Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

36 270 Regels ter bevordering van de digitale weerbaarheid van bedrijven (Wet bevordering digitale weerbaarheid bedrijven)

Nr. 4

ADVIES AFDELING ADVISERING RAAD VAN STATE EN NADER RAPPORT[1]

Hieronder zijn opgenomen het advies van de Afdeling advisering van de Raad van State d.d. 20 juli 2022 en het nader rapport d.d. 9 december 2022, aangeboden aan de Koning door de Minister van Economische Zaken en Klimaat. Het advies van de Afdeling advisering van de Raad van State is cursief afgedrukt.

Blijkens de mededeling van de Directeur van Uw kabinet van 26 april 2022, nr. 2022000973, machtigde Uwe Majesteit de Afdeling advisering van de Raad van State haar advies inzake het bovenvermelde voorstel van wet rechtstreeks aan mij te doen toekomen. Dit advies, gedateerd 20 juli 2022, nr. W18.22.0068/IV, bied ik U hierbij aan.

Het voorstel heeft de Afdeling advisering van de Raad van State (hierna: de Afdeling) aanleiding gegeven tot opmerkingen bij het wetsvoorstel. Waar het voorstel de afbakening van (beleids)verantwoordelijkheid betreft, acht de Afdeling de introductie van een zelfstandige wet niet noodzakelijk. De toedeling van taken aan de Minister van EZK vereist immers geen wettelijke regeling. Een wettelijke verankering is wel noodzakelijk waar het een bevoegdheid tot de verwerking en verstrekking van persoonsgegevens betreft. Mede uit het oogpunt van harmonisatie van wetgeving, ligt het echter in de rede een dergelijke grondslag op te nemen in de Wet beveiliging netwerk- en informatiesystemen (Wbni).

Ongeacht of de regering vasthoudt aan de introductie van een nieuwe wettelijke regeling, wijst de Afdeling op enkele onduidelijkheden in het wetsvoorstel die een nadere toelichting behoeven. Ook wijst de Afdeling op het risico van uiteenlopende analyses, onderzoeken en adviezen. Tot slot merkt de Afdeling op dat het wetsvoorstel geen grondslag biedt voor de uitwisseling van persoonsgegevens met Caribisch Nederland.

[1] De oorspronkelijke tekst van het voorstel van wet en van de memorie van toelichting zoals voorgelegd aan de Afdeling advisering van de Raad van State is ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.

kst-36270-4
ISSN 0921 - 7371
's-Gravenhage 2022

In verband met deze opmerkingen adviseert de Afdeling het voorstel te heroverwegen. Graag ga ik op deze opmerkingen in het navolgende in. De tekst van het advies treft u hieronder aan, met tussengevoegd de reactie daarop.

Bij Kabinetsmissive van 26 april 2022, no. 2022000973, heeft Uwe Majesteit, op voordracht van de Minister van Economische Zaken en Klimaat, bij de Afdeling advisering van de Raad van State ter overweging aanhangig gemaakt het voorstel van wet houdende regels ter bevordering van de digitale weerbaarheid van bedrijven (Wet bevordering digitale weerbaarheid bedrijven), met memorie van toelichting

Het wetsvoorstel beoogt een wettelijke grondslag te bieden voor taken en bevoegdheden van de Minister van Economische Zaken en Klimaat (EZK) op het gebied van de digitale weerbaarheid van het niet-vitale bedrijfsleven in Nederland.

De Afdeling advisering van de Raad van State onderschrijft het belang van de bevordering van digitale weerbaarheid van Nederlandse bedrijven. Zij maakt evenwel enkele opmerkingen bij het wetsvoorstel. Waar het voorstel de afbakening van (beleids)verantwoordelijkheid betreft, acht de Afdeling de introductie van een zelfstandige wet niet noodzakelijk. De toedeling van taken aan de Minister van EZK vereist immers geen wettelijke regeling. Een wettelijke verankering is wel noodzakelijk waar het een bevoegdheid tot de verwerking en verstrekking van persoonsgegevens betreft. Mede uit het oogpunt van harmonisatie van wetgeving, ligt het echter in de rede een dergelijke grondslag op te nemen in de Wet beveiliging netwerk- en informatiesystemen (Wbni).

Ongeacht of de regering vasthoudt aan de introductie van een nieuwe wettelijke regeling, wijst de Afdeling op enkele onduidelijkheden in het wetsvoorstel die een nadere toelichting behoeven. Ook wijst de Afdeling op het risico van uiteenlopende analyses, onderzoeken en adviezen. Tot slot merkt de Afdeling op dat het wetsvoorstel geen grondslag biedt voor de uitwisseling van persoonsgegevens met Caribisch Nederland.

In verband met deze opmerkingen dient het voorstel te worden heroverwogen.

1. Noodzaak van een zelfstandige wet

Binnen het kabinet is de Minister van Justitie en Veiligheid (JenV) verantwoordelijk voor de coördinatie van cybersecurity en de bestrijding van cybercrime. Het Nationaal Cyber Security Centrum (NCSC) voert in dit verband de taken uit die de Minister van JenV heeft op grond van de Wbni. De Minister van EZK is verantwoordelijk voor het bedrijfsleven en de bevordering van de digitalisering van ondernemers. In dat kader richt hij zich op de vergroting van de digitale weerbaarheid van het niet-vitale bedrijfsleven.[2] Deze taken worden uitgevoerd door het Digital Trust Center (DTC), dat deel uitmaakt van het Ministerie van EZK.

Het wetsvoorstel beoogt een wettelijke grondslag te bieden voor deze bestaande en enkele nieuwe taken van de Minister van EZK op dit terrein. Zo krijgt hij ook de taak om Nederlandse bedrijven te informeren en te adviseren over specifieke kwetsbaarheden, dreigingen en incidenten die betrekking kunnen hebben op hun netwerk- en informatiesystemen.[3]

---

[2] Memorie van toelichting, paragraaf 2.2 («Wettelijke grondslag voor taken en gegevensverwerking Minister van EZK»).

[3] Voorgesteld artikel 2, eerste lid, onderdeel a.

De Afdeling onderschrijft het belang van de bevordering van digitale weerbaarheid van Nederlandse bedrijven. Waar het voorstel de afbakening van beleidsverantwoordelijkheid betreft, is een nieuwe wettelijke regeling evenwel niet noodzakelijk. Het bedrijfsleven en de bevordering van de digitale weerbaarheid van bedrijven worden immers al tot de portefeuille van de Minister van EZK gerekend. De loutere toedeling van taken op dit gebied vereist op zichzelf geen wettelijke regeling en is, anders dan in het geval van de Wbni, ook niet nodig ter implementatie van een Europese richtlijn.

Een wettelijke grondslag is wel noodzakelijk waar het een bevoegdheid tot de verwerking en verstrekking van persoonsgegevens betreft. Het wetsvoorstel geeft de Minister van EZK met zoveel woorden een wettelijke grondslag om de voor zijn taakuitoefening noodzakelijke (persoons)gegevens op te vragen en te delen.[4] Het is de Afdeling echter niet duidelijk waarom deze bevoegdheid wordt neergelegd in een zelfstandige wet en niet in de Wbni. De Wbni kent de Minister van EZK al enkele bevoegdheden toe. Die hebben betrekking op aanbieders van essentiële diensten binnen de sectoren energie en digitale infrastructuur.[5] Daarnaast voorziet een recent wetsvoorstel tot wijziging van de Wbni in een grondslag voor de verstrekking van (persoons)gegevens door het NCSC, ook aan niet-vitale aanbieders.[6] De Wbni regelt dus niet alleen bevoegdheden voor de Minister van JenV, maar ook voor de Minister van EZK. Bovendien regelt het – indien het recente wetsvoorstel tot wet wordt verheven – bevoegdheden ten aanzien van het niet-vitale bedrijfsleven. Tegen die achtergrond en uit het oogpunt van harmonisatie van wetgeving, ligt het in de rede om de nieuwe bevoegdheden van de Minister van EZK ten aanzien van de verwerking en verstrekking van persoonsgegevens op te nemen in de Wbni.

Met het wetsvoorstel worden de taken en bevoegdheden van de Minister van Economische Zaken en Klimaat (EZK) vastgelegd die de Minister heeft op het gebied van de verbetering van de digitale weerbaarheid van niet-vitale bedrijven in Nederland. Deze taken zijn breed en strekken zich uit van het geven van voorlichting, het stimuleren van samenwerking, maar ook het ontvangen, analyseren, onderzoeken van en adviseren over dreigingsinformatie. Voor de uitvoering van deze taken kunnen persoonsgegevens worden verwerkt. Met dit wetsvoorstel wordt voorzien in de wettelijke grondslag hiervoor.

Het is de Afdeling niet duidelijk waarom deze taken en bevoegdheden worden neergelegd in een zelfstandige wet en niet in de Wet beveiliging netwerk- en informatiesystemen (Wbni) die reeds bevoegdheden bevat die worden toegewezen aan de Minister van EZK. Voor wat betreft de Afdeling is de Wbni de aangewezen wet voor het regelen van de voorgenoemde bevoegdheden.

Het kabinet ziet, in aanvulling op de reeds in de memorie van toelichting genoemde motivering, drie redenen om deze bevoegdheden vast te leggen in een zelfstandige wet. Deze drie redenen zijn: de aard van de

---

[4] Voorgesteld artikel 3, eerste en tweede lid.

[5] Zie artikel 4 en de artikelen 21 en 22 van de Wbni.

[6] Zie de wijziging van artikel 3, tweede lid, van de Wbni, zoals voorgesteld in het voorstel van wet tot wijziging van de Wet beveiliging netwerk- en informatiesystemen in verband met de uitbreiding van de bevoegdheid van de Minister van Justitie en Veiligheid om dreigings- en incidentinformatie over de netwerk- en informatiesystemen van niet-vitale aanbieders te verstrekken aan deze aanbieders en aan organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over dreigingen en incidenten ten behoeve van deze aanbieders, Kamerstukken II 2021/22, 36 084, nr. 2.

wetgeving, de rol van de Minister van EZK in de wetgeving en de doelgroep van dit wetsvoorstel welke onderling verbonden zijn.
Ten eerste is de aard van de Wbni anders dan het voorliggende wetsvoorstel. In de Wbni worden grotendeels de bepalingen vanuit Europese wetgeving, de NIB-richtlijn[7], vastgelegd. De Wbni bevat daarmee de omzetting van Europeesrechtelijke verplichtingen voor haar doelgroep en regelt de naleving daarvan[8]. Op grond van het onderhavige voorstel dat geen Europeesrechtelijke oorsprong kent, geldt er geen zorg- of meldplicht voor de doelgroep daarvan, te weten de niet-vitale bedrijven. Tevens is er in dit wetsvoorstel geen sprake van toezicht en handhaving.
Ten tweede verschilt de rol van de Minister van EZK in de Wbni van de rol die de Minister van EZK heeft in onderhavig voorstel. De uit de Wbni voortvloeiende taken en bevoegdheden voor de Minister van EZK betreffen het toezicht op de naleving van de zorg- en meldplicht door vitale aanbieders in bijvoorbeeld de sector energie, die als aanbieders van een essentiële dienst zijn aangewezen, en voor digitale dienstverleners. Het onderhavige wetsvoorstel kent de Minister van EZK geen toezichthoudende bevoegdheden toe, maar ziet daarentegen op het informeren en adviseren van de niet-vitale bedrijven, (ongeveer 2 miljoen), die niet vallen onder het toepassingsbereik van de Wbni.
Ten derde is de doelgroep van onderhavig voorstel anders dan de doelgroep van de Wbni. De Wbni is in hoofdzaak gericht op de digitale veiligheid van organisaties die deel uitmaken van de rijksoverheid, vitale private aanbieders en digitale dienstverleners. Hierin wordt bijvoorbeeld geregeld dat de Minister van JenV (en in de praktijk het NCSC) verantwoordelijk is voor het informeren en adviseren van vitale aanbieders en Rijksoverheidsorganisaties bij digitale dreigingen en incidenten. Het onderhavige wetsvoorstel richt zich daarentegen op de doelgroep van het niet-vitale bedrijfsleven. Hierdoor zijn ook de taken van de Minister van JenV en de Minister van EZK anders. Het NCSC (Ministerie van JenV) heeft krachtens de Wbni als primaire taak het informeren en het adviseren van vitale aanbieders en organisaties die deel uitmaken van de rijksoverheid over digitale dreigingen en incidenten. Naast het informeren en het adviseren verleent het NCSC de aanbieders in zijn doelgroep ook overige bijstand bij het treffen van maatregelen om incidenten te voorkomen en te verhelpen. Overige bijstand kan bijvoorbeeld inhouden dat aan de aanbieder uit de doelgroep ter plekke ondersteuning wordt geboden bij het duiden van het probleem en de maatregelen om dat probleem aan te pakken.

Het DTC (Minister van EZK) richt zich bij het informeren en het adviseren over digitale dreigingen en incidenten op de doelgroep van het niet-vitale bedrijfsleven. Hierbij gaat het om algemene informatie en handelingsperspectieven maar ook om specifieke dreigingsinformatie gericht op individuele bedrijven. In tegenstelling tot het NCSC verleent het DTC bij incidenten geen overige bijstand, ofwel incident response, aan de aanbieders in zijn doelgroep.

Het kabinet is van mening dat deze belangen het beste worden gediend door deze onder te brengen in deze twee te onderscheiden wetten.
De memorie van toelichting is in paragraaf (2.3) aangevuld op dit punt.

---

[7] 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).

[8] Zorg- en meldplicht en daarbij behorend toezicht vindt plaats op vitale aanbieders welke ook aanbieders van essentiële diensten en digitaledienstverleners zijn. Voor andere vitale aanbieders geldt een meldplicht maar geen toezicht.

De Afdeling merkt overigens op dat de toelichting geen aandacht besteedt aan de vraag hoe het voornoemde recente wetsvoorstel tot wijziging van de Wbni zich verhoudt tot het onderhavige. De toelichting dient op dit punt te worden aangevuld, nu de voorstellen nauw met elkaar samenhangen en ook technisch op elkaar moeten worden afgestemd.[9]

In de memorie van toelichting bij het onderhavige wetsvoorstel is toegelicht dat er een verband is tussen dit wetsvoorstel en het voorstel tot wijziging van de Wbni[10] (zie toelichting bij artikel 5). Daar is ingegaan op de samenhang tussen beide wetsvoorstellen. Het verband tussen deze twee wetsvoorstellen is gelegen in het in ruimere zin mogelijk maken van het uitwisselen van informatie over digitale dreigingen en incidenten tussen beide organisaties ten behoeve van het uitoefenen van hun onderscheidenlijke taken. Dit betreft informatie-uitwisseling die twee kanten op werkt, dat wil zeggen van NCSC naar DTC en van DTC naar NCSC.

Waar de Afdeling mogelijk refereert aan de uitbereiding van de bevoegdheid van de Minister van JenV om niet-vitale aanbieders rechtstreeks van informatie te voorzien wordt het volgende opgemerkt. Rechtstreekse informatieverstrekking vanuit het NCSC aan andere aanbieders dan vitale aanbieders en Rijksoverheidsorganisaties zal door het wetsvoorstel tot wijziging van de Wbni alleen andere aanbieders kunnen betreffen die geen schakelorganisaties hebben en indien een dreiging of incident aanzienlijke gevolgen heeft of kan hebben voor de continuïteit van hun dienstverlening. In onderhavig wetsvoorstel wordt de positie van het DTC als schakelorganisatie voor haar doelgroep wettelijk vastgelegd. Dit leidt ertoe dat het NCSC niet ook aan individuele aanbieders in de doelgroep van het DTC informatie kan verstrekken. [11]

De memorie van toelichting is in paragraaf (2.2) aangevuld op dit punt.

De Afdeling adviseert de keuze voor een zelfstandige wet in het licht van het voorgaande te heroverwegen.

Op grond van het voorgaande wordt dit voorstel tot wet gehandhaafd en zal de samenhang tussen het wetsvoorstel en de Wbni zorgvuldig worden bewaakt.

Ongeacht of de regering vasthoudt aan de introductie van een nieuwe wettelijke regeling, wijst de Afdeling op het volgende.

---

[9] Zie de samenloopbepaling in artikel II van het voorstel van wet tot wijziging van de Wet beveiliging netwerk- en informatiesystemen in verband met de uitbreiding van de bevoegdheid van de Minister van Justitie en Veiligheid om dreigings- en incidentinformatie over de netwerk- en informatiesystemen van niet-vitale aanbieders te verstrekken aan deze aanbieders en aan organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over dreigingen en incidenten ten behoeve van deze aanbieders, *Kamerstukken II* 2021/22, 36 084, nr. 2.

[10] Voorstel van wet tot wijziging van de Wet beveiliging netwerk- en informatiesystemen in verband met de uitbreiding van de bevoegdheid van de Minister van Justitie en Veiligheid om dreigings- en incidentinformatie over de netwerk- en informatiesystemen van niet-vitale aanbieders te verstrekken aan deze aanbieders en aan organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over dreigingen en incidenten ten behoeve van deze aanbieders (Kamerstukken II 2021/22, 36 084, nr. 2).

[11] Zie ook Nader rapport op Wijziging Wbni, *Kamerstukken II 2021/22, 36 084, nr. 4.*

2. Nieuwe taken Minister van Economische Zaken en Klimaat

a. Samenwerking en duidelijkheid voor de praktijk

Met het wetsvoorstel krijgt de Minister van EZK onder andere de taak om samen te werken met bestuursorganen en rechtspersonen ten behoeve van de digitale weerbaarheid. Hierbij gaat het volgens de toelichting onder meer om samenwerking met andere vakdepartementen en decentrale overheden, maar ook met onderwijsinstellingen en onderzoeksinstituten.[12] Hieruit blijkt dat verschillende departementen aanspreekpunt kunnen zijn op het terrein van cybersecurity voor dezelfde organisaties. Een belangrijk uitgangspunt daarbij is wel dat het voor alle sectoren duidelijk is voor wat zij bij welk departement zij terecht kunnen.[13]

De Afdeling adviseert de nieuwe samenwerkingstaak in de toelichting te verduidelijken en inzichtelijk te maken in welke gevallen organisaties zich kunnen wenden tot de Minister van EZK.

De Minister van EZK heeft op grond van voorgesteld artikel 2, tweede lid, twee soorten taken op het gebied van samenwerking ter versterking van de digitale weerbaarheid van de Nederlandse samenleving of ter voorkoming van nadelige maatschappelijke gevolgen in en buiten Nederland. De eerste taak ziet op het stimuleren van onderlinge samenwerking tussen bedrijven (onderling) en organisaties. De tweede taak ziet op het samenwerken met andere bestuursorganen en organisaties om te werken aan bredere oplossingen voor digitale weerbaarheid. Denk hierbij aan kennisdeling, onderzoek en sector- of branche-specifieke beelden. Anders dan de Afdeling lijkt te veronderstellen leidt deze samenwerkingstaak niet tot onduidelijkheid bij bedrijven over bij welk departement zij terecht kunnen. De samenwerking met andere vakdepartementen en decentrale overheden, maar ook met onderwijsinstellingen en onderzoeksinstituten heeft namelijk geen effect op bestaande verhoudingen tussen deze organisaties en de bedrijven en sectoren. Er verandert dus ook niets in bestaande aanspreekpunten voor bedrijven en sectoren.

b. Risico van uiteenlopende analyses, onderzoeken en adviezen

De Afdeling merkt daarnaast op dat de taken van het DTC en het NCSC lijken te (kunnen) overlappen. Op grond van het wetsvoorstel respectievelijk de Wbni, kan zowel het DTC als het NCSC een analyse uitvoeren en (technisch) onderzoek doen naar de door hen verzamelde informatie. Het DTC kan voorts op basis van het wetsvoorstel niet-vitale bedrijven informeren over digitale dreigingen en incidenten.[14] Het NCSC kan niet alleen vitale bedrijven en onderdelen van de rijksoverheid informeren over digitale dreigingen en incidenten, maar op grond van een recent wetsvoorstel ook niet-vitale bedrijven.[15]

---

[12] Memorie van toelichting, paragraaf 2.2 («Wettelijke grondslag voor taken en gegevensverwerking Minister van EZK»).

[13] Zie ook Kamerstukken II 2019/20, 26 643 en 30 821, nr. 673, p. 4.

[14] Voorgesteld artikel 2, eerste lid, onderdeel b. Zie ook de memorie van toelichting, paragraaf 2 («Hoofdlijnen van het voorstel»): «In enkele gevallen zal dit een aanvulling zijn op de informatie die zij al via een schakelorganisatie ontvangen als bedoeld in artikel 3, tweede lid, Wbni».

[15] Zie het voorstel van wet tot wijziging van de Wet beveiliging netwerk- en informatiesystemen in verband met de uitbreiding van de bevoegdheid van de Minister van Justitie en Veiligheid om dreigings- en incidentinformatie over de netwerk- en informatiesystemen van niet-vitale aanbieders te verstrekken aan deze aanbieders en aan organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over dreigingen en incidenten ten behoeve van deze aanbieders, Kamerstukken II 2021/22, 36 084, nr. 2.

In dat licht wijst de Afdeling op het risico dat een bedrijf zowel door het NCSC als het DTC wordt geïnformeerd over een digitale dreiging of een incident, en dat daaraan verschillende analyses of onderzoeken ten grondslag liggen.[16] In het geval van digitale dreigingen en incidenten is het van cruciaal belang dat er geen onduidelijkheid is over de (analyse van bepaalde) dreigings- en incidenteninformatie.[17]

De Afdeling haalt in dit punt aan dat niet-vitale bedrijven zowel door het DTC als het NCSC kunnen worden geïnformeerd en dat daaraan mogelijk verschillende analyses en onderzoeken ten grondslag kunnen liggen. Het DTC en NCSC hebben echter duidelijk te onderscheiden doelgroepen van organisaties waaraan informatie en advies over concrete digitale dreigingen en incidenten worden verstrekt en ten behoeve waarvan analyses en onderzoek naar aanleiding van (aanwijzingen voor) dergelijke dreigingen en incidenten worden gedaan. In de door de Afdeling aangehaalde wijziging van de Wbni wordt het onder bepaalde voorwaarden mogelijk voor het NCSC om in ruimere zin dreigings- en incidentinformatie te delen met andere aanbieders (niet zijnde Rijk en vitaal). Een van die voorwaarden is dat er voor die aanbieders géén schakelorganisatie beschikbaar is die deze aanbieder als doelgroep heeft. Daarnaast zorgt het wetsvoorstel ervoor dat dreigings- en incidentinformatie in ruimere zin kan worden gedeeld met het DTC en andere schakelorganisaties. Het NCSC zal informatie over niet-vitale bedrijven dus direct met het DTC kunnen delen, welke op haar beurt haar doelgroep zal kunnen informeren en adviseren. Hiermee is dubbel informeren van een niet-vitaal bedrijf niet aan de orde.

Het NCSC en DTC werken waar mogelijk samen. Voor wat betreft analyse en onderzoek zijn beide organisaties verantwoordelijk voor de eigen doelgroepen. Vanwege deze verschillende doelgroepen kan het zijn dat voor het DTC en NCSC andere bronnen, die algemene of specifieke (dreigings)informatie bevatten welke van publieke of private partijen afkomstig zijn, relevant zijn. Zo zijn niet alle kwetsbaarheden, dreigingen en incidenten relevant voor doelgroepen van het DTC. Dit geldt ook voor de door het NCSC bijgestane vitale aanbieders of overheidsorganisaties. Denk hierbij aan systemen die alleen bij de overheid worden gebruikt, of aan de andere kant van het spectrum, producten die door zzp'ers worden gebruikt maar eigenlijk gekocht zijn als consument. Dit laat onverlet dat als één van deze organisaties in de uitoefening van haar taken over informatie beschikt, die ook relevant is voor de doelgroep van de ander, deze informatie onderling uitgewisseld zal gaan worden.

Aan de memorie van toelichting is een nieuwe paragraaf (2.4) toegevoegd over de verhouding tussen het DTC en het NCSC.

In aanvulling daarop merkt de Afdeling op dat zowel het NCSC als het DTC de taak is toegekend een advies, zoals een handelingsperspectief, aan specifieke bedrijven aan te reiken. Het is daardoor mogelijk dat adviezen van de overheid gerelateerd aan eenzelfde dreiging of incident uiteenlopen en dat partijen binnen eenzelfde keten, verschillende handelsperspectieven aangereikt krijgen. Ter illustratie wijst de Afdeling op de aanpak van de problemen rond kwetsbaarheden in Citrix-software. Het NCSC kwam begin 2020 aanvankelijk met een genuanceerd advies aan afnemers om te overwegen de Citrix-servers uit te zetten, afhankelijk van de impact die dat zou hebben op de afnemer in kwestie. Al de

---

[16] Zie ook punt 2 van het advies van de Afdeling over het aanhangige wetsvoorstel tot wijziging van de Wbni, Kamerstukken II 2021/22, 36 084, nr. 4.

[17] Zie ook het standpunt van de regering hierover, Kamerstukken II 2019/20, 26 643 en 30 821, nr. 673, p. 4.

volgende dag adviseerde het NCSC dringend om alle Citrix-servers uit te zetten, omdat – zoals later bleek – de AIVD de veiligheidsrisico's anders inschatte dan het NCSC. Organisaties die de problemen met Citrix zelf al hadden opgelost, zagen zich genoodzaakt om dat advies op te volgen.[18]

De toelichting bij het wetsvoorstel stelt dat het DTC en het NCSC samenwerken om het risico van onder meer dubbele informatieverstrekking te vermijden.[19] *Er wordt evenwel geen «rangorde» aangebracht tussen de adviezen van het DTC en het NCSC. De Afdeling is van oordeel dat concrete uitgangspunten, die ertoe moeten leiden dat uiteenlopende analyses, onderzoeken en adviezen van de overheid in relatie tot eenzelfde dreiging of incident worden voorkomen, niet alleen in samenwerkingsafspraken met het NCSC, maar ook in de toelichting bij dit wetsvoorstel dienen te worden uitgewerkt.*

De Afdeling adviseert in de toelichting nader inzichtelijk te maken hoe uiteenlopende analyses, onderzoeken en adviezen van de overheid in relatie tot eenzelfde dreiging of incident kunnen worden voorkomen.

Zoals ook eerder toegelicht, hebben het DTC en NCSC beiden duidelijk te onderscheiden doelgroepen. Het NCSC richt zich op vitale aanbieders en organisaties die deel uitmaken van de rijksoverheid. De doelgroep van het DTC is het niet-vitale bedrijfsleven. Beide organisaties zullen de analyses, onderzoeken en adviezen die zij uitvoeren en geven afstemmen op de taak die zij hebben voor hun doelgroep. Hierbij wordt met name in de formulering van het advies rekening gehouden met de aard en de relevantie van het advies voor de respectievelijke doelgroepen. Daarnaast zullen het DTC en NCSC met elkaar samenwerken en informatie uitwisselen om te voorkomen dat sterk uiteenlopende analyses, onderzoeken en adviezen worden gegeven.

Het door de Afdeling geschetste risico zal in de komende jaren verder worden verkleind door de voorgenomen vorming van één nieuwe organisatie waarin verschillende cybersecurity expertise van de overheid samen zal komen[20].

In de memorie van toelichting is de nieuwe paragraaf (2.4) aangevuld op dit punt.

c. Verwachtingen sector

Met het wetsvoorstel kan het DTC het Nederlandse bedrijfsleven voorzien in analyses, onderzoek en individuele adviezen in geval van digitale dreigingen en incidenten. De regering hanteert daarbij tevens het uitgangspunt dat het van belang is dat bedrijven in Nederland hun verantwoordelijkheid op het gebied van cybersecurity kennen en nemen. Dit betekent dat zij zelf moeten investeren in hun digitale weerbaarheid.[21]

De Afdeling onderschrijft de rol van de overheid voor effectieve informatie-uitwisseling voor de digitale weerbaarheid van bedrijven maar wijst ook op het risico dat de verwachting wordt gewekt dat daarmee goeddeels in dreigings- en incidenteninformatie is voorzien, waardoor bedrijven hun eigen verantwoordelijkheid onderschatten of veronacht-

---

[18] Onderzoeksraad voor Veiligheid, Kwetsbaar door software. Lessen naar aanleiding van beveiligingslekken door software van Citrix, december 2021, p. 50–55. Zie ook Kamerstukken II, 2019/20, 26 643, nr. 660.

[19] Memorie van toelichting, paragraaf 8.2 («Afbakening doelgroep van het wetsvoorstel»).

[20] Kamerstukken II 2022/23, 26 643 nr. 915.

[21] Kamerstukken II 2019/20, 26 643 en 30 821, nr. 673, p. 3.

zamen. De Afdeling acht het van belang dat met dit wetsvoorstel ook helder wordt gecommuniceerd hoe deze nieuwe taken van de Minister van EZK zich verhouden tot de eigen verantwoordelijkheden van het niet-vitale bedrijfsleven om alert te zijn op mogelijke kwetsbaarheden, dreigingen en incidenten.

Zo is het volgens de Onderzoeksraad voor Veiligheid voor kleinere bedrijven moeilijk om hun verantwoordelijkheid voor veilige software die zij gebruiken waar te maken. Software bevat immers een steeds groter aantal onbekende kwetsbaarheden, er gelden (nog) geen wettelijke eisen voor software, fabrikanten sluiten de aansprakelijkheid voor kwetsbaarheden vaak uit of beperken die, en het testen en installeren van updates en patches vergt veel tijd en deskundigheid.[22] Tegelijkertijd kan de overheid deze verantwoordelijkheid niet volledig overnemen.

In het licht van het voorgaande, adviseert de Afdeling in de toelichting in te gaan op de verhouding tussen de verantwoordelijkheden van de Minister van EZK en die van het niet-vitale bedrijfsleven.

De verantwoordelijkheid van de overheid voor de digitale weerbaarheid van niet-vitale bedrijven is begrensd door de eigen verantwoordelijkheid van niet-vitale bedrijven. Op basis van dit wetsvoorstel kan het DTC niet-vitale bedrijven informeren en adviseren over bijvoorbeeld ernstige kwetsbaarheden bij individuele bedrijven. Hierbij dient in acht te worden genomen dat de informatie en adviezen van het DTC een (niet volledige) aanvulling zijn op de digitale weerbaarheid van een bedrijf. Zo heeft een specifieke individuele notificatie door het DTC betrekking op die concrete dreiging of kwetsbaarheid. Maar er kunnen meer kwetsbaarheden, dreigingen en incidenten zijn in de netwerk- en informatiesystemen van dat bedrijf waar het DTC géén weet van heeft. Een bedrijf is en blijft zelf verantwoordelijk voor het actief beheren en versterken van haar digitale veiligheid. De overheid speelt hierin een rol maar neemt uitdrukkelijk niet de verantwoordelijkheid van bedrijven over.

De memorie van toelichting is in paragraaf (2.2) hier nader op aangevuld.

3. Potentiële marktactiviteiten van de Minister van EZK

Op grond van het wetsvoorstel krijgt de Minister van EZK de taak om gegevens met betrekking tot digitale kwetsbaarheden, dreigingen en incidenten te onderzoeken en te analyseren, en om uitkomsten daarvan te verstrekken aan niet-vitale bedrijven.[23] De Afdeling merkt op dat in de toelichting bij het wetsvoorstel slechts beperkt inzichtelijk wordt gemaakt welke (soort) informatie de Minister voornemens is te delen met het bedrijfsleven, en in hoeverre die informatie bewerkt zal worden. Ook is onduidelijk welke soort adviezen bedrijven kunnen verwachten en wat onder analyse en onderzoek van de Minister kan worden verstaan.

Volgens de toelichting wordt voldaan aan de Wet markt en overheid omdat de taken van de Minister zich beperken tot informatievoorziening. Bedrijven dienen zelf incidenten op te lossen en preventieve maatregelen nemen.[24] De Afdeling vindt deze toelichting te summier en merkt op dat het voor de naleving van de Wet markt en overheid en Europese (mededingings- en staatssteun)regelgeving ook duidelijk moet zijn welk soort informatie wordt gedeeld, in welke mate die informatie wordt

---

[22] Onderzoeksraad voor Veiligheid, Kwetsbaar door software. Lessen naar aanleiding van beveiligingslekken door software van Citrix, december 2021, p. 73–100.
[23] Voorgesteld artikel 2, eerste lid, onderdelen a en b.
[24] Memorie van toelichting, paragraaf 8.6 («Diverse punten»).

bewerkt en welk soort adviezen en analyses worden opgesteld en uitgevoerd.[25] Bewerking van informatie en op individuele bedrijven gerichte, specifieke adviezen en analyses kan ertoe leiden dat er in het kader van dit wetsvoorstel sprake is van economische activiteiten. In dat geval zal helder moeten zijn dat de Minister van EZK zich ook houdt aan de gedragsregels uit de Wet markt en overheid, die een gelijk speelveld tussen overheden en ondernemingen moeten creëren. De toelichting maakt dit onvoldoende inzichtelijk.

De Afdeling adviseert in de toelichting bij het wetsvoorstel op te nemen welk soort informatie, analyse en advies zal worden gedeeld en in hoeverre de Minister van EZK voornemens is de informatie die wordt verzameld te bewerken voordat deze wordt gedeeld met niet-vitale bedrijven.

Daarnaast adviseert de Afdeling in de toelichting nader in te gaan op de vraag in hoeverre de taken van de Minister kunnen worden aangemerkt als economische activiteiten in de zin van de Wet markt en overheid.

Het DTC zal, conform artikel 2 van dit voorstel, gegevens over kwetsbaarheden, dreigingen en incidenten die betrekking hebben op netwerk- en informatiesystemen delen met bedrijven. Deze informatie, die bij het DTC bekend is, wordt omgezet in twee stromen. Het DTC zal algemene dreigingsinformatie delen door middel van nieuwsberichten bij beveiligingslekken of kwetsbaarheden in netwerk- en informatiesystemen welke een grote bedreiging vormen voor ondernemend Nederland. Criteria hiervoor zijn: de kans dat de kwetsbaarheid wordt misbruikt en de ernst van de schade die kan optreden bij misbruik. Het DTC maakt voor haar doelgroep nog een aantal aanvullende afwegingen voordat ze in een algemene waarschuwing de gevonden kwetsbaarheid of dreiging van uitleg voorziet en publiceert. De belangrijkste zijn: Betreft het netwerk- en informatiesystemen die door veel bedrijven gebruikt worden? Is er actie door bedrijven nodig? Is er handelingsperspectief? Indien deze afweging leidt tot een nieuwsbericht dan wordt in dit bericht aangegeven welk product of versie het betreft, welk misbruik er mogelijk is, wat het effect daarvan kan zijn en in algemene bewoordingen wat een bedrijf kan doen om de dreiging te verhelpen.

Vervolgens kan het DTC als het informatie heeft dat een kwetsbaarheid, dreiging of incident te herleiden is tot één of meerdere bedrijven, deze bedrijven hierover informeren. Het advies dat het DTC uitbrengt is in grote mate gebaseerd op de (publieke) informatie van cybersecurity onderzoekers, leveranciers van netwerk- en informatiesystemen en andere (publieke) informatie gerelateerd aan de kwetsbaarheid, dreiging of incident. Het advies houdt nadrukkelijk geen verplichtingen in voor bedrijven. Ook zal het advies van het DTC in algemene bewoordingen worden opgesteld waarbij het aan bedrijven zelf is om te beoordelen (al dan niet met behulp van ICT-dienstverleners) welke concrete maatregelen noodzakelijk zijn en kunnen worden doorgevoerd. Daarbij verleent het DTC geen ondersteuning bij het doorvoeren van deze adviezen. Concreet betekent dit dat een advies als volgt kan luiden:

Bedrijf ABC, u maakt gebruik van software van leverancier 123 op systeem met IP-adres: xxx.xxx.xxx.xxx. In deze software is een kwetsbaarheid bekend geworden die kan leiden tot toegang tot data en informatie door een derde. U kunt de volgende maatregelen nemen:

---

[25] Zie HvJEU 12 juli 2012, C-138/11, ECLI:EU:C:2012:449 (Compass-Datenbanken) en «Analyse activiteiten RDW in het licht van de bepalingen van de Wet Markt en Overheid», d.d. 3 februari 2014.

1) update de software van leverancier 123;
2) onderzoek de toegang tot dit systeem;
3) mocht u hulp nodig hebben bij de beoordeling van deze informatie en adviezen, neem contact op met je ICT leverancier.

De informatie over kwetsbaarheden, dreigingen en incidenten, waar het DTC over beschikt, zal vaak in de vorm van ruwe data zijn. Wanneer het DTC de ruwe data naar een bedrijf heeft kunnen herleiden, zal het DTC deze data verrijken met de contactgegevens van het getroffen bedrijf. Daarna zal notificatie plaatsvinden aan het individuele bedrijf. Er vindt geen verdere bewerking van de informatie plaats.

Het informeren van bedrijven (algemeen en individueel) over bij het DTC bekende kwetsbaarheden, dreigingen en incidenten in netwerk- en informatiesystemen vindt plaats in het algemeen belang. Het belang dat hier wordt gediend is enerzijds de digitale weerbaarheid van individuele ondernemingen in Nederland, anderzijds het voorkomen van nadelige maatschappelijke gevolgen voor burgers, klanten en bedrijven onderling. Een digitale verstoring bij een supermarkt heeft direct gevolgen voor het bedrijf, haar klanten, de omgeving, leveranciers en andere partners, zoals banken en accountants.
Het DTC informeert en geeft algemeen handelingsperspectief en daarmee is er ook een grens aan wat de overheid doet. Bedrijven ontvangen informatie, het is aan hen om hierop te handelen. Het gegeven handelingsperspectief, bijvoorbeeld het updaten van een systeem, is niet op het individuele bedrijf afgestemd en wordt niet door het DTC uitgevoerd. Bedrijven zijn en blijven zelf verantwoordelijk voor het nemen van de nodige maatregelen. Bedrijven zullen juist dan, wanneer zij zelf onvoldoende mogelijkheid hebben om de juiste maatregelen te nemen, een beroep doen op marktpartijen om hen te ondersteunen. Bedrijven worden ongeacht hun branche of sector, regio of bedrijfsomvang op dezelfde wijze behandeld.

Vanwege het bovengenoemde, behoort het delen van, bij het DTC bekende algemene of specifieke informatie over kwetsbaarheden, dreigingen en incidenten aan de Nederlandse bedrijven tot de uitoefening van bevoegdheden van openbaar gezag. Het bevorderen van de digitale weerbaarheid van bedrijven en daarmee ook openbare (digitale) veiligheid behoort immers tot de taken van de overheid. Daar waar marktactiviteiten beginnen, houdt de advisering van het DTC op. De in dit wetsvoorstel voorgestelde taken van de Minister van EZK zijn derhalve geen economische activiteiten en zijn de staatssteunregels daar niet op van toepassing. Uit het arrest van het Hof van Justitie van de Europese Unie (Derde kamer) van 12 juli 2012, ECLI:EU:C:2012:449, volgt dat het publiek toegankelijk maken van informatie die verzameld is ten behoeve van een wettelijke taak geen economische activiteit vormt.

De memorie van toelichting is op de punten van staatssteun en de verhouding Wet markt en overheid respectievelijk in paragraaf (4.2) aangepast.

4. Informatiedeling met Caribisch Nederland

Volgens de toelichting gelden de taken en bevoegdheden van de Minister van EZK voor Nederland inclusief Caribisch Nederland, zijnde Bonaire, Saba en Sint-Eustatius.[26] De Afdeling ondersteunt de wens van de Nederlandse regering om zich ook in te zetten voor de digitale weerbaarheid van bedrijven gevestigd in Caribisch Nederland. De

[26] Memorie van toelichting, paragraaf 2.4 («Toepassing in Caribisch Nederland»).

Afdeling merkt daarbij op dat informatie over digitale dreigingen en incidenten veelal persoonsgegevens omvat, zoals in de vorm van IP-adressen.

De Algemene verordening gegevensbescherming (AVG) is alleen van toepassing op het Europese deel van het Koninkrijk. Dit betekent dat op de gegevensverstrekking die in het kader van het wetsvoorstel aan de orde is, het regime uit de AVG ten aanzien van doorgifte van gegevens met derde landen van toepassing is.[27] Zonder een adequaatheidsbesluit van de Europese Commissie kan niet zonder meer worden uitgegaan van een «passend beschermingsniveau».[28] Daarmee ontbreekt een grondslag voor doorgifte van gegevens aan Caribisch Nederland op grond van artikel 45 AVG.

De Afdeling adviseert in de toelichting in te gaan op de naleving van de AVG en te voorzien in een grondslag voor doorgifte van gegevens aan Caribisch Nederland.

Naar aanleiding van het advies van de Afdeling is het wetsvoorstel aangevuld met een nieuw artikel waaruit blijkt dat de wet ook in Caribisch Nederland van toepassing is (artikel 7). Hiermee wordt een expliciete grondslag gecreëerd voor uitwisseling van gegevens met Caribisch Nederland. Ook daar is de nood hoog en is er sprake van behoefte aan het bevorderen van de digitale weerbaarheid. Daarnaast wordt het advies opgevolgd door in paragraaf 4.3 van de memorie van toelichting in te gaan op de naleving van de AVG ten aanzien van doorgifte van gegevens aan Caribisch Nederland.

Omdat Caribisch Nederland geen deel uitmaakt van de Europese Unie is sprake van doorgifte naar een zogeheten derde land in de zin van de AVG. Voor doorgifte geldt in aanvulling op de gebruikelijke eisen voor de verwerking van persoonsgegevens dat tevens aan de voorwaarden van Hoofdstuk V van de AVG dient te worden voldaan. Voor het voldoen aan een adequaat beschermingsniveau zijn verschillende mogelijkheden. Artikel 46 van de AVG staat doorgifte van persoonsgegevens naar een derde land toe wanneer er sprake is van passende waarborgen en betrokkenen over afdwingbare rechten en doeltreffende rechtsmiddelen beschikken. In Caribisch Nederland geldt een wettelijke regeling inzake de bescherming van persoonsgegevens – de Wet bescherming persoonsgegevens BES (Wbp BES). Deze wet biedt waarborgen voor de bescherming van deze gegevens en de rechten van betrokkenen. In verhouding tot de AVG biedt de Wbp BES een vergelijkbaar beschermingsniveau van persoonsgegevens. Zo moet aan vergelijkbare vereisten van rechtmatigheid worden voldaan, en worden de rechten en rechtsbescherming van betrokkene gewaarborgd. Net als bij de AVG heeft de betrokkene o.m. het recht op inzage in zijn of haar persoonsgegevens. Voor zover het voor een goede uitvoering van de voorgestelde taken en bevoegdheden noodzakelijk zal zijn om persoonsgegevens in Caribisch Nederland te verwerken biedt de Wbp BES aldus een passend beschermingsniveau. Zoals uitgelegd in de memorie van toelichting bij het wetsvoorstel zal het hierbij om «gewone» persoonsgegevens gaan waarbij niet meer gegevens worden verwerkt dan strikt noodzakelijk, en deze niet voor andere doeleinden worden gebruikt dan waarvoor zij oorspronkelijk zijn verzameld.

---

[27] Hoofdstuk V van de AVG.

[28] Kamerstukken II 2019/20, 32 761, nr. 161, p. 2.

De Afdeling advisering van de Raad van State heeft een aantal bezwaren bij het voorstel en adviseert het voorstel niet bij de Tweede Kamer der Staten-Generaal in te dienen, tenzij het is aangepast.

Van de gelegenheid is gebruik gemaakt om de memorie van toelichting voor wat betreft het structurele budget voor de taken van de Minister van EZK, te actualiseren (paragraaf 7). Dit structurele budget is verhoogd op basis van het huidige Regeerakkoord.

De waarnemend vice-president van de Raad van State,
S.F.M. Wortmann

Ik moge U verzoeken het hierbij gevoegde voorstel van wet en de gewijzigde memorie van toelichting aan de Tweede Kamer der Staten-Generaal te zenden.

De Minister van Economische Zaken en Klimaat,
M.A.M. Adriaansens