No.W18.22.0068/IV 's-Gravenhage, 20 juli 2022

**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**

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.[[1]](#footnote-1) 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.[[2]](#footnote-2)

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.[[3]](#footnote-3) 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.[[4]](#footnote-4) 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.[[5]](#footnote-5) 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.

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.[[6]](#footnote-6)

De Afdeling adviseert de keuze voor een zelfstandige wet in het licht van het voorgaande te heroverwegen. Ongeacht of de regering vasthoudt aan de introductie van een nieuwe wettelijke regeling, wijst de Afdeling op het volgende.

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.[[7]](#footnote-7) 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.[[8]](#footnote-8)

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.

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.[[9]](#footnote-9) 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.[[10]](#footnote-10)

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.[[11]](#footnote-11) 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.[[12]](#footnote-12)

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 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.[[13]](#footnote-13)

De toelichting bij het wetsvoorstel stelt dat het DTC en het NCSC samenwerken om het risico van onder meer dubbele informatieverstrekking te vermijden.[[14]](#footnote-14) 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.

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.[[15]](#footnote-15)

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 veronachtzamen. 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.[[16]](#footnote-16) 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.

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.[[17]](#footnote-17) 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.[[18]](#footnote-18) 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 bewerkt en welk soort adviezen en analyses worden opgesteld en uitgevoerd.[[19]](#footnote-19) 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.

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.[[20]](#footnote-20) 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 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.[[21]](#footnote-21) Zonder een adequaatheidsbesluit van de Europese Commissie kan niet zonder meer worden uitgegaan van een ‘passend beschermingsniveau’.[[22]](#footnote-22) 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.

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.  
  
  
De waarnemend vice-president van de Raad van State,

1. Memorie van toelichting, paragraaf 2.2 (‘Wettelijke grondslag voor taken en gegevensverwerking Minister van EZK’). [↑](#footnote-ref-1)
2. Voorgesteld artikel 2, eerste lid, onderdeel a. [↑](#footnote-ref-2)
3. Voorgesteld artikel 3, eerste en tweede lid. [↑](#footnote-ref-3)
4. Zie artikel 4 en de artikelen 21 en 22 van de Wbni. [↑](#footnote-ref-4)
5. 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, 36084, nr. 2. [↑](#footnote-ref-5)
6. 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, 36084, nr. 2. [↑](#footnote-ref-6)
7. Memorie van toelichting, paragraaf 2.2 (‘Wettelijke grondslag voor taken en gegevensverwerking Minister van EZK’). [↑](#footnote-ref-7)
8. Zie ook Kamerstukken II 2019/20, 26643 en 30821, nr. 673, p. 4. [↑](#footnote-ref-8)
9. 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’. [↑](#footnote-ref-9)
10. 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, 36084, nr. 2. [↑](#footnote-ref-10)
11. Zie ook punt 2 van het advies van de Afdeling over het aanhangige wetsvoorstel tot wijziging van de Wbni, Kamerstukken II 2021/22, 36084, nr. 4. [↑](#footnote-ref-11)
12. Zie ook het standpunt van de regering hierover, Kamerstukken II2019/20, 26643 en 30821, nr. 673, p. 4. [↑](#footnote-ref-12)
13. 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, 26643, nr. 660. [↑](#footnote-ref-13)
14. Memorie van toelichting, paragraaf 8.2 (‘Afbakening doelgroep van het wetsvoorstel’). [↑](#footnote-ref-14)
15. Kamerstukken II2019/20, 26643 en 30 821, nr. 673, p. 3. [↑](#footnote-ref-15)
16. Onderzoeksraad voor Veiligheid, Kwetsbaar door software. Lessen naar aanleiding van beveiligingslekken door software van Citrix, december 2021, p. 73-100. [↑](#footnote-ref-16)
17. Voorgesteld artikel 2, eerste lid, onderdelen a en b. [↑](#footnote-ref-17)
18. Memorie van toelichting, paragraaf 8.6 (‘Diverse punten’). [↑](#footnote-ref-18)
19. 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. [↑](#footnote-ref-19)
20. Memorie van toelichting, paragraaf 2.4 (‘Toepassing in Caribisch Nederland’). [↑](#footnote-ref-20)
21. Hoofdstuk V van de AVG. [↑](#footnote-ref-21)
22. Kamerstukken II 2019/20, 32761, nr. 161, p. 2. [↑](#footnote-ref-22)