Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2025–2026

36 764 Regels ter implementatie van 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) (Cyberbeveiligingswet)

Nr. 12

AMENDEMENT VAN HET LID KATHMANN

Ontvangen 18 maart 2026

De ondergetekende stelt het volgende amendement voor:

I

Na het voorgestelde artikel 21 wordt een artikel ingevoegd, luidende:

Artikel 21a (weren producten en diensten van leveranciers)

1. Indien dat naar het oordeel van Onze Minister die het aangaat, ter uitwerking van artikel 21, noodzakelijk is om risico's voor de beveiliging van netwerk- en informatiesystemen die de nationale veiligheid raken te beheersen of om incidenten die de nationale veiligheid raken te voorkomen, legt hij in overeenstemming met Onze Minister een essentiële entiteit of een belangrijke entiteit de verplichting op om in de daarbij aangewezen onderdelen van haar netwerk- en informatiesystemen uitsluitend gebruik te maken van producten of diensten van anderen dan de daarbij door Onze Minister die het aangaat genoemde partij die:

a. een staat, entiteit of persoon is waarvan bekend is of waarvoor gronden zijn te vermoeden dat deze de intentie heeft om de beveiliging van de netwerk- en informatiesystemen van de essentiële entiteit of belangrijke entiteit aan te tasten of om incidenten bij de essentiële entiteit of belangrijke entiteit te veroorzaken; of

b. nauwe banden heeft met of onder invloed staat van een staat, entiteit of persoon als bedoeld in onderdeel a, of een entiteit of persoon is ten aanzien van wie er gronden zijn om dergelijke banden of invloed te vermoeden.

2. In het kader van de beoordeling van de noodzaak, bedoeld in het eerste lid, beoordeelt Onze Minister die het aangaat in elk geval of beheersmaatregelen mogelijk en realiseerbaar zijn die de nationale veiligheidsrisico's die in het geding zijn voldoende beschermen.

kst-36764-12
ISSN 0921 - 7371
's-Gravenhage 2026

3. Indien de verplichting, bedoeld in het eerste lid, betrekking heeft op reeds in gebruik zijnde producten en diensten ten behoeve van de daarbij aangewezen onderdelen, stelt Onze Minister die het aangaat in het belang van de continuïteit van de dienstverlening een termijn vast voor het vervangen respectievelijk beëindigen van de betreffende producten en diensten.

4. Onze Minister die het aangaat spant zich samen met de betrokken entiteit en het CSIRT van de betrokken entiteit in om de continuïteit van de dienstverlening, gedurende een door Onze Minister en het CSIRT vastgestelde termijn, van de essentiële entiteit of een belangrijke entiteit te borgen, indien de verplichting, bedoeld in het eerste lid, aan de entiteit is opgelegd.

5. Het eerste lid is niet van toepassing ten aanzien van essentiële entiteiten en belangrijke entiteiten die aanbieders van openbare elektronische communicatienetwerken of aanbieders van openbare elektronische communicatiediensten zijn.

II

In artikel 80, derde lid, onder a, wordt «de artikelen 21 en 25 tot en met 30» vervangen door «de artikelen 21, 21a en 25 tot en met 30».

III

In artikel 87, derde lid, onder a, wordt «de artikelen 21 en 25 tot en met 30» vervangen door «de artikelen 21, 21a en 25 tot en met 30».

Toelichting

Dit amendement brengt het voorgestelde artikel 18 van het concept van de algemene maatregel van bestuur (amvb) behorende bij dit wetsvoorstel (het Cyberbeveiligingsbesluit), welke de interventiebevoegdheid van de vakminister regelt om essentiële entiteiten en belangrijke entiteiten de verplichting op te leggen om diensten en producten van bepaalde leveranciers in aangewezen onderdelen van hun netwerk- en informatiesystemen te weren, onder in de voorgestelde Cyberbeveiligingswet als een nieuw artikel.

Daarnaast voegt dit amendement ook waarborgen toe ter bescherming van de essentiële entiteiten en belangrijke entiteiten die verplicht worden om diensten of producten te weren. Dit betreft een nieuw artikellid dat stelt dat eerst moet worden vastgesteld dat er geen technische, operationele en organisatorische maatregelen zijn die de risico's voor de beveiliging van netwerk- en informatiesystemen die de nationale veiligheid raken te beheersen of om incidenten die de nationale veiligheid raken te voorkomen. Ook voorziet dit amendement in een inspanningsverplichting voor de vakminister en het CSIRT (een Computer security incident response team, bedoeld in artikel 10 van de NIS2-richtlijn en bedoeld in artikel 16 van de voorgestelde Cyberbeveiligingswet) van de betrokken entiteit om de continuïteit van essentiële dienstverlening van de essentiële entiteit of belangrijke entiteit te waarborgen.

De indiener ziet meerwaarde in de interventiebevoegdheid voor de vakminister. Momenteel is deze voorzien in artikel 18 van het voorgestelde Cyberbeveiligingsbesluit, als een uitwerking van de zorgplicht die geregeld is in het voorgestelde artikel 21 van het wetsvoorstel voor de Cyberbeveiligingswet. Met toenemende internationale spanningen en de groeiende capaciteiten van statelijke actoren, is de bevoegdheid om vanwege de bescherming van de nationale veiligheid riskante diensten en producten te weren noodzakelijk. Echter stelt de indiener dat dit een

dusdanig verstrekkende bevoegdheid is dat deze op het niveau van de wet geregeld dient te worden in een losstaand artikel. Interventies van de betrokken vakminister worden dan gehouden aan dit nieuwe artikel van de wet, in plaats van lagere regelgeving.

Bovendien stelt de indiener aanvullende waarborgen voor om politieke willekeur te voorkomen. Het weren van bepaalde diensten en producten in onderdelen van netwerk- en informatiesystemen, omdat deze mogelijk gebruikt worden door (leveranciers actief in) landen met een offensief cyberprogramma jegens Nederland, heeft verstrekkende gevolgen voor essentiële entiteiten en belangrijke entiteiten die hierdoor worden getroffen. De indiener ziet voor zich dat deze bevoegdheid enkel wordt gebruikt als vaststaat dat er redelijkerwijs geen technische, operationele en organisatorische maatregelen mogelijk zijn die de risico's voor de nationale veiligheid kunnen voorkomen. Het opleggen van de verplichting om diensten en producten van specifieke leveranciers te weren wordt dan een «last resort»-maatregel.

Tot slot voorziet dit amendement in een inspanningsverplichting voor de betrokken vakminister en het CSIRT. Indien blijkt dat producten en/of diensten geweerd moeten worden om de nationale veiligheid te beschermen, dienen zij in overleg met de desbetreffende essentiële entiteit(en) en belangrijke entiteit(en) te bezien wat er nodig is om de continuïteit van hun dienstverlening voor te zetten. Zo wordt er naast een wettelijke bevoegdheid om diensten en producten te weren, ook voorzien in een uitgestoken hand richting deze entiteit(en), bijvoorbeeld door expertise te leveren voor het uitfaseren van diensten en/of producten of indien mogelijk een nadeelcompensatie te treffen. De indiener is van mening dat deze inspanning om de entiteit tegemoet te komen recht doet aan de zwaarte van de interventiebevoegdheid.

De indiener verwijst naar de brede coalitie van bedrijven en organisaties die hun zorgen hebben geuit over de interventiebevoegdheid in het voorgestelde artikel 18 van het Cyberbeveiligingsbesluit. Zij voorziet dat, om het draagvlak voor deze verstrekkende maar noodzakelijke bevoegdheid te behouden, de overheid zich bereid moet tonen om mét entiteiten samen te werken om het weren van diensten en producten op een ordentelijke wijze te laten verlopen. Een eenzijdige en niet wettelijk afgekaderde bevoegdheid stuit op weerstand en wijkt af van de geest van het wetsvoorstel voor de Cyberbeveiligingswet, waarin verplichtingen voor bedrijven en coöperatie vanuit de overheid juist in balans worden gebracht.

Hieronder volgt nadere toelichting over het amendement, gebaseerd op de conceptversie van het Cyberbeveiligingsbesluit die ter advisering is voorgelegd aan de Afdeling advisering van de Raad van State en geredigeerd:[1]

Inleidende opmerkingen voorstel

Nederland wordt steeds vaker geconfronteerd met cyberaanvallen op (al dan niet vitale) processen door statelijke en criminele actoren.[2] Naar verwachting zal de cyberdreiging de komende jaren aanhouden, omdat het relatief makkelijk is om een digitaal aanvalsprogramma op te zetten. Dergelijke aanvallen zijn ook steeds moeilijker herleidbaar tot de

[1] Het concept van het Cyberbeveiligingsbesluit ligt thans ter advies voor bij de Afdeling advisering van de Raad van State en is te raadplegen op https://wetgevingskalender.overheid.nl/regeling/WGK027199.
[2] Kamerstukken II 2022/23, 26 643, nr. 1007.

aanvaller. De inlichtingen- en veiligheidsdiensten identificeren in hun meest recente jaarverslagen een sterke toename van het aantal landen dat offensieve cyberprogramma's ontwikkelt en inzet bij het nastreven van hun politieke doelstellingen. In het licht van de hiervoor bedoelde ontwikkelingen, aanvallen en dreigingen voorziet het nieuw voorgestelde artikel 21a, eerste lid, van de Cyberbeveiligingswet (Cbw) in de bevoegdheid van de betrokken vakminister om, in overeenstemming met de Minister van Justitie en Veiligheid, een essentiële entiteit of belangrijke entiteit de verplichting op te leggen om in onderdelen van haar netwerk- en informatiesystemen producten of diensten van specifieke leveranciers te weren en zo de risico's, die voortvloeien uit de hiervoor bedoelde offensieve cyberprogramma's, te beheersen.

Het voorgestelde artikel 21a, eerste lid, Cbw is een uitwerking van algemene zorgplicht van artikel 21 Cbw. Essentiële entiteiten en belangrijke entiteiten zijn primair zelf verantwoordelijk voor het in het kader van deze zorgplicht treffen van ten minste de maatregelen ter beheersing van de risico's voor de beveiliging van hun netwerk- en informatiesystemen en ter voorkoming van incidenten, zoals opgesomd in artikel 21 Cbw en nader uitgewerkt in hoofdstuk 4 Cbb, waaronder maatregelen betreffende de beveiliging van de toeleverancierskketen. Het kan echter voorkomen dat de levering van producten en diensten aan een essentiële entiteit of belangrijke entiteit van een specifieke leverancier risico's met zich brengt voor de beveiliging van de netwerk- en informatiesystemen die de nationale veiligheid raken. Het kan met het oog daarop noodzakelijk zijn om ter bescherming van de nationale veiligheid vanuit de rijksoverheid de verplichting, bedoeld in het voorgestelde artikel 21a, eerste lid, Cbw, aan die entiteit op te leggen. Daarbij zal onder meer steeds worden beoordeeld of de ingrijpendheid van de maatregel in redelijke verhouding staat tot het ermee beoogde doel én of er geen minder ingrijpende maatregelen zijn om dat doel te bereiken.

Reikwijdte

De betrokken vakminister maakt gebruik van de in het voorgestelde artikel 21a, eerste lid, Cbw opgenomen bevoegdheid indien hij van oordeel is dat dit noodzakelijk is om risico's voor de beveiliging van de netwerk- en informatiesystemen die de nationale veiligheid raken te beheersen of om incidenten die de nationale veiligheid raken te voorkomen. Wat onder incident als bedoeld in het voorgestelde artikel 21a, eerste lid, Cbw wordt verstaan volgt uit artikel 1 Cbw. Hierin is bepaald dat een incident in de zin van de Cbw en onderliggende regelgeving een gebeurtenis is 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. Bij de inzet van de bevoegdheid zal het moeten gaan om leveranciers die ofwel zelf de intentie hebben om de beveiliging van de netwerk- en informatiesystemen van essentiële entiteiten of belangrijke entiteiten aan te tasten of incidenten bij die entiteiten te veroorzaken, dan wel leveranciers die nauwe banden hebben met of onder controle staan van een partij met een dergelijke intentie. Hierbij is het niet van belang of een partij in laatstbedoelde zin een statelijke actor is of een andere entiteit. Van nauwe banden of controle in bovenbedoelde zin kan in het eerste geval bijvoorbeeld sprake zijn indien de leverancier afkomstig is, of onder controle staat van een partij, uit een land met wetgeving die particuliere partijen verplicht samen te werken met de overheid van dat land, in het bijzonder staatsorganen die zijn belast met een inlichtingen- of militaire taak. Van de intentie in bovenbedoelde zin zal in datzelfde geval sprake kunnen zijn als het land, waaruit de leverancier zelf of de partij die controle heeft over die

leverancier, een actief offensief programma heeft dat is gericht op Nederland en Nederlandse belangen of een gespannen relatie met Nederland heeft, die acties die Nederlandse belangen aantasten voorstelbaar maken.

De betrokken vakminister zal ten aanzien van de betrokken essentiële entiteit of belangrijke entiteit moeten bepalen met betrekking tot welke onderdelen van haar netwerk- en informatiesystemen het noodzakelijk is om daarbinnen producten of diensten van specifieke leveranciers te weren. Het zal gaan om onderdelen waarvoor geldt dat de toegang daartoe, vanwege de gevoeligheid van die onderdelen, in geval van misbruik een risico voor de nationale veiligheid oplevert. Bij risico voor de nationale veiligheid kan gedacht worden aan sabotage, beïnvloeding of spionage door statelijke actoren of andere derde partijen van netwerk- en informatiesystemen van de entiteit. Ook de inzet van ransomware kan een risico vormen voor de nationale veiligheid als het gaat om de continuïteit van (vitale) processen, het weglekken en/of publiceren van vertrouwelijke of gevoelige informatie en de aantasting van de integriteit van de digitale ruimte.[3]

De beoordeling of en ten aanzien van welke onderdelen van netwerk- en informatiesystemen het opleggen van de verplichting om producten of diensten van een specifieke leverancier te weren noodzakelijk is zal per geval en dus per individuele entiteit geschieden. In die beoordeling wordt onder meer meegenomen of en in welke mate er bij een entiteit sprake is van kritieke onderdelen waarvoor geldt dat misbruik een risico voor de nationale veiligheid kan vormen en of de maatregelen die de entiteit heeft getroffen of nog kan treffen ter beheersing van een dergelijk risico voldoende zijn. Als er sprake is van het gebruik van producten of diensten van eenzelfde leverancier bij meerdere essentiële entiteiten of belangrijk entiteiten, zal de uitkomst van de beoordeling dus van entiteit tot entiteit kunnen verschillen. De verplichting om producten of diensten van een specifieke leverancier te weren zal dus niet generiek kunnen worden opgelegd. In lijn hiermee zal er vanuit de rijksoverheid bijvoorbeeld ook niet een lijst van te weren (producten of diensten van) leveranciers worden opgesteld. Wel zijn er verschillende openbare producten beschikbaar die voor entiteiten behulpzaam kunnen zijn bij de afweging van welke leveranciers zij producten of diensten zullen afnemen, zoals de handreiking *Cybercheck: ook jij hebt supply chain risico's!*.[4]

De bevoegdheid uit het voorgestelde artikel 21a, eerste lid, Cbw kan niet worden toegepast op essentiële entiteiten en belangrijke entiteiten die aanbieders van openbare elektronische communicatienetwerken of aanbieders van openbare elektronische communicatiediensten zijn. Dit is geregeld in het voorgestelde artikel 21a, vijfde lid, Cbw. De reden voor deze regeling is dat de Telecommunicatiewet (hierna: Tw) en daaronder liggende regelgeving voor deze aanbieders al in een sectorspecifiek vergelijkbaar regime voorziet. Met artikel het voorgestelde 21a, vijfde lid, Cbw wordt voorkomen dat er een dubbele grondslag ontstaat ten aanzien van die aanbieders. Immers, op grond van artikel 11.a1, tweede lid, Tw (zoals gewijzigd in artikel 99, onderdeel B, Cbw) is het al mogelijk om bij of krachtens amvb technische, operationele en organisatorische maatregelen vast te stellen, om de risico's voor de beveiliging van hun netwerken of diensten te beheersen, teneinde de gevolgen van beveiligingsincidenten op de nationale veiligheid of openbare orde te beperken. Met het oog op voortzetting van de huidige sectorale wetgeving bevat het

[3] Cybersecuritybeeld Nederland 2024.
[4] Te raadplegen op https://www.ncsc.nl/documenten/publicaties/2024/april/18/cybercheck-ook-jij-hebt-supply-chain risicos.

nieuwe tweede lid van artikel 11a.1 Tw een wettelijke grondslag die in materieel opzicht een ongewijzigde basis biedt voor het Besluit veiligheid en integriteit telecommunicatie (hierna: Bvit). De delegatiegrondslag voor het Bvit in artikel 11a.1, tweede lid, Tw is net zoals voorheen – met artikel 11a.1, vierde lid, Tw (oud) – gebaseerd op een benadering die alle gevaren omvat. De maatregelen kunnen dus onverminderd bijdragen aan de bescherming van veiligheidsbelangen in brede zin, waaronder risico's voor de nationale veiligheid. Daarbij kan worden gedacht aan sabotage of spionage van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten.

Het Bvit kent in artikel 2, tweede en derde lid, vergelijkbare bepalingen als het voorgestelde artikel 21a, eerste en derde lid, Cbw. Op grond van het Bvit heeft de Minister van Economische Zaken onder meer maatregelen getroffen met betrekking tot de bescherming van de toeleveringsketen van de mobiele telecommunicatienetwerken. Dit zijn reeds langere tijd geldende maatregelen op grond van nationaal beleid dat ongewijzigd wordt voortgezet. Zowel met betrekking tot de grondslag als de maatregelen die op grond van het Bvit zijn genomen doen er zich in materiële zin geen wijzigingen voor.

Beoordeling

De bovengenoemde verplichting wordt opgelegd door de vakminister, in overeenstemming met de Minister van Justitie en Veiligheid, als die naar zijn oordeel noodzakelijk is om risico's voor de beveiliging van de netwerk- en informatiesystemen die de nationale veiligheid raken te beheersen of om incidenten die de nationale veiligheid raken te voorkomen.

De beoordeling of de hierboven bedoelde verplichting zou moeten worden opgelegd sluit aan bij het in artikel 2 Cbw beschreven doel van de Cbw, te weten het met het oog op het in stand houden van kritieke maatschappelijke of economisch belangrijke functies of activiteiten verhogen van de cyberbeveiliging. Dit past eveneens in de Nederlandse Cybersecuritystrategie (2022–2028) waarin een digitaal veilig Nederland het uitgangspunt is.

Bij de beoordeling van risico's ten aanzien van onder meer spionage en sabotage door statelijke actoren bij digitale producten en diensten hanteert het kabinet de overwegingen die zijn vermeld in de brief van de Minister van Justitie en Veiligheid aan de Tweede Kamer over C2000.[5] De criteria die in het voorgestelde artikel 21a, eerste lid, Cbw zijn vermeld zijn in lijn met de overwegingen in genoemde Kamerbrief, met dien verstande dat in overweging 3A de term «vitale infrastructurele installaties of werken» is geactualiseerd naar «kritieke infrastructuur». Het gaat om de volgende overwegingen:

1.
Is de partij die de dienst of het product levert afkomstig, of staat hij onder controle van een partij, uit een land met wetgeving die commerciële of particuliere partijen verplicht samen te werken met de overheid van dat land, in het bijzonder met staatsorganen die zijn belast met een inlichtingen- of militaire taak, of is de partij een staatsbedrijf?

2.
Is de partij die de dienst of het product levert afkomstig uit een land met een actief offensief programma gericht op Nederland en Nederlandse

[5] Kamerstukken II 2018/19, 25 124, nr. 96.

belangen of een land waarmee de Nederlandse relatie dusdanig gespannen is dat acties die Nederlandse belangen aantasten voorstelbaar zijn?

Indien het antwoord op de in bovenstaande overwegingen geformuleerde vragen positief is, zal er sprake zijn van een partij die nauwe banden heeft met of onder controle staat van een staat of entiteit die de intentie heeft om de beveiliging van de netwerk- of informatiesystemen van een essentiële entiteit of belangrijke entiteit aan te tasten of om incidenten bij die entiteit te veroorzaken, of waarvoor gronden zijn om dergelijke banden of controle te vermoeden. Dan komen de volgende overwegingen aan de orde:

3A.
Krijgt de partij die de dienst of het product levert uitgebreide toegang tot gevoelige locaties, gevoelige ICT-systemen of de kritieke infrastructuur, waarbij misbruik een nationaal veiligheidsrisico kan vormen?

3B.
Zijn er beheersmaatregelen mogelijk en realiseerbaar die de nationale veiligheidsrisico's die in het geding zijn voldoende beschermen?

De reikwijdte van de op te leggen verplichting is beperkt tot die onderdelen die in de beschikking worden aangewezen. Bij de afweging welke onderdelen in de beschikking worden aangewezen, komen bovenstaande overwegingen als volgt aan bod. Eerst worden de kritieke onderdelen van de entiteit in kaart gebracht. Dit zijn de onderdelen waarvoor geldt dat de leverancier uitgebreide toegang tot gevoelige locaties, gevoelige ICT-systemen of de kritieke infrastructuur krijgt, waarbij misbruik een nationaal veiligheidsrisico kan vormen (overweging 3A). Vervolgens wordt beoordeeld of het opleggen van de verplichting in relatie tot die onderdelen noodzakelijk is om risico's die de nationale veiligheid raken te beheersen: dit houdt in dat er geen andere maatregelen mogelijk en realiseerbaar zijn om deze risico's voldoende te beheersen (overweging 3B). Hiertoe wordt met name de toereikendheid van de maatregelen die de essentiële entiteit of belangrijke entiteit in het kader van de wettelijke zorgplicht reeds heeft genomen of nog geacht wordt te moeten nemen in ogenschouw genomen. De kritieke onderdelen waarvoor geldt dat er geen andere beheersmaatregelen zijn om het risico voldoende te beheersen worden vervolgens aangewezen in de beschikking, waarmee de reikwijdte van de verplichting om uitsluitend gebruik te maken van vertrouwde leveranciers tot die aangewezen onderdelen is beperkt.

De volgende procesmatige stappen worden in het kader van de beoordeling in elk geval doorlopen:
1. het bepalen van het risico;
2. het plan van aanpak voor het (technisch) onderzoek;
3. het vaststellen van de kritieke onderdelen; en
4. het identificeren van de reeds getroffen en aanvullend mogelijke beveiligingsmaatregelen. De betrokken entiteit wordt hierbij zo veel als mogelijk betrokken en in de gelegenheid gesteld een zienswijze hierop te geven.

Termijn vervanging of beëindiging in gebruik zijnde producten of diensten

Het zal voor een essentiële entiteit of belangrijke entiteit niet altijd mogelijk zijn om per direct gevolg te geven aan de op grond van het voorgestelde artikel 21a, eerste lid, Cbw opgelegde verplichting, zonder hiermee de continuïteit van de dienstverlening in gevaar te brengen, als

de entiteit de in de beschikking genoemde producten of diensten van een specifieke leverancier nog in gebruik heeft. In zo'n geval zal de vakminister op grond van het voorgestelde artikel 21a, derde lid, Cbw, in het belang van de continuïteit van de dienstverlening, in de beschikking een termijn opnemen voor de vervanging of beëindiging van die in gebruik zijnde producten of diensten.

Inspanningsverplichting

De vakminister spant zich samen met de betrokken entiteit en het CSIRT in om het vervangen of beëindigen van in gebruik zijnde producten of diensten te ondersteunen, ten behoeve van de continuïteit van de dienstverlening van de betrokken entiteit die moet voldoen een verplichting als bedoeld in het voorgestelde artikel 21a, eerste lid, Cbw. De vakminister, de betrokken entiteit(en) en het CSIRT verkennen passende maatregelen die noodzakelijk worden geacht om in gebruik zijnde producten of diensten te vervangen of te beëindigen, binnen de door de vakminister gestelde termijn, zoals bedoeld in het voorgestelde artikel 21a, derde lid, Cbw. Ook stellen de vakminister en het CSIRT een redelijke termijn vast waarbinnen deze ondersteuning wordt verleend en wat noodzakelijk wordt geacht om de continuïteit van de dienstverlening in stand te houden. Deze termijn kan per casus verschillen, afhankelijk van de ingrijpendheid van de beschikking, zoals bedoeld in het voorgestelde artikel 21a, eerste lid, Cbw.

Rechtsbescherming

De aan een essentiële entiteit of belangrijke entiteit op te leggen verplichting, bedoeld in het voorgestelde artikel 21a, eerste lid, Cbw, is een besluit in de zin van de Algemene wet bestuursrecht (hierna: Awb). Tegen het besluit staan rechtsmiddelen (bezwaar, beroep en hoger beroep) open. Dit houdt in dat de betrokken entiteit bij de vakminister die de verplichting bij beschikking heeft opgelegd, in bezwaar kan gaan tegen de beschikking. Na de bezwaarprocedure bij de vakminister staat de rechtsgang bij de rechter en hoger beroepsrechter open, uiteraard voor zover de betrokken entiteit procesbelang heeft.

Rol van de toezichthouder

Als een essentiële entiteit of belangrijke entiteit een beschikking als bedoeld in het voorgestelde artikel 21a, eerste lid, Cbw opgelegd heeft gekregen, is er een rol voor de toezichthouder. Die ziet er op toe dat de beschikking wordt nageleefd door de betrokken entiteit.

Eigendomsregulering

Het Cbw biedt met het voorgestelde artikel 21a, eerste lid, de grondslag om een beschikking op te leggen die kan leiden tot eigendomsregulering van essentiële entiteiten en belangrijke entiteiten. Van eigendomsregulering is sprake wanneer de gebruiksmogelijkheden van de eigendom worden beperkt, zonder dat de beschikking over het eigendom verloren gaat. Bij een beschikking op basis van artikel 18, eerste lid, Cbb is sprake van regulering van eigendom en geen (de facto) onteigening: het leidt immers niet tot verlies van eigendom dan wel dat de beschikking over het eigendom verloren gaat. De producten en diensten waarop de beschikking betrekking heeft behouden waarde, blijven eigendom van de entiteit en kunnen door haar te gelde worden gemaakt.

Artikel 1 van het Eerste Protocol bij het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (hierna: EP EVRM) beschermt het recht op eigendom. Een beschikking op grond van het voorgestelde artikel 21a, eerste lid, Cbw vormt een inmenging in het in artikel 1 EP EVRM vervatte eigendomsrecht van essentiële entiteiten en belangrijke entiteiten. Van belang is dat het begrip «eigendom» in de zin van artikel 1 EP EVRM een autonome betekenis heeft. Dat betekent dat dit begrip een eigen betekenis heeft die losstaat van de betekenis die in de rechtstelsels van de verdragsstaten aan het begrip «eigendom» wordt gegeven. Bij de vraag of sprake is van eigendom in de zin van artikel 1 EP EVRM gaat het er volgens het Europees Hof voor de Rechten van de Mens (hierna: EHRM) uiteindelijk om dat in de omstandigheden van het geval sprake is van een «*title to a substantive interest*». Uit jurisprudentie valt af te leiden dat het in algemene zin dient te gaan om op economische, op geld waardeerbare aanspraken en belangen.[6] Toekomstige inkomsten die nog niet betaald zijn en waarop naar nationaal recht ook nog geen vaststaand recht bestaat, kwalificeren volgens het EHRM bijvoorbeeld niet als eigendom in de zin van artikel 1 EP EVRM.

Het EHRM erkent dat een staat ter borging van het algemeen belang (het gebruik van) eigendom mag reguleren en aan beperkingen mag onderwerpen als aan een aantal voorwaarden wordt voldaan. Een inbreuk op het eigendomsrecht is gerechtvaardigd wanneer er sprake is van regulering van eigendom en deze aan de legaliteitstoets, de legitimiteitstoets en de evenredigheidstoets «*fair balance*») voldoet.

De legaliteitstoets houdt in dat de inmenging in het eigendomsrecht voorzien moet zijn bij wet of daarop gebaseerde regelgeving. De toepasselijke nationale regeling moet voldoende toegankelijk, precies en voorzienbaar zijn. Het voorgestelde artikel 21a, eerste lid, Cbw voldoet aan deze vereisten.

De legitimiteitstoets houdt in dat de inmenging enkel mag plaatsvinden in het algemeen belang en dat deze een legitiem doel dient. Het EHRM laat staten een ruime beoordelingsmarge bij het vaststellen van wat als een legitieme doelstelling in het kader van het algemeen belang kan gelden; nationale veiligheid kan daar ook onder geschaard worden. Hierbij is wel van belang dat wordt overwogen of de ingrijpendheid van de maatregel in redelijke verhouding staat tot het ermee beoogde legitieme doel (proportionaliteit) en of er geen andere, minder ingrijpende maatregelen mogelijk zijn om ditzelfde doel te bereiken (subsidiariteit). Bij de beschikking op grond van het voorgestelde artikel 21a, eerste lid, Cbw zal de vakminister aandacht moeten besteden aan de proportionaliteit en de subsidiariteit van dat besluit. Zoals volgt uit het voorgestelde artikel 21a, tweede lid, Cbw, zal de vakminister bij de beschikking op grond van het voorgestelde artikel 21a, eerste lid, Cbw, moeten beoordelen of kan worden volstaan met de maatregelen die de betrokken entiteit reeds heeft genomen of nog kan nemen. Indien dat niet het geval is, moet de vakminister beoordelen tot welke onderdelen van de netwerk- en informatiesystemen het weren van producten en diensten van specifieke leveranciers zou moeten uitstrekken.

---

[6] EHRM 30 november 2004, ECLI:CE:ECHR:2004:1130JUD004893999 (*Öneryıldız/Turkije*), rechtsoverweging 124; EHRM 11 januari 2007, ECLI:CE:ECHR:2007:0111JUD007304901 (*Anheuser-Busch Inc./Portugal*), rechtsoverwegingen 75 tot en met 78; EHRM 23 maart 2010, ECLI:CE:ECHR:2011:1018JUD000907407 (*Mullai e.a./Albanië*), rechtsoverweging 97.

De evenredigheidstoets vraagt om een beoordeling of met de beschikking op grond van het voorgestelde artikel 21a, eerste lid, Cbw sprake is van een rechtvaardig en evenwichtig resultaat, oftewel «*fair balance*», tussen het algemeen belang en de belangen van – in dit geval – de entiteit die wordt geraakt door de inmenging in haar eigendomsrecht. Bij de beoordeling of sprake is van een «*fair balance*» dienen verschillende aspecten in ogenschouw te worden genomen. De toepassing van de in het voorgestelde artikel 21a, eerste lid, Cbw opgenomen bevoegdheid mag niet leiden tot een individuele en buitensporige last voor de betrokken entiteit. Er moet bovendien een redelijke mate van evenredigheid bestaan tussen de gebruikte middelen en het nagestreefde doel. Een van de aspecten die een belangrijke rol speelt in het kader van de «*fair balance*» is de voorzienbaarheid van de maatregel (in casu de toepassing van de in het voorgestelde artikel 21a, eerste lid, Cbw opgenomen bevoegdheid). Hiermee wordt bedoeld of de maatregel in de lijn der verwachting ligt, ook al bestond er nog geen concreet zicht op de omvang waarin, de plaats waar en het moment waarop de ontwikkeling zich zou voordoen. Voorts wordt met het voorgestelde artikel 21a, vierde lid, Cbw, een inspanningsverplichting opgelegd aan de vakminister en het CSIRT, om binnen een redelijke termijn en indien mogelijk maatregelen te treffen om de dienstverlening van essentiële entiteiten en belangrijke entiteiten te borgen, indien de verplichting, bedoeld in het voorgestelde artikel 21a, eerste lid, Cbw, aan deze entiteiten is opgelegd. Essentiële entiteiten en belangrijke entiteiten zijn op grond van artikel 21 Cbw verplicht om passende en evenredige technische, operationele en organisatorische maatregelen te 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 gebruiken, te beheersen. Ook moeten zij deze maatregelen nemen om incidenten te voorkomen. Daarmee is echter niet altijd op voorhand te zeggen dat die risico's voldoende kunnen worden beheerst wanneer in specifiek aan te wijzen onderdelen van de netwerk- en informatiesystemen niet uitsluitend producten of diensten van vertrouwde leveranciers worden gebruikt (en welke leveranciers als vertrouwd worden gezien). In sommige gevallen kan er sprake zijn van schade die voortvloeit uit het (vroegtijdig, voor afloop van de afschrijvingstermijn) moeten vervangen van producten, hetgeen op het moment van aanschaf niet voorzienbaar was. In zulke gevallen kan het noodzakelijk zijn nadeelcompensatie te bieden, om de vereiste «*fair balance*» te bereiken.

Nadeelcompensatie

Titel 4.5 van de Awb behelst een codificatie van het égalitébeginsel en geeft de belangrijkste materiële en procedurele regels voor de toekenning van nadeelcompensatie. In artikel 4:126, eerste lid, Awb is bepaald dat indien een bestuursorgaan in de rechtmatige uitoefening van zijn publiekrechtelijke bevoegdheid of taak schade veroorzaakt die uitgaat boven het normale maatschappelijke risico en die een benadeelde in vergelijking met anderen onevenredig zwaar treft, het bestuursorgaan de benadeelde desgevraagd een vergoeding toekent. De op grond van de onderhavige bevoegdheid op te leggen beschikkingen vallen onder de reikwijdte van deze bepaling en meer algemeen titel 4.5 Awb.

Schade op grond van het égalitébeginsel komt alleen voor vergoeding in aanmerking voor zover de schade onevenredig is en in rechtstreeks verband staat tot het genomen besluit. Van onevenredige schade is sprake indien de schade op een beperkte groep burgers of bedrijven drukt

(speciale last) en de schade boven het normaal maatschappelijke of ondernemersrisico uitstijgt (abnormale last).[7]

Voor de volledigheid wordt opgemerkt dat bij de beantwoording van de vraag of er een redelijk evenwicht bestaat tussen de eisen van het algemeen belang van de samenleving en de bescherming van de fundamentele rechten van het individu in het licht van artikel 1 EVRM EP, zoals hierboven is toegelicht, betrekt het EHRM de vraag of er een schadevergoeding is toegekend, alsmede de omvang daarvan. Op grond van de regeling in titel 4.5 Awb wordt de vraag naar de vergoedbaarheid van de schade en de omvang van de schadevergoeding los behandeld van de vraag naar de rechtmatigheid van het schadeveroorzakend overheidshandelen. Dit komt niet in strijd met de bescherming die artikel 1 EVRM EP beoogt te bieden, mits bestuursorganen zich er bij het nemen van een schadeveroorzakend besluit al rekenschap van geven dat het besluit aanleiding kan vormen voor aanspraken op nadeelcompensatie. In verband daarmee dient bij het nemen van het besluit tevens te worden bezien of er voor de afhandeling van een verzoek om nadeelcompensatie een met voldoende waarborgen omklede rechtsgang openstaat.[8] Dit is het geval nu een entiteit op grond van artikel 4:126, eerste lid, Awb een aanvraag voor nadeelcompensatie kan indienen.

Vrij verkeer van goederen

Een op grond van het voorgestelde artikel 21a, eerste lid, Cbw genomen beschikking is een kwantitatieve invoerbeperking (of maatregel van gelijke werking) in de zin van artikel 34 Verdrag betreffende de werking van de Europese Unie (hierna: VWEU). Een beperking in het vrije verkeer van goederen is slechts toegestaan indien dit gerechtvaardigd kan worden wegens een dwingende reden van algemeen belang, of in geval van discriminatoire maatregelen: een van de belangen opgesomd in artikel 36 VWEU, waaronder de bescherming van de openbare orde en openbare veiligheid, hetgeen ook de nationale veiligheid omvat. Een maatregel die leidt tot een beperking in het vrije verkeer van goederen moet voorts geschikt zijn om het beoogde doel te bereiken en niet verder gaan dan noodzakelijk is.

Zoals hierboven toegelicht vindt een op grond van het voorgestelde artikel 21a, eerste lid, Cbw opgelegde maatregel (in casu de verplichting tot het weren van bepaalde diensten of producten van bepaalde leveranciers) zijn rechtvaardiging in het beschermen van de nationale veiligheid. Het opleggen van een dergelijke maatregel is enkel aan de orde als de maatregel geschikt is om het nagestreefde belang te beschermen en als – gelet op de geconstateerde risico's voor de beveiliging van de netwerk- en informatiesystemen die de nationale veiligheid raken – die risico's niet afdoende te ondervangen zijn met de maatregelen die de betrokken entiteit in het kader van de zorgplicht reeds heeft genomen, zoals bepaald in het voorgestelde artikel 21b, tweede lid, Cbw. De maatregel zal in dat geval niet verder gaan dan nodig voor het beoogde doel en geschikt zijn om het beoogde doel te bereiken.

---

[7] Zie onder meer ABRvS 15 juli 2015, ECLI:NL:RVS:2015:2195 en ABRvS 30 mei 2012, ECLI:NL:RVS:2012:BW6926. Zie ook hoofdstuk 4.1 in het algemeen deel van de memorie van toelichting bij de wijziging van de Awb en enkele andere wetten in verband met het nieuwe omgevingsrecht en nadeelcompensatierecht (Kamerstukken II 2018/19, 35 256, nr. 3).

[8] ABRvS 16 april 2003, ECLI:NL:RVS:2003:AF7355 en ABRvS 9 juli 2003, ECLI:NL:RVS:2003:AH9396.

Bij een beschikking op basis van het voorgestelde artikel 21a, eerste lid, Cbw, die betrekking heeft op reeds in gebruik zijnde producten of diensten in de daarbij aangewezen onderdelen van de netwerk- en informatiesystemen van de betrokken entiteit, is tevens van belang dat de internationale afspraken tussen het Koninkrijk der Nederlanden en derde landen over investeringsbescherming in acht worden genomen. Onder deze afspraken wordt een buitenlandse investeerder in Nederland (en worden Nederlandse investeerders in het betreffende derde land) beschermd tegen onder meer onredelijk en/of discriminatoir handelen van de overheid. Daarnaast bieden deze afspraken voorwaarden op basis waarvan onteigend mag worden, namelijk indien de maatregel die tot (de facto) onteigening leidt non-discriminatoir is, in het publiek belang is en waartegenover een gepaste schadevergoeding wordt geboden. Indien een overheid jegens die investeerder niet redelijk heeft gehandeld of de voorwaarden voor onteigening heeft geschonden, kan de investeerder daartegen compensatie eisen. Dit is alleen van belang waar het gaat om een reeds bestaande investering.

Uit hetgeen hiervoor ten aanzien van de eigendomsregulering en nadeelcompensatie is besproken (vraagstukken waarvoor de toetsing dezelfde beginselen volgt), kan worden geconcludeerd dat beschikkingen op grond van het voorgestelde artikel 21a, eerste lid, Cbw in beginsel geen schending opleveren van de internationale investeringsbeschermingsafspraken op dit terrein. De vakminister zal bij het opleggen van beschikkingen op grond van het voorgestelde artikel 21a, eerste lid, Cbw steeds per geval toetsen aan de genoemde specifieke vereisten.

Verder is van belang dat een dergelijke beschikking geen afbreuk doet aan de handelsafspraken over diensten en goederen aangegaan onder de Wereldhandelsorganisatie (*World Trade Organization*) en bilaterale en regionale handelsakkoorden van de Europese Unie met derde landen. Deze akkoorden voorzien onder bepaalde voorwaarden in een uitzondering op de regels van markttoegang en non-discriminatoire behandeling. Zo kan een dergelijke beschikking gezien het doel van de maatregel gerechtvaardigd worden met een beroep op de algemene uitzondering voor de bescherming van de nationale veiligheid. Bij het nemen van de beschikking op grond van het voorgestelde artikel 21a, eerste lid, Cbw zal de vakminister moeten toetsen of dergelijke beperkende maatregelen noodzakelijk zijn om deze doelstelling te verwezenlijken, en er dus geen alternatieve maatregel bestaat die de handel minder beperkt en waarvan redelijkerwijs geacht wordt dat een staat die maatregel neemt. Uit het voorgestelde artikel 21a, eerste lid, Cbw blijkt dat de beschikking uitsluitend wordt opgelegd indien het opleggen van de verplichting om in onderdelen van de netwerk- en informatiesystemen producten of diensten van specifieke leveranciers te weren noodzakelijk is om risico's die de nationale veiligheid raken te beheersen. Hieruit volgt tevens dat een dergelijke maatregel alleen wordt opgelegd indien andere maatregelen, meer in het bijzonder de maatregelen die de betrokken entiteit in het kader van de wettelijke zorgplicht al heeft genomen, onvoldoende zijn om de risico's voor de nationale veiligheid te beheersen.

Wat betreft een beroep op de uitzonderingen ter bescherming van de nationale veiligheid geldt nog specifiek dat een staat maatregelen kan nemen die het nodig acht ter bescherming van het wezenlijke belang van haar veiligheid en die (voor zover hier relevant) enkel worden toegepast in tijd van oorlog of van gevaarlijke internationale spanningen. Daarnaast kan een staat maatregelen nemen tot handhaving van de internationale

vrede en veiligheid ingevolge haar verplichtingen krachtens het Handvest van de Verenigde Naties.

Gezien het doel van en de vereiste onderbouwing van de verplichting, bedoeld in het voorgestelde artikel 21a, eerste lid, Cbw, namelijk de bescherming van de nationale veiligheid, is een beschikking op grond van het voorgestelde artikel 21a, eerste lid, Cbw – afhankelijk van de specifieke situatie – in beginsel te rechtvaardigen onder de geldende uitzonderingsgronden van de handelsafspraken. De vakminister zal bij het opleggen van een beschikking op grond van het voorgestelde artikel 21a, eerste lid, Cbw steeds per geval toetsen aan de genoemde specifieke vereisten.

Kathmann