Cbw geldt voor de entiteiten in de zorg voortaan 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 aanvullende bepalingen verwerking persoonsgegevens in de zorg en het Besluit elektronische gegevensuitwisseling door zorgaanbieders gelden er aanvullende bepalingen ten aanzien van verwerking persoonsgegevens in de zorg. Op grond van de Wet kwaliteit, klachten en geschillen zorg geldt voor zorgaanbieders een verplichting om kwalitatief goede zorg te leveren en om te voldoen aan de beveiligingsvoorschriften NEN7510.

Farmaceutische entiteiten
In de Geneesmiddelenwet 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 geneesmiddelen 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. In de memorie van toelichting op de Wwke is ingegaan op verschillende verantwoordelijkheden rondom producenten van nucleair materiaal, omdat deze naar verwachting, bij lagere regelgeving, onder het bereik van die wet gebracht zullen worden.

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 is geïmplementeerd in de Wet medisch-wetenschappelijk onderzoek met mensen.

Medische hulpmiddelen
Voor entiteiten die medische hulpmiddelen vervaardigen geldt op dit moment sectorspecifieke regelgeving die ziet op de kwaliteit en de werking van medische hulpmiddelen en het melden van incidenten. Dit is vastgelegd in de Verordening (EU) 2017/745,[62] over medische hulpmiddelen. De Wet medische hulpmiddelen strekt ter uitvoering van die verordening. Deze wet stelt eisen aan de

[62] Verordening (EU) 2017/745 van het Europees Parlement en de Raad van 5 april 2017 betreffende medische hulpmiddelen, tot wijziging van Richtlijn 2001/83/EG, Verordening (EG) nr. 178/2002 en Verordening (EG) nr. 1223/2009, en tot intrekking van Richtlijnen 90/385/EEG en 93/42/EEG van de Raad (*PbEU* 2017, L 117).

marktdeelnemers (fabrikanten, distributeurs, importeurs, Europees gemachtigden, aangemelde instanties en zorginstellingen die zelf hulpmiddelen maken). Meldingen van incidenten met medische hulpmiddelen dienen door een fabrikant gemeld te worden bij de IGJ.

8. Gevolgen

8.1 Gevolgen voor burgers en bedrijven

8.1.1 Inleiding

De Cbw bevat verplichtingen voor entiteiten die essentiële entiteit of belangrijke entiteit zijn, of als zodanig zijn aangewezen, en voor entiteiten die domeinnaamregistratiediensten verlenen. De door de Cbw veroorzaakte regeldruk bestaat uit een stijging van administratieve lasten en inhoudelijke nalevingskosten voor deze entiteiten. Momenteel is de schatting dat de Cbw van toepassing zal zijn op 8.100 entiteiten. Overheidsinstanties zijn hierbij niet meegerekend, want zij vallen niet onder de regeldruktoets.

Een klein deel van de entiteiten die onder het toepassingsbereik van de Cbw vallen, vallen onder het toepassingsbereik van de Wbni, die bij de inwerkingtreding van de Cbw komt te vervallen. Voor deze organisaties zal de toename in regeldruk als gevolg van de Cbw beperkter zijn dan voor de organisaties die op dit moment niet onder de Wbni vallen. Het aantal organisaties dat onder de Cbw valt is van significant groter dan onder de Wbni.

De Cbw heeft geen gevolgen voor de regeldruk voor burgers, evenmin voor organisaties en bedrijven die geen essentiële entiteit, belangrijke entiteit of entiteit die domeinnaamregistratiediensten verleent, in de zin van de Cbw zijn.

In de volgende paragrafen wordt ingegaan op de regeldruk van de zorgplicht, governanceverplichtingen, meldplicht en registratieplicht. Ook wordt ingegaan op de toezichtslasten en de eenmalige kennisnamekosten.

De NIS2-richtlijn wordt geïmplementeerd in de Cbw en de daarbij behorende lagere regelgeving. Van de zaken die bij amvb worden geregeld, zoals onder meer de zorgplicht, wordt in de nota van toelichting bij de amvb ingegaan op de regeldrukkosten.

8.1.2 Zorgplicht

Op grond van artikel 21 Cbw 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.

De maatregelen worden nader geconcretiseerd in een amvb. Om die reden zal in de nota van toelichting van die amvb eveneens nader worden ingegaan op de nalevingskosten die voortvloeien uit de uitwerking van de zorgplicht. Dit kan onder meer afhankelijk zijn van de mate waarin de maatregelen overeenkomen met de maatregelen die entiteiten reeds toepassen, bijvoorbeeld omdat ze reeds onder de Wbni vallen. Paragraaf 5.2 gaat nader in op de zorgplicht.

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. Deze entiteiten zullen minder inhoudelijke nalevingskosten ervaren dan de entiteiten dat nog niet hebben gedaan. De laatstgenoemde entiteiten kunnen een aanzienlijke regeldruk ervaren bij het implementeren van de zorgplichtmaatregelen.

Voor entiteiten die niet reeds onder de Wbni vallen is de schatting dat zij een toename van 22% aan ICT-beveiligingskosten nodig hebben om aan de zorgplicht te voldoen. Dit percentage is opgenomen in de impact assessment van de NIS2-richtlijn, opgesteld door de Europese Commissie, waarbij wel

wordt opgemerkt dat de impact assessment is geschreven op basis van het originele voorstel van de Europese Commissie, dat op sommige punten afwijkt van de uiteindelijk aangenomen richtlijn. Voor entiteiten die reeds onder de Wbni vielen, is de schatting van de Europese Commissie dat zij een toename van maximaal 12% aan ICT-beveiligingskosten nodig hebben om aan de zorgplicht te voldoen.[63]

Ook zonder wetgeving zullen essentiële entiteiten en belangrijke 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.

8.1.3 Governance

Artikel 24 Cbw bevat verplichtingen in het kader van governance, die regeldruk kunnen veroorzaken.

Allereerst moet het bestuur van een essentiële entiteit en belangrijke entiteit de beveiligingsmaatregelen die in het kader van de zorgplicht genomen worden, goedkeuren en toezien op de uitvoering daarvan. 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. Er bestaat de mogelijkheid om de vereisten aan de training nader te duiden bij amvb. Indien hiervan gebruik wordt gemaakt, zullen ook de bijbehorende geschatte kosten berekend worden.

8.1.4 Meldplicht

Op grond van artikel 25 Cbw moeten essentiële entiteiten en belangrijke entiteiten significante incidenten melden bij het CSIRT en de toezichthoudende instantie. De meldplicht is een informatieverplichting en daarmee een administratieve last.

Het uitgangspunt is dat de meldplicht op een lastenluwe manier wordt ingericht. Er wordt naar gestreefd het meldportaal 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 de meldplicht niet leiden tot een groot aantal meldingen voor entiteiten, omdat alleen significante incidenten dienen te worden gemeld. Dat zijn incidenten 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.

---

[63] *Commission staff working document impact assessment report accompanying the document "Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148", SWD(2020) 345 final,* te raadplegen op: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020SC0345.

Voor het verrichten van een melding zal het veelal gaan om de volgende handelingen. Nadat de entiteit kennis heeft genomen van het significante incident, zal een schriftelijke en eventueel telefonische vroegtijdige waarschuwing moeten worden gedaan. Verder moet de entiteit informatie verzamelen en verstrekken aan het CSIRT en de toezichthoudende instantie. Nadat het incident is afgehandeld, moet een eindverslag worden ingediend. De tijd die het de entiteiten zal kosten om een melding en vervolghandelingen te doen onder de meldplicht zal verschillen per incident en zal onder andere afhankelijk zijn van de ernst en complexiteit van het significante incident. Omdat het gaat om grootschalige of complexe incidenten wordt ingeschat dat de melding en extra vervolghandelingen gemiddeld 480 minuten kosten per incident. Dit omvat 380 minuten voor het doen van de vroegtijdige waarschuwing, melding, update, initiële beoordeling, eventueel tussentijds verslag, eventueel voortgangsverslag en eindverslag en 100 minuten voor extra handelingen op het verzoek van het CSIRT of de toezichthoudende instantie. Deze inschatting is op basis van de huidige Wbni gemaakt en afgestemd met NCSC.

Als uurtarief wordt € 54 gehanteerd, een gangbaar tarief voor theoretisch opgeleide kenniswerkers.[64] Voor een entiteiten die niet onder de Wbni vallen en onder de Cbw gaan vallen, is de meldplicht bij significante incidenten nieuw. Voor nieuwe entiteiten bedragen de administratieve lasten per melding 480 minuten (€54 * (480 min / 60) = € 432). Voor entiteiten die reeds onder de Wbni vallen wordt een kleinere toename verwacht in regeldrukkosten, 180 minuten per melding (€ 54 * (180 min / 60) = € 162). Als rekenvoorbeeld voor het totaal, 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 € 432) + (100 x € 162) = € 405.000.

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.

8.1.5 Registratieplicht

Entiteiten die onder de reikwijdte van de Cbw vallen dienen zich te registreren bij de Minister van Justitie en Veiligheid. 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 hiervan binnen twee weken te worden doorgegeven.

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 (€ 54 × 2 uur = € 108). Latere wijzigingen worden geschat op 30 minuten per wijziging (€ 54 × 0,5 uur = € 27).

Uitgaande van 8.100 eerste registraties van entiteiten, betekent dit eenmalige regeldrukkosten van 8.100 × € 108 = € 874.800. Indien uitgegaan wordt van 1.000 wijzigingen per jaar, geeft dit structurele jaarlijkse regeldrukkosten van 1.000 x € 27 = € 27.000.

8.1.6 Overige verplichtingen

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

Voor de in artikel 42 Cbw bedoelde entiteiten geldt de verplichting om een vertegenwoordiger in de EU 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.

[64] Handboek Meting Regeldrukkosten, versie 2.1 (2023), p. 14.

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 de Cbw 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.

Essentiële entiteiten en belangrijke 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 Toezichtlasten

De Cbw geeft de toezichthouder de bevoegdheid om een kritieke entiteit te onderwerpen aan steekproefsgewijze of ad hoc audits. Een steekproefsgewijze audit zal naar schatting eens in de vier jaar uitgevoerd worden. Uitgaande van een risico-gebaseerde aanpak, zal een toezichthouder redelijke grond hebben om een ad hoc audit uit te willen voeren. In het geval van een steekproefsgewijze audit kan uitgegaan worden van een gemiddelde audit van complex moeilijkheidsniveau door een toezichthouder, hiervoor wordt standaard 540 minuten gerekend. Uitgaande van een uurtarief van € 54 komt dit uit op een minimale toezichtlast van (€ 54 x (540 min / 60) =) € 486 per vier jaar per entiteit. Uitgaande van een inspectiecyclus van vier jaar (2.025 entiteiten per jaar) zou dit jaarlijks op een totaal van € 984.150 uitkomen. Als entiteiten reeds passende weerbaarheidsmaatregelen hebben genomen zal dit het meest voorkomende scenario zijn.

In het geval van een ad hoc audit (op basis van een concrete aanleiding) kan er uitgegaan worden van correcties die moeten worden aangebracht als gevolg van de inspectie of audit. Hiervoor wordt een standaardtijdsbepaling van 480 minuten gerekend. Ook kan er in dit geval extra informatie opgevraagd worden door de toezichthouder als bewijs van uitvoering van beveiligingsbeleid. Hiervoor wordt 120 minuten gerekend. Uitgaande van een uurtarief van € 54 komt dit uit op een mogelijke maximale incidentele toezichtslast van (€ 54 x (540 min + 480 min + 120 min / 60) =) € 1.026 per entiteit. De totale regeldrukkosten van deze variant zijn niet vooraf vast te stellen omdat dit afhankelijk is van naleving door entiteiten en de grootte van het risico op verstoring van de continuïteit.

De toezichthoudende instanties kunnen essentiële entiteiten en belangrijke entiteiten verplichten tot het uitvoeren van een audit door een onafhankelijke en gekwalificeerde deskundige of besluiten om over te gaan tot het uitvoeren van 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 op basis van de Awb onderwerpen aan (steekproefsgewijze) inspecties en verzoeken om informatie, gegevens, documenten en bewijzen van uitvoering van het cyberbeveiligingsbeleid. De bevoegdheden uit de Awb zijn van toepassing op alle entiteiten. Het is niet vast te stellen hoe vaak de toezichthoudende instantie dit instrument 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

Essentiële entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen zullen eenmalig tijd moeten 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 € 54 komt dit uit op € 864 per entiteit aan eenmalige kennisnamekosten. Vermenigvuldigd met het aantal betrokken organisaties (8.100) komt dit uit op een totaal van € 6.998.400,-.

8.2 Financiële gevolgen voor de overheid

De Cbw 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 NIS2-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 zoals verwerkt in de miljoenennota 2025. Deze bedragen zijn inclusief de budgettaire gevolgen horende bij de Wwke.

Tabel 1: budgettaire gevolgen per departement

(in mln. €)	2024	2025	2026	2027	2028	Structureel
EZK	7,30					
EZ		9,30	12,33	12,39	12,91	12,91
KGG		7,02	9,84	9,78	9,26	9,26
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	7,06	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**	**56,06**	**67,04**	**71,55**	**76,49**	**79,24**

De kosten voor het Ministerie van Infrastructuur en Waterstaat zijn bij Miljoenennota 2025 binnen de begroting opgenomen.

Voor het Ministerie van Onderwijs, Cultuur en Wetenschap geldt dat nader onderzocht wordt wat de kosten na 2024 zijn. Het Ministerie van Onderwijs, Cultuur en Wetenschap brengt de budgettaire gevolgen op dit moment in kaart en verwerkt dit bij Voorjaarsnota 2025 conform de regels van budgetdiscipline op de begroting van het Ministerie van Onderwijs, Cultuur en Wetenschap.

Voor het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties geldt dat de kosten van de Cbw en van de BZK-gerelateerde kosten voor CER worden gedekt binnen de beleidsartikelen 6 en 7 van de begroting van Binnenlandse Zaken en Koninkrijksrelaties als onderdeel van hoofdstuk 7 van de Rijksbegroting.

Hierbij dient opgemerkt te worden dat de ingeschatte uitgaven voor de uitvoering van de Cbw gebaseerd zijn op het op dit moment verwachte aantal entiteiten dat onder de reikwijdte van de NIS2-richtlijn komt te vallen. Op basis hiervan hebben de verantwoordelijke departementen een raming opgenomen in hun begrotingen. Naar gelang de implementatie van de Cbw vordert kunnen meer betrouwbare ramingen worden gemaakt en bijstellingen nodig blijken te zijn. Bijvoorbeeld door voorgestelde wijzingen vanuit de consultatie op de amvb of een uitvoeringstoets.

9. Adviezen, consultatie en uitvoerings- en handhaafbaarheidstoetsen

9.1 Inleiding

Een eerdere versie van dit wetsvoorstel is voor advies voorgelegd aan de AP en het Adviescollege toetsing regeldruk (hierna: ATR), opengesteld voor consultatie op www.internetconsultatie.nl. en voor commentaar toegezonden aan belangenorganisaties en entiteiten. Daarnaast hebben de betrokken vakdepartementen uitvoeringstoetsen laten uitvoeren op het wetsvoorstel. Hieronder volgt een globale bespreking van de adviezen, de reacties uit de consultatie en de beoordeling van de uitvoeringstoetsen.

Waar de nummers van de besproken artikelen verschillen, worden de artikelen van die eerdere versie als volgt aangeduid: ([artikelnummer] oud).

9.2 Advies Autoriteit persoonsgegevens

De AP wijst in haar advies erop dat artikel 35, tweede lid, NIS2-richtlijn niet juist dan wel niet volledig is geïmplementeerd in het concept-wetsvoorstel, zodat aanvulling van de wettekst en de toelichting op dit punt noodzakelijk is. Naar aanleiding van deze reactie van de AP is in artikel 58 Cbw een derde lid ingevoegd ter implementatie van artikel 35, tweede lid, NIS2-richtlijn en is de artikelsgewijze toelichting op artikel 58 Cbw op dit punt aangevuld.

Daarnaast concludeert de AP in haar advies dat – gelet op de vereisten van de Avg – uit het wetsvoorstel niet blijkt welke persoonsgegevens uitgewisseld kunnen worden in het kader van de samenwerking tussen verschillende instanties als bedoeld in de artikelen 52, eerste en tweede lid, 53, 55, eerste lid, 56 en 57 (oud) Cbw dan wel dat een dwingende delegatiegrondslag ontbreekt om dit in nadere regelgeving te bepalen, terwijl dit wel noodzakelijk is. Dit advies wordt niet gevolgd. Voor een CSIRT is het bijvoorbeeld niet mogelijk om van tevoren te zien welke persoonsgegevens zich bevinden in dreigings- en incidentinformatie. Daardoor is het niet mogelijk dit vooraf te identificeren. Door dit wel te specificeren kan dit een belemmering vormen voor de wettelijke taakuitvoering van een CSIRT.

Ten aanzien van bijzondere categorieën van persoonsgegevens wijst de AP op de noodzaak om bij amvb dwingend te bepalen welke categorieën van bijzondere persoonsgegevens verwerkt kunnen worden door het CSIRT en de bevoegde autoriteit, als dat noodzakelijk is voor hun taakuitoefening als bedoeld in artikel 64a, tweede lid, Cbw. Naar aanleiding van dit advies is artikel 64 Cbw (64a oud) zodanig aangepast dat bij wet is bepaald welke categorieën van bijzondere persoonsgegevens verwerkt kunnen worden.

Ten aanzien van bewaartermijnen acht de AP het wenselijk als dergelijke termijnen worden bepaald. Gelet op deze reactie is in artikel 65, eerste lid, Cbw een delegatiegrondslag opgenomen om in lagere regelgeving regels te stellen over de bewaartermijnen van persoonsgegevens, niet zijnde bijzondere categorieën van persoonsgegevens. Ten aanzien van dat laatste is in artikel 65, tweede lid, Cbw bepaald dat deze door het CSIRT en de bevoegde autoriteit niet langer worden bewaard dan

noodzakelijk voor de uitvoering van hun taken op grond van de Cbw, doch uiterlijk binnen 60 maanden na de eerste verwerking worden verwijderd.

Ook adviseert de AP om te definiëren wat wordt verstaan onder vertrouwelijke gegevens als bedoeld in artikel 66 Cbw (65 oud), dan wel een grondslag op te nemen die dwingend voorschrijft om in gedelegeerde regelgeving te bepalen welke gegevens dit zijn. Dit advies wordt niet gevolgd. Door vertrouwelijke gegevens te definiëren is de kans aanzienlijk dat daarmee de NIS2-richtlijn onjuist of onvolledig wordt geïmplementeerd. De definitie zal immers een clausulering impliceren, terwijl de richtlijn die clausulering niet bevat of beoogd. Wel is naar aanleiding van dit advies de artikelsgewijze toelichting op artikel 66 Cbw, waarin de context en enkele voorbeelden van vertrouwelijke gegevens staan, op punten aangescherpt.

9.3 Advies Adviescollege toetsing regeldruk

Het ATR adviseert om het nut en noodzaak in de toelichting bij het voorstel beter te onderbouwen door te verduidelijken waar en in welke mate de bestaande wetgeving tekort schiet op het punt van toegenomen dreigingen. Naar aanleiding hiervan is punt 1 in hoofdstuk 4 aangevuld.

Het ATR adviseert om in de toelichting van de implementatiewetgeving te verduidelijken of, en zo ja, waar en waarom wordt gekozen voor zwaardere eisen dan de minimumeisen van de richtlijnen. Op dit moment is er geen aanleiding om te kiezen voor zwaardere eisen dan de minimumeisen van de richtlijn. Ook in de consultatiereacties zijn zorgen over het stellen van eventuele zwaardere eisen geuit. Naar aanleiding hiervan is de passage over mogelijke extra eisen onder de zorgplicht in de paragraaf over de zorgplicht (thans paragraaf 5.2) verwijderd.

Het ATR adviseert om een MKB-toets uit te laten voeren voor de lagere regelgeving waarmee de verplichtingen nader worden uitgewerkt. Conform het advies van de ATR wordt een MKB-toets uitgevoerd op de amvb.

Het ATR adviseert te waarborgen dat organisaties weten wat de verplichtingen precies inhouden en hoe die nageleefd moeten worden. Eén van de uitgangspunten van de memorie van toelichting bij dit wetsvoorstel is dat deze leesbaar en te begrijpen moet zijn voor entiteiten die nog onbekend zijn met cyberbeveiliging. Bij het opstellen daarvan is hier telkens aandacht aan besteed. Daarnaast worden er handreikingen gepubliceerd die begeleiding kunnen bieden in het implementeren van de verschillende vereisten die de Cbw bevat.

Het ATR adviseert om een jaar na de inwerkingtreding van de Cbw een invoeringstoets uit te voeren. Naar aanleiding van dit advies is een evaluatiebepaling opgenomen in de Cbw (artikel 93 Cbw), met dien verstande dat niet is gekozen voor de door het ATR geadviseerde termijn van één jaar. Kort na de inwerkingtreding van de Cbw kan nog geen diepgaand beeld worden gekregen van de effecten van de wet, omdat er nog te weinig ervaring mee zal zijn opgedaan en dus ook geen gegevens kunnen worden geleverd. Daarom is gekozen voor een evaluatietermijn van vijf jaar. De evaluatie wordt om de vijf jaar herhaald. In de evaluatie van de Cbw wordt in ieder geval de werking van de Cbw in de praktijk, met bijzondere aandacht voor de gevolgen voor de doelgroep en de uitvoering, meegenomen.

Het ATR adviseert om inzicht te geven in de orde van grootte van de regeldrukgevolgen van die zaken die nog bij amvb worden geregeld. De NIS2-richtlijn wordt geïmplementeerd in de Cbw en in de aan die wet onderliggende amvb. In de nota van toelichting bij de amvb wordt ingegaan op de regeldrukkosten.

Het ATR adviseert de beschrijving en de berekening van de regeldrukgevolgen aan te vullen met de nog ontbrekende elementen, conform de Rijksbrede methodiek.

9.4 Samenloop

In diverse consultatiereacties, waaronder die van de Vereniging van Nederlandse Gemeenten (hierna: VNG), wordt aandacht gevraagd voor entiteiten die onder meerdere sectoren vallen omdat zij voldoen aan meerdere definities uit de bijlagen van de Cbw. Dit kan betekenen dat entiteiten onder de verantwoordelijkheid vallen van verschillende ministers, en daarmee te maken kunnen krijgen met verschillende CSIRT's, toezichthouders en lagere regelgeving. In paragraaf 5.6.7 is daarom opgenomen toezichthouders onderling werkafspraken maken om ervoor te zorgen dat zij doeltreffend en doelmatig uitvoering geven aan hun taken. Eenzelfde passage is opgenomen voor CSIRT's.

9.5 Toepassingsbereik

Algemeen
In de consultatie hebben verschillende organisaties gevraagd naar welke entiteiten er precies onder het toepassingsbereik van de Cbw vallen. De reactie hierop is als volgt. Deze memorie van toelichting kan alleen een algemene toelichting geven op het toepassingsbereik van de Cbw; het is niet mogelijk om hier in te gaan op specifieke gevallen.

Gemeenten en gemeenschappelijke regelingen
Volgens Omni-U Services B.V. (hierna: Omni-U) worden door de toevoeging van gemeenten en gemeenschappelijke regelingen aan bijlage 1 van de Cbw, gemeenten bestempeld als essentiële entiteit terwijl dat uit de NIS2-richtlijn niet zou blijken. Bovendien lijkt artikel 8, eerste lid, onderdeel h, Cbw in strijd te zijn met artikel 3, eerste lid, NIS2-richtlijn, waaruit zou volgen dat alleen de centrale overheid en grote regionale overheden als essentiële entiteiten worden bestempeld. De organisatie stelt dat andere overheidsentiteiten daarmee als belangrijk zouden moeten worden geclassificeerd, onder verwijzing naar artikel 3, tweede lid, NIS2-richtlijn. Hierover wordt het volgende toegelicht. Hoewel gemeenten en gemeenschappelijke regelingen niet in de bijlagen van de NIS2-richtlijn staan, zijn deze wel toegevoegd aan bijlage 1 van de Cbw, omdat gebruik is gemaakt van de in artikel 2, vijfde lid, onderdeel a, NIS2-richtlijn opgenomen mogelijkheid voor lidstaten om overheidsinstanties op lokaal niveau onder het toepassingsbereik van de NIS2-richtlijn te plaatsen. De richtlijn schrijft niet voor of zulke overheidsinstanties als essentiële entiteit of als belangrijke entiteit aangemerkt moeten worden. De lidstaten hebben daarin dus beleidsruimte. Deze overheidsinstanties leveren diensten die vallen onder andere essentiële sectoren uit de bijlage van de NIS2-richtlijn, daarmee worden zij als essentiële entiteiten aangemerkt. In paragraaf 5.1.2 is nader toegelicht waarom de keuze is gemaakt om deze overheidsinstanties aan te merken als essentiële entiteit.

Onderzoeksorganisaties
Omni-U geeft aan dat een specificatie is toegevoegd aan de soort entiteit onderzoeksorganisaties. Die specificatie staat niet in bijlage II van de NIS2-richtlijn. Omni-U vraagt of hiermee organisaties worden uitgesloten die mogelijk wel onder het toepassingsbereik van de NIS2-richtlijn zouden moeten vallen. De toelichting hierop is dat de specificatie volgt uit artikel 6, onderdeel 41, NIS2-richtlijn.

Onderwijsinstellingen
Universiteiten van Nederland en Vereniging Hogescholen wijzen op artikel 2, vijfde lid, onderdeel b, NIS2-richtlijn. Hierin is bepaald dat lidstaten kunnen bepalen dat de NIS2-richtlijn van toepassing is op onderwijsinstellingen, met name wanneer zij kritieke onderzoeksactiviteiten verrichten. Universiteiten van Nederland en Vereniging Hogescholen vragen naar het in de Cbw opnemen van de zinsnede "met name wanneer zij kritieke onderzoeksactiviteiten verrichten" en de door de EU bedoelde interpretatie van wat kritische onderzoeksactiviteiten zijn. Er is geen aanleiding gezien om de bedoelde zinsnede en interpretatie op te nemen in de Cbw, omdat dit geen juridische meerwaarde bevat en bovendien kan leiden tot onduidelijkheden.
De Nederlandse Federatie van Universitair Medische Centra vraagt naar het opnemen van de mogelijkheid om academische ziekenhuizen aan te wijzen in de artikelen 11 en 13 Cbw (11 en 14 oud). De reactie hierop is als volgt. Academische ziekenhuizen zijn als zorgaanbieder werkzaam op het gebied van de patiëntenzorg en staan mede ten dienste van het wetenschappelijk geneeskundig onderwijs en onderzoek aan de universiteiten waaraan zij zijn verbonden. Zij vervullen mede topklinische en topreferentiefuncties in de gezondheidszorg. Voorts verlenen zij medewerking aan de opleiding tot medisch specialist. Een academisch ziekenhuis is zodanig niet een onderwijsinstelling als bedoeld in artikel 1.1, onderdeel g, Wet op het hoger onderwijs en wetenschappelijke onderzoek.

Academische ziekenhuizen vallen vanuit de sector gezondheidszorg al onder de Cbw. Er is daarom geen aanleiding om academische ziekenhuizen aan te kunnen wijzen onder de Cbw. De academische ziekenhuizen werken binnen het Universitair Medisch Centrum samen met universiteiten met een faculteit geneeskunde. Het is van belang dat binnen dit samenwerkingsverband onderlinge afspraken worden gemaakt om voor een passend niveau van informatiebeveiliging te zorgen.

Andere sectoren
De Unie van Waterschappen wijst erop dat de sectoren *keren en beheren waterkwantiteit* en *opslag, productie en verwerking nucleair materiaal* niet staan vermeld in de Cbw. De toelichting hierop is dat de NIS2-richtlijn alleen van toepassing is op de sectoren uit de bijlagen van de NIS2-richtlijn. De genoemde sectoren zijn daarin niet opgenomen, waardoor de NIS2-richtlijn niet van toepassing is op deze sectoren. Wel kunnen deze sectoren worden aangewezen op grond van artikel 7 Wwke, waarbinnen kritieke entiteiten kunnen worden aangewezen op grond van artikel 6, eerste lid, Wwke. Kritieke entiteiten in de zin van de Wwke zijn op grond van artikel 8, eerste lid, onderdeel i, Cbw van rechtswege essentiële entiteiten in de zin van de Cbw.

Een organisatie vraagt zich af of voor de subsector 'vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek' onder de Cyberbeveiligingswet uitsluitend 'fabrikanten' worden verstaan zoals gedefinieerd in Verordening (EU) 2017/745 en Verordening (EU) 2017/746. Dat klopt. De distribiteur of importeur van een medisch hulpmiddel valt niet onder de NIS2. Hierdoor kunnen de verplichtingen van de fabrikant niet overgaan op een distribiteur of importeur. Wel worden deze partijen gezien als onderdeel van de toeleveringsketen. Dat betekent dat de entiteit die onder de Cbw valt, in dit geval de fabrikant, verantwoordelijk is om erop toe te zien dat de netwerk- en informatiesystemen van de toeleveranciers een voldoende beveiligingsniveau hebben.
Een aantal partijen uit de energiesector, waaronder E-Mobility Consulting, vragen of de Cbw niet ook van toepassing zou moeten zijn op "laaddienstverleners", gezien het de mogelijke impact van incidenten bij deze dienstverleners op het elektriciteitsnet. Na gesprekken met de sector is geconcludeerd dat de "laaddienstverleners" binnen de laadpaalinfrastructuur onder de sector vervoer vallen en daarbinnen onder de subsector weg als exploitanten van intelligente vervoerssystemen (ITS) als bedoeld in artikel 4, onderdeel 1, van Richtlijn 2010/40/EU van het Europees Parlement en de Raad. Daarmee vallen zij onder de Cbw, mits zij ook voldoen aan de omvangscriteria die voortvloeien uit de NIS2-richtlijn.
De Dutch Datacenter Association (DDA) geeft aan dat de definitie van een datacenter en de diensten die een datacenter levert, onduidelijk is. Vele datacenters in Nederland verhuren faciliteiten als ruimte, koeling en stroom aan klanten. Deze klanten plaatsen hun servers in de gebouwen van de datacenter operator. Deze datacentereigenaren hebben dus geen zeggenschap over de ICT in het datacenter. Dit roept onduidelijkheden op ten aanzien van de zorgplicht, aldus DDA. De reactie hierop is als volgt. De beveiligingsmaatregelen die entiteiten moeten treffen op grond van de Cbw betreffen "haar werkzaamheden of voor het verlenen van haar diensten". Zie artikel 21, eerste lid, Cbw (23, eerste lid oud). Indien klanten van aanbieders van datacenters zelf bepaalde activiteiten uitvoeren in een datacenter maar deze niet als dienst afnemen van de aanbieder, dan valt dit buiten de zorgplicht van de aanbieder van de datacenter.
Schiphol is van mening dat de term "aanbieders van netwerken voor de levering van inhoud" ambigue is. Het transporteren van data is ook een vorm van inhoud. Schiphol vraagt of een internet service provider (hierna: ISP) ook onder deze dienst valt. De reactie hierop is als volgt. Een ISP kan verschillende diensten aanbieden, maar een veelvoorkomende dienst die ISP's aanbieden is het verlenen van toegang tot het internet: de internettoegangsdienst. Dit is een dienst die valt onder een (openbare) elektronische communicatiedienst zoals gedefinieerd in de Tw. Het verlenen van toegang tot het internet valt niet onder de definitie van een "netwerk voor de levering van inhoud".
HVG Law, EY accountants & EY adviseurs vraagt om een nadere toelichting van de definities van de digitale sectoren, met name aangaande aanbieders van beheerde diensten en aanbieders van beheerde beveiligingsdiensten. De reactie hierop is als volgt. In de Cbw wordt geen nadere uitwerking gegeven aan de bedoelde definities. Door de opname in de NIS2-richtlijn zijn deze immers Europeesrechtelijk geharmoniseerd. Indien blijkt dat er in de praktijk onduidelijkheid is of blijft bestaan, zal worden bezien hoe deze zo goed mogelijk kan worden weggenomen. Met het oog op Europese harmonisatie is het daarbij wenselijk om met betrekking tot uitleg van de definities in internationaal verband afstemming te zoeken, bij andere lidstaten, de Europese Commissie of Enisa.

Met betrekking tot aanbieders van beheerde diensten en beheerde beveiligingsdiensten wordt opgemerkt dat een aanbieder van een beheerde beveiligingsdienst ook altijd een aanbieder van een beheerde dienst is.

Voornaamste economische activiteit
Ter implementatie van het bepaalde hierover in de NIS2-richtlijn is in de bijlagen van de Cbw geregeld dat de Cbw niet van toepassing is op entiteiten binnen de sectoren drinkwater, afvalwater en afvalstoffenbeheer wanneer de genoemde activiteiten "niet hun voornaamste economische activiteit is" of een vergelijkbare formulering. Het Verbond van Nederlandse Ondernemingen – Nederlands Christelijk Werkgeversverbond (hierna: VNO-NCW) en de Koninklijke Vereniging MKB-Nederland (hierna: MKB-Nederland) vragen of dit verder kan worden geconcretiseerd. De mate waarin een bedrijf een bepaalde activiteit uitvoert is voor entiteiten in overige sectoren niet relevant om te bepalen of de entiteit onder de Cbw valt. Wel kan een bedrijf bij de toepassing van de zorgplicht een risicogebaseerde benadering hanteren, waarbij de maatregelen die zij treffen voor de beveiliging van hun netwerk- en informatiesystemen passend en evenredig zijn aan de risico's voor hun dienstverlening.

Complexe bedrijfsstructuren
In verschillende reacties wordt gevraagd naar de toepassing van de Cbw op bedrijven met complexe bedrijfsstructuren, bijvoorbeeld als organisaties bestaan uit meerdere rechtspersonen. Om te bepalen of een organisatie binnen een dergelijke structuur onder de Cbw valt, moet een organisatie als eerste vaststellen of zij voldoen aan de definitie van 'entiteit', zoals gedefinieerd in artikel 1 Cbw. Zoals hierboven aangegeven kan vervolgens op basis van de omvang van de entiteit en de definities uit de bijlage worden bepaald of een entiteit van rechtswege onder de Cbw valt. Om vast te stellen of er sprake is van een verbonden of partneronderneming, dient gebruik te worden gemaakt van de Aanbeveling 2003/361/EG. De gegevens van verbonden of partnerondernemingen worden meegeteld voor het bepalen van de omvang van een organisatie, maar van elke entiteit moet zelfstandig worden bepaald of deze onder de Cbw valt. Binnen een groep van ondernemingen kunnen dus meerdere entiteiten bestaan die een essentiële entiteit of belangrijke entiteit zijn en moeten voldoen aan de verplichtingen uit de Cbw.
In diverse consultatiereacties wordt gevraagd naar de toepassing van overweging 16 NIS2-richtlijn, waarin staat dat lidstaten bij het toepassen van de Aanbeveling 2003/361/EG rekening kunnen houden met de mate van onafhankelijkheid die er tussen de netwerk- en informatiesystemen van verbonden of partnerondernemingen bestaat. In de Cbw is hier geen verdere invulling aan gegeven.

Jurisdictie
In diverse consultatiereacties wordt gevraagd naar de jurisdictie ten aanzien van een entiteit of verschillende entiteiten die binnen een groep ondernemingen actief is of zijn in meerdere lidstaten. Hierover wordt het volgende toegelicht. Artikel 26 NIS2-richtlijn gaat over de jurisdictie en is geïmplementeerd in artikel 4 Cbw. Indien een lidstaat jurisdictie heeft over een entiteit, moet die entiteit ook in die lidstaat voldoen aan de daar geldende wetgeving.

Veiligheidsregio's
In een consultatiereactie wordt gevraagd naar de positie van de veiligheidsregio's onder de Cbw en in een andere consultatiereactie wordt voorgesteld om de veiligheidsregio's onder het toepassingsbereik van de Cbw te laten vallen. Als reactie hierop wordt gewezen op artikel 5 Cbw, waarin artikel 2, zevende lid, NIS2-richtlijn is geïmplementeerd. Uit artikel 5 Cbw volgt dat de Cbw niet van toepassing is op de veiligheidsregio's, omdat zij in hoofdzaak activiteiten uitvoeren op het gebied van nationale en openbare veiligheid. De NIS2-richtlijn biedt op dit punt niet de beleidsruimte voor lidstaten om hiervan af te wijken.

Samenhang met Wwke
Diverse consultatiereacties hebben betrekking op de samenhang tussen de Cbw en de Wwke. Zo vraagt KPN B.V. naar de verhouding tussen de verplichtingen uit de Cbw en de Wwke. In hoofdstuk 2 van de memorie van toelichting van zowel de Cbw als de Wwke staat in algemene zin omschreven dat een incident betrekking kan hebben op zowel de netwerk- en informatiesystemen als op andere fysieke aspecten die de essentiële dienstverlening kan raken, en in dit geval dus de verplichtingen van

beide wetten gelden. Voor entiteiten in de sector digitale infrastructuur geldt echter dat de Cbw *lex specialis* is op de Wwke, en dat daarmee onder andere de zorgplicht en meldplicht uit de Cbw voorgaan op de zorgplicht en meldplicht uit de Wwke. Entiteiten in de sector digitale infrastructuur hoeven dus enkel aan deze verplichtingen uit de Cbw te voldoen. Dit staat ook toegelicht in de memorie van toelichting op het wetsvoorstel Wwke. KPN B.V. vraagt daarnaast om verwijdering van de zinsnede "verstoring van andere fysieke aspecten die de essentiële dienstverlening raken" uit paragraaf 2.3. Dit is niet mogelijk. Uit artikel 21, tweede lid, NIS2-richtlijn volgt immers dat de zorgplicht ook betrekking heeft op deze aspecten. Verwijdering zou daarmee leiden tot onvolledige implementatie van de NIS2-richtlijn.

9.6 Digitale sector

Een groot aantal consultatiereacties zien op de digitale sector. Deze reacties worden in deze paragraaf behandeld.

9.6.1 Wijziging Telecommunicatiewet

In een consultatiereactie is gereageerd op de voorgestelde wijziging van de Telecommunicatiewet (hierna: Tw). De Tw behoudt een zorgplicht die qua reikwijdte vergelijkbaar is met (en dus niet gelijk is aan) de beveiliging van diensten zoals voorzien in het huidige artikel 11a.1, eerste lid, en die verschilt van de reikwijdte van de zorgplicht uit de Cbw. In de hiervoor bedoelde consultatiereactie wordt bezwaar gemaakt tegen dit voorstel, omdat de artikelen 40 en 41 van de Richtlijn (EU) 2018/1972[65], ook wel de Telecomcode genoemd, worden geschrapt. Dit roept de vraag op wat de zorgplicht voor telecomaanbieders nu precies zal inhouden en of er niet sprake is van een dubbele zorgplicht. Deze onduidelijkheid is onwenselijk en daarom moeten de betreffende artikelen in de Tw worden geschrapt, aldus deze consultatiereactie. De reactie hierop is als volgt. De voorgestelde verwijdering van de bedoelde artikelen uit de Tw wordt niet overgenomen. Zoals ook in de artikelsgewijze toelichting op artikel 98 Cbw (89 oud) is toegelicht, is de formulering van de zorgplicht uit de Tw anders dan de formulering van de zorgplicht uit de Cbw. De zorgplicht uit de Tw heeft een bredere reikwijdte, omdat deze ziet op de totale beveiliging van de openbare elektronische communicatienetwerken en de openbare elektronische communicatiediensten, en niet alleen op de netwerk- en informatiesystemen. Het is daarom noodzakelijk om de zorgplicht in de Tw te behouden. Daarnaast klopt het dat middels de NIS2-richtlijn de artikelen 40 en 41 Telecomcode komen te vervallen, maar dit is niet gebeurd voor artikel 108 Telecomcode waarin is geregeld dat lidstaten alle noodzakelijke maatregelen nemen om de beschikbaarheid van spraakcommunicatiediensten en internettoegangsdiensten die worden geleverd via openbare elektronische communicatienetwerken, zo volledig mogelijk te waarborgen in geval van door calamiteit veroorzaakte netwerkuitval of in geval van overmacht. Hierbij moeten de lidstaten er ook voor zorgen dat aanbieders van spraakcommunicatiediensten alle nodige maatregelen nemen om een ononderbroken toegang tot de noodhulpdiensten en een ononderbroken transmissie van waarschuwingen aan het publiek te waarborgen. Deze is in de huidige Tw geïmplementeerd in artikel 11a.1, tweede lid en wordt na inwerkingtreding van de Cbw artikel 11a.1, derde lid.

BTG merkt met betrekking tot de wijziging van de Tw op dat ten behoeve van artikel 98 Cbw (89 oud) meer richtlijnen dienen te komen voor de passende en evenredige technische, operationele en organisatorische maatregelen om de risico's voor de beveiliging van de diensten te beheersen. De maatregelen die hier genoemd staan, dienen verduidelijking te krijgen. Er wordt genoemd dat er rekening gehouden dient te worden met desbetreffende Europese en internationale normen, maar dit is heel globaal. Hierbij adviseert BTG ook het gebruik van specifieke Europese en internationale normen als kader te benoemen met als doel inconsistenties en onduidelijkheid te voorkomen. Artikel 98 Cbw (89 oud) is als volgt aangepast. De verwijzing in artikel 11a.1, eerste lid, Tw naar de Europese en internationale normen is geschrapt. De huidige laatste zin uit artikel 11a.1, eerste lid, Tw is in de bepaling opgenomen, namelijk: "Deze maatregelen zorgen, gezien de stand van de techniek,

[65] Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling van het Europees wetboek voor elektronische communicatie (herschikking) (*PbEU* 2018, L 321).

voor een veiligheidsniveau dat is afgestemd op de risico's die zich voordoen." Hierdoor is de formulering van artikel 11a.1, eerste lid, Tw hetzelfde als die bij de implementatie van de Telecomcode in de Tw was geregeld maar waarbij alleen de verwijzingen naar aanbieders van openbare elektronische communicatienetwerken en de beveiliging van netwerken is verwijderd.

9.6.2 Database met domeinregistratiegegevens

Op de Cbw-artikelen over een database met domeinregistratiegegevens zijn meerdere reacties gekomen, waaronder van Stichting Brein, SIDN, Vereniging van Registrars, Ripe RCC, Realtime Register, Metaregistrars, ICANN Business Constituency, Coalition for Online Accountability en de Messaging, Malware and Mobile Anti-Abuse Working group.

Verificatie registratiegegevens
Diverse consultatiereacties gaan over het wel of niet expliciet vaststellen van verificatiemethodes in de Cbw. Er zijn verschillende verificatiemethodes aangedragen voor het verifiëren van domeinnaamregistratiegegevens. Deze procedures zullen in overleg met de sector worden ingevuld. Er wordt momenteel met verschillende lidstaten gezamenlijk gewerkt aan een document om op dit punt tot afspraken voor minimumharmonisatie voor mogelijke verificatiemethodes te komen. Hiermee kan niet worden voorkomen dat er lidstaten zijn die van deze afspraken af gaan wijken. Voor de Nederlandse implementatie zullen vervolgens (zoals voorgesteld in één van de consultatiereacties) samen met belanghebbende partijen eenduidige verificatiemethodes worden gekozen, die gebaseerd zijn op het eerder genoemde Europese afstemming. Indien noodzakelijk geacht kunnen bij ministeriële regeling eisen aan verificatiemethodes worden gesteld die de benodigde duidelijkheid verschaffen. Zoals de NIS2-richtlijn voorschrijft dienen de registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen door middel van beleidslijnen en procedures ervoor zorgen dat de het register op te nemen informatie juist en volledig is. Uit overweging 111 NIS2-richtlijn moeten topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen onder meer ten minste één van de manieren om met de domeinnaamhouder contact op te nemen, verifiëren. De informatie die deze entiteiten registreren is opgesomd in artikel 49, tweede lid, Cbw. Er zijn daarnaast vragen gesteld welke nationale regels leidend zijn betreffende verificatieprocedures voor entiteiten die domeinregistratiediensten verlenen in verschillende lidstaten. Het doel van de afspraken tussen de lidstaten over verificatieprocedures is om minimumharmonisatie te bewerkstelligen. De Nederlandse inzet hierbij is om samen te werken met de registers voor topleveldomeinnamen en de toezichthouders zodat er goed rekening kan worden gehouden met de uitvoeringspraktijk.

Privacy- en proxydiensten
Er is door verschillende partijen aangegeven dat het onduidelijk is of aanbieders van privacy- en proxy-registratiediensten als entiteiten die domeinnaamdiensten verlenen, ook contactgegevens van de domeinnaamhouder moeten verstrekken aan een legitieme toegangvragende partij. Het is onvoldoende om slechts gegevens van de betreffende privacy- of proxy-registratiedienstverlener te geven bij een gemotiveerd verzoek van een legitieme partij. De gegevens van de desbetreffende houder dienen geregistreerd te worden. De artikelsgewijze toelichting op artikel 49 (50 oud) is hierop aangevuld.

Bulkregistraties
In een aantal consultatiereacties is opgebracht dat bulkregistraties door gebruik van algoritmes, software of automatische protocollen expliciet uitgesloten moeten worden. Dit punt is niet overgenomen, omdat een gedegen verificatieproces het geautomatiseerd registreren van domeinnamen door algoritmes (bulkregistraties) kan mitigeren.

Een aantal organisaties wijst op het feit dat het openbaren van bepaalde verificatieprocedures, zoals beschreven in artikel 49, derde lid, Cbw (50, derde lid oud) kan leiden tot het uitbuiten van deze informatie. Dit punt is begrijpelijk. Echter stelt artikel 49, derde lid, Cbw niet vast tot op welk detail niveau deze procedures moet worden uitgewerkt en hierdoor kan specifieke gevoelige informatie achterwege blijven.

Daarnaast is ingebracht om een zogeheten 'Thick WHOIS' model van topleveldomeinnaam registers aan het houden. Dit punt wordt niet overgenomen. In Nederland is het .nl-topleveldomein al naar dit model ingericht, zonder dat dit model verplicht is. Daarnaast schrijft de NIS2-richtlijn het gebruik van een bepaalde techniek niet voor. Het doel van de NIS2-richtlijn is om de database met juiste en volledige domeinnamen te vullen.

Betaling
Een punt uit de consultatie betrof gratis toegang tot de gegevens uit de database bedoeld in artikel 49 Cbw. Dit punt wordt niet overgenomen omdat kosteloze verstrekking niet een uit de NIS2-richtlijn vloeiende verplichting is.

Dubbel verifiëren
Een ingebracht punt betreft het aanvullen van artikel 49, vijfde lid, Cbw (50, vijfde lid oud) met voorschriften die tot doel hebben het voorkomen dat domeinnaamregistratiegegevens dubbel worden verzameld. De suggestie die gedaan wordt is om hierbij ook meermaals verifiëren op te nemen. Dit punt wordt meegenomen in het kader van de praktische uitwerking van de verificatiemethodes.

Toegang tot welke gegevens
Een opgebracht punt in de consultatie betreft welke gegevens opgevraagd mogen worden bij een verzoek om toegang tot specifieke domeinnaamregistratiegegevens. De gegevens die middels artikel 50 Cbw (51 oud) kunnen worden opgevraagd, gaat uitsluitend om gegevens zoals beschreven in artikel 49, tweede lid, Cbw (50, tweede lid oud).

Openbaarmaking gegevens
Betreffende de handhaafbaarheid van het openbaar maken van gegevens is een vraag gesteld wanneer het openbaar maken van de registraties, als bedoeld in artikel 49, vierde lid, Cbw (50, vierde lid oud) verplicht is. De openbaarmaking dient onverwijld na de registratie van een domeinnaam plaats te vinden.

9.7 Zorgplicht

Maatregelen in het kader van de zorgplicht
Meerdere consultatiereacties gaan over de onduidelijkheid over de maatregelen die essentiële entiteiten en belangrijke entiteiten moeten nemen in het kader van de zorgplicht. Daarnaast wordt in meerdere consultatiereacties ervoor gepleit om de zorgplicht te beperken tot alleen de maatregelen die worden voorgeschreven door de NIS2-richtlijn. Hierop wordt als volgt gereageerd. Onder de Cbw komt één amvb waarin regels worden gesteld ter nadere invulling van de maatregelen die essentiële entiteiten en belangrijke entiteiten in het kader van de zorgplicht moeten nemen. In het kader van de implementatie van de NIS2-richtlijn zullen geen andere maatregelen worden voorgeschreven dan die worden voorgeschreven in artikel 21, tweede lid, NIS2-richtlijn. De zorgplichtmaatregelen zijn in verband met de hiervoor bedoelde consultatiereacties opgenomen in artikel 21 Cbw. Voor een nadere toelichting op de maatregelen wordt verwezen naar paragraaf 5.2.3. De hiervoor bedoelde amvb zal daarnaast een delegatiegrondslag bevatten om bij ministeriële regeling van de minister die het aangaat, indien nodig, sectorspecifieke regels te stellen over de maatregelen. Die regels blijven binnen het kader van de bepaling, maar kunnen de maatregelen wel nader concretiseren.
Voor de sectoren digitale infrastructuur (met uitzondering van internetknooppunten en openbare elektronische communicatienetwerken en -diensten), beheer van ICT-diensten (business-to-business) en digitale aanbieders zijn de drempelwaardes van de meldplicht alsmede de beveiligingsmaatregelen in het kader van de zorgplicht ingevuld middels Europese uitvoeringshandelingen.[66] Er kan echter niet

[66] Uitvoeringsverordening (EU) 2024/2690 van de Commissie van 17 oktober 2024 tot vaststelling van regels voor de toepassing van Richtlijn (EU) 2022/2555 wat betreft de technische en methodologische vereisten van de maatregelen voor het beheer van cyberbeveiligingsrisico's en nadere specificatie van de gevallen waarin een incident als significant wordt beschouwd met betrekking tot DNS-dienstverleners, registers voor topleveldomeinnamen, aanbieders van cloudcomputingdiensten, aanbieders van datacentrumdiensten, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, aanbieders van onlinemarktplaatsen,

worden uitgesloten dat in de toekomst op nationaal niveau, bijvoorbeeld in het kader van nationale veiligheid, alsnog nadere of aanvullende maatregelen voor deze sectoren noodzakelijk kunnen zijn. Derhalve is de delegatiegrondslag, opgenomen in artikel 21, vijfde lid, Cbw, om regels te kunnen stellen ook van toepassing voor entiteiten die binnen de reikwijdte van de uitvoeringsverordening vallen. Dit is in lijn met de minimumharmonisatie die de NIS2-richtlijn op grond van artikel 5 NIS2-richtlijn nastreeft.

Meerdere partijen, waaronder VNO-NCW en Cyberveilig Nederland (hierna: CVNL), hebben in het kader van de beveiliging van de toeleveringsketen gevraagd naar de samenhang van NIS2-richtlijn met andere Europese regelgeving, zoals de zogeheten Verordening cyberweerbaarheid[67] (*Cyber Resilience Act*) en de zogeheten Radioapparatenrichtlijn[68]. Naar aanleiding van deze reacties is de artikelsgewijze toelichting op artikel 21 Cbw aangevuld.

Bestaande normenkaders of certificering
Uit de consultatiereacties van diverse organisaties, waaronder International Business Machines Corporation (hierna: IBM), FME, CVNL, Dutch Cloud Community, Huawei Technologies (Netherlands) B.V. (hierna: Huawei) en het Verbond van Handelaren in Chemische Producten (VHCP), blijkt dat er behoefte is aan het in de Cbw of onderliggende regelgeving expliciet verwijzen naar of het erkennen van bestaande normenkaders of certificering. De reactie hierop is als volgt. Het door entiteiten hanteren van een eigen normenkader kan in belangrijke mate bijdragen aan een succesvolle aanpak van de cyberveiligheid. Een dergelijk normenkader geeft entiteiten houvast bij het beheersen van de risico's met betrekking tot de beveiliging van hun netwerk- en informatiesystemen. Het voldoen aan een eigen normenkader betekent niet per definitie dat een entiteit voldoet aan de maatregelen die bij of krachtens de Cbw worden voorgeschreven. Wel wordt daarbij opgemerkt dat bij vaststellen van de maatregelen in lagere regelgeving nadrukkelijk rekening zal worden gehouden met bestaande normenkaders. Datzelfde geldt ook voor de door Enisa krachtens artikel 25 NIS2-richtlijn op te stellen richtsnoeren over technische gebieden die in het kader van de zorgplicht in acht kunnen worden genomen én over de daarover reeds bestaande nationale en internationale normen. Met dat laatste wordt ook bevorderd dat partijen die Europees opereren zoveel als mogelijk te maken krijgen met een eenduidige invulling van de zorgplicht binnen de diverse lidstaten.

NEN7510
De Nederlandse Vereniging van Ziekenhuizen, de Stichting Samenwerkende ICT-leveranciers in de Zorg (SILIZO), de Nederlandse Vereniging van Organisaties voor ICT in de Zorg (OIZ), NedXis en de Nederlandse Federatie van Universitaire Medische Centra vragen in het aandacht voor het binnen de zorgsector voldoen aan de zorgplicht op grond van de Cbw en NEN7510. Hierover wordt het volgende toegelicht. Omdat de maatregelen die op grond van de Cbw moeten worden genomen op onderdelen verschillen van die in de NEN7510, zullen deze voorschriften naast elkaar bestaan. Wel wordt naar verwachting bij de aankomende herziening van de NEN7510 aangesloten op de maatregelen in het kader van de zorgplicht van de Cbw. Daarnaast zal mogelijk in een ministeriële regeling van de Minister van Volksgezondheid, Welzijn en Sport krachtens de Cbw worden verwezen naar sectorale normen zoals de NEN7510 en de ISO-normen.

Toekomstbestendigheid
Cisco geeft aan dat de NIS2-richtlijn en daarmee de Cbw niet toekomstbestendig zijn als gevolg van de opkomst van generatieve kunstmatige intelligentie. De reactie hierop is als volgt. Essentiële entiteiten en belangrijke entiteiten moeten bij het maken van hun risicobeoordeling en het treffen van

van onlinezoekmachines en van platforms voor socialenetwerkdiensten, en verleners van vertrouwensdiensten (*PbEU* L 2024/2690).
[67] Verordening van het Europees Parlement en de Raad betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordeningen (EU) nr. 168/2013 en (EU) 2019/1020 en Richtlijn (EU) 2020/1828 (Verordening cyberweerbaarheid), nog niet gepubliceerd.
[68] Richtlijn 2014/53/EU van het Europees Parlement en de Raad van 16 april 2014 betreffende de harmonisatie van de wetgevingen van de lidstaten inzake het op de markt aanbieden van radioapparatuur en tot intrekking van Richtlijn 1999/5/EG (*PbEU* 2014, L 153).

mitigerende maatregelen ook rekening houden met nieuwe technologieën of nieuwe vormen van dreigingen. Dat geldt dus ook voor generatieve kunstmatige intelligentie.

9.8 Governance

Uit een aantal consultatiereacties, waaronder die van de Koninklijke Vereniging van Nederlandse Reders (hierna: KVNR), NLdigital, Vewin en de Vereniging Energie-Nederland, blijkt dat in de eerdere versie van dit wetsvoorstel het onvoldoende duidelijk is wat onder het bestuur, bedoeld in artikel 25 (26 oud) Cbw, moet worden verstaan. Naar aanleiding van deze reacties is in paragraaf 5.3, voor de verschillende private rechtsvormen die het Nederlandse rechtsstelsel kent, gespecificeerd op wie de verplichtingen van artikel 25 (26 oud) Cbw rusten.

Governance – overheidsorganisaties
Volgens de VNG, het Interprovinciaal Overleg (IPO) en de Unie van Waterschappen merkt het wetsvoorstel onterecht de ambtelijke leiding aan als het bestuur van overheidsinstanties. Zo geeft de Unie van Waterschappen aan dat de ambtelijke leiding voor haar taakuitvoering afhankelijk is van de financiering van het bestuur van het waterschap. Naar aanleiding van deze reacties is artikel 24 Cbw zodanig gewijzigd, dat de governanceverplichtingen gelden voor de politieke leiding van overheidsinstanties.

9.9 Meldplicht

Definities
Uit enkele consultatiereacties, waaronder die van De Nederlandse ggz, de N.V. Nederlandse Spoorwegen (hierna: de NS) en Stichting Connect2Trust, blijkt dat onduidelijkheid bestaat over enkele definities, waaronder die van significante incidenten en significante cyberdreigingen, en welke incidenten moeten worden gemeld. Naar aanleiding van deze reacties is in artikel 1 Cbw ten aanzien van enkele begrippen (waaronder de hiervoor genoemde begrippen) de dynamische verwijzing naar de definitie van die begrippen in artikel 6 NIS2-richtlijn verwijderd en zijn de definities uitgeschreven. Daarnaast is de paragraaf over de meldplicht (thans paragraaf 5.4) aangevuld, waarin wordt benadrukt dat de meldplicht alleen ziet op significante incidenten.

Significant incident
In meerdere reacties, waaronder die van NLconnect, KPN B.V., IBM, CVNL, VNO-NCW, MKB Nederland, de koninklijke Vereniging van de Nederlandse Chemische Industrie (VNCI), KVNR en het Centraal Bureau Levensmiddelenhandel (hierna: CBL), wordt aandacht gevraagd voor de criteria om vast te stellen wanneer sprake is van een significant incident. In reactie hierop wordt ten eerste gewezen op artikel 25 Cbw, waarin is bepaald welke parameters gelden voor het aannemen van een dergelijk incident. Daarnaast is in artikel 35 Cbw een delegatiegrondslag opgenomen om bij of krachtens amvb nadere regels te stellen om die parameters verder uit te werken. Van deze delegatiegrondslag zal, juist ter verdere concretisering en verduidelijking van de drempelwaarden voor het al dan niet aannemen van een significant incident, gebruik worden gemaakt. In het kader van deze nadere regeling kunnen ook bij ministeriële regeling voor sectoren en subsectoren specifieke drempelwaarden worden bepaald. Bij het bepalen van de drempelwaarden in genoemde nadere regelgeving zal voor zover mogelijk gestreefd worden naar harmonisering met andere lidstaten.

Meldportaal
Meerdere partijen, waaronder Netbeheer Nederland, de Nederlandse Vereniging voor Ziekenhuizen (hierna: VZVZ) en de Unie van Waterschappen, vragen naar de totstandkoming van één meldportaal voor meldingen die entiteiten moeten doen op grond van verschillende wetgeving. Het op deze wijze voldoen aan de in meerdere wetten geregelde meldplichten heeft de aandacht, maar op dit moment is het (technisch) niet mogelijk om een dergelijk meldportaal te maken.

Termijn van 24 uur
Enkele organisaties, waaronder de Branchevereniging ICT en Telecommunicatie Grootgebruikers (hierna: BTG) en Cisco Systems International, geven aan dat de termijn van 24 uur te kort is. In reactie hierop wordt benadrukt dat die termijn dwingend wordt bepaald door de NIS2-richtlijn.

Daarnaast wordt hierbij opgemerkt dat deze termijn gaat lopen vanaf het moment dat kennis is gekregen van het significante incident én dat het een vroegtijdige waarschuwing betreft, waarbij nog niet alle informatie voorhanden hoeft te zijn.

Foutieve meldingen
NLdigital vraagt zich af hoe omgegaan wordt met foutieve meldingen. Het CSIRT voert een triageproces uit waarbij elke melding bekeken wordt. Er wordt beoordeeld of een melding ziet op een significant incident en dus verder behandeld moet worden.

Overig
De VZVZ vraagt of een entiteit bij het melden van een significant incident kan aangeven dat zij in meerdere sectoren valt. Dat zal inderdaad mogelijk zijn. In het formulier om een melding te doen, dat momenteel wordt ontwikkeld, is een optie om aan te geven in welke sectoren in relatie tot het gemelde significante incident de entiteit valt. Daarnaast geeft VZVZ aan dat het risico bestaat dat er een melding wordt gedaan aan de verkeerde bevoegde autoriteit. In reactie hierop wordt opgemerkt dat in de Cbw per sector is geregeld wie de bevoegde autoriteit is. Mocht een melding onverhoopt toch bij een verkeerde bevoegde autoriteit zijn gedaan, dan zal die autoriteit de melding moeten doorzenden naar de juiste bevoegde autoriteit. Zie hiervoor ook artikel 2:3 Awb.
De NS geeft aan dat de zinsnede "onverwijld of, indien dat niet mogelijk is" in de artikelen 26 en 27 (28 en 29 oud) Cbw een striktere verplichting is dan de zinsnede "onverwijld en in elk geval" in artikel 23 NIS2-richtlijn. In reactie hierop wordt benadrukt dat geen sprake is van een striktere verplichting. Er is gekozen voor de formulering "onverwijld of, indien dat niet mogelijk is", zodat duidelijk is dat een entiteit de daarin opgenomen handelingen onverwijld moet uitvoeren. Indien dat niet lukt, dan moet een entiteit dat binnen de daarin aangegeven termijn doen. Een passage als "onverwijld en in elk geval" zou bij strikte lezing immers betekenen dat een entiteit tweemaal de verplichting zou moeten uitvoeren. Dat is niet de bedoeling. Naar aanleiding van deze consultatiereactie is de artikelsgewijze toelichting bij de artikelen 26 en 27 (28 en 29 oud) Cbw aangevuld.
CVNL pleit ervoor om de meldplicht, onder andere voor de cybersecuritysector, nader uit te werken op Europees niveau en niet bij amvb. De reactie hierop is als volgt. Voor de sectoren digitale infrastructuur (met uitzondering van openbare elektronische communicatienetwerken en -diensten en internetknooppunten), beheer van ICT-diensten (business-to-business) en digitale aanbieders zijn de drempelwaardes van de meldplicht alsmede de beveiligingsmaatregelen ingevuld middels Europese uitvoeringshandelingen.[69]

9.10 Gegevens

Meerdere organisaties vragen naar wat wordt verstaan onder vertrouwelijke gegevens als bedoeld in artikel 66 Cbw (65 oud) en hoe de vertrouwelijkheid van die gegevens wordt geborgd. Voor wat betreft het nader duiden van vertrouwelijke gegevens is ervoor gekozen om in de Cbw geen definitie op te nemen van vertrouwelijke gegevens. Voor de onderbouwing wordt verwezen naar de reactie op het advies van de AP. Daarnaast wordt verwezen naar de artikelsgewijze toelichting bij artikel 66 Cbw voor een toelichting op en voorbeelden van vertrouwelijke gegevens. Voor wat betreft het waarborgen van de vertrouwelijkheid van de desbetreffende gegevens wordt opgemerkt dat dat het verstrekken van vertrouwelijke gegevens door een CSIRT slechts ter uitvoering van haar taken aan derden kan verstrekken indien aldaar de geheimhouding van de gegevens voldoende is gewaarborgd.

Het IPO heeft een aantal vragen gesteld over het verwerken van persoonsgegevens. Hierover wordt toegelicht dat de Avg van toepassing is op het verwerken van persoonsgegevens op basis van de

[69] Uitvoeringsverordening (EU) 2024/2690 van de Commissie van 17 oktober 2024 tot vaststelling van regels voor de toepassing van Richtlijn (EU) 2022/2555 wat betreft de technische en methodologische vereisten van de maatregelen voor het beheer van cyberbeveiligingsrisico's en nadere specificatie van de gevallen waarin een incident als significant wordt beschouwd met betrekking tot DNS-dienstverleners, registers voor topleveldomeinnamen, aanbieders van cloudcomputingdiensten, aanbieders van datacentrumdiensten, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, aanbieders van onlinemarktplaatsen, van onlinezoekmachines en van platforms voor socialenetwerkdiensten, en verleners van vertrouwensdiensten (*PbEU* L 2024/2690).

wettelijke taken uit de Cbw. De Cbw kent duidelijke doelen en wettelijke taken toe aan de CSIRT's en bevoegde autoriteiten. Daarmee kan op basis van de Avg een goede DPIA worden uitgevoerd op het verwerken van persoonsgegevens door de verwerkingsverantwoordelijke.

9.11 CSIRT

Taken van het CSIRT
Meerdere organisaties, waaronder CVNL, VNO-NCW, MKB-Nederland en KVNR, hebben vragen gesteld over de taken van een CSIRT. InEen vraagt naar het verruimen van het takenpakket van Z-CERT. De taken van een CSIRT zijn opgenomen in artikel 16, derde lid, Cbw en zijn voorgeschreven door de NIS2-richtlijn. Wat entiteiten op basis van dat wettelijk kader mogen verwachten van hun CSIRT, zal worden uitgewerkt in beleid. Een onderdeel van dat beleid is dat zodra een groot incident plaatsvindt, een CSIRT aan de hand van het beleid voorrang verleent aan specifieke meldingen. Bij grote incidenten werken de CSIRT's met elkaar samen en bij (zeer) grote incidenten treedt de nationale crisisstructuur in werking.

In een consultatiereactie wordt gevraagd naar het verkrijgen van informatie van overheidsorganisaties die zich bezig houden met de nationale veiligheid via een CSIRT. Onder de Cbw kan dit alleen als zijnde een relevante partij. Voor de andere informatie die een CSIRT bezit, geldt dat de grondslag van deze uitwisseling wordt gevonden in andere wet- en regelgeving, zoals de Wet op de inlichtingen- en veiligheidsdiensten 2017 en de Wbdwb. In de praktijk vindt er dus uitwisseling plaats op basis van een ander wetgevend kader.

Forensische gegevens
Een organisatie vraagt naar de wijze van het verzamelen van forensische gegevens door een CSIRT. In reactie hierop wordt benadrukt dat een CSIRT niet geautomatiseerd en continu gegevens verzamelt van entiteiten om deze te analyseren op forensische gegevens. Forensische gegevens die zien op een specifieke entiteit worden alleen verzameld voor het verlenen van bijstand aan die entiteit en met informatie die door die entiteit is gedeeld.

Niet-intrusief scannen
Naar aanleiding van de vragen van uit enkele consultatiereacties, waaronder die van IBM, over het niet-intrusief scannen door een CSIRT wordt toegelicht dat deze taak van het CSIRT geen invloed heeft op de dienstverlening van entiteiten. Zodra bij het scannen kwetsbaarheden zijn gevonden bij een entiteit, wordt zij daarover geïnformeerd door het CSIRT.

"Nationale CSIRT"
CVNL pleit voor het expliciet aanwijzen van het NCSC als nationale CSIRT. Dit is juridisch niet mogelijk in de Cbw. In de praktijk zal het NCSC in binnen- en buitenland, ook zonder formele aanwijzing, als het zogeheten "nationale CSIRT" opereren, ook gelet op de overige taken die het NCSC op grond van de Cbw vervult en de cruciale positie die het NCSC inneemt in het versterken van de digitale weerbaarheid.

9.12 Handhaving

Eisen aan besluit en rechtsbescherming
Uit enkele consultatiereacties blijkt dat het niet duidelijk is aan welke eisen een besluit van de toezichthoudende instantie moet voldoen en welke rechtsmiddelen entiteiten kunnen aanwenden tegen een belastend besluit van de toezichthoudende instantie (zoals de verplichting om een overtreding van de Cbw openbaar te maken of om een audit uit te voeren). Naar aanleiding van deze reacties is in de memorie van toelichting een paragraaf toegevoegd (thans paragraaf 5.9), waarin wordt ingegaan op de eisen die gelden voor de toezichthoudende instantie bij besluiten en de rechtsbescherming daartegen.

Inzet handhavingsinstrument
Uit een aantal consultatiereacties, waaronder die van NLconnect en NLdigital, blijkt dat niet duidelijk is wanneer welk instrument kan worden ingezet door de toezichthouders. In reactie hierop wordt

opgemerkt dat de toezichthouders bij het nemen van handhavingsmaatregelen, gelet op de vereisten hierover uit de Awb en de algemene beginselen van behoorlijk bestuur, een afwegingskader zullen hanteren, waarbij rekening wordt gehouden met de omstandigheden van elk afzonderlijk geval (zoals de ernst van de overtreding).

Audit
In een consultatiereactie wordt gevraagd waarom een audit ingezet kan worden bij ISO-gecertificeerde partijen. In reactie hierop wordt opgemerkt dat het door een entiteit voldoen aan bijvoorbeeld genoemde certificering zal bijdragen aan het versterken van de eigen digitale weerbaarheid, maar dat dit niet zonder meer betekent dat daarmee ook aan de verplichtingen in de Cbw wordt voldaan. De toezichthouder zal bij het beoordelen of in een specifiek geval een audit zal worden gelast uiteraard wel ook rekening houden met een certificering.
Volgens Huawei is in de Cbw de bevoegdheid van de bevoegde autoriteit tot het opleggen van een audit uitgebreid ten opzichte van de bevoegdheid die de NIS2-richtlijn voorschrijft. In reactie hierop wordt toegelicht dat er geen sprake is van een dergelijke uitbreiding, omdat de NIS2-richtlijn die ruimte niet biedt aan lidstaten.
In meerdere consultatiereacties, waaronder die van Huawei en CIO Platform Nederland, wordt aangegeven dat in artikel 82 (80 oud) Cbw moet worden opgenomen dat de bevoegde autoriteit een audit alleen kan opleggen in bepaalde situaties, aangezien bij belangrijke entiteiten het toezicht ex post plaatsvindt. In reactie wordt gewezen op artikel 80 Cbw, dat al voorziet in een dergelijke clausulering.

Samenloop
Het Interprovinciaal Overleg (hierna: IPO) merkt op dat aangezien een entiteit onder meerdere bevoegde autoriteiten kan vallen, de vraag is hoe de toezichthouders zich tot elkaar verhouden als er een cyberincident plaatsvindt waarbij persoonsgegevens betrokken zijn. Het IPO pleit ervoor om in de Cbw te regelen dat een entiteit, zoals een provincie, niet voor dezelfde feiten een boete ontvangt van zowel de ene als de andere bevoegde autoriteit. In reactie hierop wordt gewezen op artikel 58 Cbw, over de samenwerking met toezichthoudende autoriteiten in het kader van inbreuken in verband met persoonsgegevens en het opleggen van een bestuurlijke boete vanwege een dergelijke inbreuk.

Centralisatie toezicht
In een aantal consultatiereacties, waaronder die van HVG Law, EY accountants en EY adviseurs, wordt voorgesteld om het toezicht op de naleving van de Cbw bij een centrale toezichthouder te beleggen dan wel meer gecentraliseerd en niet versnipperd over meerdere toezichthouders. In reactie hierop wordt toegelicht dat ervoor is gekozen om het toezicht te beleggen bij de sectorale toezichthouders, vanwege de sectorale kennis die een toezichthouder moet hebben en het kunnen combineren van sectoraal toezicht vanuit verschillende wetten bij een sectorale toezichthouder. Dit voorstel wordt daarom niet overgenomen.

Verplichting tot openbaarmaking overtreding
Enkele consultatiereacties, waaronder die van CIO Platform Nederland en ProRail B.V., zien op de artikelen in de Cbw waarin wordt geregeld dat de bevoegde autoriteit een entiteit kan verplichten een overtreding (deels) openbaar te maken. Deze reacties lijken te suggereren dat deze artikelen de verplichting voor entiteiten bevat om elke overtreding van de Cbw openbaar te maken. Daarnaast wordt in relatie tot die artikelen aangegeven dat terughoudend moet worden omgegaan met het opleggen van deze verplichting om eventuele (reputatie)schade door openbaring te beperken of voorkomen. In reactie hierop wordt allereerst erop gewezen dat hetgeen in de genoemde artikelen is geregeld, dwingend wordt voorgeschreven door de NIS2-richtlijn. Deze artikelen zien alleen op de bevoegdheid van de bevoegde autoriteit om een entiteit al dan niet de genoemde verplichting op te leggen. Het gaat dus niet om een verplichting (van rechtswege) voor entiteiten om altijd een overtreding openbaar te maken. Hierbij wordt tevens gewezen naar paragraaf 5.9, waarin wordt ingegaan op de eisen die gelden voor de bevoegde autoriteit bij het nemen van het besluit tot het opleggen van deze verplichting en de rechtsbescherming daartegen. Ook geldt hier dat de bevoegde autoriteit een afwegingskader zal hanteren bij het nemen van het besluit, waarbij rekening wordt gehouden met de omstandigheden van het specifieke geval.

Controlefunctionaris
Uit enkele consultatiereacties blijkt dat de indruk bestaat dat artikel 69 Cbw voor alle essentiële entiteiten de verplichting bevat om een controlefunctionaris aan te wijzen. Dit is niet het geval. Artikel 69 Cbw betreft alleen de bevoegdheid van de bevoegde autoriteit om als handhavingsinstrument ten aanzien van een essentiële entiteit voor een bepaalde periode een controlefunctionaris aan te wijzen en niet op een algehele verplichting voor alle essentiële entiteiten.

Verzoek tot schorsing certificering of vergunning
De Unie van Waterschappen geeft aan dat de bevoegdheid van de toezichthoudende instantie om een verzoek tot schorsing van certificeringen of vergunningen in te dienen zonder verplichting voor de certificerings- of vergunningsinstantie om dit verzoek te honoreren, kan leiden tot inconsistenties en mogelijke juridische geschillen. De Unie van Waterschappen pleit voor een specificatie van de criteria waarop deze verzoeken moeten worden beoordeeld. De reactie hierop is als volgt. Artikel 32, vijfde lid, NIS2-richtlijn verplicht lidstaten om te regelen dat de bevoegde autoriteit de bevoegdheid heeft om een dergelijk verzoek te doen, zonder een nadere clausulering. Het voorschrijven van de bedoelde criteria zou een inperking betekenen van hetgeen in de NIS2-richtlijn is bepaald.

Uitzondering overheidsinstanties
In meerdere consultatiereacties wordt gevraagd waarom overheidsinstanties worden uitgezonderd van de artikelen 75, 76 en 77 Cbw. In reactie hierop wordt erop gewezen dat dit dwingend voortvloeit uit artikel 32, vijfde lid, NIS2-richtlijn.

Overig
Meerdere organisaties, waaronder NOREA en de VNG, geven aan dat het toezicht niet direct kan ingaan op het moment dat de Cbw in werking treedt, omdat er dan nog veel onduidelijk is over de verplichtingen in de Cbw en het implementeren daarvan de nodige tijd vergt. In reactie hierop wordt erop gewezen dat de toezichthoudende instantie, mede gelet op de regels in de Awb en de algemene beginselen van behoorlijk bestuur, daar rekening mee zullen houden, wanneer dat aangewezen is.
Een aantal organisaties, waaronder NLdigital en de Vereniging Energie-Nederland, stellen vragen over bestuurlijke boetes en boetebeleidsregels. In reactie hierop wordt toegelicht dat de toezichthoudende instanties beleidsregels zullen opstellen om de hoogte van de boete te bepalen, uiteraard met inachtneming van de in de Cbw vastgestelde maxima. In deze beleidsregels zal ook ingegaan worden op de berekening van de wereldwijde omzet.

9.13 Overige opmerkingen

Dwingende regels uit de NIS2-richtlijn
Enkele consultatiereacties zien op zaken die door de NIS2-richtlijn dwingend worden geregeld. Zo worden in enkele consultatiereacties andere formuleringen van artikelen uit de Cbw voorgesteld, zoals het voorstel van VNO-NCW, MKB Nederland, NLconnect en NLdigital om een clausulering aan te brengen in artikel 74, tweede lid, onderdeel b, Cbw. Daarnaast wordt in enkele consultatiereacties, waaronder in die van terlouw.legal, de BTG en Cisco Systems International, gepleit voor veranderingen in de meldplicht, zoals het hanteren van andere (langere) termijnen. In een internetconsultatiereactie wordt gepleit voor de verplichting om een minimaal percentage van de jaaromzet in te zetten voor cyberbeveiliging. In de consultatie uit de Stichting Digitale Infrastructuur Nederland (DINL) bezwaren tegen het aanleggen en beheren van een nieuw register van IP-adressen. En in een andere consultatiereactie wordt aangegeven dat de brede omschrijving uit de NIS2-richtlijn van beheerders van ICT-diensten (business-to-business) zorgt voor onduidelijkheid in de te nemen maatregelen in het kader van de zorgplicht, meldplicht en registratieplicht. Verder zijn er reacties, zoals die van SURF en de VNCI, waarin bezwaren worden geuit tegen de verplichting om in het kader van het nationale register ook de IP-bereiken te moeten verstrekken. Deze reactie ziet ook op de vraag van VNO-NCW en MKB Nederland om in de Cbw te regelen dat het CSIRT binnen 24 uur bijstand verleent. En in de consultatiereacties van VNO-NCW, MKB Nederland en CBL wordt ervoor gepleit om voor bepaalde sectoren, zoals digitale infrastructuur en beheer van ICT-diensten, te regelen dat de Cbw alleen op entiteiten uit deze sectoren van toepassing is wanneer hun activiteiten binnen deze sector de voornaamste activiteit is van deze entiteiten. Tot slot is er ook de reactie van IBM, waarin wordt aangemoedigd om in artikel 16, derde lid, onderdeel b, (17, tweede lid, onderdeel b, oud) Cbw

de vermelding van "relevante partijen" in te perken of te verwijderen, omdat entiteiten anders terughoudend zullen zijn met het melden van incidenten.
Over al het voorgaande wordt opgemerkt dat de NIS2-richtlijn daarover dwingende bepalingen bevat. Lidstaten hebben geen ruimte om over te gaan tot een andere of aanvullende regeling (zoals aanvullende verplichtingen of aangepaste termijnen) of beschrijving.

ISAC haven wijst op verschillen tussen de bijlagen van de Cbw en de bijlage van de Wwke en stelt voor om dezelfde sectoren en subsectoren te hanteren in deze bijlagen. In reactie hierop wordt toegelicht dat de Cbw strekt tot de implementatie van de NIS2-richtlijn en de Wwke strekt tot de implementatie van de CER-richtlijn. Deze richtlijnen vertonen op sommige punten gelijkenissen, maar zijn niet geheel identiek aan elkaar, zo ook ten aanzien van de sectoren en subsectoren die onder de reikwijdte van de richtlijnen vallen. Dit verklaart waarom de bijlagen van de Cbw niet gelijk zijn aan de bijlage van de Wwke.

Bepalingen uit NIS2-richtlijn niet geïmplementeerd in Cbw
In enkele consultatiereacties is erop gewezen dat sommige bepalingen uit de NIS2-richtlijn niet zijn geïmplementeerd in de Cbw. Naar aanleiding hiervan wordt het volgende toegelicht. Sommige bepalingen uit de NIS2-richtlijn zijn al geïmplementeerd in het bestaand recht. Dit verklaart waarom sommige bepalingen uit de NIS2-richtlijn ontbreken in de Cbw. De reden hiervoor is dus niet dat deze bepalingen niet worden geïmplementeerd, maar dat deze bepalingen al zijn geïmplementeerd (niet in de Cbw, maar in andere wetgeving). De transponeringstabel biedt een overzicht van de bepalingen uit de NIS2-richtlijn die wel moeten worden geïmplementeerd en waar deze zijn geïmplementeerd (in de Cbw of bestaande wetgeving, zoals de Awb) en de bepalingen die niet hoeven te worden geïmplementeerd, bijvoorbeeld omdat de bepaling is gericht op de Europese Commissie of omdat de bepaling strekt tot feitelijke uitvoering.

Samenhang met andere Europese wetgeving
Meerdere partijen, waaronder VNO-NCW, MKB Nederland, NLconnect, IBM en CVNL, vragen naar de samenhang van de NIS2-richtlijn met andere Europese wetgeving, waaronder de Verordening cyberweerbaarheid (*Cyber Resilience Act*) en de zogeheten Radioapparatenrichtlijn. Naar aanleiding van deze reacties is de artikelsgewijze toelichting op artikel 21 Cbw aangevuld.

Entiteiten die domeinnaamregistratiediensten verlenen
Omni-U betwist, onder verwijzing naar overweging 15 NIS2-richtlijn, dat entiteiten die domeinnaamregistratiediensten verlenen een aparte categorie entiteiten betreffen, naast essentiële entiteiten en belangrijke entiteiten. Dit is onjuist. Uit onder meer artikel 3, derde lid, en overweging 18 NIS2-richtlijn volgt dat de NIS2-richtlijn entiteiten onderverdeelt in drie categorieën: essentiële entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen. Overweging 15 NIS2-richtlijn ziet op de zorgplicht en de meldplicht en aangezien deze verplichtingen alleen van toepassing zijn op essentiële entiteiten en belangrijke entiteiten, is het vanzelfsprekend dat de overweging alleen ingaat op die entiteiten.

Registratie
ISAC haven heeft enkele vragen gesteld over het nationale register van entiteiten. Over dat register wordt het volgende toegelicht. De registratieplicht geldt vanaf het moment dat de Cbw in werking treedt. Tussen 18 oktober 2024 en de inwerkingtreding van de Cbw is registratie op vrijwillige basis mogelijk. Voor het uitvoeren van de registratie is inloggen via e-Herkenning vereist. Daarmee kan worden gevalideerd dat een persoon gerechtigd is om namens een entiteit het registratieproces te doorlopen. Bij de registratie zal worden gevraagd naar de lidstaten waarin de entiteit diensten als bedoeld in de bijlagen bij de Cbw verleent, zodat bij een eventueel incident kan worden bepaald met welke autoriteiten in andere lidstaten samen kan worden gewerkt.

Caribisch Nederland
In een consultatiereactie wordt aangegeven dat de regering zou vinden dat er in Caribisch Nederland nog geen regels hoeven te gelden voor cyberbeveiliging en dat een lager cyberbeveiligingsniveau geen reden kan zijn om geen wettelijke ondergrens neer te zetten. Dit is niet het geval. Zoals ook in paragraaf 5.8 is toegelicht zijn de onderwerpen die in de NIS2-richtlijn worden geregeld op dit

moment niet uitvoerbaar in Caribisch Nederland en wordt op dit moment eerst uitvoering gegeven aan enkele randvoorwaarden voor het verhogen van de digitale weerbaarheid op de BES. Denk aan het in kaart brengen van welke processen op de BES mogelijk maatschappelijk ontwrichtende effecten hebben en betere bescherming behoeven. Het is goed denkbaar dat in de toekomst uitvoerbare wetgeving komt waarmee de bescherming van bepaalde infrastructuur in Caribisch Nederland tegen digitale risico's wordt gewaarborgd.

Verwijzingen in de Cbw
In enkele consultatiereacties wordt gevraagd naar welke artikelen uit welke regelingen er in de Cbw wordt verwezen, omdat die aanduiding in sommige bepalingen in de Cbw ontbreekt. Hierover wordt het volgende toegelicht. Daar waar in wet- en regelgeving wordt verwezen naar een artikel zonder verwijzing naar andere wet- en regelgeving, wordt verwezen naar het artikel uit diezelfde wet of regeling.

Definities
CVNL wijst erop dat in artikel 1 Cbw een aantal essentiële begrippen ontbreken, zoals "cyberhygiëne" en "bestuurder", en betreurt dat voor de definities niet wordt verwezen naar het Cybersecuritywoordenboek. In reactie hierop wordt erop gewezen dat artikel 1 Cbw alleen de begrippen bevat die voorkomen in de Cbw en die definiëring behoeven. De definities in artikel 1 Cbw moeten voor een volledige en juiste implementatie van de NIS2-richtlijn aansluiten bij de definities uit de NIS2-richtlijn. Het gebruik maken van de definities uit het Cybersecuritywoordenboek is derhalve niet mogelijk.
In enkele reacties, waaronder die van Omni-U en NLdigital, wordt gesteld dat de bijlagen van de Cbw verschillen van de bijlagen van de NIS2-richtlijn, waaronder enkele definities. Dit is niet juist. Er zijn geen inhoudelijke aanpassingen gemaakt. In de bijlagen van de Cbw wordt vastgehouden aan de aanduidingen in de bijlagen bij de NIS2-richtlijn, tenzij deze vervangen kunnen worden door verwijzingen naar Nederlandse wetgeving die hetzelfde inhouden. Dit laatste is het geval ten aanzien van het begrip zorgaanbieder.

Taal- en stijlfouten
In enkele consultatiereacties is gewezen op fouten in het conceptwetsvoorstel op het gebied van de interpunctie, spelling, grammatica en opmaak. Deze fouten zijn hersteld.

9.14 Uitvoerings- en handhaafbaarheidstoetsen

De betrokken vakdepartementen hebben uitvoerings- en handhaafbaarheidstoetsen laten uitvoeren op een concept van het wetsvoorstel en hebben deze als volgt beoordeeld.

Ministerie van Binnenlandse Zaken en Koninkrijkrelaties
De RDI heeft een toets uitgevoerd op de Cbw. De RDI gaat toezicht houden op de sector overheid en heeft zich in de toets daarom geconcentreerd op de onderdelen uit de Cbw die raken aan toezicht. De RDI acht het conceptwetsvoorstel dat is voorgelegd uitvoerbaar, handhaafbaar en fraudebestendig. Wel heeft de RDI in de toets een aantal aandachtspunten kenbaar gemaakt. Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties neemt deze aandachtspunten ter harte, onder andere de verdere benodigde afstemming in de lagere regelgeving voor de sector overheid.

Ministerie van Economische Zaken en Ministerie van Klimaat en Groene Groei
Een eerdere versie van dit wetsvoorstel is aan de RDI voorgelegd voor een toets op de uitvoerbaarheid en handhaafbaarheid van het wetsvoorstel. De RDI heeft in haar reactie opmerkingen gemaakt en suggesties gedaan ten aanzien van verschillende onderwerpen uit het wetsvoorstel. Het gaat hierbij om de verstrekking van vertrouwelijke gegevens, de informatie-uitwisseling tussen autoriteiten, de audit, de aanwijzing van de vertegenwoordiger, de governance in relatie tot de handhaving hierop, de hoogte van de bestuurlijke boete, de database met domeinregistratiegegevens, de uitzondering van de root-naamservers en definities van de sectoren ruimtevaart en elektriciteitsproducent. Deze onderwerpen zijn nader met de RDI besproken. Dit heeft geleid tot aanpassingen van meerdere artikelen en de memorie van toelichting. Met betrekking tot de reactie van de RDI ten aanzien van de definitie van elektriciteitsproducent wordt hieronder nader ingegaan.

De RDI heeft in haar uitvoerbaarheids- en handhaafbaarheidstoets aangegeven dat het vanuit de doelstelling van de NIS2-richtlijn niet de bedoeling is dat een bedrijf met zonnepanelen en met een bepaalde omvang in lijn met de size-gap criteria van de NIS2-richtlijn, zonder meer onder de reikwijdte van de Cbw komt te vallen wanneer dit bedrijf energie opwekt voor eigen gebruik. Elektriciteitsproducenten vallen als soort entiteit binnen de reikwijdte van de NIS2-richtlijn. Het gaat hierbij om producenten als bedoeld in artikel 2, onderdeel 38, van Richtlijn (EU) 2019/944.[70] In de laatstgenoemde bepaling wordt een producent gedefinieerd als een natuurlijke persoon of rechtspersoon die elektriciteit opwekt.
In het kader van duurzaamheid wekken steeds meer bedrijven voor hun eigen gebruik elektriciteit op met bijvoorbeeld zonnepanelen op daken, zonder dat dit hun hoofdactiviteit betreft. Op basis van de definitie zouden dit soort partijen echter wel kwalificeren als elektriciteitsproducent. Als zij daarnaast aan de overige omvangscriteria voldoen, zouden ze binnen de reikwijdte van de Cbw vallen. Dit kan leiden tot een situatie dat veel bedrijven die in beginsel niet actief zijn in één van de sectoren uit de Cbw, als elektriciteitsproducent alsnog onder het toepassingsbereik van de Cbw komen te vallen. Daardoor worden deze partijen met wettelijke verplichtingen belast die vanuit de bedoeling van de NIS2-richtlijn niet voor hen bestemd zijn. Daarnaast kan dit nadelige gevolgen hebben voor de uitvoerbaarheid van het toezicht van de RDI.
Naar aanleiding van deze reactie van de RDI is de definitie van elektriciteitsproducten nader afgebakend, binnen de bedoeling van de NIS2-richtlijn, naar producenten als bedoeld in artikel 2, onderdeel 38, van Richtlijn (EU) 2019/944, voor zover de opwekking van elektriciteit hun belangrijkste commerciële of professionele activiteit vormt, of zij één of meerdere productie-installaties met een cumulatief nominaal vermogen van ten minste 100 megawatt beheren.
Hiermee wordt enerzijds een nadere afbakening gegeven naar de bedoeling van de NIS2-richtlijn. Anderzijds wordt met de 100 megawatt aangesloten bij de huidige drempel vanuit de Wbni, waardoor partijen die elektriciteitsproductie niet als belangrijkste commerciële of professionele activiteit hebben, maar toch een significant vermogen beheren net als onder de Wbni, wel onder het bereik van de Cbw vallen.
Ten overvloede wordt nog opgemerkt dat elektriciteitsproducenten die zelf opgewekte elektriciteit, bijvoorbeeld door zonnepanelen, gebruiken voor hun eigen gebruik in de regel niet kwalificeren als elektriciteitsbedrijf die de functie van levering verrichten, welke in bijlage 1 van de Cbw is opgenomen als soort entiteit. Voor zover het gaat om een elektriciteitsbedrijf die de functie verricht van levering, gaat het immers om een natuurlijke persoon of rechtspersoon die ten minste één van de volgende functies vervult: productie, transmissie, distributie, aggregatie, vraagrespons, energieopslag, levering of aankoop van elektriciteit, en die verantwoordelijk is voor de met deze functies verband houdende commerciële, technische of onderhoudswerkzaamheden, maar die geen eindafnemer is. Dergelijke partijen zullen in de regel eindafnemer zijn en daarmee niet vallen binnen de reikwijdte van de definitie van elektriciteitsbedrijf die de functie van levering verrichten.

Ministerie van Financiën
Onder de Cbw is het Ministerie van Financiën aangewezen als bevoegde autoriteit voor de financiële sector. Voor de Cbw geldt dat er voor de financiële sector sectorspecifieke wetgeving is op het gebied van digitale operationele weerbaarheid (Verordening digitale operationele weerbaarheid). Die verordening is een lex specialis ten opzichte van de NIS2-richtlijn.
Het Ministerie van Financiën moet ook als entiteit aan de Cbw voldoen. Aangezien een groot deel van de onderdelen uit de richtlijnen ten tijde van de toets nog uitgewerkt wordt in lagere regelgeving (amvb) is de impact hiervan op de bedrijfsvoering van het ministerie nu nog niet te toetsen. Concluderend acht het Ministerie van Financiën de Cbw, waar het de taak als bevoegde autoriteit ten aanzien van financiële instellingen betreft, uitvoerbaar en handhaafbaar. Wel blijft het essentieel om blijvend de samenhang tussen de Verordening digitale operationele weerbaarheid, de Wwke en de Cbw te bekijken. Dit in samenwerking met de sector, toezichthouders en de NCTV.

Ministerie van Infrastructuur en Waterstaat

[70] Richtlijn (EU) 2019/944 van het Europees Parlement en de Raad van 5 juni 2019 betreffende gemeenschappelijke regels voor de interne markt voor elektriciteit en tot wijziging van Richtlijn 2012/27/EU (*PbEU* 2019, L 158).

De uitkomst van de handhaafbaarheid-, uitvoerbaarheid- en fraudegevoeligheidtoets van de Inspectie Leefomgeving en Transport gaf geen aanleiding om het wetsvoorstel aan te passen.

Ministerie van Landbouw, Visserij, Voedselzekerheid en Natuur
De uitkomst van de handhaafbaarheid-, uitvoerbaarheid- en fraudegevoeligheid-toets van de Nederlandse Voedsel- en Warenautoriteit (hierna: NVWA) gaf geen aanleiding om het wetsvoorstel aan te passen. De NVWA ziet geen reden waarom de Cbw voor de NVWA niet handhaafbaar, uitvoerbaar en fraudebestendig zou zijn, mits zij voldoende tijd krijgt om de Cbw te kunnen implementeren, de benodigde technische expertise kan inhuren en voor deze inhuur en andere benodigdheden voldoende middelen krijgt. Daarnaast gaf de NVWA aan dat de reikwijdte en de te handhaven normen ten tijde van de toets nog bij amvb moeten worden vastgesteld.
Bovendien wijst de NVWA op het belang van het maken van werkafspraken tussen toezichthouders.
De reactie ten aanzien van het punt over de te handhaven normen is als volgt. Naar aanleiding van de consultatie is besloten om de zorgplichtmaatregelen in de wet op te nemen.

Ministerie van Volksgezondheid, Welzijn en Sport
De Inspectie Gezondheidszorg en Jeugd (IGJ) komt op basis van de toets tot de conclusie dat het wetsvoorstel vanuit het perspectief van toezicht en handhaafbaarheid en de uitvoering in de praktijk aanpassing behoeft van artikel 70a Cbw. Artikel 70a Cbw betreft een verkeerde implementatie van artikel 32, lid 2, onderdeel c, NI2-richtlijn en bevat, gelet op de tekst van de richtlijn, nationaal een onnodige beperking. De reactie hierop is als volgt. Het artikel is komen te vervallen.
De inspectie verzoekt daarnaast om in de memorie van toelichting meer duidelijkheid te verschaffen over een aantal vragen die het voorstel oproept en verzoekt om de paragraaf over de verwerking van bijzondere persoonsgegevens door de bevoegde autoriteit de toelichting aan te passen, zodat meer ruimte wordt gelaten om de autoriteit een keuze te maken uit passende beveiligingsmaatregelen, toegespitst op de praktijk en passend bij de sector zorg. Ook ziet de inspectie aanleiding tot het maken van een aantal inhoudelijke adviezen.

Ministerie van Justitie en Veiligheid
In verband met de grote gevolgen van de Cbw voor het NCSC, heeft het NCSC reeds in een vroege fase van het implementatietraject een uitvoeringstoets uitgevoerd op basis van de NIS2-richtlijn en de op dat moment bekende implementatiekeuzes. Uit deze uitvoeringstoets bleek dat het NCSC de Cbw uitvoerbaar acht, mits rekening gehouden werd met een aantal voorwaarden, zoals de juridische grondslag voor de uitvoering van de taken van het NCSC, een realistisch groeipad in de uitvoering van deze taken en de daarvoor beschikbare financiële middelen. Deze punten zijn meegewogen in het wetgevingstraject, en bij het verstrekken van de opdracht aan het NCSC voor de uitvoering van de taken die volgen uit deze wet.

10. Overgangsrecht en inwerkingtreding

De Cbw voorziet in overgangsrecht (artikel 95 Cbw). Dit is nodig, omdat de Cbw voorziet in het verval van de Wbni en er voor het moment van dat verval besluiten kunnen zijn genomen op grond van de Wbni of meldingen kunnen zijn gedaan op grond van artikel 10 of 13 Wbni. In artikel 95 Cbw wordt geregeld welk recht van toepassing is indien er voor het verval van de Wbni een besluit is genomen op grond van de Wbni of een melding is gedaan op grond van artikel 10 of 13 Wbni.

Met betrekking tot de inwerkingtreding van de Cbw is in artikel 104 Cbw bepaald dat de Cbw in werking treedt op een bij koninklijk besluit te bepalen tijdstip, dat voor de verschillende artikelen of onderdelen daarvan verschillend kan worden vastgesteld. Op grond van dit artikel kan worden gekozen voor een gefaseerde inwerkingtreding. Dit is denkbaar in het geval dat bepaalde onderdelen van de Cbw nog niet in werking kunnen treden, terwijl dat bij andere onderdelen van de Cbw wel het geval is. De verwachting is dat bij de inwerkingtreding van (onderdelen van) de Cbw een uitzondering wordt gemaakt op de vaste verandermomenten en de minimuminvoeringstermijn, omdat de Cbw ziet op de implementatie van een bindende EU-rechtshandeling.

11. Transponeringstabel

Bepaling uit 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 (*PbEU* 2022, L 333)	**Bepaling in Cbw of bestaande regeling**	**Omschrijving beleidsruimte**	**Toelichting**
Artikel 1, eerste en tweede lid	-	-	Deze bepalingen behoeven geen implementatie in nationale wetgeving, omdat deze een uitleg betreffen van de inhoud van de richtlijn.
Artikel 2, eerste lid	De artikelen 4 en 8, eerste lid, onderdeel f, en tweede lid, Cbw	-	-
Artikel 2, tweede lid	De artikelen 8, 9 en 12 Cbw	-	-
Artikel 2, derde lid	Artikel 8, eerste lid, onderdeel i, Cbw	-	-
Artikel 2, vierde lid	Artikel 4, vierde lid, Cbw	-	-
Artikel 2, vijfde lid, aanhef en onderdeel a	Artikel 8, eerste lid, onderdeel h, Cbw	-	-
Artikel 2, vijfde lid, aanhef en onderdeel b	De artikelen 11 en 13 Cbw	-	-
Artikel 2, zesde lid	-	-	Deze bepaling behoeft geen implementatie in nationale wetgeving, omdat het een uitleg betreft van hetgeen de richtlijn lidstaten nadrukkelijk niet belet.
Artikel 2, zevende lid	Artikel 5 Cbw	-	-
Artikel 2, achtste lid	De artikelen 23, 32, 45 en 48 Cbw	De mogelijkheid om specifieke entiteiten vrij te stellen van bepaalde verplichtingen.	De genoemde artikelen uit de Cbw voorzien in de bevoegdheid van Onze Minister die het aangaat tot het ontheffen van bepaalde entiteiten van bepaalde verplichtingen. Die bevoegdheid strekt tot de entiteiten en verplichtingen, bedoeld in artikel 2, achtste lid, NIS2-richtlijn.
Artikel 2, negende lid	De artikelen 5, tweede lid, 23, tweede lid, 32, tweede lid, 45, tweede lid, en 48, tweede lid, Cbw	-	-
Artikel 2, tiende lid	Artikel 7 Cbw	-	-
Artikel 2, elfde lid	Artikel 67 Cbw	-	-
Artikel 2, twaalfde lid	-	-	Deze bepaling behoeft geen implementatie in nationale wetgeving, omdat het ziet op de uitleg dat de richtlijn van toepassing is onverminderd enkele

			andere genoemde EU-wetgeving.
Artikel 2, dertiende lid	Artikel 66 Cbw	-	-
Artikel 2, veertiende lid	Artikel 63 Cbw	-	-
Artikel 3, eerste lid, onderdelen a tot en met f	De artikelen 8 en 9 Cbw	-	-
Artikel 3, eerste lid, aanhef en onderdeel g	Artikel 10 Cbw	De mogelijkheid om de entiteiten die voor 16 januari 2023 door Nederland zijn aangemerkt als aanbieder van essentiële diensten overeenkomstig de NIS1-richtlijn, te beschouwen als essentiële entiteit.	Artikel 10 Cbw voorziet in de bevoegdheid om deze aanbieders van essentiële diensten aan te wijzen als essentiële entiteit in de zin van de Cbw.
Artikel 3, tweede lid	Artikel 12 Cbw	-	-
Artikel 3, derde lid	Artikel 43 Cbw	-	-
Artikel 3, vierde lid	Artikel 44 Cbw	De mogelijkheid om te bepalen dat de in artikel 3, derde lid, NIS2-richtlijn bedoelde entiteiten voor het opstellen van de lijst meer informatie moeten aanleveren dan in artikel 3, vierde lid, NIS2-richtlijn worden genoemd.	In artikel 44, eerste lid, onderdeel f, Cbw is voorzien in de mogelijkheid om voor te schrijven dat entiteiten meer informatie moeten aanleveren dan die in artikel 3, vierde lid, NIS2-richtlijn staan genoemd.
Artikel 3, vijfde lid	-	-	Deze bepaling behoeft geen implementatie in nationale wetgeving, omdat het ziet op een feitelijke handeling van de centrale overheid.
Artikel 3, zesde lid	-	-	Deze bepaling ziet op een mogelijkheid van lidstaten en dit behoeft geen implementatie in nationale wetgeving.
Artikel 4, eerste lid	De artikelen 22, eerste lid, en 31, eerste lid, Cbw	-	-
Artikel 4, tweede lid, onderdeel a	Artikel 22, tweede lid, Cbw	-	-
Artikel 4, tweede lid, onderdeel b	Artikel 31, tweede lid, Cbw	-	-
Artikel 4, derde lid	-	-	Deze bepaling behoeft geen implementatie in nationale wetgeving.
Artikel 5	-	De mogelijkheid om nationale bepalingen te treffen of te handhaven om een hoger cyberbeveiligingsniveau te waarborgen.	Er is geen gebruik gemaakt van deze mogelijkheid.
Artikel 6	Artikel 1 Cbw, voor zover de begrippen in de Cbw voorkomen	-	-
Artikel 7, eerste lid	Artikel 19, eerste lid, Cbw	-	-
Artikel 7, tweede lid	Artikel 19, tweede lid, Cbw	-	-
Artikel 7, derde lid	-	-	Deze bepaling behoeft geen implementatie in nationale wetgeving, omdat het ziet op een feitelijke handeling van de centrale overheid.
Artikel 7, vierde lid	Artikel 19, derde lid, Cbw	-	-
Artikel 8, eerste en tweede lid	Artikel 15 Cbw	-	-
Artikel 8, derde en vierde	Artikel 14 Cbw	-	-

lid			
Artikel 8, vijfde en zesde lid	-	-	Deze bepalingen behoeven geen implementatie in nationale wetgeving, omdat deze zien op feitelijke handelingen van de centrale overheid.
Artikel 9, eerste lid	Artikel 18 Cbw	De mogelijkheid om meer dan één cybercrisisbeheerautoriteit en aan te wijzen of in te stellen.	-
Artikel 9, tweede lid	-	-	Nederland gaat niet over tot het instellen van meerdere cybercrisisbeheerautoriteiten.
Artikel 9, derde lid	-	-	Deze bepaling behoeft geen implementatie in nationale wetgeving, omdat het ziet op een feitelijke handeling van de centrale overheid.
Artikel 9, vierde lid	Artikel 20 Cbw	-	-
Artikel 9, vijfde lid	-	-	Deze bepaling behoeft geen implementatie in nationale wetgeving, omdat het ziet op een feitelijke handeling van de centrale overheid.
Artikel 10, eerste lid	Artikel 16 Cbw	-	-
Artikel 10, tweede lid	-	-	Deze bepaling behoeft geen implementatie in nationale wetgeving, omdat het ziet op een feitelijke handeling van de centrale overheid.
Artikel 10, derde lid	Artikel 16, derde lid, onderdeel i, Cbw	-	-
Artikel 10, vierde lid	De artikelen 52 en 52 Cbw	-	-
Artikel 10, vijfde lid	Artikel 16, derde lid, onderdeel g, Cbw	-	-
Artikel 10, zesde lid	Artikel 16, derde lid, onderdeel f, Cbw	-	-
Artikel 10, zevende lid	Artikel 54, eerste lid, Cbw	-	-
Artikel 10, achtste lid	Artikel 54, tweede lid, Cbw	-	-
Artikel 10, negende en tiende lid	-	-	Deze bepalingen behoeven geen implementatie in nationale wetgeving, omdat deze zien op feitelijke handelingen van de centrale overheid.
Artikel 11, eerste lid	-	-	Deze bepaling behoeft geen implementatie in nationale wetgeving.
Artikel 11, tweede lid	-	-	Deze bepaling behoeft geen implementatie in nationale wetgeving, omdat het ziet op een feitelijke handeling van de centrale overheid.
Artikel 11, derde lid	Artikel 16, derde, vierde en vijfde lid, Cbw	-	-
Artikel 11, vierde lid	Artikel 16, zesde lid, Cbw	-	-
Artikel 11, vijfde lid	Artikel 16, zevende lid, Cbw	-	-
Artikel 12, eerste lid	Artikel 17 Cbw	-	-

Artikel 12, tweede lid	-	-	Deze bepaling is gericht op Enisa.
Artikel 13, eerste lid	Artikel 51 Cbw	-	-
Artikel 13, tweede lid	De artikelen 25 tot en met 29 en 33 Cbw	-	-
Artikel 13, derde lid	Artikel 39 Cbw	-	-
Artikel 13, vierde lid	Artikel 51 Cbw	-	-
Artikel 13, vijfde lid	De artikelen 56 en 59 Cbw	-	-
Artikel 13, zesde lid	-	-	Deze bepaling behoeft geen implementatie in nationale wetgeving, omdat het ziet op een feitelijke handeling van de centrale overheid.
Artikel 14, eerste lid	-	-	Deze bepaling ziet op de oprichting van de samenwerkingsgroep.
Artikel 14, tweede lid	-	-	Deze bepaling is gericht op de samenwerkingsgroep.
Artikel 14, derde lid	-	-	Deze bepaling ziet op de samenstelling van de samenwerkingsgroep.
Artikel 14, vierde, zesde, zevende en negende lid	-	-	Deze bepalingen zijn gericht op de samenwerkingsgroep.
Artikel 14, vijfde lid	-	-	Deze bepaling behoeft geen implementatie in nationale wetgeving, omdat het ziet op een feitelijke handeling van de centrale overheid.
Artikel 14, achtste lid	-	-	Deze bepaling ziet op een bevoegdheid van de Europese Commissie.
Artikel 15, eerste lid	-	-	Deze bepaling ziet op de oprichting van het CSIRT-netwerk.
Artikel 15, tweede lid	-	-	Deze bepaling is gericht op het CSIRT-netwerk, de Europese Commissie en Enisa.
Artikel 15, derde, vierde en vijfde lid	-	-	Deze bepalingen zijn gericht op het CSIRT-netwerk.
Artikel 15, zesde lid	-	-	Deze bepaling is gericht op het CSIRT-netwerk en EU-CyCLONe.
Artikel 16, eerste lid	-	-	Deze bepaling ziet op de oprichting van EU-CyCLONe.
Artikel 16, tweede lid	-	-	Deze bepaling is gericht op EU-CyCLONe, de Europese Commissie en Enisa.
Artikel 16, derde, vierde, vijfde en zevende lid	-	-	Deze bepalingen zijn gericht op EU-CyCLONe.
Artikel 16, zesde lid	-	-	Deze bepaling is gericht op EU-CyCLONe en het CSIRT-netwerk.
Artikel 17	-	-	Deze bepaling is gericht op de EU.
Artikel 18, eerste, tweede en derde lid	-	-	Deze bepalingen zijn gericht op Enisa.
Artikel 19, eerste tot en met negende lid	-	-	Deze bepalingen zien met name op de invulling van collegiale toetsingen en

			behoeven om diverse redenen geen implementatie in nationale wetgeving. Ten aanzien van enkele bepalingen is de reden dat deze enkel gericht zijn de samenwerkingsgroep, de Europese Commissie en Enisa.
Artikel 20, eerste en tweede lid	Artikel 24 Cbw	-	-
Artikel 21, eerste, tweede en derde lid	Artikel 21 Cbw	-	-
Artikel 21, vierde lid	De artikelen 69 tot en met 86 Cbw	-	-
Artikel 21, vijfde lid	-	-	Deze bepaling is gericht op de Europese Commissie.
Artikel 22, eerste lid	-	-	Deze bepaling is gericht op de samenwerkingsgroep.
Artikel 22, tweede lid	-	-	Deze bepaling is gericht op de Europese Commissie.
Artikel 23, eerste lid	De artikelen 25 tot en met 29, 30, eerste lid, en 39, eerste lid, Cbw	-	-
Artikel 23, tweede lid	Artikel 30, tweede lid, Cbw	-	-
Artikel 23, derde lid	Artikel 25, tweede lid, Cbw	-	-
Artikel 23, vierde lid	De artikelen 26 tot en met 29 Cbw	-	-
Artikel 23, vijfde lid	Artikel 36 Cbw	-	-
Artikel 23, zesde lid	Artikel 39, tweede lid, Cbw	-	-
Artikel 23, zevende lid	Artikel 37 Cbw	-	-
Artikel 23, achtste lid	Artikel 39, derde lid, Cbw	-	-
Artikel 23, negende lid	Artikel 39, vijfde lid, Cbw	-	-
Artikel 23, tiende lid	Artikel 40 Cbw	-	-
Artikel 23, elfde lid	-	-	Deze bepaling ziet op een bevoegdheid van de Europese Commissie.
Artikel 24, eerste lid	-	De mogelijkheid om essentiële entiteiten en belangrijke entiteiten te verplichten bepaalde ICT-producten, -diensten en -processen te gebruiken.	Er is geen gebruik gemaakt van de mogelijkheid.
Artikel 24, tweede lid	-	-	Deze bepaling ziet op een bevoegdheid van de Europese Commissie.
Artikel 24, derde lid	-	-	Deze bepaling is gericht op de Europese Commissie.
Artikel 25, eerste lid	-	-	Deze bepaling ziet op een aanmoediging.
Artikel 25, tweede lid	-	-	Deze bepaling is gericht op Enisa.
Artikel 26, eerste en tweede lid	Artikel 4, eerste tot en met vijfde lid, Cbw	-	-
Artikel 26, derde lid	Artikel 42 Cbw	-	-
Artikel 26, vierde lid	-	-	Deze bepaling behoeft geen implementatie in nationale wetgeving.
Artikel 26, vijfde lid	Artikel 60 Cbw	-	-
Artikel 27, eerste lid	-	-	Deze bepaling is gericht op Enisa.
Artikel 27, tweede lid	Artikel 47, eerste tot en	-	-

	met vierde lid, Cbw		
Artikel 27, derde lid	Artikel 47, vijfde lid, Cbw	-	-
Artikel 27, vierde lid	-	-	Deze bepaling behoeft geen implementatie in nationale wetgeving, omdat het ziet op een feitelijke handeling van de centrale overheid.
Artikel 27, vijfde lid	Artikel 48, eerste lid, aanhef, Cbw	-	-
Artikel 28, eerste lid	Artikel 49, eerste lid, Cbw	-	-
Artikel 28, tweede lid	Artikel 49, tweede lid, Cbw	-	-
Artikel 28, derde lid	Artikel 49, derde lid, Cbw	-	-
Artikel 28, vierde lid	Artikel 49, vierde lid, Cbw	-	-
Artikel 28, vijfde lid	Artikel 50 Cbw	-	-
Artikel 28, zesde lid	Artikel 49, vijfde lid, Cbw	-	-
Artikel 29, eerste, tweede en derde lid	Artikel 62 Cbw	-	-
Artikel 29, vierde lid	Artikel 44, eerste lid, onderdeel e, Cbw	-	-
Artikel 29, vijfde lid	-	-	Deze bepaling is gericht op Enisa.
Artikel 30, eerste lid	Artikel 33, eerste lid, Cbw	-	-
Artikel 30, tweede lid	De artikelen 33, tweede lid, en 39, eerste lid, Cbw	-	-
Artikel 31, eerste lid	Hoofdstuk 15 Cbw	-	-
Artikel 31, tweede lid	-	-	Deze bepaling behoeft geen implementatie in nationale wetgeving, omdat het ziet op feitelijke handelingen van de centrale overheid.
Artikel 31, derde lid	Artikel 58, eerste lid, Cbw	-	-
Artikel 31, vierde lid	Hoofdstuk 15 Cbw	-	-
Artikel 32, eerste lid	Hoofdstuk 15 Cbw in samenhang met de titels 5.3 en 5.4 Awb	-	-
Artikel 32, tweede lid, aanhef en onderdeel a	De artikelen 5:15 en 5:18 Awb	-	-
Artikel 32, tweede lid, aanhef en onderdelen b en c	Artikel 71 Cbw	-	-
Artikel 32, tweede lid, aanhef en onderdeel d	Artikel 70 Cbw	-	-
Artikel 32, tweede lid, aanhef en onderdeel e	De artikelen 5:16 en 5:17 Awb	-	-
Artikel 32, tweede lid, aanhef en onderdeel f	De artikelen 5:15, 5:16 en 5:17 Awb	-	-
Artikel 32, tweede lid, aanhef en onderdeel g	De artikelen 5:16 en 5:17 Awb	-	-
Artikel 32, tweede lid, tweede volzin	Artikel 71, tweede lid, Cbw	-	-
Artikel 32, tweede lid, derde volzin	Artikel 71, eerste lid, onderdeel b, Cbw	-	-
Artikel 32, tweede lid, vierde volzin	Artikel 71, vierde lid, Cbw	-	-
Artikel 32, derde lid	Artikel 5:16 Awb, zie toelichting	-	Artikel 5:16 Awb verschaft aan toezichthouders een algemene bevoegdheid om inlichtingen te vorderen. De toezichthouder moet zijn vordering motiveren en daarbij de wettelijke

			grondslag noemen.[71] Onderdeel van die motiveringsplicht is dat de toezichthouder motiveert waarom de gevorderde informatie noodzakelijk is voor het uitoefenen van de toezichthoudende taak.[72] De vordering van de toezichthouder moet voldoende concreet zijn.[73]
Artikel 32, vierde lid, aanhef en onderdeel a	-	-	Het kunnen geven van een waarschuwing behoeft geen opname in wet- of regelgeving.
Artikel 32, vierde lid, aanhef en onderdeel b	Artikel 73 Cbw	-	-
Artikel 32, vierde lid, aanhef en onderdeel c	Artikel 74 Cbw	-	-
Artikel 32, vierde lid, aanhef en onderdeel d	Artikel 73 Cbw	-	-
Artikel 32, vierde lid, aanhef en onderdeel e	Artikel 38 Cbw	-	-
Artikel 32, vierde lid 4, aanhef en onderdeel f	Artikel 71, eerste lid, onderdeel c, Cbw	-	-
Artikel 32, vierde lid, aanhef en onderdeel g	Artikel 69 Cbw	-	-
Artikel 32, vierde lid, aanhef en onderdeel h	Artikel 72 Cbw	-	-
Artikel 32, vierde lid, aanhef en onderdeel i	Artikel 79 Cbw	-	-
Artikel 32, vijfde lid	De artikelen 75 tot en met 78 Cbw	-	-
Artikel 32, zesde lid	Artikel 5:1 Awb	-	Zie paragraaf 5.6.6 voor een toelichting hierop.
Artikel 32, zevende lid	Reeds geïmplementeerd door middel van bestaand recht, zie toelichting	-	Zie paragraaf 5.9 voor een toelichting hierop.
Artikel 32, achtste lid	Reeds geïmplementeerd door middel van bestaand recht, zie toelichting	-	Zie paragraaf 5.9 voor een toelichting hierop.
Artikel 32, negende lid	Artikel 56, tweede lid, Cbw en artikel 28, vierde lid, Wwke	-	-
Artikel 32, tiende lid	Artikel 57 Cbw	-	-
Artikel 33, eerste lid	Artikel 80 Cbw	-	-
Artikel 33, tweede lid, aanhef en onderdeel a	De artikelen 5:15 en 5:18 Awb	-	-
Artikel 33, tweede lid, aanhef en onderdeel b	Artikel 82 Cbw	-	-
Artikel 33, tweede lid, aanhef en onderdeel c	Artikel 81 Cbw	-	-
Artikel 33, tweede lid, aanhef en onderdeel d	De artikelen 5:16 en 5:17 Awb	-	-
Artikel 33, tweede lid,	De artikelen 5:15, 5:16 en	-	-

[71] *Kamerstukken II* 2004/05, 29708, nr. 7, p. 11.
[72] Zie ook ECLI:NL:RVS:2021:1674, rechtsoverweging 4.2: "Gelet op artikel 5:13 van de Awb maakt een toezichthouder slechts van zijn bevoegdheden gebruik voor zover dat redelijkerwijs voor de vervulling van zijn taak nodig is. De inspectie kan dus geen inzage vorderen van andere informatie dan die welke verband houden met de wettelijke voorschriften waarop het toezicht in het concrete geval betrekking heeft. Daarnaast moet zij motiveren waarom de gevraagde informatie noodzakelijk is voor het uitoefenen van het toezicht."
[73] Zie ook ECLI:NL:RVS:2016:378, rechtsoverweging 2.5: "Zoals de Afdeling eerder heeft overwogen (uitspraak van 2 mei 2012 in zaak nr. 201110374/1/V6), moeten uit het oogpunt van rechtszekerheid hoge eisen worden gesteld aan de kenbaarheid van een vordering tot het verlenen van medewerking."

aanhef en onderdeel e	5:17 Awb		
Artikel 33, tweede lid, aanhef en onderdeel f	De artikelen 5:16 en 5:17 Awb	-	-
Artikel 33, derde lid	Artikel 5:16 Awb, zie toelichting	-	Artikel 5:16 Awb verschaft aan toezichthouders een algemene bevoegdheid om inlichtingen te vorderen. De toezichthouder moet zijn vordering motiveren en daarbij de wettelijke grondslag noemen.[74] Onderdeel van die motiveringsplicht is dat de toezichthouder motiveert waarom de gevorderde informatie noodzakelijk is voor het uitoefenen van de toezichthoudende taak.[75] De vordering van de toezichthouder moet voldoende concreet zijn.[76]
Artikel 33, vierde lid, aanhef en onderdeel a	-	-	Het kunnen geven van een waarschuwing behoeft geen opname in wet- of regelgeving.
Artikel 33, vierde lid, aanhef en onderdeel b	Artikel 84 Cbw	-	-
Artikel 33, vierde lid, aanhef en onderdeel c	Artikel 85 Cbw	-	-
Artikel 33, vierde lid, aanhef en onderdeel d	Artikel 84 Cbw	-	-
Artikel 33, vierde lid, aanhef en onderdeel e	Artikel 38 Cbw	-	-
Artikel 33, vierde lid, aanhef en onderdeel f	Artikel 82, eerste lid, onderdeel c, Cbw	-	-
Artikel 33, vierde lid, aanhef en onderdeel g	Artikel 83 Cbw	-	-
Artikel 33, vierde lid, aanhef en onderdeel h	Artikel 86 Cbw	-	-
Artikel 33, vijfde lid	Reeds geïmplementeerd door middel van bestaand recht, zie toelichting	-	Zie de paragrafen 5.6.6 en 5.9 voor een toelichting hierop.
Artikel 33, zesde lid	Artikel 57 Cbw	-	-
Artikel 34, eerste lid	De artikelen 79 en 86 Cbw	-	-
Artikel 34, tweede lid	De artikelen 79, eerste lid, en 86, eerste lid, Cbw	-	-
Artikel 34, derde lid	Reeds geïmplementeerd door middel van bestaand recht, zie toelichting	-	Zie paragraaf 5.9 voor een toelichting hierop.
Artikel 34, vierde lid	Artikel 79, derde lid, Cbw	-	-
Artikel 34, vijfde lid	Artikel 86, derde lid, Cbw	-	-
Artikel 34, zesde lid	De artikelen 74 en 85 Cbw jo. artikel 5:32, eerste lid,	De mogelijkheid om te voorzien in de	-

[74] *Kamerstukken II* 2004/05, 29708, nr. 7, p. 11.
[75] Zie ook ECLI:NL:RVS:2021:1674, rechtsoverweging 4.2: "Gelet op artikel 5:13 van de Awb maakt een toezichthouder slechts van zijn bevoegdheden gebruik voor zover dat redelijkerwijs voor de vervulling van zijn taak nodig is. De inspectie kan dus geen inzage vorderen van andere informatie dan die welke verband houden met de wettelijke voorschriften waarop het toezicht in het concrete geval betrekking heeft. Daarnaast moet zij motiveren waarom de gevraagde informatie noodzakelijk is voor het uitoefenen van het toezicht."
[76] Zie ook ECLI:NL:RVS:2016:378, rechtsoverweging 2.5: "Zoals de Afdeling eerder heeft overwogen (uitspraak van 2 mei 2012 in zaak nr. 201110374/1/V6), moeten uit het oogpunt van rechtszekerheid hoge eisen worden gesteld aan de kenbaarheid van een vordering tot het verlenen van medewerking."

	Awb	bevoegdheid tot het opleggen van dwangsommen.	
Artikel 34, zevende lid	Artikel 79 Cbw	-	-
Artikel 34, achtste lid	-	-	Het Nederlands rechtsstelsel voorziet in bestuurlijke boeten.
Artikel 35, eerste lid	Artikel 58, tweede lid, Cbw	-	-
Artikel 35, tweede lid	Artikel 58, derde lid, Cbw	-	-
Artikel 35, derde lid	Artikel 58, vierde lid, Cbw	-	-
Artikel 36	Hoofdstuk 15 Cbw	-	-
Artikel 37, eerste lid	De artikelen 60 en 61 Cbw	-	-
Artikel 37, tweede lid	-	-	Voor de bedoelde gecoördineerde aanpak is geen wetgeving nodig.
Artikel 38, eerste en tweede lid	-	-	Deze bepalingen betreffen een bevoegdheid van de Europese Commissie.
Artikel 38, derde lid	-	-	Deze bepaling is gericht op het Europees Parlement en de Europese Raad.
Artikel 38, vierde en vijfde lid	-	-	Deze bepalingen zijn gericht op de Europese Commissie.
Artikel 38, zesde lid	-	-	Deze bepaling ziet op de inwerkingtreding van een gedelegeerde handeling.
Artikel 39, eerste, tweede en derde lid	-	-	Deze bepalingen zien op bijstand aan de Europese Commissie door een comité.
Artikel 40	-	-	Deze bepaling is gericht op de Europese Commissie.
Artikel 41, eerste lid	Zie toelichting	-	De NIS2-richtlijn wordt geïmplementeerd in de Cyberbeveiligingswet.
Artikel 41, tweede lid	-	-	Deze bepaling ziet op een feitelijke uitvoering.
Artikel 42	-	-	Deze bepaling noopt niet tot aanpassing van bestaande wet- en regelgeving.
Artikel 43	Artikel 98 Cbw	-	-
Artikel 44	Artikel 103 Cbw	-	-
Artikel 45	-	-	Deze bepaling ziet op de inwerkingtreding van de NIS2-richtlijn.
Artikel 46	-	-	Deze bepaling ziet op de adressaten van de NIS2-richtlijn.

ARTIKELSGEWIJZE TOELICHTING

Artikel 1 (begripsbepaling)

Definities uit artikel 6 NIS2-richtlijn
Artikel 1 Cbw bevat de definitie van begrippen uit de Cbw. De meeste definities in artikel 1 Cbw zijn identiek, dan wel inhoudelijk gelijk aan de definities in artikel 6 NIS2-richtlijn. Dit is ook het geval bij de begrippen waarvoor in artikel 6 NIS2-richtlijn wordt verwezen naar een definitie in andere EU-wetgeving.

Overheidsinstantie
De definitie van een overheidsinstantie betreft die uit artikel 6, onderdeel 35, NIS2-richtlijn en komt aan de orde in paragraaf 5.1.2.

Aanbieders van openbare elektronische communicatienetwerken en -diensten
Indien een aanbieder van een openbaar elektronisch communicatienetwerk of -dienst een openbare recursieve DNS-dienst (*publicly available recursive DNS service*) als bedoeld in artikel 6, onderdeel 20, subonderdeel a, NIS2-richtlijn verricht als onderdeel van de internettoegangsdienst, dan moet dit worden beschouwd als een openbare elektronische communicatiedienst en niet eveneens als een DNS-dienst. Hiermee wordt voorkomen dat eenzelfde dienst onder twee verschillende sectoren komt te vallen en hierdoor onder twee verschillende jurisdictieregimes komt te vallen (het regime, bedoeld in artikel 4, tweede lid, Cbw, voor de elektronische communicatiedienst respectievelijk het regime, bedoeld in artikel 4, derde lid, Cbw).

Artikel 2 (doel van deze wet)

In artikel 2 Cbw is het doel van de Cbw omschreven. Hetgeen in artikel 2 Cbw 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)

De NIS2-richtlijn bevat diverse grondslagen om uitvoeringshandelingen, gedelegeerde handelingen en richtsnoeren vast te stellen. Indien deze worden vastgesteld, is het mogelijk dat er in nationale wet- en regelgeving regels nodig zijn ter uitvoering daarvan. Artikel 3 Cbw bevat daarom een delegatiegrondslag om bij of krachtens amvb regels te kunnen stellen ter uitvoering van de op grond van de NIS2-richtlijn vastgestelde uitvoeringshandelingen, gedelegeerde handelingen en richtsnoeren. Dit betreft een facultatieve grondslag, omdat de mogelijkheid bestaat dat niet alle op grond van de NIS2-richtlijn vastgestelde uitvoeringshandelingen, gedelegeerde handelingen of richtsnoeren nopen tot het stellen van regels ter uitvoering daarvan.

Artikel 4 (toepassingsbereik en jurisdictie)

Artikel 4 Cbw ziet op het toepassingsbereik en de jurisdictie.

Artikel 4, eerste lid, Cbw strekt tot de implementatie van de artikelen 2, eerste lid, en 26, eerste lid, aanhef, NIS2-richtlijn en regelt dat het bepaalde bij of krachtens de Cbw met betrekking tot essentiële entiteiten en belangrijke entiteiten van toepassing is op die entiteiten, als zij in Nederland zijn gevestigd en hun diensten verlenen of hun activiteiten verrichten in Nederland of een andere lidstaat van de EU. Deze bepaling ziet alleen op essentiële entiteiten en belangrijke entiteiten, en niet op entiteiten die domeinnaamregistratiediensten verlenen, omdat artikel 2, eerste lid, NIS2-richtlijn alleen ziet op essentiële entiteiten en belangrijke entiteiten. Dit heeft tot gevolg dat voor het van toepassing zijn van het bepaalde bij of krachtens de Cbw over entiteiten die domeinnaamregistratiediensten verlenen, het niet vereist is dat deze entiteiten hun diensten verlenen of hun activiteiten verrichten in Nederland of een andere lidstaat van de EU. Dit komt tot uiting in artikel 4, vierde lid, Cbw, waarin artikel 26, eerste lid, onderdeel b, NIS2-richtlijn, met in achtneming van artikel 2, eerste lid, NIS2-richtlijn, is geïmplementeerd.

Artikel 4, tweede lid, Cbw strekt tot de implementatie van artikel 26, eerste lid, onderdeel a, NIS2-richtlijn en ziet specifiek op essentiële entiteiten en belangrijke entiteiten die aanbieders van openbare elektronische communicatienetwerken of aanbieders van openbare elektronische communicatiediensten zijn. Voor deze aanbieders geldt dat het bepaalde bij of krachtens de Cbw over essentiële entiteiten en belangrijke entiteiten die aanbieders van openbare elektronische communicatienetwerken of aanbieders van openbare elektronische communicatiediensten zijn, alleen op hen van toepassing is als zij hun diensten in Nederland aanbieden.

Artikel 4, derde lid, Cbw strekt tot de implementatie van artikel 26, eerste lid, onderdeel b, jo. artikel 2, eerste lid, NIS2-richtlijn en ziet specifiek op de daarin genoemde entiteiten. Het bepaalde bij of krachtens de Cbw over essentiële entiteiten en belangrijke entiteiten zijn alleen van toepassing op die entiteiten, als zij hun hoofdvestiging of vertegenwoordiger in Nederland hebben en hun diensten verlenen of hun activiteiten verrichten in Nederland of een andere lidstaat van de EU.

Artikel 4, vierde lid, Cbw heeft betrekking op entiteiten die domeinnaamregistratiediensten verlenen. Voor de toelichting op deze bepaling wordt verwezen naar de toelichting bij artikel 4, eerste lid, Cbw.

Artikel 4, vijfde lid, Cbw strekt tot de implementatie van artikel 26, eerste lid, onderdeel b, en tweede lid, NIS2-richtlijn en ziet kort gezegd op het bepalen waar een entiteit haar hoofdvestiging heeft. 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 Cbw toegepast worden en zo worden bepaald of de Cbw 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 die zijn hoofdvestiging in Frankrijk heeft en die in Nederland een aanbieder van openbare telecommunicatienetwerken – of diensten is. Ook op deze entiteit is de Cbw van toepassing.

De artikelen 42, 60 en 61 Cbw kunnen verplichtingen bevatten of tot verplichtingen leiden ten aanzien van entiteiten die niet onder het toepassingsbereik van de Cbw, geregeld in artikel 4, eerste tot en met vierde lid, Cbw vallen. Om ervoor te zorgen dat deze verplichtingen ook voor die entiteiten gelden, is in artikel 4, zesde lid, Cbw geregeld dat het bepaalde bij de eerdergenoemde artikelen van toepassing is, ook op deze entiteiten. Op deze wijze is de verplichting tot het aanwijzen van een vertegenwoordiger te allen tijde van toepassing onder de genoemde voorwaarden. Ook kunnen de bevoegde autoriteiten onder de genoemde omstandigheden wederzijdse bijstand verlenen, ook in gevallen dat een entiteit volgens artikel 4, eerste tot en met vierde lid, Cbw niet binnen het toepassingsbereik van de Cbw zou vallen.

Artikel 5 (overheidsinstanties die activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving)

In artikel 5 Cbw is geregeld op welke overheidsinstanties de Cbw niet van toepassing is.

Artikel 5, eerste lid, Cbw betreft de implementatie van artikel 2, zevende lid, NIS2-richtlijn. Overheidsinstanties die hoofdzakelijk 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 in artikel 5, eerste lid, uitgezonderd van het toepassingsbereik van de Cbw. Deze activiteiten vallen namelijk binnen de uitsluitende verantwoordelijkheid van lidstaten. Artikel 5, eerste lid, Cbw ziet alleen op overheidsinstanties die in hoofdzaak deze activiteiten uitvoeren. Overheidsinstanties die activiteiten verrichten die daar slechts zijdelings verband mee houden vallen wél onder het bereik van de Cbw. 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.

In elk geval het Ministerie van Defensie en de politie vallen op grond van artikel 5 Cbw buiten het toepassingsbereik van de Cbw.

Artikel 5 Cbw sluit aan op artikel 5 Wwke, waarin een soortgelijke bepaling uit de CER-richtlijn (artikel 1, zesde lid, CER-richtlijn) is geïmplementeerd.

Artikel 6 (root-naamservers)

Root-naamservers distribueren de root-zonefile, het wereldwijde register van de toegewezen topleveldomeinnamen. Dit register wordt gezien als onderdeel van de publieke kern van het internet. Het beheer van de DNS-root wordt onder toepassing van het multistakeholdermodel voor internetgovernance uitgevoerd door de Internet Cooperation for Assigned Named and Numbers (ICANN). Het DNS van het internet maakt momenteel gebruik van dertien root-naamservers om het DNS te laten functioneren. Deze zijn internationaal gekoppeld. Elke root-naamserver bestaat uit tientallen tot honderden wereldwijd verspreide zelfstandige servers, die elkaar in geval van verstoringen kunnen vervangen.

De intentie van de Europese wetgever is dat root-naamservers zijn uitgezonderd van het toepassingsbereik van de NIS2-richtlijn. Dit volgt uit de in artikel 6, onderdeel 20, NIS2-richtlijn opgenomen definitie van DNS-dienstverlener, uit bijlage I van de NIS2-richtlijn, onder de sector digitale infrastructuur en uit overweging 32 van de NIS2-richtlijn. Zonder aanvullende regeling in de Cbw bestaat echter het risico dat root-naamservers alsnog onder het toepassingsbereik van de Cbw komen te vallen, bijvoorbeeld als RIPE NCC (onderhouder van één van de dertien DNS root-naamservers van het internet) als essentiële entiteit of belangrijke entiteit kwalificeert doordat het andersoortige activiteiten verricht of diensten aanbiedt die onder de NIS2-richtlijn vallen. In dat geval zouden alle verplichtingen uit de Cbw alsnog op RIPE NCC rusten, inclusief de root-naamserver omdat de verplichtingen zien op de hele entiteit. Om ervoor te zorgen dat de root-naamserveractiviteiten te allen tijde van de Cbw is uitgesloten regelt artikel 6 Cbw dat de Cbw niet van toepassing is op root-naamservers.

Artikel 7 (entiteiten uitgezonderd van Verordening (EU) 2022/2554)

Artikel 7 Cbw 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.

Hierbij wordt aangetekend dat andere financiële entiteiten die onder de Verordening digitale operationele weerbaarheid zijn aangewezen wel binnen het bereik van de Cbw vallen, mits zij ook uit hoofde van de NIS2-richtlijn onder het toepassingsbereik van de richtlijn vallen. Het gaat om kredietinstellingen, exploitanten van handelsplatformen en centrale tegenpartijen (zie bijlage 1 van de Cbw, onder de sectoren bankwezen en infrastructuur financiële markt). Op deze entiteiten zijn niet alle verplichtingen van de Cbw van toepassing. Zo gelden voor hen niet de zorgplicht (artikel 21 Cbw), de verplichtingen over governance (artikel 24 Cbw) en de meldplicht (de artikelen 25 tot en met 30 Cbw), voor zover zij niet tevens kwalificeren als ander soort entiteit onder de Cbw, maar geldt bijvoorbeeld wel de verplichting uit artikel 43 Cbw over het verstrekken van informatie ten behoeve van het nationale register. Paragraaf 2.4 gaat hier nader op in.

Tot slot wordt hierbij aangetekend dat financiële entiteiten die ook diensten verlenen in een andere sector, zoals de sector digitale infrastructuur, zowel onder de NIS2-richtlijn (voor zover het gaat om

de digitale infrastructuur) vallen, als onder de Verordening digitale operationele weerbaarheid, uiteraard voor zover zij onder het toepassingsbereik van die verordening vallen.

Artikel 8 (essentiële entiteit van rechtswege)

Eerste lid
Artikel 8, eerste lid, Cbw strekt tot de implementatie van de artikelen 2, eerste en tweede lid, en 3, eerste lid, NIS2-richtlijn. Voor een toelichting wordt verwezen naar paragraaf 5.1.1.

Tweede lid
Artikel 8, tweede lid, Cbw 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 Cbw 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 5.1.1.

Aanwijzing bij besluit of regeling
In artikel 9 Cbw is geregeld dat een entiteit kan worden aangewezen als essentiële entiteit bij besluit of regeling van de vakminister. Deze aanwijzing betreft een besluit in de zin van artikel 1:3 Awb. Dit betekent dat de vakminister bij de aanwijzing moet voldoen aan de in de Awb gestelde eisen aan besluitvorming door bestuursorganen en dat tegen het aanwijzingsbesluit bestuursrechtelijke rechtsbescherming open staat. Dit geldt ook indien de vakminister ervoor kiest om een entiteit bij regeling aan te wijzen als essentiële entiteit. Ook dan gelden onverkort de hiervoor bedoelde eisen uit de Awb en bestuursrechtelijke rechtsbescherming.
Het is aan de vakminister om te kiezen tussen een aanwijzing bij besluit of een aanwijzing bij regeling. Het is denkbaar dat de keuze valt voor de aanwijzing bij besluit in de gevallen waarin de openbaarheid van een aanwijzing als essentiële 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, 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.

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

Artikel 10 Cbw 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 Cbw is geregeld dat entiteiten die op grond van de Wbni 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 (aanwijzing onderwijsinstelling als essentiële entiteit)

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 13 Cbw. Paragraaf 5.1.3 gaat hier nader op in.

Artikel 11 Cbw biedt de Minister van Onderwijs, Cultuur en Wetenschap de mogelijkheid om instellingen voor hoger onderwijs aan te wijzen als essentiële entiteit. Deze aanwijzing kan bij regeling

of besluit. Het is aan de Minister van Onderwijs, Cultuur en Wetenschap om te bepalen of de aanwijzing geschiedt bij regeling of bij besluit. Voor een nadere toelichting op de aanwijzing bij regeling of besluit wordt verwezen naar de artikelsgewijze toelichting op artikel 8 Cbw.

Artikel 12 (belangrijke entiteit van rechtswege)

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

Artikel 12, tweede lid, Cbw 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 (aanwijzing onderwijsinstelling als belangrijke entiteit)

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 13 Cbw. Paragraaf 5.1.3 gaat hier nader op in.

Artikel 13 Cbw biedt de Minister van Onderwijs, Cultuur en Wetenschap de mogelijkheid om instellingen voor hoger onderwijs aan te wijzen als belangrijke entiteit. Deze aanwijzing kan bij regeling of besluit. Het is aan de Minister van Onderwijs, Cultuur en Wetenschap om te bepalen of de aanwijzing geschiedt bij regeling of bij besluit. Voor een nadere toelichting op de aanwijzing bij regeling of besluit wordt verwezen naar de artikelsgewijze toelichting op artikel 8 Cbw.

Artikel 14 (aanwijzing en taken centrale contactpunt)

Artikel 14 Cbw strekt tot de implementatie van artikel 8, derde en vierde lid, NIS2-richtlijn. In artikel 14 Cbw wordt de Minister van Justitie en Veiligheid aangewezen als het centrale contactpunt, bedoeld in artikel 8, vierde lid, NIS2-richtlijn. Deze minister heeft als centrale contactpunt de in artikel 14 Cbw 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 Wbni 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 EU. Dit om de grensoverschrijdende samenwerking en communicatie tussen de autoriteiten te vergemakkelijken en een doeltreffende uitvoering van de NIS2-richtlijn mogelijk te maken.[77]

Artikel 15 (aanwijzing en taken bevoegde autoriteit)

In artikel 15, eerste lid, Cbw 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 de Cbw.

De verantwoordelijkheid voor de sector overheid wordt verdeeld over de Minister van Binnenlandse Zaken en Koninkrijksrelaties (voor alle overheidsinstanties, behalve de waterschappen) en de Minister van Infrastructuur en Waterstaat voor de waterschappen. Dit laatste is in overeenstemming met de

[77] Overweging 39 NIS2-richtlijn.

verantwoordelijkheid op grond van de Waterschapswet en de taken van de waterschappen in de vitale infrastructuur, die uitsluitend betrekking hebben op diens beleidsterreinen.

In artikel 15, tweede lid, Cbw wordt de Minister van Economische Zaken aangewezen als de bevoegde autoriteit voor de entiteiten die domeinnaamregistratiediensten verlenen.

De Cbw biedt de mogelijkheid om instellingen voor hoger onderwijs als essentiële entiteit (artikel 11) of als belangrijke entiteit (artikel 13) onder de reikwijdte van de wet te brengen. In artikel 15, derde lid, Cbw wordt daarom de Minister van Onderwijs, Cultuur en Wetenschap aangewezen als de bevoegde autoriteit voor die instellingen.

In artikel 15, vierde lid, Cbw is geregeld dat voor de sector onderzoek de bevoegde autoriteit de minister is die reeds is aangewezen als bevoegde autoriteit voor de sector of subsector waarin die onderzoeksorganisatie haar onderzoeksactiviteiten verricht. Voor bijvoorbeeld een onderzoeksorganisatie die onderzoek doet in de sector levensmiddelen is de Minister van Landbouw, Visserij, Voedselzekerheid en Natuur de bevoegde autoriteit en voor een onderzoeksorganisatie die onderzoek doet naar ruimtevaart de Minister van Economische Zaken. Voor onderzoeksorganisaties die onderzoek doen in een sector waarvoor op grond van de Cbw nog geen bevoegde autoriteit is aangewezen, is de bevoegde autoriteit de minister die het aangaat. Dat betekent bijvoorbeeld dat voor een onderzoeksorganisatie die onderzoek doet op onderwerpen die onder de beleidsverantwoordelijkheid van het Ministerie van Defensie vallen, de Minister van Defensie de bevoegde autoriteit is.

Met artikel 15, vijfde lid, Cbw wordt bewerkstelligd dat ten aanzien van een entiteit die op grond van artikel 6 Wwke is aangewezen als kritieke entiteit en niet behoort tot een in de bijlage van de Wwke genoemde sectoren, dezelfde instantie de bevoegde autoriteit is.

In artikel 15, zesde lid, Cbw is geregeld welke taken de bevoegde autoriteit heeft.

Artikel 16 (aanwijzing en taken CSIRT)

Aanwijzing CSIRT van alle essentiële entiteiten en belangrijke entiteiten
Artikel 16, eerste lid, Cbw betreft de implementatie van artikel 10, eerste lid, NIS2-richtlijn. In artikel 16, eerste lid, Cbw is geregeld dat bij of krachtens amvb het CSIRT wordt aangewezen voor alle essentiële entiteiten en belangrijke entiteiten. Deze bepaling ziet op de aanwijzing van het CSIRT voor alle essentiële entiteiten en belangrijke entiteiten, dus ook de entiteiten die op grond van artikel 10 Cbw zijn aangewezen als essentiële entiteit, de instellingen voor hoger onderwijs die op grond van de artikelen 11 of 13 Cbw zijn aangewezen als essentiële entiteit respectievelijk belangrijke entiteit en de kritieke entiteiten als bedoeld in artikel 6, eerste lid, Wwke. De laatstgenoemde entiteiten zijn op grond van artikel 8, eerste lid, onderdeel i, Cbw van rechtswege ook essentiële entiteit. Voor alle hiervoor genoemde entiteiten moet dus het CSIRT worden aangewezen.
De aanwijzing van een CSIRT kan geschieden voor een hele sector of subsector, voor alle entiteiten die binnen een soort entiteit of categorie van entiteiten vallen en voor specifieke essentiële entiteiten en belangrijke entiteiten.

Delegatiegrondslag
Artikel 16, tweede lid, Cbw betreft een delegatiegrondslag om bij ministeriële regeling regels te stellen over bepaalde vereisten van de organisatie die wordt belast met de uitvoering van de CSIRT-taken. De organisaties die daar naar verwachting mee worden belast, verschillen namelijk op het gebied van eigenaarschap, aansturing en financiering. Tegelijkertijd veronderstelt de Cbw een gelijk niveau van dienstverlening tussen de CSIRT's en dient elk CSIRT de taken uit de Cbw te kunnen uitvoeren. Om dit mogelijk te maken kan het nodig zijn om regels te stellen over onder andere de wijze van informeren aan de vakminister, het aanstellingsbeleid, verantwoording en inzicht in de kostenontwikkeling.

De taken van het CSIRT
In de overige leden van artikel 16 Cbw zijn de taken van het CSIRT opgenomen. Dit betreft de implementatie van artikel 11, derde, vierde en vijfde lid, NIS2-richtlijn en het voortzetten van

bestaand beleid uit de Wbni ten aanzien van de samenwerking in brede zin met de Minister van Economische Zaken uit hoofde van de Wbdwb.
Hierbij wordt opgemerkt dat in artikel 16, derde lid, onderdeel b, Cbw de in artikel 11, derde lid, onderdeel b, NIS2-richtlijn gebruikte terminologie "relevante belanghebbenden" niet is overgenomen. Het betreft in dit verband immers niet de belanghebbenden in de zin van artikel 1:2 Awb. Om die reden is in artikel 16, derde lid, onderdeel b, Cbw gekozen voor de terminologie "andere relevante partijen".

Relevante partijen
Het CSIRT kan, ter uitvoering van zijn taken, informatie delen met relevante partijen. Partijen kunnen relevant zijn omdat de informatie die het CSIRT heeft relevant is voor hun cyberweerbaarheid of die van 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. Uiteraard mag dit niet verhinderen dat partijen die geraakt zijn, geïnformeerd mogen worden. 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).

Minister van Economische Zaken
Met de Cbw wordt de Wbni ingetrokken. Daarom dient het in de Wbni bepaalde met betrekking tot de informatieverstrekking vanuit CSIRT's aan de Minister van Economische Zaken ter uitvoering van de taken en bevoegdheden die de Wbdwb aan hem toekent, in de Cbw beleidsneutraal te worden omgezet. Hiertoe wordt de Minister van Economische Zaken in artikel 16, derde lid, onderdeel b, Cbw genoemd als een partij waarvoor een CSIRT tot taak heeft om informatie aan te verstrekken en een samenwerkingsrelatie mee tot stand te brengen (artikel 16, zesde lid, Cbw). In het kader van de uitoefening van deze taken kunnen de CSIRT's relevante gegevens, waaronder persoonsgegevens, met de Minister van Economische Zaken delen.

Schakelorganisaties
Een aantal organisaties is op grond van de Wbni aangewezen als een organisatie die objectief kenbaar tot taak (OKTT) heeft om andere organisaties of het publiek te informeren over dreigingen en incidenten met betrekking tot andere netwerk- en informatiesystemen[78] of CSIRT.[79] Met het intrekken van de Wbni komen die aanwijzingen te vervallen. Wat deze organisaties met elkaar gemeen hebben, is dat zij ten behoeve van een achterban informatie verspreiden, welke zij ontvangen van het NCSC. Deze organisaties, die fungeren als schakelorganisatie voor een achterban van aanbieders, kunnen onder het regime van de Cbw onder omstandigheden worden gekwalificeerd als een relevante partij als bedoeld in artikel 16, derde 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 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.

[78] Het gaat om de Stichting Nationale Beheersorganisatie Internet Providers, de Stichting Cyber Weerbaarheidscentrum Brainport, de Vereniging Cyberveilig Nederland, de Stichting Connect2Trust, de Stichting FERM en de Stichting NL CISO Circle of Trust.
[79] SURFcert is hier een voorbeeld van.

Nederlandse inlichtingen- en veiligheidsdiensten
De Nederlandse inlichtingen- en veiligheidsdiensten hebben op grond van de artikelen 8, tweede lid, onderdeel a tot en met f, en 10, tweede lid, onderdeel a tot en met g, Wet op de inlichtingen- en veiligheidsdiensten 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 essentiële entiteit of belangrijke 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.

Artikel 17 (aanwijzing en taken coördinator bekendmaking kwetsbaarheden)

In artikel 12, eerste lid, NIS2-richtlijn is bepaald dat elke lidstaat één van zijn CSIRT's aanwijst als coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden. In artikel 17, eerste lid, Cbw is geregeld dat in Nederland die coördinator bij amvb wordt aangewezen. In artikel 17, tweede lid, Cbw zijn, ter implementatie van artikel 12 NIS2-richtlijn, de taken van die coördinator opgenomen.

Artikel 18 (aanwijzing en taken cybercrisisbeheerautoriteit)

In artikel 18 Cbw wordt de Minister van Justitie en Veiligheid aangewezen als de cybercrisisbeheerautoriteit, bedoeld in artikel 9, eerste lid, NIS2-richtlijn. Deze rol wordt feitelijk vervuld door onderdelen die werken onder de verantwoordelijkheid van de Minister van Justitie en Veiligheid, te weten de NCTV en het NCSC. Beide organisatieonderdelen hebben een rol bij een grootschalige cybercrisis, zoals vastgelegd in het Landelijk Crisisplan Digitaal.[80] Het beleggen van de taken en verantwoordelijkheid rondom het beheer van grootschalige cyberbeveiligingsincidenten en crises bij de Minister van Justitie en Veiligheid in de Cbw, 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 19 (nationale cyberbeveiligingsstrategie)

Artikel 19 Cbw 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 20 (nationaal plan voor grootschalige cyberbeveiligingsincidenten en crisisrespons)

Artikel 20 Cbw strekt tot de implementatie van artikel 9, vierde lid, NIS2-richtlijn. In Nederland bestaat al een dergelijk plan, namelijk het Landelijk Crisisplan Digitaal.

Artikel 21 (zorgplicht)

Artikel 21 Cbw ziet op de zorgplicht en betreft de implementatie van artikel 21 NIS2-richtlijn. Paragraaf 5.2 gaat uitgebreid in op de zorgplicht.

Beveiliging van de toeleveringsketen
Artikel 21, eerste lid, Cbw bepaalt dat essentiële entiteiten en belangrijke entiteiten passende en evenredige technische, operationele en organisatorische maatregelen moeten nemen om de risico's voor de beveiliging van hun netwerk- en informatiesystemen, die zij voor hun werkzaamheden of voor

[80] *Kamerstukken II* 2022/23, 26643, nr. 955.

het verlenen van hun diensten gebruiken, te beheersen. Ook nemen zij deze maatregelen om incidenten te voorkomen of de gevolgen van incidenten voor de afnemers van hun diensten en voor andere diensten te beperken. Artikel 21, derde lid, Cbw bevat een opsomming van waar de maatregelen ten minste uit moeten bestaan. Eén van de in die opsomming genoemde aspecten is de beveiliging van de toeleveringsketen (artikel 21, derde lid, onderdeel d, Cbw). Hierover wordt in artikel 21, tweede lid, onderdeel d, en derde lid, NIS2-richtlijn aangegeven dat dit met inbegrip is van beveiligingsgerelateerde 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 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. Producten met digitale elementen die vanaf medio 2027 in de EU op de markt worden gebracht, moeten op grond van de Verordening cyberweerbaarheid (*Cyber Resilience Act*) aan de daarin gestelde cybersecurity-eisen voldoen (en draadloos verbonden apparaten vanaf augustus 2025 op grond van de gedelegeerde handeling onder de zogeheten Radioapparatenrichtlijn). Deze eisen gelden voor fabrikanten, importeurs en distributeurs van de volgende producten: hardware, software én los aangeboden componenten voor deze producten. Deze eisen zullen behulpzaam zijn bij de beveiliging van de toeleveringsketen van essentiële entiteiten en belangrijke entiteiten. Bij de aankoop van producten kunnen afnemers, waaronder deze entiteiten, hogere eisen stellen dan waartoe de Verordening cyberweerbaarheid de fabrikant verplicht.

Lagere regelgeving
De hiervoor genoemde maatregelen worden geconcretiseerd in een amvb. Artikel 21, vijfde lid, Cbw biedt hiervoor de grondslag. Die amvb zal daarnaast een delegatiegrondslag bevatten om bij ministeriële regeling van de minister die het aangaat, indien nodig, sectorspecifieke regels te stellen over de maatregelen.
Deze delegatiegrondslag in artikel 21, vijfde lid, Cbw biedt ook de mogelijkheid om aan essentiële entiteiten en belangrijke entiteiten op te leggen dat zij bepaalde ICT-producten, ICT-diensten en ICT-processen moeten gebruiken die zijn gecertificeerd op grond van artikel 49 van de zogeheten cyberbeveiligingsverordening[81]. Dit ter implementatie van artikel 24, eerste lid, NIS2-richtlijn. Op grond van artikel 24, tweede lid, NIS2-richtlijn heeft de Europese Commissie een vergelijkbare bevoegdheid. Zij kan via gedelegeerde handelingen aan essentiële entiteiten en belangrijke entiteiten opleggen dat zij gebruik moeten maken van bepaalde ICT-producten, ICT-diensten en ICT-processen of een certificaat moeten verkrijgen die ook op grond van artikel 49 cyberbeveiligingsverordening is vastgesteld.
Mocht de wens bestaan om aan entiteiten uit een bepaalde sector verplichte certificering op te leggen, dan zal moeten worden beoordeeld of dit beter op nationaal niveau (via de delegatiegrondslag van artikel 21, vijfde lid, Cbw) of via de gedelegeerde handelingen van de Europese Commissie (bedoeld in artikel 24, tweede lid, NIS2-richtlijn) kan worden geregeld. Een belangrijke overweging om het op Europees niveau te regelen kan zijn: het creëren van een gelijk speelveld voor sectoren die internationaal georiënteerd zijn. Mocht dit laatste het geval zijn, dan kan Nederland hiervoor internationaal pleiten, maar in hoeverre dit kan worden gerealiseerd hangt ook af van de wens van de Europese Commissie en andere lidstaten om gebruik te maken van dit certificeringsinstrument op Europees niveau. Voor de 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 cyberbeveiligingsverordening verplicht te stellen moet worden beoordeeld of het schema geschikt is om de (vermoedelijke) conformiteit met bepaalde eisen van de zorgplicht uit de Cbw aan te tonen. Tot slot, indien er wordt gekozen voor verplichte certificering zal onder andere rekening moeten worden houden met de gevolgen die de maatregelen hebben voor de fabrikanten of

[81] Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening) (*PbEU* 2019, L 151).

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. Dit wordt in beoordeeld aan de hand van een regeldruktoets.
Bij het in lagere regelgeving stellen van regels over de maatregelen zal zoveel als mogelijk rekening worden gehouden met bestaande normenkaders. Datzelfde geldt ook voor de door Enisa krachtens artikel 25 NIS2-richtlijn op te stellen richtsnoeren over technische gebieden die in het kader van de zorgplicht in acht moeten worden genomen én over de daarover reeds bestaande nationale en internationale normen. Met dat laatste wordt ook bevorderd dat partijen die Europees opereren zoveel als mogelijk te maken krijgen met een eenduidige invulling van de zorgplicht binnen de diverse lidstaten.

Artikel 22 (sectorspecifieke rechtshandelingen zorgplicht)

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, waaronder die over het toezicht en de handhaving, dan niet van toepassing zijn op die entiteiten. Zo wordt voorkomen dat entiteiten aan verschillende wettelijke kaders moeten voldoen die (minimaal) hetzelfde niveau van cyberbeveiliging regelen. Artikel 4 NIS2-richtlijn is geïmplementeerd in de artikelen 22 en 31 Cbw.

Hierbij gaat het meer concreet om de zorgplicht en de meldplicht uit de Cbw, die dan niet van toepassing zijn op de betrokken entiteiten. Als de zorgplicht niet van toepassing is op een entiteit, zijn ook de verplichtingen over de governance (artikel 24 Cbw) niet van toepassing op die entiteit. Dit is geregeld in artikel 24, dertiende lid, Cbw. Die verplichtingen op het gebied van de governance zijn immers bedoeld ten behoeve van het voldoen aan de zorgplicht.

Het voorgaande ziet alleen op sectorspecifieke rechtshandelingen waardoor de zorgplicht, de meldplicht en de verplichtingen over de governance niet meer van toepassing zijn op entiteiten. De andere bepalingen uit de Cbw blijven van toepassing op die entiteiten.

Artikel 23 (ontheffing zorgplicht)

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.

Artikel 2, achtste lid, 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 te ontheffen van bepaalde verplichtingen, waaronder de zorgplicht. Deze activiteiten vallen namelijk binnen de uitsluitende verantwoordelijkheid van lidstaten en verantwoorden daarmee om ook deze entiteiten te ontheffen van bepaalde verplichtingen.

Artikel 23 Cbw strekt tot de implementatie van artikel 2, achtste lid, NIS2-richtlijn, specifiek ten aanzien van de zorgplicht. De bevoegdheid om de hiervoor bedoelde entiteiten te ontheffen van de zorgplicht wordt belegd bij de vakminister. De vakminister kan overgaan tot het verlenen van een ontheffing in overeenstemming met de Minister van Justitie en Veiligheid.

Artikel 24 (governance)

Artikel 24 Cbw strekt tot de implementatie van artikel 20 NIS2-richtlijn en gaat over governance. Zie paragraaf 5.3 voor een nadere toelichting.

In de Nederlandse vertaling van de NIS2-richtlijn wordt gesproken over de "bestuursorganen" van essentiële entiteiten en belangrijke entiteiten. Uit de overwegingen van de NIS2-richtlijn en ook uit enkele andere vertalingen blijkt evenwel dat daarmee geen "bestuursorgaan" in de zin van het nationale (bestuurs)recht wordt bedoeld, maar het bestuur van een organisatie.[82]

Wat vervolgens onder het bestuur van een organisatie moet worden verstaan, valt echter niet af te leiden uit de NIS2-richtlijn. Een nadere uitleg van "bestuur van een organisatie" wordt wel gegeven in de Verordening digitale operationele weerbaarheid. De reden dat in dit kader naar deze Verordening wordt gekeken, is omdat zowel de Engelse versie van die verordening als de Engelse versie van de NIS2-richtlijn de term "management bodies" bevat en het in de rede ligt dat wat hieronder wordt verstaan in beide EU-wetgeving niet wezenlijk van elkaar verschilt. Zowel de Verordening digitale operationele weerbaarheid als de NIS2-richtlijn dienen immers ter verhoging van de digitale weerbaarheid. Bovendien is de Verordening digitale operationele weerbaarheid een lex specialis ten opzichte van de NIS2-richtlijn.

In de Verordening digitale operationele weerbaarheid is de term "management bodies" vertaald naar "leidinggevende organen" (en dus niet als "bestuursorganen") en bovendien (anders dan het geval in de NIS2-richtlijn) wél gedefinieerd. Uit artikel 3, onderdeel 30, Verordening digitale operationele weerbaarheid volgt (onder verwijzing naar Richtlijn 2014/65) dat onder leidinggevend orgaan wordt verstaan:
het (de) overeenkomstig het nationale recht aangewezen orgaan (organen) van een beleggingsonderneming, marktexploitant of dienstverlener op het gebied van datarapportage, dat (die) gemachtigd is (zijn) de strategie, doelstellingen en algemene leiding van de entiteit vast te stellen, en fungeert (fungeren) als toezichthouder op en bewaker van de besluitvorming van het management. Het leidinggevend orgaan omvat personen die daadwerkelijk het beleid van de entiteit bepalen.
Wanneer in deze richtlijn verwezen wordt naar het leidinggevend orgaan en de leidinggevende functie en de toezichthoudende functie van het leidinggevend orgaan krachtens nationaal recht worden toegewezen aan verschillende organen of aan verschillende leden binnen één orgaan, wijst de lidstaat de verantwoordelijke organen of de verantwoordelijke leden van het leidinggevend orgaan aan in overeenstemming met diens nationale recht, tenzij in deze richtlijn anders is bepaald;

Hieruit wordt afgeleid dat onder "management body":
- het dagelijks bestuur wordt verstaan en niet een toezichthoudend orgaan (in een zogenoemd two-tier bestuursmodel); en
- uitvoerende bestuurders van een bestuur worden verstaan en niet de niet-uitvoerende bestuurders van het bestuur (in een zogenoemd one-tier bestuursmodel).

Het bestuur is bij rechtspersonen de gebruikelijke term in het Nederlandse recht, op basis van Boek 2 van het BW. Aan het bestuur is opgedragen de rechtspersoon te besturen, zoals in de artikelen 2:129 (voor de naamloze vennootschap) en 2:239 (voor de besloten vennootschap) BW is opgenomen. Het toezichthoudende orgaan is de raad van commissarissen (zie de artikelen 2:140 en 2:250 BW).

Gelet op de definitie van "management bodies" in de Verordening digitale operationele weerbaarheid en het daarin gemaakte onderscheid tussen het dagelijks bestuur enerzijds en een toezichthoudend orgaan anderzijds, en gelet op de in Nederland gangbare terminologie, is artikel 20 NIS2-richtlijn zodanig in artikel 24 Cbw geïmplementeerd dat de hierin opgenomen verplichtingen rusten op het bestuur van een entiteit.

De maatregelen die een entiteit voornemens is te nemen in het kader van de zorgplicht, moeten door het bestuur daarvan worden goedgekeurd (artikel 24, eerste lid, Cbw). Het gaat in dit verband om het

[82] 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".

ter goedkeuring voorleggen aan de leden van het bestuur gezamenlijk. De normadressaat van artikel 24, eerste lid, Cbw is de essentiële entiteit of belangrijke entiteit in kwestie.

Daarnaast is het aan alle individuele bestuursleden om te voldoen aan de opleidingsverplichting, bedoeld in artikel 24, tweede tot en met zesde lid, Cbw, omdat het bestuur als geheel verantwoordelijk is voor genomen beslissingen, waaronder de te treffen cyberbeveiligingsmaatregelen.

In het geval dat een essentiële entiteit of belangrijke entiteit zowel een bestuur als een raad van commissarissen kent, rusten de verplichtingen van artikel 24 Cbw niet op laatstgenoemd orgaan. Tevens geldt dat essentiële entiteiten en belangrijke entiteiten die een naamloze vennootschap of besloten vennootschap zijn en statutair hebben bepaald dat bepaalde bestuurstaken worden verdeeld over één of meer niet-uitvoerende bestuurders en één of meer uitvoerende bestuurders, de verplichtingen van artikel 24 Cbw enkel rusten op de uitvoerende bestuursleden (zie artikel 24, achtste lid, Cbw).

Bij maatschappen, vennootschappen onder firma (vof) en commanditaire vennootschappen (cv) bestaat er geen bestuur als orgaan. Daarom berust in het geval dat een essentiële entiteit of belangrijke entiteit een maatschap of een vof is, de verplichting tot het goedkeuren van de cyberbeveiligingsmaatregelen (artikel 24, eerste lid, Cbw) op alle individuele maten van de maatschap dan wel op alle individuele vennoten van de vof. Dit geldt ook voor de opleidingsverplichting in artikel 24, tweede tot en met zesde lid, Cbw.

In het geval dat een essentiële entiteit of belangrijke entiteit een cv is, rust de verplichting tot het goedkeuren van de cyberbeveiligingsmaatregelen (artikel 24, eerste lid, Cbw) enkel op de beherende vennoten en niet op de stille vennoten. Dit geldt ook voor de opleidingsverplichting (artikel 24, tweede tot en met zesde lid, Cbw). Nu stille vennoten niet meebeslissen en ook niet aansprakelijk zijn voor beslissingen van de vennootschap zouden de verplichtingen van artikel 24 Cbw het geldend recht doorkruisen als deze op stille vennoten zouden rusten. Dat is niet wenselijk.

Paragraaf 5.3 gaat in op de verplichtingen uit artikel 24 Cbw voor overheidsinstanties.

De artikelen 25 tot en met 29 (meldplicht significante incidenten en de fasen van de melding)

In de artikelen 25 tot en met 29 Cbw is artikel 23, eerste, derde en vierde lid, NIS2-richtlijn geïmplementeerd. Artikel 25 Cbw ziet op de meldplicht voor essentiële entiteiten en belangrijke entiteiten van significante incidenten. De artikelen 26 tot en met 29 zien op de verschillende fasen van de melding. Paragraaf 5.4 gaat ook in op de meldplicht.

Artikel 26 Cbw gaat over het geven van een vroegtijdige waarschuwing over een significant incident. In artikel 26, eerste lid, Cbw is bepaald dat entiteiten dat onverwijld moeten doen of, indien dat niet mogelijk is, binnen 24 uur nadat zij kennis hebben gekregen van dat incident. Dit betreffen klokuren. De passage "onverwijld of, indien dat niet mogelijk is, binnen 24 uur" wijkt af van de in artikel 23, vierde lid, onderdeel a, NIS2-richtlijn gebruikte bewoordingen van "onverwijld en in elk geval binnen 24 uur". Hiermee is echter geen inhoudelijke wijziging ten opzichte van het bepaalde in de NIS2-richtlijn beoogd. Er is gekozen voor een andere formulering in de Cbw, omdat een strikte lezing van de bewoordingen "onverwijld en in elk geval binnen 24 uur" uit de NIS2-richtlijn zou betekenen dat entiteiten tweemaal een vroegtijdige waarschuwing moeten geven. Dat is niet de bedoeling. Voor de duidelijkheid is daarom artikel 26, eerste lid, Cbw zodanig geformuleerd dat duidelijk is dat entiteiten éénmaal een vroegtijdige waarschuwing moeten geven. Dat doen zij onverwijld. Indien dat niet lukt, dan rust op hen de verplichting om in elk geval binnen 24 uur na de kennisname van het incident, een vroegtijdige waarschuwing te geven. Deze toelichting is ook van toepassing op artikel 26, eerste en tweede lid, Cbw, waarin eveneens de passage "onverwijld of, indien dat niet mogelijk is" voorkomen.

De meldplicht bestaat uit de volgende fasen:

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.

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.

Artikel 30 (informeren van ontvangers van diensten)

Artikel 30 Cbw strekt tot de implementatie van artikel 23, eerste en tweede lid, NIS2-richtlijn.

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.[83]

Artikel 31 (sectorspecifieke rechtshandelingen meldplicht)

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, waaronder die over het toezicht en de handhaving, dan niet van toepassing zijn op die entiteiten. Zo wordt voorkomen dat entiteiten aan verschillende wettelijke kaders moeten voldoen die (minimaal) hetzelfde niveau van cyberbeveiliging regelen. Artikel 4 NIS2-richtlijn is geïmplementeerd in de artikelen 22 en 31 Cbw.

Hierbij gaat het meer concreet om de zorgplicht, de verplichtingen over de governance en de meldplicht uit de Cbw, die dan niet van toepassing zijn op de betrokken entiteiten. De andere bepalingen uit de Cbw blijven van toepassing op die entiteiten.

Artikel 32 (ontheffing meldplicht)

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.

Artikel 2, achtste lid, 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 te ontheffen van bepaalde verplichtingen, waaronder de meldplicht. Deze activiteiten vallen namelijk binnen de uitsluitende verantwoordelijkheid van lidstaten en verantwoorden daarmee om ook deze entiteiten te ontheffen van bepaalde verplichtingen.

Artikel 32 Cbw strekt tot de implementatie van artikel 2, achtste lid, NIS2-richtlijn, specifiek ten aanzien van de meldplicht. De bevoegdheid om de hiervoor bedoelde entiteiten te ontheffen van de meldplicht wordt belegd bij de vakminister. De vakminister kan overgaan tot het verlenen van een ontheffing in overeenstemming met de Minister van Justitie en Veiligheid.

Artikel 33 (vrijwillige meldingen van significante incidenten, incidenten, bijna-incidenten en cyberdreigingen)

Artikel 33 Cbw 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.

Essentiële entiteiten en belangrijke entiteiten kunnen te maken hebben met incidenten (die niet worden gekwalificeerd als significant), bijna-incidenten en cyberdreigingen. Deze termen zijn gedefinieerd in artikel 1 Cbw. 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 25 Cbw. De Cbw regelt daarom dat essentiële entiteiten en belangrijke entiteiten op vrijwillige basis 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.

[83] Zie ook overweging 104 NIS2-richtlijn.

Ook entiteiten die geen essentiële entiteit of belangrijke entiteit zijn kunnen te maken hebben met significante incidenten, incidenten, bijna-incidenten en cyberdreigingen. Artikel 33, eerste lid, Cbw regelt 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. Iedereen wordt aangemoedigd om bijna-incidenten te melden, aangezien dit soort meldingen waardevolle informatie kunnen bevatten die gedeeld kan worden om bij andere organisaties incidenten te voorkomen. Het CSIRT kan daarnaast ook bijstand verlenen na een vrijwillige melding.

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.[84]

Artikel 34 (vrijwillige meldingen van kwetsbaarheden)

Artikel 34 Cbw 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 17 Cbw.

Artikel 35 (nadere regels over meldingen van significante incidenten)

De delegatiegrondslag in artikel 35 Cbw biedt de mogelijkheid om bij amvb nadere regels te stellen ter uitwerking van de artikelen 25 tot en met 30, 33 en 34. Deze delegatiegrondslag wordt besproken in paragraaf 5.4.

Artikel 36 (taken CSIRT na melding significant incident)

Artikel 36 Cbw 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 37 (openbaarmaking significant incident door CSIRT of bevoegde autoriteit)

Artikel 37 Cbw strekt tot de implementatie van artikel 23, zevende lid, NIS2-richtlijn en ziet op het informeren van het publiek over een significant incident.

Artikel 38 (inkennisstelling natuurlijke personen of rechtspersonen door entiteit)

Artikel 38 Cbw 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 39 (informatieverstrekking over gemelde significante incidenten, incidenten, bijna-incidenten en cyberdreigingen)

Artikel 39 Cbw 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.

[84] Zie ook artikel 30, tweede lid, en overweging 105 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 worden gedaan bij het CSIRT en de bevoegde autoriteit. De vrijwillige meldingen van incidenten, bijna-incidenten en cyberdreigingen als bedoeld in artikel 32, eerste lid, onderdeel a, Cbw moeten door essentiële entiteiten en belangrijke entiteiten worden gedaan bij het CSIRT. 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 25 en 33, eerste lid, onderdeel a, Cbw.

Dit artikel schrijft niet voor dat ook de toezichthoudende instantie (in de Cbw 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 40 (informatieverstrekking over gemelde significante incidenten, incidenten, bijna-incidenten en cyberdreigingen door essentiële entiteiten die tevens kritieke entiteiten zijn)

Artikel 40 Cbw 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.[85]

Artikel 41 (informatieverstrekking in verband met incidenten met betrekking tot financiële entiteiten)

Artikel 41 Cbw 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 42 (aanwijzing vertegenwoordiger)

Artikel 42 Cbw bevat de verplichting voor bepaalde entiteiten om een vertegenwoordiger aan te wijzen. Wat onder vertegenwoordiger wordt verstaan, is gedefinieerd in artikel 1 Cbw. Artikel 42 Cbw betreft de implementatie van artikel 26, derde lid, NIS2-richtlijn.

Artikel 43 (nationaal register van entiteiten)

[85] Overweging 30 NIS2-richtlijn.

Artikel 43 Cbw 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 de Cbw 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 44 Cbw is opgenomen welke informatie entiteiten moeten aanleveren bij de Minister van Justitie en Veiligheid ten behoeve van dat register.

Artikel 43, derde lid, Cbw bepaalt dat de Minister van Justitie en Veiligheid een registratie kan wijzigen, weigeren of beëindigen, als de grond voor registratie is gewijzigd, vervallen of ontbreekt. Een wijziging van een registratie is bijvoorbeeld denkbaar in het geval dat een entiteit in het nationale register is opgenomen als essentiële entiteit en inmiddels niet meer kwalificeert als essentiële entiteit, maar wel als belangrijke entiteit. Dit is een voorbeeld van een geval waarin de Minister van Justitie en Veiligheid de registratie wijzigt. Een weigering van een registratie is denkbaar in het geval dat een entiteit op grond van het bepaalde bij of krachtens de Cbw niet kwalificeert als essentiële entiteit, belangrijke entiteit of entiteit die domeinnaamregistratiediensten verleent. Een beëindiging van een registratie is denkbaar in het geval dat een entiteit in het register is opgenomen als essentiële entiteit, belangrijke entiteit of entiteit die domeinnaamregistratiediensten verleent, maar op een gegeven moment niet meer als zodanig te kwalificeren is. Dit kan bijvoorbeeld het geval zijn bij een essentiële entiteit die bepaalde activiteiten niet meer verricht of bepaalde diensten niet meer verleent, waardoor deze entiteit op grond van de Cbw niet meer wordt aangemerkt als essentiële entiteit (noch als belangrijke entiteit en entiteit die domeinnaamregistratiediensten verleent).

Artikel 44 (informatieverstrekking ten behoeve van nationale register)

Artikel 44 Cbw 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 de Cbw 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 44, eerste lid, onderdeel c, Cbw 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 de Cbw. 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 de Cbw.

De delegatiegrondslag in artikel 44, eerste lid, onderdeel f, Cbw 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 44, vierde lid, Cbw 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 45 (ontheffing verplichting informatieverstrekking nationale register)

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.

Artikel 2, achtste lid, 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 te ontheffen van bepaalde verplichtingen, waaronder de verplichting om informatie te verstrekken ten behoeve van het nationale register. Deze activiteiten vallen namelijk binnen de uitsluitende verantwoordelijkheid van lidstaten en verantwoorden daarmee om ook deze entiteiten te ontheffen van bepaalde verplichtingen.

Artikel 45 Cbw strekt tot de implementatie van artikel 2, achtste lid, NIS2-richtlijn, specifiek ten aanzien van de verplichting om informatie te verstrekken ten behoeve van het nationale register. De bevoegdheid om de hiervoor bedoelde entiteiten te ontheffen van die verplichting wordt belegd bij de vakminister. De vakminister kan overgaan tot het verlenen van een ontheffing in overeenstemming met de Minister van Justitie en Veiligheid.

Artikel 46 (toegang tot nationale register)

Artikel 46 Cbw 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 47 (informatieverstrekking ten behoeve van register van Enisa)

Artikel 47 Cbw strekt tot de implementatie van artikel 27 NIS2-richtlijn. De in artikel 47, eerste lid, Cbw 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 48 (ontheffing verplichting informatieverstrekking register van Enisa)

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.

Artikel 2, achtste lid, 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 te ontheffen van bepaalde verplichtingen, waaronder de verplichting om informatie te verstrekken ten behoeve van het register van Enisa. Deze activiteiten vallen namelijk binnen de uitsluitende verantwoordelijkheid van lidstaten en verantwoorden daarmee om ook deze entiteiten te ontheffen van bepaalde verplichtingen.

Artikel 48 Cbw strekt tot de implementatie van artikel 2, achtste lid, NIS2-richtlijn, specifiek ten aanzien van de verplichting om informatie te verstrekken ten behoeve van het register van Enisa. De bevoegdheid om de hiervoor bedoelde entiteiten te ontheffen van die verplichting wordt belegd bij de vakminister. De vakminister kan overgaan tot het verlenen van een ontheffing in overeenstemming met de Minister van Justitie en Veiligheid.

Artikel 49 (database met domeinnaamregistratiegegevens)

Artikel 49 Cbw 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 worden in artikel 1 Cbw gedefinieerd.

Artikel 49, eerste lid, Cbw 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 DNS.

Artikel 49, tweede lid, Cbw schrijft voor welke gegevens de database moet bevatten. Dit betreffen 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 is onvoldoende om de gegevens te verstrekken van de aanbieder van de privacy- of proxy-registratiedienst die mogelijk bij het registratieproces van de domeinnaam is gebruikt. De registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen dienen de registratiegegevens van de uiteindelijke domeinnaamhouder te registeren.

Artikel 49, derde lid, Cbw bevat de verplichting voor registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen om het beleid en de procedures, waaronder verificatieprocedures, vast te stellen om ervoor te zorgen dat de database juiste en volledige informatie bevat. Dat beleid en die procedures zien op het verzamelen en bijhouden van nauwkeurige en volledige domeinnaamregistratiegegevens en het voorkomen en corrigeren van onjuiste registratiegegevens. De verificatieprocedures kunnen bijvoorbeeld betrekking hebben op controles vooraf die worden uitgevoerd bij de registratie, en controles achteraf die worden uitgevoerd na de registratie. Uit overweging 111 van de NIS2-richtlijn volgt dat in het kader van verificatie, de registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen onder meer ten minste één van de verificatie manieren moeten gebruiken om met de domeinnaamhouder contact op te nemen. 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 (artikel 50, derde lid, Cbw). Bij het vaststellen van het beleid en procedures houden de entiteiten zoveel mogelijk rekening met richtsnoeren en normen die in internationaal verband zijn ontwikkeld (overweging 111 van de NIS2-richtlijn).

Artikel 49, vierde lid, Cbw 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 NIS2-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.

Artikel 49, vijfde lid, Cbw regelt dat de registers voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten verlenen, samenwerken om te voorkomen dat domeinnaamregistratiegegevens tweemaal worden verzameld. Op deze wijze worden administratieve lasten voorkomen. Afspraken over deze samenwerking kunnen bijvoorbeeld gemaakt worden in de vorm van contractuele afspraken tussen het register voor topleveldomeinnamen en de entiteiten die domeinnaamregistratiediensten onder die topleveldomeinnaam verlenen.

Artikel 49, zesde lid, Cbw betreft de grondslag voor een ministeriële regeling van de Minister van Economische Zaken. Door middel van die grondslag kan hij nadere regels stellen over het bepaalde in artikel 49 Cbw die van administratieve of uitvoeringstechnische aard zijn.

Artikel 50 (verzoeken om toegang tot gegevens over registratie van domeinnamen)

Artikel 50 Cbw betreft de implementatie van artikel 28, vijfde lid, NIS2-richtlijn. Net als artikel 49 Cbw is artikel 50 Cbw alleen van toepassing op registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen.

Artikel 50, eerste lid, Cbw verplicht het register voor topleveldomeinnamen en de entiteit die domeinnaamregistratiediensten verleent op een rechtmatig en naar behoren gemotiveerd verzoek van een legitieme toegang vragende partij die daar om verzoekt, toegang te verlenen tot specifieke gegevens over de registratie van domeinnamen. 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 verzoeken en dat onderbouwt, heeft derhalve recht op die gegevens die voor de desbetreffende verzoeker nodig zijn voor de doeleinden van het toegangsverzoek. Het kan onder meer gaan om de bevoegde autoriteit, bedoeld in de Cbw, om autoriteiten die krachtens het Unie- of nationale recht bevoegd zijn voor het voorkomen, onderzoeken, opsporen of vervolgen van strafbare feiten, en om CSIRT's. Het verzoek moet vergezeld gaan van een motivering aan de hand waarvan kan worden beoordeeld of toegang tot de gegevens noodzakelijk is. De beschikbaarheid en tijdige toegankelijkheid van domeinnaamregistratiegegevens voor verzoekers, waaronder bevoegd autoriteiten en CSIRT's 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.

Artikel 50, tweede lid, Cbw schrijft voor dat het register voor topleveldomeinnamen en de entiteit die domeinnaamregistratiediensten verleent onverwijld doch uiterlijk binnen 72 uur moet reageren op het verzoek. Met een reactie wordt een inhoudelijke reactie (met bijvoorbeeld de desbetreffende gegevens of een uitleg wanneer de gegevens komen of dat het verzoek onvoldoende gemotiveerd is) bedoeld en geen uitsluitend procedurele reactie.

Artikel 50, derde lid, Cbw schrijft voor dat het register voor topleveldomeinnamen en de entiteit die domeinnaamregistratiediensten verleent, beleid en procedures moeten openbaren met betrekking tot de bekendmaking van gegevens.

Artikel 50, vierde lid, Cbw betreft de grondslag voor een ministeriële regeling van de Minister van Economische Zaken. Door middel van die grondslag kan hij nadere regels stellen over het bepaalde in artikel 50 Cbw die van administratieve of uitvoeringstechnische aard zijn.

Artikel 51 (samenwerking en informatie-uitwisseling tussen instanties)

Artikel 51 Cbw 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 AP, de bevoegde autoriteiten van de Wwke en rechtshandhavingsautoriteiten.

Artikel 52 (samenwerking en informatie-uitwisseling tussen CSIRT's)

Artikel 52 Cbw strekt tot de implementatie van artikel 10, vierde lid, NIS2-richtlijn.

Artikel 53 (informatie-uitwisseling met entiteiten en gemeenschappen van entiteiten)

Artikel 53 Cbw implementeert artikel 10, vierde lid, jo. artikel 29 NIS2-richtlijn. Dit artikel regelt dat CSIRT's relevante informatie uitwisselen met essentiële entiteiten, belangrijke entiteiten, entiteiten die domeinnaamregistratiediensten verlenen en gemeenschappen van entiteiten als bedoeld in artikel 29 van de NIS2-richtlijn. Met gemeenschappen van entiteiten wordt bedoeld: een groep van essentiële entiteiten en belangrijke entiteiten en, indien van toepassing, hun leveranciers of dienstverleners.

Artikel 54 (samenwerking en informatie-uitwisseling met derde landen)

Artikel 54 Cbw 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 54 Cbw 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 CSIRT 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 CSIRT's 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 de Cbw. 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 EU: een zogenaamde *command-and-control server*, veelgebruikt bij datadiefstal, 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 EU te delen, om te voorkomen dat partijen die zijn gevestigd buiten de EU, 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 EU.

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. Allereerst zal daarbij gekeken worden of er sprake is van een adequaatheidsbesluit. Mocht dit er niet zijn, dan zal gekeken worden naar standaardbepalingen en certificeringsmechanismen of bindende bedrijfsvoorschriften. In overige gevallen kan doorgifte plaatsvinden op basis van artikel 49 Avg. 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.

Artikel 54, tweede lid, Cbw 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 55 (samenwerking en informatie-uitwisseling tussen bevoegde autoriteiten van deze wet)

Artikel 55 Cbw strekt tot de implementatie van artikel 13, vijfde lid, NIS2-richtlijn. Paragraaf 5.6.7 gaat in op de samenwerking tussen de toezichthoudende instanties.

Artikel 56 (samenwerking en informatie-uitwisseling met bevoegde autoriteiten Wet weerbaarheid kritieke entiteiten)

Artikel 56 Cbw 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.[86]

Artikel 57 (samenwerking met bevoegde autoriteit Verordening (EU) 2022/2554)

Artikel 57 Cbw 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, Verordening betreffende digitale operationele weerbaarheid voor de financiële sector door de Europese toezichthoudende autoriteiten wordt opgesteld en geactualiseerd, gebruiken om dergelijke aanbieders ten behoeve van artikel 57, tweede lid, Cbw te identificeren.

Artikel 58 (samenwerking met toezichthoudende autoriteiten in het kader van inbreuken in verband met persoonsgegevens)

Artikel 58 Cbw strekt tot de implementatie van de artikelen 31, derde lid, en 35 NIS2-richtlijn.

Artikel 58, eerste lid, Cbw ziet op de samenwerking tussen de bevoegde autoriteit met de toezichthoudende autoriteiten uit hoofde van de Avg.

Artikel 58, tweede lid, Cbw 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 58, derde lid, Cbw strekt tot de implementatie van artikel 35, tweede lid, NIS2-richtlijn. Deze bepaling gaat over de gevallen waarin één gedraging zowel een inbreuk in verband met persoonsgegevens als bedoeld in artikel 4, onderdeel 12, Avg inhoudt, als een schending van een verplichting uit de Cbw. Als de AP of een andere bevoegde toezichthoudende autoriteit, bedoeld in de artikelen 55 en 56 Avg, in zulke gevallen al een bestuurlijke boete heeft opgelegd voor de inbreuk in verband met persoonsgegevens, dan mag de bevoegde autoriteit, bedoeld in de Cbw, voor diezelfde gedraging geen bestuurlijke boete opleggen op grond van de Cbw in verband met de schending van een verplichting uit de Cbw. Overigens, zoals ook is bepaald in artikel 35, tweede lid, NIS2-richtlijn, blijft de bevoegde autoriteit bevoegd om andere handhavingsmaatregelen dan een bestuurlijke boete (zoals een last onder dwangsom) op te leggen in geval van een schending van een verplichting uit de Cbw. Eenzelfde gedraging kan onder de Cbw en de Avg tot een verschil in ernst van de overtreding en bijhorende gevolgen voor individuen en maatschappij leiden. Het ligt daarom in de rede dat de AP en de toezichthouders onder de Cbw in overleg treden wanneer een in artikel 58, derde lid, bedoeld geval optreedt, alvorens een bestuurlijke boete wordt opgelegd, om zo ervoor te zorgen dat het opleggen van de boete door de een niet onevenredig afbreuk doet aan de mogelijkheid van de andere toezichthouder om doeltreffend, evenredig en afschrikkend te sanctioneren.[87]

Artikel 58, vierde lid, Cbw 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.

[86] Overweging 30 NIS2-richtlijn.
[87] Artikel 34 NIS2-richtlijn en artikel 83 Avg.

Artikel 59 (informatie-uitwisseling met andere bevoegde autoriteiten)

Artikel 59 Cbw strekt tot de implementatie van artikel 13, vijfde lid, NIS2-richtlijn.

Artikel 60 (samenwerking met en bijstandsverzoek van de bevoegde autoriteit van een andere lidstaat van de Europese Unie)

Artikel 60 Cbw 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. 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 60, eerste lid, Cbw genoemde entiteiten.

Verder schrijft de NIS2-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 met elkaar samenwerken om zo tot effectief toezicht te komen, ook over grenzen heen. Het bijstandsverzoek van een bevoegde autoriteit van een andere lidstaat kan zien op het verstrekken van informatie of op het nemen van toezichtsmaatregelen, met inbegrip van inspecties ter plaatse, toezicht elders of audits. Verder is in artikel 60 Cbw verduidelijkt dat de jurisdictieregeling van artikel 4 Cbw 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 60, tweede lid, Cbw 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 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 61 (bijstandsverzoek aan de bevoegde autoriteit van een andere lidstaat van de Europese Unie)

Artikel 61 Cbw 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.

Artikel 62 (informatie-uitwisseling tussen entiteiten)

Artikel 62, eerste lid, Cbw strekt tot de implementatie van artikel 29, eerste lid, NIS2-richtlijn en gaat over het op vrijwillige basis uitwisselen van relevante informatie over cyberbeveiliging door entiteiten. Het is in het kader van hun cyberweerbaarheid van belang dat zij in staat worden gesteld om van elkaar te leren en elkaar te helpen bij het voorkomen, detecteren en reageren op incidenten of om van incidenten te herstellen. In een aantal gevallen zullen entiteiten ook hun dienstverleners en leveranciers willen betrekken, aangezien deze partijen ook invloed kunnen hebben op de

cyberweerbaarheid van entiteiten. Artikel 62, tweede lid, Cbw, waarin artikel 29, tweede lid, NIS2-richtlijn is geïmplementeerd, regelt dat de hiervoor bedoelde informatie-uitwisseling kan plaatsvinden binnen gemeenschappen van entiteiten en, indien van toepassing, hun leveranciers en dienstverleners op basis van informatie-uitwisselingsregelingen op het gebied van cyberbeveiliging met betrekking tot de potentieel gevoelige aard van de uitgewisselde informatie. Artikel 62, derde lid, Cbw bevat een delegatiegrondslag om bij of krachtens amvb regels te stellen ter uitvoering van het bepaalde in artikel 29, derde lid, van de NIS2-richtlijn.

Artikel 29, vierde lid, NIS2-richtlijn is overigens geïmplementeerd in artikel 44, eerste lid, onderdeel e, Cbw.

Artikel 63 (verwerkingsverantwoordelijkheid)

Artikel 63 Cbw regelt de verwerkingsverantwoordelijkheid.

Artikel 64 (bijzondere categorieën van persoonsgegevens)

Dit artikel biedt de grondslag voor de verwerking van bijzondere categorieën van persoonsgegevens door het CSIRT en de bevoegde autoriteit. Voor een toelichting over dit onderwerp wordt verwezen naar paragraaf 6.5.

Artikel 65 (bewaring van gegevens)

Artikel 65, eerste lid, Cbw schrijft voor dat bij of krachtens amvb regels worden gesteld over de bewaring van persoonsgegevens die ter uitvoering van de Cbw worden verwerkt.

Artikel 65, tweede lid, Cbw bepaalt dat de bijzondere categorieën van persoonsgegevens die door het CSIRT en de bevoegde autoriteit worden verwerkt niet langer worden bewaard dan noodzakelijk is ter uitvoering van hun taken op grond van de Cbw, maar dat deze in elk geval uiterlijk binnen 60 maanden na de eerste verwerking worden verwijderd.

Artikel 66 (vertrouwelijke gegevens)

Artikel 66 Cbw gaat over de uitwisseling van vertrouwelijke gegevens en voorziet in de waarborgen voor die gegevensuitwisseling. Deze waarborgen vloeien voort uit artikel 2, dertiende lid, NIS2-richtlijn. In de praktijk zal het met name gaan om vertrouwelijke gegevens waarover het CSIRT beschikt bij de uitvoering van de taken in het kader van de meldplicht, waarover de coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden beschikt bij de taak van het optreden als tussenpersoon en waarover de toezichthouder beschikt bij haar taken ten aanzien van de meldplicht en het toezicht op de naleving van het bepaalde bij of krachtens de Cbw.

Onder vertrouwelijke gegevens worden in beginsel die gegevens verstaan die door entiteiten vertrouwelijk aan het CSIRT en de bevoegde autoriteit zijn verstrekt. Daaronder vallen in ieder geval bedrijfsgeheimen. Bij bedrijfsgeheimen kan worden 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).

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 entiteiten vertrouwelijk aan de overheid zijn meegedeeld. In artikel 5.1, eerste lid, onderdeel c, Wet open overheid (hierna: Woo) is bepaald dat het openbaar maken van deze gegevens ingevolge die wet achterwege moet blijven. In relatie tot de Cbw kan hierbij worden gedacht aan gegevens die door een entiteit in het kader van de meldplicht van de Cbw aan de overheid zijn verstrekt en daarbij zijn aangemerkt als vertrouwelijke bedrijfs- of fabricagegegevens. Overigens ligt het 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.

Deze bijzondere openbaarheidsregel geldt echter niet voor milieu-informatie. De Woo kent aparte regels voor milieu-informatie, omdat dit voortvloeit uit het Verdrag van Aarhus[88] en Richtlijn 2003/4/EG[89]. Voor de definitie van milieu-informatie wordt in de Woo verwezen naar artikel 19.1a Wet milieubeheer. Zo geldt dat als er sprake is van een zwaarwegend belang, waaronder het belang van het milieu valt, dan mag een bestuursorgaan informatie actief openbaar maken, ook al zijn één 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 5.1, 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 5.1, 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 67 (verstrekking van gegevens in relatie tot nationale veiligheid, openbare veiligheid en defensie)

In artikel 67 Cbw is artikel 2, elfde lid, NIS2-richtlijn geïmplementeerd. In artikel 67 Cbw is bepaald dat de Cbw geen betrekking heeft op de verstrekking van informatie 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). Gerubriceerde informatie zal dus niet worden uitgewisseld in het kader van de Cbw. Te denken valt bijvoorbeeld aan inlichtingenberichten.

Artikel 68 (toezichthouders)

Artikel 68 Cbw ziet op de aanwijzing van natuurlijke personen die zijn belast met het toezicht op de naleving van het bepaalde bij of krachtens de Cbw. Deze natuurlijke personen beschikken na de aanwijzing over de bevoegdheden uit titel 5.2 Awb en de toezichtsbevoegdheden in de Cbw.

Artikel 69 (controlefunctionaris)

Artikel 69 Cbw 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.

Algemeen

[88] Verdrag betreffende toegang tot informatie, inspraak bij besluitvorming en toegang tot de rechter inzake milieuaangelegenheden (*Trb*. 2001, 73).
[89] Richtlijn 2003/4/EG van het Europees Parlement en de Raad van 28 januari 2003 inzake de toegang van het publiek tot milieu-informatie en tot intrekking van Richtlijn 90/313/EEG van de Raad (*PbEU* 2003, L 41).

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 69 Cbw. 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 de Cbw 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 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 69, tweede lid, Cbw staan de taken van de controlefunctionaris omschreven.

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.

In de Cbw is ervoor gekozen om de kosten van een controlefunctionaris te laten dragen door de betrokken entiteit (zie artikel 69, derde lid, Cbw). Indien de toezichthouder bij een essentiële entiteit een controlefunctionaris aanwijst, bestaat er een sterk vermoeden dat die entiteit niet voldoet aan de zorgplicht en/of de meldplicht. Daarom is het redelijk om de kosten te laten dragen door die entiteit.

Artikel 69, vierde lid, Cbw 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, zoals professionele kwalificaties.

Artikel 70 (beveiligingsscan)

Artikel 70 Cbw 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.

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 70 en 81 Cbw.

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.

Artikel 71 (audit)

Artikel 71 Cbw gaat over de bevoegdheid van de toezichthoudende instantie om een essentiële entiteit te verplichten tot het uitvoeren van een audit. Artikel 71 Cbw implementeert artikel 32, tweede lid, onderdelen b, c en g, een na laatste en laatste alinea, en artikel 32, vierde lid, onderdeel f, NIS2-richtlijn.

De toezichthoudende instantie kan essentiële entiteiten en belangrijke entiteiten verplichten zich aan een audit 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 71 en 82 Cbw.

Bij een audit onderzoekt een onafhankelijke en gekwalificeerde deskundige de opzet en werking van de door de entiteit genomen beheers- of beveiligingsmaatregelen. 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.

In artikel 71, vierde lid, Cbw is bepaald dat de kosten van een audit worden gedragen door de betrokken entiteit. Dit betreft een implementatie van de NIS2-richtlijn. Van deze regel kan worden afgeweken als deze kosten naar het oordeel van de bevoegde autoriteit moeten worden gedragen door haarzelf.

Artikel 72 (openbaarmaking overtreding)

Artikel 72 Cbw strekt tot de implementatie van artikel 32, vierde lid, onderdeel h, NIS2-richtlijn en ziet op de bevoegdheid van de toezichthoudende instantie 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.

De toezichthoudende instantie kan essentiële entiteiten en belangrijke entiteiten verplichten om door de entiteit begane overtredingen van de Cbw (gedeeltelijk) openbaar te maken. Dit volgt uit de artikelen 72 en 83 Cbw, waarin de artikelen 32, vierde lid, onderdeel h, en 33, vierde lid, onderdeel g, NIS2-richtlijn.

Artikel 73 (aanwijzing)

Artikel 73 Cbw 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.

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 de Cbw. 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 73 en 84 Cbw.

De aanwijzing heeft 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.

Artikel 74 (last onder bestuursdwang)

Artikel 74 Cbw 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.

Op grond van de artikelen 74 en 85 Cbw 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.

De artikelen 75 tot en met 77 (einddatum beëindiging overtreding, verzoek tot schorsing certificering of vergunning en verzoek tot schorsing leden van het bestuur)

In de artikelen 75 tot en met 77 Cbw is artikel 32, vijfde lid, NIS2-richtlijn geïmplementeerd. De hierin opgenomen bevoegdheden van de toezichthoudende instantie zijn alleen van toepassing ten aanzien

van essentiële entiteiten. Voor een uitgebreide toelichting hierop wordt verwezen naar paragraaf 5.6.4.

Artikel 78 (uitzondering voor overheidsinstanties)

Artikel 78 Cbw strekt tot de implementatie van artikel 32, vijfde lid, laatste zin, NIS2-richtlijn.

Artikel 79 (bestuurlijke boete)

Artikel 79 Cbw 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 toezichthoudende instantie om een bestuurlijke boete op te leggen aan een essentiële entiteit. Voor een uitgebreide toelichting op deze bevoegdheid wordt verwezen naar paragraaf 5.6.5.

Artikel 80 (reikwijdte)

Artikel 80 Cbw strekt tot de implementatie van artikel 33, eerste lid, NIS2-richtlijn en maakt een belangrijk onderscheid tussen het toezicht op essentiële entiteiten en dat op belangrijke entiteiten. Paragraaf 5.6.2 gaat hier nader op in.

Artikel 81 (beveiligingsscan)

Artikel 81 Cbw strekt tot de implementatie van artikel 33, tweede lid, onderdeel c, NIS2-richtlijn en ziet op de bevoegdheid van de toezichthoudende instantie om een beveiligingsscan uit te voeren of uit te laten voeren bij een belangrijke entiteit. Voor een toelichting op dit instrument wordt verwezen naar de artikelsgewijze toelichting van artikel 70 Cbw.

Artikel 82 (audit)

Artikel 82 Cbw gaat over de bevoegdheid van de toezichthoudende instantie om een belangrijke entiteit te verplichten tot het uitvoeren van een audit. Artikel 82 Cbw implementeert artikel 33, tweede lid, onderdelen b en f, een na laatste en laatste alinea, en artikel 33, vierde lid, onderdeel f, NIS2-richtlijn.

De toezichthoudende instantie kan essentiële entiteiten en belangrijke entiteiten verplichten zich aan een audit 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 71 en 82 Cbw.

Bij een audit onderzoekt een onafhankelijke en gekwalificeerde deskundige de opzet en werking van de door de entiteit genomen beheers- of beveiligingsmaatregelen. 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.

In artikel 82, vierde lid, Cbw is bepaald dat de kosten van een audit worden gedragen door de betrokken entiteit. Dit betreft een implementatie van de NIS2-richtlijn. Van deze regel kan worden afgeweken als deze kosten naar het oordeel van de toezichthoudende instantie moeten worden gedragen door haarzelf.

Artikel 83 (openbaarmaking overtreding)

Artikel 83 Cbw strekt tot de implementatie van artikel 33, vierde lid, onderdeel g, NIS2-richtlijn en ziet op de bevoegdheid van de toezichthoudende instantie 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 84 (aanwijzing)

Artikel 84 Cbw ziet op de implementatie van artikel 33, vierde lid, onderdeel b, NIS2-richtlijn en ziet op de bevoegdheid van de toezichthoudende instantie tot het opleggen van een bindende aanwijzing aan een belangrijke entiteit. Voor een toelichting op deze bevoegdheid wordt verwezen naar de artikelsgewijze toelichting bij artikel 73 Cbw.

Artikel 85 (last onder bestuursdwang)

Artikel 85 Cbw 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 toezichthoudende instantie tot het opleggen van een last onder bestuursdwang aan een belangrijke entiteit. Voor een toelichting op deze bevoegdheid wordt verwezen naar de artikelsgewijze toelichting bij artikel 74 Cbw.

Artikel 86 (bestuurlijke boete)

Artikel 86 Cbw 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 toezichthoudende instantie om een bestuurlijke boete op te leggen aan een belangrijke entiteit. Paragraaf 5.6.5 gaat uitgebreid in op deze bevoegdheid.

Artikel 87 (reikwijdte)

Artikel 87 Cbw verduidelijkt dat de artikelen 88 tot en met 90 Cbw alleen van toepassing zijn op de entiteit die domeinnaamregistratiediensten verleent, die op grond van de Cbw niet tevens essentiële entiteit of belangrijke entiteit is. Indien een entiteit die domeinnaamregistratiediensten verleent ook op grond van de Cbw 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 88 tot en met 90 (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 5.6.2 gaat hier nader op in.

De artikelen 91 en 92 (last onder dwangsom en bestuurlijke boete)

De NIS2-richtlijn bevat geen specifieke bepalingen over het toezicht op de naleving van de verplichtingen die zijn geïmplementeerd in artikel 24, tweede tot en met zesde lid, Cbw, die van toepassing zijn op leden van het bestuur van essentiële entiteiten en belangrijke entiteiten. De NIS2-richtlijn bevat alleen 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 de leden van het bestuur van essentiële entiteiten en belangrijke entiteiten ten aanzien van de handhaving van de verplichtingen uit artikel 24, tweede tot en met zesde lid, Cbw is

gekozen voor de bevoegdheid van de toezichthoudende instantie tot het opleggen van een last onder dwangsom en bestuurlijke boete. Paragraaf 5.6.2 gaat hier nader op in.

Artikel 93 (evaluatiebepaling)

In artikel 93 Cbw is bepaald dat de doeltreffendheid en effectiviteit van de Cbw uiterlijk vijf jaar na de inwerkingtreding van de Cbw wordt geëvalueerd en vervolgens elke drie jaar. Uit artikel 40 NIS2-richtlijn volgt dat de Europese Commissie uiterlijk op 17 oktober 2027 en vervolgens om de 36 maanden de werking van de NIS2-richtlijn evalueert. Door te kiezen voor een termijn van vijf jaar en daarna voor termijnen van drie jaar, kan bij de evaluatie van de Cbw worden aangesloten bij de evaluatiecyclus van de Europese Commissie van de NIS2-richtlijn.

Artikel 94 (totstandkoming nationaal register)

Artikel 3 NIS2-richtlijn bepaalt dat lidstaten uiterlijk op 17 april 2025 een lijst opstellen van essentiële entiteiten, belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen. In de Cbw is dit geïmplementeerd als het nationale register. De hiervoor genoemde datum wordt echter niet behaald. Daarom is in artikel 94 Cbw opgenomen dat het nationale register uiterlijk één maand na de inwerkingtreding van artikel 43 Cbw tot stand komt.

Artikel 95 (besluiten en meldingen op grond van de Wet beveiliging netwerk- en informatiesystemen)

Artikel 95 Cbw voorziet in overgangsrecht. Dit is nodig, omdat de Cbw voorziet in het verval van de Wbni en er voor het moment van dat verval besluiten kunnen zijn genomen op grond van de Wbni of meldingen kunnen zijn gedaan op grond van artikel 10 of 13 Wbni. In artikel 95 Cbw wordt geregeld welk recht van toepassing is indien er voor het verval van de Wbni een besluit is genomen op grond van de Wbni of een melding is gedaan op grond van artikel 10 of 13 Wbni.

Artikel 95, eerste lid, Cbw ziet op besluiten die zijn genomen op grond van de Wbni. Te denken valt bijvoorbeeld aan een bestuurlijke boete vanwege de schending van de zorgplicht uit de Wbni. In artikel 95, eerste lid, Cbw is geregeld tot welk tijdstip het oude recht van toepassing blijft wanneer er voor het verval van de Wbni een besluit is genomen op grond van de Wbni.

Artikel 95, tweede lid, Cbw ziet op meldingen die zijn gedaan op grond van artikel 10 of 13 Wbni. Het is nodig om een regeling te treffen voor de entiteiten waarop na de inwerkingtreding van de Cbw de meldplicht uit de Cbw van toepassing is. Als een entiteit op grond van artikel 10 of 13 Wbni een melding heeft gedaan en artikel 25 Cbw van toepassing is op die entiteit, wordt de op grond van de Wbni gedane melding aangemerkt als een vroegtijdige waarschuwing als bedoeld in artikel 26 Cbw. De laatste volzin van artikel 95, tweede lid, Cbw ziet op de gevallen waarin de op grond van de Wbni gedane melding ziet op een inbreuk als bedoeld in artikel 10, eerste lid, onderdeel b, Wbni. In die gevallen is de melder op grond van artikel 10 Wbni namelijk alleen verplicht om een melding te doen bij de Minister van Justitie en Veiligheid (en niet ook bij de bevoegde autoriteit). Omdat de meldplicht uit de Cbw een dubbele meldplicht betreft bij zowel het CSIRT als de bevoegde autoriteit, wordt in de laatste volzin geregeld dat de Minister van Justitie en Veiligheid de melding van een hiervoor bedoelde inbreuk moet doorsturen aan de bevoegde autoriteit.

Artikel 96 (bijstand ten behoeve van andere entiteiten)

De Wbni zal worden ingetrokken (zie artikel 103 Cbw). Een aantal organisaties dat direct voorafgaand daaraan krachtens artikel 3, eerste lid, Wbni als vitale aanbieder of als andere aanbieder die onderdeel is van de rijksoverheid recht heeft op bijstand door, alsook op informatie en advies van, het NCSC in geval van dreigingen en incidenten, zal geen essentiële entiteit of belangrijke entiteit als bedoeld in de Cbw zijn en daarom buiten de toepasselijkheid van bijvoorbeeld artikel 16 Cbw vallen. Het gaat daarbij met name om organisaties waarop de Cbw krachtens artikel 5 Cbw niet van toepassing is of die zijn uitgezonderd van de definitie van overheidsinstantie in artikel 1 Cbw (bijvoorbeeld de rechterlijke macht). Zonder een aanvullende regeling zouden deze organisaties door de intrekking van

de Wbni hun vorenbedoelde recht op bijstand verliezen en dat is ongewenst. Het is in het belang van onder meer de nationale veiligheid dat bedoelde organisaties hun recht op bijstand behouden, zodat zij op basis daarvan maatregelen kunnen nemen ter voorkoming of beperking van incidenten en daarmee nadelige maatschappelijke gevolgen kunnen worden voorkomen of beperkt. In artikel 96 Cbw is daarom geregeld dat organisaties die direct voorafgaand aan de intrekking van de Wbni vitale aanbieder of tot de rijksoverheid behorende organisatie zijn als bedoeld in artikel 3, eerste lid, Wbni, zoals die wet luidde op de dag voorafgaand aan genoemde intrekking, en waarop de Cbw niet van toepassing is, recht blijven hebben op bijstand, informatie en advies in geval van dreigingen of incidenten met betrekking tot hun netwerk- of informatiesystemen. Die bijstand zal aan die organisaties worden verleend door het NCSC, zoals momenteel krachtens de Wbni het geval is, dan wel door een andere bij of krachtens amvb hiervoor aangewezen instantie.

Artikel 97 (wijzigingen van de NIS2-richtlijn)

Artikel 97 Cbw ziet op wijzigingen van bepalingen uit de NIS2-richtlijn waarnaar in de Cbw wordt verwezen.

Artikel 98 (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 zorgplicht en meldplicht was geregeld in de Richtlijn (EU) 2018/1972[90], ook wel Telecomcode genoemd, en is in Nederland geïmplementeerd in de Telecommunicatiewet (hierna: Tw).

In de NIS2-richtlijn zijn de maatregelen met betrekking tot de beveiliging van elektronische communicatienetwerken en -diensten onder de werking van de NIS2-richtlijn gebracht. De NIS2-richtlijn heeft grotendeels de maatregelen inzake de beveiliging van de telecomsector uit de Telecomcode, doordat de NIS2-richtlijn eveneens de artikelen 40 en 41 Telecomcode heeft geschrapt. Die artikelen gaan over de meldplicht, zorgplicht en het toezicht hierop. Bij de implementatie van de NIS2-richtlijn is bezien of als gevolg hiervan relevante bepalingen met betrekking tot de meldplicht, de zorgplicht en het toezicht uit de Tw moeten worden gewijzigd.

Allereerst kan de meldplicht in de Tw, opgenomen in artikel 11a.2 Tw, worden vervangen door de meldplicht zoals opgenomen in de Cbw. Artikel 11a.2 Tw kan dus komen te vervallen.

Voor wat betreft de zorgplicht in de Tw, opgenomen in artikel 11a.1, eerste lid, Tw, geldt dat deze niet gelijkluidend is aan de zorgplicht, bedoeld in artikel 21, eerste lid, NIS2-richtlijn en geïmplementeerd in artikel 22 Cbw. 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 de essentiële entiteit 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 Tw 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, 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

[90] Richtlijn (EU) 2018/1972 van het Europees Parlement en de Raad van 11 december 2018 tot vaststelling van het Europees wetboek voor elektronische communicatie (herschikking) (*PbEU* 2018, L 321).

openbare elektronische communicatiediensten kan weliswaar worden gesteld dat een hoger niveau van beveiliging van netwerk- en informatiesystemen tot een hoger beveiligingsniveau zou moeten leiden van de 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. Met uitzondering van de verwijzing naar de beveiliging van netwerken (die dus is geschrapt) behoudt artikel 11a.1, eerste lid, Tw de huidige formulering.

Nederland heeft de afgelopen jaren ook maatregelen genomen met betrekking tot de mobiele openbare elektronische communicatienetwerken, 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 en de Regeling veiligheid en integriteit telecommunicatie. In het Besluit veiligheid en integriteit telecommunicatie 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 veiligheid en integriteit telecommunicatie 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 regelt artikel 98 Cbw dat een delegatiegrondslag in de Tw wordt opgenomen. Dit is geregeld in het voorgestelde artikel 11a.1, tweede lid (nieuw), Tw.

Met onderdeel E van artikel 98 Cbw wordt het toezicht op de meldplicht in de Tw geschrapt aangezien de meldplicht alsmede het toezicht hierop volledig wordt geregeld in de Cbw.

Artikel 99 (wijziging Wet bevordering digitale weerbaarheid bedrijven)

De Wbdwb legt de taken en bevoegdheden van de Minister van Economische Zaken vast op het gebied van de verbetering van de digitale weerbaarheid van het niet-vitale bedrijfsleven in Nederland. De taken zijn onder meer: het verwerken en verspreiden van informatie over kwetsbaarheden, dreigingen en incidenten aan bedrijven en het samenwerken met andere bestuursorganen en organisaties op het gebied van digitale weerbaarheid. Tevens regelt die wet de rechtstreekse informatie-uitwisseling tussen het NCSC en het CSIRT voor digitale diensten. Ten slotte voorziet die wet in de voorwaarden waaronder vertrouwelijke gegevens die bij de Minister van Economische Zaken berusten, verstrekt mogen worden aan derden.

De Wbdwb moet vanwege de intrekking van de NIS1-richtlijn en de Wbni worden aangepast. Dat wordt in artikel 99 Cbw geregeld. Daarbij is het uitgangspunt dat het bestaand beleid beleidsneutraal wordt omgezet en dat de informatiepositie van de Minister van Economische Zaken die de Wbdwb aan hem toekent, wordt behouden.

Sommige definities die zijn opgenomen in de Wbdwb moeten als gevolg van het verval van de NIS1-richtlijn en de Wbni en de komst van de Cbw worden vervangen. Zo kan niet meer worden gesproken van vitale aanbieders of digitaledienstverleners als bedoeld in artikel 1 Wbni. Dat moet worden vervangen door een verwijzing naar essentiële entiteiten of belangrijke entiteiten in de zin van de Cbw. Als gevolg hiervan moeten er ook wijzigingen plaatsvinden in de begripsbepaling van de Wbdwb (artikel 1 Wbdwb). Dit wordt geregeld in onderdeel A. Deze wijzigingen, die dus nodig zijn vanwege het verval van de NIS1-richtlijn en de Wbni en de komst van de Cbw, leiden tot een wijziging van de doelgroep van de Wbdwb. Het principe blijft dat organisaties die als essentiële entiteiten of belangrijke entiteiten onder de werking van de Cbw vallen, geen doelgroep zijn onder de Wbdwb. Het doel van de Wbdwb is immers dat bedrijven die niet in aanmerking komen voor de informatievoorziening vanuit een CSIRT, door de Minister van Economische Zaken van de relevante informatie over kwetsbaarheden, dreigingen en incidenten kunnen worden voorzien.

De keuze om in het kader van de implementatie van de NIS2-richtlijn de CSIRT's niet meer bij wet aan te wijzen heeft tot gevolg dat de bepalingen inzake informatie-uitwisseling tussen de Minister van Economische Zaken op grond van de Wbdwb en de CSIRT's dienen te worden aangepast. Op basis van

de Wbni is de Minister van Justitie en Veiligheid het CSIRT voor aanbieders van essentiële diensten en de is de Minister van Economische Zaken het CSIRT voor digitale diensten. Deze aanwijzing komt te vervallen met de intrekking van de Wbni. Daarom regelen de onderdelen B en C dat de artikelen 2, tweede lid, en 4 Wbdwb zodanig worden aangepast, dat de informatie-uitwisseling tussen de Minister van Economische Zaken op grond van de Wbdwb en de CSIRT's mogelijk blijft.

Artikel 100 (wijziging Wet open overheid)

Voor wat betreft de uitzondering op de Woo, 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 Tw.

Artikel 101 (wijziging Wet op de economische delicten)

Ter implementatie van de NIS2-richtlijn wordt de Tw gewijzigd, zie de artikelsgewijze toelichting bij artikel 98 Cbw. Meer specifiek geldt dat artikel 11a.1, Tw, zodanig wordt gewijzigd dat de verwijzing naar artikel 11a.1, 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°, Wet op de economische delicten in de zinsnede met betrekking tot de Tw "11a.1, vijfde en zesde lid," geschrapt.

Artikel 102 (wijziging Algemene wet bestuursrecht)

Artikel 102 Cbw voorziet in een bijzondere bevoegdheidsregeling voor een aantal sectoren.

Voor de volgende sectoren wordt de rechtbank Rotterdam aangewezen als bevoegde rechtbank voor beroep in eerste instantie: energie, bankwezen, infrastructuur voor de financiële markt, gezondheidszorg, digitale infrastructuur, beheer van ICT-diensten (business-to-business), post- en koeriersdiensten en productie, verwerking en distributie van levensmiddelen. Dit geldt ook voor de subsectoren spoor en vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek.

Voor de volgende sectoren wordt het College van Beroep voor het bedrijfsleven aangewezen als hoger beroepsinstantie: energie, bankwezen, infrastructuur voor de financiële markt, digitale infrastructuur, beheer van ICT-diensten (business-to-business), post- en koeriersdiensten en productie, verwerking en distributie van levensmiddelen. Dit geldt ook voor de subsector spoor.

De reden voor deze bijzondere bevoegdheidsregeling is als volgt. Het is aannemelijk dat besluiten op grond van de Cbw in veel gevallen in samenhang met besluiten op grond van betrokken sectorale wet- en regelgeving zullen worden genomen. In die gevallen is het niet wenselijk dat voor besluiten op grond van sectorale wetten een bijzondere bestuursrechter bevoegd is, terwijl voor besluiten op grond van de Cbw de gewone bevoegdheidsregeling zou gelden. Voorts zal in het algemeen een goed oordeel over besluiten op grond van de Cbw niet gevormd kunnen worden zonder inzicht in de betrokken sector. Indien voor die sector een bijzondere bestuursrechter bevoegd is verklaard, zal die rechter inhoudelijke deskundigheid hebben opgebouwd ten aanzien van die sector. Het ligt dan voor de hand die rechter ook te laten oordelen over besluiten ten aanzien van die sector op grond van de Cbw.

Deze bijzondere bevoegdheidsregeling en de motivering daarvan sluit aan op de regeling die is getroffen voor de besluiten die op grond van de Wbni zijn genomen ten aanzien van de organisaties uit de betrokken (sub)sectoren. Voorts sluit deze bijzondere bevoegdheidsregeling aan op de regeling die is getroffen voor de besluiten die op grond van de Wwke zijn genomen ten aanzien van entiteiten uit de sectoren die ook voorkomen in de Cbw.

Artikel 103 (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 104 (inwerkingtreding)

Artikel 104 Cbw bepaalt dat de Cbw in werking treedt op een bij koninklijk besluit te bepalen tijdstip, dat voor de verschillende artikelen of onderdelen daarvan verschillend kan worden vastgesteld. Op grond van dit artikel kan worden gekozen voor een gefaseerde inwerkingtreding. Dit is denkbaar in het geval dat bepaalde onderdelen van de Cbw nog niet in werking kunnen treden, terwijl dat bij andere onderdelen van de Cbw wel het geval is. De verwachting is dat bij de inwerkingtreding van (onderdelen van) de Cbw een uitzondering wordt gemaakt op de vaste verandermomenten en de minimuminvoeringstermijn, omdat de Cbw ziet op de implementatie van een bindende EU-rechtshandeling.

Artikel 105 (citeertitel)

Dit artikel bevat de citeertitel van deze wet: Cyberbeveiligingswet.

Bijlagen

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

De Minister van Justitie en Veiligheid,