Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2017–2018

34 883 Regels ter implementatie van richtlijn (EU) 2016/1148 (Cybersecuritywet)

Nr. 5

VERSLAG

Vastgesteld 22 maart 2018

De vaste commissie voor Justitie en Veiligheid, belast met het voorbereidend onderzoek van dit voorstel van wet, heeft de eer als volgt verslag uit te brengen. Onder het voorbehoud dat de hierin gestelde vragen en gemaakte opmerkingen voldoende zullen zijn beantwoord, acht de commissie de openbare behandeling van het voorstel van wet genoegzaam voorbereid.

INHOUDSOPGAVE

kst-34883-5
ISSN 0921 - 7371
's-Gravenhage 2018

I. ALGEMEEN

1. Inleiding

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van onderhavig voorstel voor een Cybersecuritywet (hierna: Csw). Zij onderschrijven het belang van het vergoten van de digitale paraatheid en het verkleinen van de gevolgen van cyberincidenten door alle Europese lidstaten. Zij hebben slechts enkele vragen.

De leden van de CDA-fractie hebben met belangstelling kennisgenomen van onderhavig wetsvoorstel. Nederland kende met de Wet gegevensverwerking en meldplicht cybersecurity (Wgmc) al belangrijke regelgeving voor aanbieders van essentiële diensten (AED's). Echter achten voornoemde leden bevordering van eenduidigheid tussen lidstaten op het gebied van netwerk- en informatiebeveiliging van belang gezien het internationale karakter. Deze leden hebben nog enkele vragen.
Allereerst zetten zij grote vraagtekens bij de naam van de wet. Ongeacht het belang van de wet is de reikwijdte niet dermate groot dat het gehele cybersecuritydomein hiermee wordt bereikt. Op het vlak van cybersecurity zijn er veel meer onderwerpen die hier niet aan bod komen. De aan het woord zijnde leden vragen de regering of deze wet gebruikt zal worden als raamwerk voor eventuele verdere wetgeving op het gebied van cybersecurity. Zo nee, is deze naam dan de meest gepaste en bruikbare naam voor de implementatie van de 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 (hierna: NIB-richtlijn)?
De leden van de CDA-fractie vragen aandacht voor de snel naderende implementatietermijn van 9 mei 2018. Ziet de regering reden voor zorg dat de implementatietermijn niet gehaald wordt nu er nog maar zeven weken zijn waarin zowel de Tweede als de Eerste Kamer onderhavig wetsvoorstel behandelen alvorens de deadline is verstreken?

De leden van de D66-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel cybersecuritywet. Deze leden onderschrijven het belang van de NIB-richtlijn ter bevordering van de cybersecurity in Nederland en in de EU. Zij hebben nog enkele vragen en opmerkingen.

De leden van de GroenLinks-fractie delen het belang van een samenhangende en gemeenschappelijke EU-strategie op het beveiligen van netwerk- en informatiesystemen. Het dagelijkse leven van velen speelt zich steeds vaker af via moderne communicatietechnologieën. En steeds meer diensten worden uitsluitend nog via internet aangeboden. Deze ontwikkelingen nopen tot maatregelen om de veiligheid van informatie en netwerken op niveau te houden. Deze leden hebben nog enkele vragen.

De leden van de SP-fractie hebben kennisgenomen van het wetsvoorstel. Zij hebben hierbij enkele vragen en opmerkingen.

De leden van de SGP-fractie hebben kennisgenomen van het wetsvoorstel dat de NIB-richtlijn implementeert. Zij hebben enkele vragen over dit voorstel, met name gericht op de administratieve lasten. Voornoemde leden vinden het belangrijk dat er goede regels zijn voor de beveiliging van informatiesystemen, maar willen tegelijkertijd voorkomen dat er te grote lasten of onveiligheid uit voort vloeien.

2. De NIB-richtlijn

2.1 Reikwijdte

De leden van de VVD-fractie constateren dat daar waar de AED's actief aangewezen moeten worden de regelgeving automatisch geldt voor digitale dienstverleners (DSP's) die binnen de definities vallen. Deze leden vragen op welke wijze organisaties kunnen toetsen of de definitie van een DSP op hen van toepassing is. Kunnen zij in geval van twijfel ergens terecht met hun vragen?

De leden van de CDA-fractie vragen ten aanzien van de reikwijdte van de NIB-richtlijn en het wetsvoorstel of voldoende duidelijk is en zal zijn voor AED's welke werkzaamheden onder de NIB-richtlijn zullen vallen en welke niet.

3. Gemaakte implementatiekeuze op hoofdlijnen

De leden van de CDA-fractie constateren dat er verschillende implementatiekeuzes zijn gemaakt om de NIB-richtlijn te vervatten in nationale wetgeving. Zo merken deze leden op dat er, in afwijking van de NIB-richtlijn, voor een dubbele melding van ernstige ICT-incidenten is gekozen: zowel bij de computer security incident response team (hierna: CSIRT) als bij de bevoegde autoriteit. De Autoriteit Persoonsgegevens merkt in haar advies op dat een meldplichtig Csw-incident ook een datalek kan zijn. Voornoemde leden vragen of het (technisch) mogelijk is dat op het meldformulier ook de mogelijkheid van datalek kan worden opgenomen waarna de melding ook bij de Autoriteit Persoonsgegevens verschijnt.
Daarnaast vragen deze leden of de regering verder kan toelichten waarom er gekozen is voor het aanwijzen van verschillende vakministers als bevoegde autoriteit. Ziet de regering in dat dit wellicht tot fragmentatie kan leiden en tot onduidelijkheid bij de AED's die met de bevoegde autoriteit te maken zullen krijgen? Hoe beziet de regering de mogelijkheid van één bevoegde autoriteit voor handhaving en sanctionering? Bestaan er onder de Wgmc AED's die op basis van de Csw onder verschillende ministeries zullen vallen waardoor zij bij verschillende ministeries melding moeten doen? Hoe gaat de samenwerking tussen de vakministers ten aanzien van deze AED's eruit zien?
Ook lezen de leden van de CDA-fractie dat er een nationale strategie voor de beveiliging van netwerk- en informatiesystemen vastgesteld dient te worden waarin de strategische doelstellingen en concrete beleidsmaatregelen worden bepaald voor de in de bijlage II genoemde sectoren en voor de digitale diensten van bijlage III. Hiervoor wordt de Nationale Cybersecurity Strategie (NCSS) gebruikt. Deze verscheen in 2011 en is in 2013 herzien vanwege snelle ontwikkelingen in het cyberdomein. Is de NCSS uit 2013 thans nog actueel? Met het verschijnen van de Algemene verordening gegevensbescherming (Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG,hierna: AVG), de Csw en binnenkort de e-privacyverordening (COM (2017) 10: voorstel voor een verordening van het Europees Parlement en de Raad met betrekking tot de eerbiediging van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie, en tot intrekking van Richtlijn 2002/58/EG (richtlijn betreffende privacy en elektronische communicatie)) naast de ontwikkelingen op technologisch vlak is er veel veranderd sinds 2013. Geeft dit reden tot actualisering van de NCSS?

De leden van de D66-fractie vragen de regering een overzicht in tabelvorm te maken van de verschillende CSIRTs en bevoegde autoriteiten voor de verschillende relevante sectoren en voor AED's en DSP's.
Voornoemde leden constateren daarnaast dat er sprake is van een dubbele meldplicht in het wetsvoorstel. Zij vragen nader toe te lichten welke maatregelen genomen worden om de lasten voor bedrijven in relatie tot deze dubbele meldplicht zo veel mogelijk te verlagen.

4. Verhouding tot de Wgmc

De leden van de VVD-fractie vragen om een overzicht van alle inhoudelijke verschillen en verschillen in reikwijdte tussen de Wgmc en de Csw. Ook vragen zij of er regels zijn uit de Wgmc die niet overgenomen worden in de Csw en dus zouden komen te vervallen met de intrekking van de Wgmc.

De leden van de D66-fractie vragen de regering nader toe te lichten waarom voorwaarden waaronder vertrouwelijke gegevens met betrekking tot aanbieders verstrekt mogen worden alleen van toepassing zijn op gegevens die gemeld zijn bij het NCSC en niet op gegevens die gemeld zijn bij de bevoegde autoriteit. Daarnaast vragen deze leden waarom dergelijke gegevens gedeeld worden met de Algemene Inlichtingen- en Veiligheidsdienst (hierna: AIVD). Welke organisaties vallen nog meer onder de «beperkte kring»? Kunnen ethisch hackers die melding doen bij de NCSC van onbekende kwetsbaarheden erop vertrouwen dat dergelijke informatie terecht komt bij de maker van de software waarin de onbekende kwetsbaarheid is gevonden, in plaats van bij de AIVD?
Voornoemde leden constateren dat de NIB-richtlijn niet ziet op waterkeringen, maar dat de regering het goed en continu functioneren van bepaalde waterkeringen wel als vitaal voor Nederland ziet. De Minister van Infrastructuur en Waterstaat blijft volgens de regering voor die waterkeringen een vitale aanbieder. Hoe verhoudt de Minister zich in dit kader tot de waterschappen die verantwoordelijk zijn voor het beheer van waterkeringen? Ziet de regering andere diensten van de waterschappen, zoals waterzuiveringsinstallaties, niet als vitaal?

De leden van de SP-fractie vragen de regering toe te lichten waarom primaire waterkeringen die onder beheer van waterschappen vallen niet vallen onder de reikwijdte van het wetsvoorstel, terwijl dit wel geldt voor de waterkeringen die rechtstreeks onder de Minister van Infrastructuur en Waterstaat vallen. Deze leden merken hierbij tevens op dat het proces »keren en beheren waterkwantiteit» wel als vitaal is aangemerkt door de Nationaal Coördinator Terrorismebestrijding en Veiligheid. Deze leden zijn benieuwd of het uitsluiten van waterschappen zal leiden tot vermijdbare risico's.

5. Digitale dienstverleners

5.1 Aanhef

De leden van de CDA-fractie lezen dat in de NIB-richtlijn definities zijn opgenomen van drie soorten digitale diensten die onder de richtlijn vallen. Hiervoor is geen verdere regelgeving vereist, er dient uit de overwegingen van de NIB-richtlijn te worden opgemaakt of een digitale dienst onder de richtlijn valt. Hoe beoordeelt de regering de zorgen uit de praktijk dat onvoldoende duidelijk is welke bedrijven een digitale dienstverlener zijn? Is het mogelijk dat bedrijven in één jaar wel kunnen worden aangemerkt als digitale dienstverlener, waarna zij in een volgend jaar (na wijziging van de bedrijfsactiviteiten) niet meer een digitale

dienstverlener zijn? Hoe wordt de voorlichting aan bedrijven op dit gebied vormgegeven?

5.2 Cloudcomputerdiensten

De leden van de D66-fractie vragen de regering nader toe te lichten of de huidige definitie van cloud computerdiensten niet te breed is en voldoende rekening houdt met de verschillende niveaus van criticaliteit van IaaS, PaaS en SaaS.

5.3 Omzet- en personeelseisen DSP's

De leden van de D66-fractie vragen de regering waarom de beveiligingseisen van de verplichting om ernstige incidenten te melden gelden voor DSP's met meer dan 50 medewerkers en een omzet hoger dan 10 miljoen euro per jaar. Is het niet zo dat er ook DSP's denkbaar zijn die vitale diensten leveren met een omzet hoger dan 10 mln. euro, maar minder dan 50 medewerkers hebben?

De leden van de SP-fractie lezen in het wetsvoorstel en de memorie van toelichting dat kleine en micro-ondernemingen krachtens de richtlijn zijn uitgezonderd van de verplichtingen die volgen uit het zijn van een digitale dienstverlener. Deze leden zijn benieuwd met welke argumentatie deze uitzondering is gecreëerd en vragen de regering toe te lichten welke gevolgen deze uitzondering heeft voor de veiligheid die dit wetsvoorstel tracht te waarborgen. Deze leden zijn tevens benieuwd hoe de veiligheid van de dienstverlening van deze groep organisaties alsnog kan worden gewaarborgd. Daarnaast zijn deze leden benieuwd of deze maatregel zal leiden tot het minder vaak inschakelen van kleine en micro-ondernemingen omdat deze als gevolg van de uitzondering niet onder de Cybersecuritywet vallen. Tevens zijn deze leden benieuwd hoeveel kleine en micro-ondernemingen nu onder de noemer digitale dienstverlener vallen, in welke mate deze bedrijven wel onder de huidige wet vallen en of sprake is van verminderde veiligheid als gevolg van de implementatie van deze richtlijn.

6. Relatie met sectorale wetten en bevoegdheden

6.1 Ministerie van Volksgezondheid, Welzijn en Sport

De leden van de CDA-fractie zien dat de reikwijdte van de regelgeving ook onderdeel is van de gezondheidszorg. Uit recente ervaringen met cyberaanvallen blijkt dat bij gezondheidszorginstanties de beveiliging niet altijd op orde is. Wordt er naar aanleiding van invoering van het onderhavige wetsvoorstel en van kracht gaan van de NIB-richtlijn ook een nulmeting uitgevoerd ten aanzien van de gezondheidszorgsector? Met name waar het gaat om ziekenhuizen? Zo nee, hoe kan dan beoordeeld worden of de beveiliging op dit moment op orde is? Wordt er in andere sectoren een nulmeting gedaan?

De leden van de D66-fractie vragen de regering nader toe te lichten waarom bepaalde zorgaanbieders, zoals ziekenhuizen, niet worden aangewezen als AED. In het recente verleden zijn er immers meerdere voorbeelden geweest van cyberaanvallen, die ook ziekenhuizen raakten en die grote gevolgen hadden voor de mogelijkheid om zorg te verlenen.

7. Handhaving (toezicht en sancties)

De leden van de CDA-fractie lezen dat de bevoegde autoriteit over instrumentarium uit de Algemene wet bestuursrecht beschikt wat betreft de handhaving ten aanzien van de verplichtingen voor de AED's en DSP's. Nu er enerzijds verplichtingen voortvloeien uit de Csw en anderzijds uit de Wgmc vragen deze leden of de handhaving van beide verplichtingen op dezelfde wijze verloopt. Beschikt men over dezelfde bevoegdheden? Ook wat betreft de bindende aanwijzing en bestuurlijke herstelsancties?

De Csw maakt mogelijk dat AED's een zogenoemde audit opgelegd kunnen worden. Dient er sprake te zijn van enige aanleiding om over te gaan tot het opleggen van een audit of kan dit ook periodiek worden ingesteld? Ook vragen deze leden waarom er geen audits voor DSP's mogelijk zijn? De leden lezen dat de AED zelf de kosten van de audit draagt tenzij anders bij algemene maatregel van bestuur (hierna: amvb) bepaald. Is de regering voornemens om dit per amvb te wijzigen? Daarnaast vragen de aan het woord zijnde leden in welke gevallen de bevoegde autoriteit zelf de audit zal uitvoeren, zeker nu de kosten dan voor zijn rekening zullen komen.

Ook constateren de leden dat het uiteindelijk mogelijk is om bij overtreding van de normen bestuurlijke boetes op te leggen. Er is gekozen voor de maximale hoogte van een boete zoals geregeld is in de Wet op het financieel toezicht. In de memorie van toelichting lezen de aan het woord zijnde leden dat er grote verschillen bestaan tussen de boeteplafonds in sectorale wetgeving. Wat voor reden ligt hieraan ten grondslag? Is een lager boeteplafond in bepaalde sectoren gewenst en zo ja, zal er dan bij het opleggen van een bestuurlijke boete rekening worden gehouden met de sector waar de overtreding plaatsvindt?

Verder hebben voornoemde leden nog vragen over schadevergoedingen naar aanleiding van cyberaanvallen. Welke mogelijkheden zijn er voor personen die schade ondervinden van een cyberaanval die vermeden had kunnen worden als de beveiliging van een AED of DSP op orde was? Is dan nog relevant of een AED een bestuurlijke boete opgelegd is vanwege het niet op orde hebben van beveiliging? Geeft dit grond voor schadevergoeding in het geval van schade?

8. Consultatiereacties

De leden van de CDA-fractie lezen dat de regering ingaat op het advies van Nederland ICT om het Digital Trust Centre op termijn aan te merken als CSIRT. Daarbij geeft Nederland ICT aan dat er op dit moment sprake is van 37 verschillende meldplichten die in het geval van organisaties die onder verschillende meldplichten vallen tot een ongewenste administratieve last vallen. Deze leden vragen de regering in te gaan op de wenselijkheid van zoveel verschillende meldplichten. Ongeacht van de praktische uitwerking door het te beleggen bij het Digital Trust Centre vragen voornoemde leden naar de wenselijkheid van centralisatie van meldingen die voortvloeien uit verschillende richtlijnen en wetgeving.

De leden van de SP-fractie merken op dat de Autoriteit Persoonsgegevens heeft geadviseerd andere partijen dan vitale aanbieders en digitale dienstverleners onder het wetsvoorstel te laten vallen. Zij merken op dat de regering aangeeft dat via het Digital Trust Centre andere partijen kunnen worden ondersteund op het vlak van cybersecurity en merken tevens met instemming op dat zij het Digital Trust Centre niet als computercrisisteam in wil zetten voor toezicht en handhaving bij de niet-vitale processen. Deze leden zijn echter benieuwd of en hoe de

regering verdere invulling wil geven aan dit advies van de Autoriteit Persoonsgegevens en vragen de regering tevens haar beweegredenen aan te geven indien zij het advies niet opvolgt.

De leden van de SGP-fractie begrijpen dat het de bedoeling is de dubbele meldplicht zoveel mogelijk te kunnen laten plaatsvinden door één handeling. In dit licht vragen zij in hoeverre het waar is dat er – zoals uit consultatiereacties blijkt – er wel sprake is van tientallen meldplichten, afhankelijk van de verschillende sectoren. Deze leden vragen of er mogelijkheden zijn dit aantal meldplichten terug te dringen dan wel ervoor te zorgen dat meldingen die betrekking hebben op één incident in één keer gedaan kunnen worden bij de verschillende instanties, om de administratieve lasten zoveel mogelijk te beperken.

9. Grondrechtentoets

De leden van de SP-fractie merken op dat de regering in de memorie van toelichting aangeeft nog geen CSIRT aan te wijzen voor digitale dienstverleners. Zij menen dat deze taak een der belangrijkste is uit het wetsvoorstel en vragen de regering toe te lichten welke organisatie zij in gedachten heeft voor deze functie of welke criteria zij wil hanteren voor het aanwijzen van deze CSIRT.

10. Gevolgen voor de rijksbegroting

De leden van de VVD-fractie lezen dat de dekking voor de kosten die gepaard gaan met de Csw voor het Ministerie van Economische Zaken en Klimaat en het Ministerie van Infrastructuur en Waterstaat geregeld wordt bij de voorjaarnota 2018. Betekent dit dat deze dekking nu al geregeld is bij voorjaarnota? De voorjaarnota 2018 is de Kamer immers nog niet bekend. En als dit niet het geval is, wat zijn dan de gevolgen voor de rijksbegroting en voor de uitvoering van de Csw-taken door de beide ministeries als het niet lukt om de benodigde dekking te regelen bij de voorjaarsnota?

II. ARTIKELSGEWIJS

Artikel 5

De leden van de SGP-fractie vragen of inzichtelijk gemaakt kan worden welke aanbieders en groepen van aanbieders respectievelijk zullen worden aangewezen als essentiële dienst en als vitale aanbieder. Kan tevens een nadere duiding worden gegeven van het precieze verschil tussen beide begrippen? Wat is het criterium om vast te stellen of een dienst alleen een vitale dienst is of ook een essentiële dienst? Wanneer is iets een essentiële dienst en wanneer een vitale dienst? Wat zijn de consequenties hiervan voor de praktijk?[1]

Artikel 9

De leden van de D66-fractie constateren dat artikel 9 Csw de bevoegdheid geeft om bij of krachtens amvb nadere regels te stellen over de te treffen beveiligingsmaatregelen. Is de regering voornemens dergelijke nadere regels te stellen?

---

[1] Dit zou ook onder 2.1 Reikwijdte kunnen worden gezet.

Artikel 18

De leden van de GroenLinks-fractie vragen waarom ervoor gekozen is het aan de rechtspersoon of het orgaan over te laten om er al dan niet voor te kiezen de gevraagde persoonsgegevens aan de Minister van Justitie en Veiligheid te verstrekken, ook al gaat het om persoonsgegevens waarvan verstrekking onverenigbaar is met de doeleinden waarvoor deze gegevens zijn verzameld. Het roept eveneens de vraag op wat vervolgens met deze verstrekte persoonsgegevens kan worden gedaan. Wie heeft bijvoorbeeld toegang tot deze gegevens, met wie kunnen deze gegevens worden gedeeld en staat deze bevoegdheid in verhouding tot het te bereiken doel. Voornoemde leden vragen de regering kortom naar een analyse van de noodzakelijkheid en proportionaliteit van deze wettelijke mogelijkheid om te verzoeken om persoonsgegevens waarvan verstrekking in strijd is met het beginsel van doelbinding.
Uit de memorie van toelichting maken deze leden op dat de Autoriteit Persoonsgegevens en de krachtens de AVG in te stellen departementale functionaris voor de gegevensbescherming toezicht zullen houden op de verwerkingen. Op welke wijze wordt de Autoriteit Persoonsgegevens in staat gesteld om alomvattend toe te zien op de naleving? En waarom wordt in de bedoelde passage van de memorie van toelichting onderscheid gemaakt naar verwerking van persoonsgegevens en andere gegevens, zoals vertrouwelijke bedrijfsgegevens? Klopt het dat alle gegevens vernietigd zullen worden zodra de verwerking ervan niet meer noodzakelijk is voor de uitoefening van die taken?

Artikel 20

De leden van de SGP-fractie vragen aandacht voor de openbaarheid van mogelijk vertrouwelijke gegevens en problemen met de beveiliging. Door diverse instanties is er aandacht voor gevraagd dat op grond van een verzoek in het kader van de Wet openbaarheid van bestuur (hierna: Wob) op geen enkele wijze gegevens openbaar moeten komen die duidelijk maken waar en bij wat voor (soort) bedrijf kwetsbaarheden in de beveiliging zijn. In hoeverre is op grond van dit wetsvoorstel en de uitzonderinggronden in de Wob volledig gewaarborgd dat deze gegevens niet openbaar worden? In hoeverre gaat het om vertrouwelijke bedrijfsgegevens dan wel om beveiligingsgegevens? Kunnen beide wetten in de uitwerking nog botsen?
Voornoemde leden vragen over het vierde lid van artikel 20 of het niet gewenst is om de opmerking uit de memorie van toelichting dat het «in beginsel slechts in uitzonderlijke gevallen nodig is om herleidbare gegevens te verstrekken» niet in de wettekst opgenomen dient te worden.

Artikel 23

De leden van de GroenLinks-fractie kunnen zich onder omstandigheden voorstellen dat het voor de publieke bewustwording en het voorkomen en/of beheersen van incidenten nodig is de openbaarheid te zoeken. Tegelijkertijd vragen deze leden of met het oog op transparantie van de toepassing van de Csw de bevoegde autoriteit zou moeten voorzien in een jaarlijks verslag, waarin geaggregeerde informatie wordt geboden over bijvoorbeeld de aard en de omvang van incidenten en meldingen.

De voorzitter van de commissie,
Van Meenen

Adjunct-griffier van de commissie,
Schoor