Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2017–2018

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

Nr. 6

NOTA NAAR AANLEIDING VAN HET VERSLAG

Ontvangen 25 april 2018

I. Algemeen

1. Inleiding

Met belangstelling heb ik kennis genomen van het verslag van de vaste commissie voor Justitie en Veiligheid over het wetsvoorstel houdende regels ter implementatie van richtlijn (EU) 2016/1148 (Cybersecuritywet, hierna ook: Csw). Graag maak ik van de gelegenheid gebruik om de gestelde vragen te beantwoorden en op enkele punten een nadere toelichting te geven. Bij de beantwoording heb ik de volgorde van het verslag aangehouden. Waar dit de helderheid en overzichtelijkheid ten goede kwam, heb ik vragen samengenomen in de beantwoording.

De leden van de CDA-fractie vragen of deze wet gebruikt zal worden als raamwerk voor eventuele verdere wetgeving op het gebied van cybersecurity. Zo nee, is «Cybersecuritywet» dan een geschikte naam voor de implementatie van de NIB-richtlijn?

Bij eventuele verdere wetgeving over cybersecurity zal per geval worden bekeken welke wet daarvoor geschikt is. Als citeertitel is Cybersecuritywet gekozen omdat het wetsvoorstel zowel over de beveiliging van ICT gaat als over de verwerking van gegevens en over een meldplicht, en omdat de citeertitel Wet gegevensverwerking en meldplicht cybersecurity (Wgmc) te lang is om daar nog een derde onderwerp aan toe te voegen. Door de incorporatie – zonder materiële wijzigingen – van de bepalingen van de Wgmc in de Csw regelt de Csw overigens ook andere onderwerpen dan alleen de implementatie van de NIB-richtlijn, zoals de plicht voor buiten de NIB-richtlijn vallende vitale aanbieders («andere vitale aanbieders» in de zin van artikel 5, eerste lid, onder b, Csw) om ernstige inbreuken op de beveiliging te melden bij het NCSC.

De genoemde leden 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

kst-34883-6
ISSN 0921 - 7371
's-Gravenhage 2018

waarin zowel de Tweede als de Eerste Kamer onderhavig wetsvoorstel behandelen alvorens de deadline is verstreken?

Enige overschrijding van de implementatietermijn is inmiddels onvermijdelijk. Voor aanbieders van een essentiële dienst (AED) eindigt de implementatietermijn overigens materieel een half jaar later, op 9 november 2018.[1] Als het parlement het wetsvoorstel voor het zomerreces aanvaardt, dan kan de Csw in de zomer met een beperkte vertraging in werking treden voor het centrale contactpunt, voor digitaledienstverleners (DSP's) en voor de vrijwillige melding van incidenten (artikel 16 Csw) en op 9 november 2018 op tijd voor AED's en andere meldplichtige vitale aanbieders. Om dit ook juridisch-technisch mogelijk te maken, heb ik bij nota van wijziging artikel 35 Csw (over de inwerkingtreding van de Csw) aangepast. De Wgmc en het Besluit meldplicht cybersecurity (Bmc), die geen regels stellen over DSP's, blijven gelden tot 9 november 2018.

2. De NIB-richtlijn

2.1 Reikwijdte

De leden van de VVD-fractie 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?

Ik betrek in mijn antwoord ook de vraag van de leden van de CDA-fractie over de zorgen uit de praktijk dat onvoldoende duidelijk is welke bedrijven als DSP onder de NIB-richtlijn en dus onder de Csw vallen. De Minister van Economische Zaken en Klimaat beziet nog op welke manier aan digitaledienstverleners tijdig over de Csw kan worden gecommuniceerd, zodat zij – bijvoorbeeld aan de hand van een checklist of overzicht – eenvoudiger kunnen nagaan of zij onder de Csw vallen. Onderdeel hiervan betreft de toetsing in hoeverre een onderneming die een digitale dienst aanbiedt (een onlinemarktplaats, onlinezoekmachine of cloudcomputerdienst) als DSP moet worden aangemerkt. Hierbij wordt ook betrokken waar men terecht kan met vragen. Onderzocht wordt ook of een lijst kan worden bijgehouden van DSP's.

De leden van de CDA-fractie vragen of voor AED's voldoende duidelijk is welke werkzaamheden onder de NIB-richtlijn vallen en welke niet.

Een AED valt alleen onder de NIB-richtlijn voor zover hij een essentiële dienst aanbiedt, dus niet voor eventuele andere diensten die hij aanbiedt. Wat wel en niet een essentiële dienst is, volgt uit bijlage II bij de richtlijn en uit de aanwijzing op grond van artikel 5 Csw. Die aanwijzing zal vergelijkbaar zijn met de manier waarop meldplichtige vitale aanbieders nu zijn aangewezen bij of krachtens het Bmc, waarin een tabel is opgenomen met kolommen voor sector, vitale aanbieder en product of dienst. Financiële instellingen worden bijvoorbeeld alleen aangewezen voor zover zij betalings- of effectenverkeer afwikkelen. Zij vallen dus bijvoorbeeld niet onder de Csw voor zover zij financieel advies geven. Mij hebben tot nu toe geen signalen bereikt dat de betrokken organisaties onzeker zouden zijn over de precieze reikwijdte van de aanwijzing. Net als het Bmc zal ook de «opvolger» van het Bmc een algemene maatregel van bestuur (amvb) zijn, die wordt gepubliceerd in het Staatsblad.

[1] Strikt genomen geldt dat half jaar extra alleen voor het aanwijzen van AED's, zie artikel 5, eerste lid, van de NIB-richtlijn. Maar zolang de AED's nog niet zijn aangewezen, kunnen de voor hen geldende bepalingen uiteraard nog niet in werking treden.

3. Gemaakte implementatiekeuze op hoofdlijnen

De leden van de D66-fractie vragen nader toe te lichten welke maatregelen genomen worden om de lasten voor bedrijven in relatie tot de dubbele meldplicht zo veel mogelijk te verlagen. De leden van de CDA-fractie vragen of het (technisch) mogelijk is, voor het geval dat een meldplichtig Csw-incident tevens een datalek is, dat het Csw-meldformulier ook kan worden gebruikt om het datalek te melden bij de Autoriteit persoonsgegevens.

Op dit moment wordt onderzocht of de meldingen binnen dit wetsvoorstel kunnen worden gedaan door één handeling en zo ja, hoe en op welke termijn. De regering vindt het wenselijk om de meldprocessen van verschillende meldplichten zo veel mogelijk op elkaar af te stemmen, om onnodige administratieve lasten te voorkomen. Wel wil de regering eerst voorrang geven aan het inrichten van de meldprocessen die vallen onder het wetsvoorstel. Mogelijk kan vervolgens, op basis van opgedane ervaringen, bekeken worden of stroomlijning met andere verplichte meldingen, zoals die bij de Autoriteit persoonsgegevens, wenselijk en haalbaar is. Daarbij speelt ook de vraag in welke mate er overlap is van te verstrekken gegevens tussen verschillende cybersecurity-gerelateerde meldplichten zoals die bij de Autoriteit persoonsgegevens. De door de leden van de CDA-fractie gedane suggestie zal bij de verdere implementatie van het meldproces voor AED's en DSP's worden meegenomen.

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?

Voor de in het wetsvoorstel gemaakte keuze heeft de doorslag gegeven dat de vakministers en DNB voor de meeste sectoren van bijlage II van de NIB-richtlijn nu al de toezichthouder zijn voor zover het gaat om bestaande sectorale wetgeving. Voor die sectoren heeft aanwijzing van de vakministers en DNB als bevoegde autoriteit het voordeel dat het cybersecurity-toezicht kan worden ingebed in het bestaande sectorale toezicht, zodat de betrokken AED's er niet een toezichthouder bij krijgen. Cybersecurity dient de beschikbaarheid en betrouwbaarheid van de dienst. Dat zijn belangen die de vakministers en DNB zich bij uitstek aantrekken. Zij hebben ook meer sectorspecifieke kennis dan een centrale cybersecurity-toezichthouder zou kunnen verwerven. Fragmentatie zal zo veel mogelijk worden voorkomen door de samenwerking tussen de bevoegde autoriteiten te stimuleren, uiteraard met inachtneming van wetgeving over verstrekken van informatie aan derden, zoals het Csw-regime voor het verstrekken van vertrouwelijke gegevens (artikel 22).

De leden van de CDA-fractie vragen of er onder de Wgmc AED's bestaan 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?

Er wordt niet voorzien dat een AED onder meer dan één bevoegde autoriteit zal vallen. In die zin is dus geen afstemming nodig tussen de vakministers. Wel zou zich de situatie kunnen voordoen dat een DSP een incident moet melden bij de Minister van Economische Zaken en Klimaat (op grond van artikel 13, eerste lid, onder b, Csw) en een AED datzelfde incident moet melden bij de bevoegde autoriteit waar die AED onder valt

(op grond van artikel 10, derde lid, Csw). Het gaat dan om een situatie (zoals voorzien in artikel 16, vijfde lid, van de NIB-richtlijn) dat een AED voor de verlening van de essentiële dienst afhankelijk is van een digitale dienst als bedoeld in bijlage III bij de NIB-richtlijn (zoals een cloudcomputerdienst), en een meldplichtig incident bij de verlener van die digitale dienst ook aanzienlijke gevolgen heeft voor de essentiële dienst. In dat geval zullen beide bevoegde autoriteiten, met inachtneming van wetgeving over verstrekken van informatie aan derden, zoals artikel 22 Csw, met elkaar afstemmen om tegenstrijdig handelen te voorkomen.

Ook vragen de leden van de CDA-fractie of de Nationale Cyber Security Strategie (NCSS) uit 2013 nog actueel is. Met het verschijnen van de Algemene verordening gegevensbescherming (AVG), de Csw en binnenkort de e-privacyverordening, en naast de ontwikkelingen op technologisch vlak is er veel veranderd sinds 2013.

In het regeerakkoord is een ambitieuze Nederlandse cybersecurityagenda (NCSA) aangekondigd, die onlangs aan de Tweede Kamer is aangeboden. De NCSA bouwt voort op de resultaten die bereikt zijn met NCSS 1 uit 2011 en NCSS 2 uit 2013, en zij vervangt NCSS 2. De visie van deze strategieën is nog actueel en blijft leidend in de Nederlandse inzet: »*Nederland zet samen met zijn internationale partners in op een veilig en open cyberdomein, waarin de kansen die digitalisering onze samenleving biedt, volop worden benut, aan dreigingen het hoofd wordt geboden en fundamentele rechten en waarden worden beschermd.*» De NCSA geeft een gezamenlijke koers aan, waardoor het voor overheden en private partijen inzichtelijker wordt waarop zij (afgestemde) activiteiten kunnen richten. De NCSA beziet verschillende maatregelen in samenhang, verbindt ze in richtinggevende doelstellingen en versterkt zo het effect van de maatregelen. Daarmee blijft Nederland voorop lopen in zijn aanpak van cybersecurity. De NCSA ziet niet specifiek op thema's als de AVG en e-privacy maar bevat de notie dat cybersecurity niet geïsoleerd wordt benaderd maar nadrukkelijk in samenhang wordt bezien met onderwerpen als fundamentele rechten en waarden. Burgers moeten erop kunnen rekenen dat hun grondrechten zowel online als offline gewaarborgd zijn.

De leden van de D66-fractie vragen de regering een overzicht in tabelvorm te maken van de verschillende CSIRT's en bevoegde autoriteiten voor de verschillende relevante sectoren en voor AED's en DSP's.

Die vraag levert de volgende twee tabellen op.

Bevoegde autoriteit	**Sector of soort dienst**
Onze Minister van Economische Zaken en Klimaat	energie digitale infrastructuur digitale diensten als bedoeld in bijlage III bij de NIB-richtlijn (onlinemarktplaats, onlinezoekmachine of cloudcomputerdienst)
De Nederlandsche Bank N.V.	bankwezen infrastructuur voor de financiële markt
Onze Minister van Infrastructuur en Waterstaat	vervoer levering en distributie van drinkwater
Onze Minister voor Medische Zorg	gezondheidszorg

CSIRT	Categorie
Onze Minister van Justitie en Veiligheid	AED's
Nog nader te bepalen bij koninklijk besluit (zie de nota van wijziging)	DSP's

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 Wgmc wordt beleidsneutraal, zonder materiële wijzigingen, geïncorporeerd in de Csw en in verband daarmee ingetrokken. Alle Wgmc-regels komen materieel terug in de Csw. Nieuw zijn de volgende bepalingen ter implementatie van de NIB-richtlijn:

1. de verplichting voor AED's om ernstige incidenten ook te melden bij de bevoegde autoriteit;
2. de verplichting voor DSP's om ernstige incidenten te melden bij het CSIRT voor DSP's en bij de bevoegde autoriteit;
3. de behandeling van niet-meldplichtige incidenten;
4. beveiligingsverplichtingen voor AED's en DSP's;
5. bepalingen over de taken van het centrale contactpunt voor Nederland, het CSIRT voor DSP's en de bevoegde autoriteit, over de verwerking van persoonsgegevens door die instanties en over de verstrekking door hen van incidentinformatie en vertrouwelijke gegevens over aanbieders;
6. voor AED's en DSP's: bepalingen over toezicht en sancties.

Zie nader de volgende tabel.

Overeenkomsten en verschillen tussen Wgmc en Csw

Bepaling Csw	Bepaling Wgmc	Toelichting
Artikel 1 Csw	Artikel 1 Wgmc	Van diverse begrippen uit de NIB-richtlijn zijn definities toegevoegd. De Csw voegt AED's als subgroep toe aan het Wgmc-begrip vitale aanbieder.
Artikel 2 Csw	nvt	Art. 2 Csw wijst de Minister van JenV aan als centraal contactpunt; CSIRT voor AED's; instantie voor vrijwillige meldingen.
Artikel 3 Csw	Artikel 2 Wgmc	T.o.v. art. 2 Wgmc is art. 3 Csw uitgebreid met de drie in art. 2 Csw genoemde taken.
Artikel 4 Csw	nvt	Art. 4 Csw wijst de vakministers en DNB aan als bevoegde autoriteit en geeft hun de bijbehorende taken, en regelt de aanwijzing van het CSIRT voor DSP's.
Artikel 5 Csw	Artikel 5 Wgmc	Aanwijzing o.g.v. art. 5 Wgmc betekent dat de vitale aanbieder onder de meldplicht bij het NCSC valt.
	nvt	Aanwijzing o.g.v. art. 5 Csw betekent voor een AED dat hij daarnaast moet voldoen aan de beveiligingsverplichtingen van art. 7–9 Csw en de meldplicht bij de bevoegde autoriteit.
Artikel 6 Csw	nvt	Art. 6 Csw implementeert art. 1 lid 7 NIB-richtlijn en voorkomt onnodige dubbeling met eventuele sectorspecifieke EU-regels.
Artikelen 7, 8 en 9 Csw	nvt	Beveiligingsverplichtingen voor AED's en DSP's.

Bepaling Csw	Bepaling Wgmc	Toelichting
Artikel 10 lid 1 en 2 Csw	Artikel 6 lid 1 Wgmc	Art. 6 Wgmc verplicht aangewezen vitale aanbieders om een ernstige inbreuk of een verlies van integriteit te melden bij het NCSC, inclusief bijna-ongelukken. Art. 10 Csw voegt daar voor AED's aan toe dat een ernstig incident (exclusief een bijna-ongeluk) ook moet worden gemeld bij de bevoegde autoriteit. Art. 6 Wgmc («inbreuk») geldt niet voor een DDoS-aanval, art. 10 lid 1 onder a Csw wel («incident»), maar alleen als zo'n aanval aanzienlijke gevolgen heeft voor de continuïteit. Een bijna-ongeluk na een DDoS-aanval blijft uitgezonderd van de meldplicht bij het NCSC (artikel 10 lid 1 onder b Csw).
Artikel 10 lid 3 en 5 Csw	nvt	Deze bepalingen implementeren art. 16 lid 5 NIB-richtlijn (meldplicht AED bij incident DSP).
Artikel 10 lid 4	nvt	Deze bepaling implementeert art. 14 lid 4 NIB-richtlijn.
Artikel 11 Csw	Artikel 6 lid 2 Wgmc	Art. 11 Csw is terminologisch aangepast aan de NIB-richtlijn («melding» en «incident»).
Artikel 12 lid 1 Csw	Artikel 7 Wgmc	Terminologisch aangepast aan de NIB-richtlijn («melding», «continuïteit», «netwerk- en informatie-systemen»).
Artikel 12 lid 2 Csw	nvt	Deze bepaling regelt de situatie waarin de aanbieder een incident alleen heeft gemeld bij de sectorale bevoegde autoriteit en (in afwijking van artikel 10, eerste of derde lid, Csw) niet ook bij het NCSC.
Artikelen 13 en 14 Csw	nvt	Meldplicht DSP's.
Artikel 15 Csw	Artikel 8 Wgmc	Mogelijkheid van nadere regels over de meldplicht.
Artikel 16 Csw	nvt	Vrijwillige melding van incidenten, implementatie van art. 20 NIB-richtlijn.
Artikel 17 lid 1 Csw	Artikel 3 Wgmc	Reikwijdte aangepast aan art. 3 Csw, terminologie aangepast aan de Algemene verordening gegevens-bescherming.
Artikel 17 lid 2 en 3 Csw	nvt	Verwerking persoonsgegevens door de bevoegde autoriteit en het CSIRT voor DSP's.
Artikel 18 Csw	Artikel 4 Wgmc	Reikwijdte aangepast aan art. 3 Csw, formulering aangepast aan de Algemene verordening gegevens-bescherming.
Artikel 19 Csw	nvt	Implementatie van art. 10 lid 3, 14 lid 5 en 16 lid 6 NIB-richtlijn.
Artikel 20 Csw	Artikel 9 Wgmc	Zie voor de verschillen de gedetailleerde opsomming in de memorie van toelichting, Kamerstukken 34 883, nr. 3, p. 50–51.
Artikelen 21 en 22 Csw	nvt	Deze bepalingen zijn vergelijkbaar met art. 20 Csw en regelen de verstrekking van vertrouwelijke gegevens door het CSIRT voor DSP's en door de bevoegde autoriteit.
Artikel 23 Csw	nvt	Implementatie van art. 14 lid 6 en 16 lid 7 NIB-richtlijn.
Artikelen 24–29 Csw	nvt	Implementatie van art. 15, 17 en 21 NIB-richtlijn.
Artikel 30–34 Csw	nvt	Diverse juridisch-technische bepalingen.
Artikel 35 Csw	Artikel 10 Wgmc	Inwerkingtreding
Artikel 36 Csw	Artikel 11 Wgmc	Citeertitel

De leden van de D66-fractie vragen 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.

Dat is een misverstand. Ook artikel 22 Csw (over de bevoegde autoriteit) stelt voorwaarden waaronder vertrouwelijke gegevens met betrekking tot aanbieders verstrekt mogen worden aan derden. De passage in de memorie van toelichting die aanleiding geeft voor de vraag van deze leden (p. 6 midden) staat in een paragraaf over de Wgmc-bepalingen die

zonder materiële wijzigingen worden geïncorporeerd in de Csw. De Wgmc bevat geen regels over de bevoegde autoriteit.

Daarnaast vragen deze leden waarom dergelijke gegevens gedeeld worden met de Algemene Inlichtingen- en Veiligheidsdienst (hierna: AIVD).

Vertrouwelijke gegevens met betrekking tot aanbieders worden aan de AIVD en de MIVD verstrekt in het belang van de nationale veiligheid, ten behoeve van de uitvoering van de taken die aan die diensten zijn opgedragen.

Verder vragen deze leden welke organisaties nog meer vallen onder de «beperkte kring».

Deze vraag reageert op de passage in de memorie van toelichting die uitlegt aan wie en onder welke voorwaarden de Minister van Justitie en Veiligheid, ter uitvoering van de in artikel 3 Csw bedoelde taken, vertrouwelijke herleidbare gegevens met betrekking tot aanbieders mag verstrekken. Dat regime is opgenomen in artikel 20 Csw, dat voor een groot deel identiek is aan artikel 9 Wgmc. Een uitgebreide beschrijving van de precieze reikwijdte van artikel 20 Csw is opgenomen in de artikelsgewijze toelichting. Naast verstrekking aan AIVD en MIVD biedt artikel 20 Csw onder voorwaarden ruimte voor verstrekking van vertrouwelijke herleidbare gegevens met betrekking tot aanbieders aan CSIRT's en aan andere daartoe bij ministeriële regeling aangewezen computercrisisteams (tweede lid), aan de bevoegde autoriteit of een (andere) betrokken Minister (derde lid en vierde lid, onder a) en aan andere organisaties of het publiek (vierde lid, onder b).

Ook vragen deze leden of ethische hackers die melding doen bij de NCSC van onbekende kwetsbaarheden erop kunnen vertrouwen dat dergelijke informatie terecht komt bij de maker van de software waarin de onbekende kwetsbaarheid is gevonden, in plaats van bij de AIVD.

De toenmalige Staatssecretaris van Veiligheid en Justitie heeft in het algemeen overleg met de Tweede Kamer op 20 januari 2016 het belang van meldingen door ethische hackers in het kader van responsible disclosure benadrukt.[2] Het NCSC behandelt elke melding vertrouwelijk. Het NCSC kan waar nodig bemiddelen om ethische hackers in contact te brengen met de bedrijven waarvan het de kwetsbaarheid (in producten bijvoorbeeld) betreft. De AIVD (en MIVD) voorzien van informatie over een onbekende kwetsbaarheid kan geschieden in het belang van het kunnen vervullen van hun wettelijke taken in het belang van de nationale veiligheid. Het NCSC zal altijd met de melder contact opnemen om de kwetsbaarheid te bespreken en te overleggen over te zetten stappen.

Ten slotte lezen de leden van de D66-fractie dat de Minister van Infrastructuur en Waterstaat (IenW) voor bepaalde waterkeringen een vitale aanbieder blijft. Zij vragen hoe die Minister zich in dit kader verhoudt tot de waterschappen die verantwoordelijk zijn voor het beheer van waterkeringen? De leden van de SP-fractie vragen 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 IenW vallen.

---

[2] Kamerstukken II 2015/16, 29 544, nr. 702.

De Csw ziet zowel op aanbieders van een essentiële dienst in de zin van de NIB-richtlijn als op andere voor Nederland vitale aanbieders. Voor die laatste categorie aanbieders waren in de Wgmc al regels gegeven, die nu beleidsneutraal in de Csw zijn opgenomen. Tot die groep behoren thans de door de Minister van IenW aangewezen waterkeringen of onderdelen daarvan. Op dit moment zijn geen keringen van waterschappen aangewezen. Het gaat bij de aanwijzing alleen om die objecten waar de gevolgen van falen het grootst zijn. De Minister van IenW heeft onlangs met de waterschappen afgesproken om een addendum op het Bestuursakkoord Water (BAW) op te stellen met daarin een besluitvormende agenda voor onder meer cybersecurity. Het uitvoeren van een nieuwe vitaliteitsbeoordeling van de sector keren & beheren waterkwantiteit kan hierin een afspraak worden. Uit deze vitaliteitsbeoordeling kan voortvloeien dat waterschappen voor bepaalde keringen alsnog worden aangemerkt als vitale aanbieder.

De leden van de D66-fractie vragen of de regering andere diensten van de waterschappen, zoals waterzuiveringsinstallaties, niet als vitaal ziet.

Waterzuiveringsinstallaties van waterschappen zijn onderwerp van een vitaliteitsbeoordeling voor het proces van inzamelen, transporteren en zuiveren van afvalwater en hemelwater. Die beoordeling wordt momenteel verricht door de Minister van IenW, in overleg met de Unie van Waterschappen en de VNG. Hieruit kan volgen dat de Minister van IenW deze processen als «vitaal» identificeert. De beoordeling wordt na de zomer van 2018 afgerond.

5. Digitaledienstverleners (DSP's)

5.1 Aanhef

De leden van de CDA-fractie vragen om een reactie op de zorgen uit de praktijk dat onvoldoende duidelijk is welke bedrijven een DSP zijn. Is het mogelijk dat bedrijven in één jaar wel kunnen worden aangemerkt als DSP, waarna zij in een volgend jaar (na wijziging van de bedrijfsactiviteiten) niet meer een DSP zijn?

Het is inderdaad mogelijk dat een bedrijf op het ene moment wel kwalificeert als DSP in de zin van dit wetsvoorstel, en op een ander moment niet. Die wijziging kan het gevolg zijn van een wijziging van bedrijfsactiviteiten, of een wijziging in de omvang van omzet of personeelsbestand (zie ook onder 5.3). Ook het omgekeerde kan zich voordoen. Dergelijke wijzigingen zijn eigen aan het dynamische karakter van ondernemingen en zijn ook voor DSP's vrijwel onvermijdelijk. Daarom is het juist belangrijk om over de criteria te communiceren, zoals in reactie op de vraag van de leden van de VVD-fractie de VVD is geantwoord (paragraaf 2.1).

5.2 Cloudcomputerdiensten

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

Bij de identificatie van AED's vervult het criterium criticaliteit of vitaliteit (het belang van de aangeboden dienst met het oog op de instandhouding van kritieke maatschappelijke en/of economische activiteiten) een belangrijke rol. Daarentegen kent de NIB-richtlijn voor digitale diensten, waaronder clouddiensten, een andere systematiek. De NIB-richtlijn is van toepassing op alle DSP's die binnen de definities vallen en geen kleine of

micro-onderneming zijn (zie hierna, par. 5.3). In de richtlijn is gedefinieerd wat onder een cloudcomputerdienst moet worden verstaan, namelijk «een digitale dienst die toegang mogelijk maakt tot een schaalbare en elastische pool van deelbare computercapaciteit» (artikel 4, onder 19). In de memorie van toelichting (paragraaf 5) wordt hierbij ter verduidelijking van de definitie een veelgebruikte driedeling van clouddiensten gehanteerd, namelijk Infrastructure as a Service (Iaas), Platform as a Service (PaaS) en Software as a Service (Saas). Deze indeling hanteert de Europese Commissie ook in haar communicatie[3] over de implementatie van de NIB-richtlijn.

5.3 Omzet- en personeelseisen DSP's

De leden van de D66-fractie vragen de regering waarom de beveiligingseisen en 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?

Deze vraag geeft mij de gelegenheid om te wijzen op een fout in de tekst over omzet- en personeelseisen in de memorie van toelichting (paragraaf 5, p. 10) en het nader rapport (punt 2, p. 4). Anders dan ik daar stel, valt een verlener van een digitale dienst als bedoeld in bijlage III bij de NIB-richtlijn, slechts buiten de NIB-richtlijn en de Csw als hij voldoet aan *beide* criteria, genoemd in artikel 2, tweede lid, van de bijlage bij de Aanbeveling van de Europese Commissie over kleine, middelgrote en micro-ondernemingen,[4] dus alleen als:
– bij hem minder dan 50 personen werkzaam zijn **en**
– zijn jaaromzet of het jaarlijkse balanstotaal 10 miljoen euro niet overschrijdt.

Als de dienstverlener aan één van de criteria niet voldoet, is de NIB-richtlijn op hem van toepassing.

De leden van de SP-fractie vragen waarom de NIB-richtlijn niet geldt voor kleine en micro-DSP's en vragen welke gevolgen deze uitzondering heeft voor de veiligheid die dit wetsvoorstel tracht te waarborgen. Hoe kan de veiligheid van de dienstverlening van deze groep organisaties alsnog worden gewaarborgd? Zal deze maatregel leiden tot het minder vaak inschakelen van kleine en micro-ondernemingen omdat deze als gevolg van de uitzondering niet onder de Csw vallen?

Het uitzonderen van kleine en micro-ondernemingen die een digitale dienst verlenen als bedoeld in de richtlijn heeft te maken met de verwachte, in het algemeen geringe maatschappelijke gevolgen van incidenten bij deze ondernemingen. Daarnaast zou de regeldruk voor deze ondernemingen relatief hoog uitpakken. Kleine en micro-ondernemingen kunnen altijd vrijwillig een melding doen. Het beleid van de overheid op het gebied van cybersecurity is erop gericht om het algehele niveau van cybersecurity, onder meer bij het bedrijfsleven, zowel bij de aanbieders als afnemers van digitale diensten, op een hoger niveau te krijgen. Zo wordt in de NCSA (zie paragraaf 3) onder meer aandacht besteed aan standaarden voor Internet-of-things-apparaten (gebruiksvoorwerpen met een internetverbinding, bijvoorbeeld een thermostaat die met de

[3] Europese Commissie, «Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union» (Com (2017), 476 final, Annex I).
[4] Aanbeveling 2003/361/EG van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (PbEG 2003, L 124).

smartphone kan worden bediend), het stimuleren van bedrijven om veiliger software te maken en het verbeteren van voorlichtingscampagnes op het gebied van cyberhygiëne. Daarnaast is het Ministerie van Economische Zaken en Klimaat in nauwe samenwerking met het NCSC bezig om het Digital Trust Centre op te richten, dat bedrijven zal helpen hun cyberweerbaarheid te verhogen, onder andere door betrouwbare en onafhankelijke informatie te verschaffen over digitale kwetsbaarheden en door het geven van advies. Het DTC beoogt de komende jaren het ontstaan van een stelsel van intermediaire organisaties tot stand te helpen brengen.[5]
In reactie op de vraag over het inschakelen van kleine en micro-ondernemingen: inkopers van digitale diensten zullen zich in eerste instantie laten leiden door de kosten en de kwaliteit van de dienst (zoals gebruiksgemak en veiligheid) en in mindere mate door de vraag of de aanbieder onder de Csw valt.

Ten slotte vragen deze leden hoeveel kleine en micro-ondernemingen nu onder de noemer digitaledienstverlener 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.

Zoals ik hiervoor heb besproken op de vraag van D66, zijn verleners van digitale diensten uitsluitend digitaledienstverleners in de zin van dit wetsvoorstel als zij geen kleine of micro-onderneming zijn. Kleine of micro-ondernemingen die digitale diensten aanbieden, vallen op dit moment niet onder de Wgmc, nu de Minister van Economische Zaken en Klimaat geen van die ondernemingen als vitaal heeft aangemerkt. De vervanging van de Wgmc door de Csw leidt dus niet tot verminderde veiligheid, waarbij nogmaals zij gewezen op het feit dat deze digitale-dienstverleners van zowel de Wgmc als de Csw zijn uitgesloten primair vanwege de verwachte geringe maatschappelijke gevolgen van incidenten bij deze ondernemingen.

6. Relatie met sectorale wetten en bevoegdheden

6.1 Ministerie van Volksgezondheid, Welzijn en Sport

De leden van de CDA-fractie vragen of er naar aanleiding van invoering van het onderhavige wetsvoorstel en van kracht gaan van de NIB-richtlijn een nulmeting wordt uitgevoerd in de gezondheidszorgsector, met name voor 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 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.

Het is aan de bevoegde autoriteit om het toezicht op de onder haar vallende sector of sectoren te organiseren. Een inventarisatie om het huidige niveau van veiligheid vast te stellen, kan inzicht verschaffen waar, op basis van de eisen van de Csw, verbetering van het veiligheidsniveau nodig is.
In Nederland is de aanwijzing van AED's gekoppeld aan vitale processen. In de huidige situatie in Nederland heeft de Minister voor Medische Zorg de zorg niet als een vitaal proces aangemerkt. De belangrijkste reden hiervoor is dat uitval van een deel van de zorg niet automatisch leidt tot grote maatschappelijke schade. In veel gevallen kan zorg namelijk

[5] Kamerstukken II 2017/18, 26 643, nr. 488.

overgenomen worden door een andere zorgaanbieder. De zorg bestaat uit heel veel kleine en grote aanbieders die veel informatie met elkaar wisselen. Het aanwijzen van enkele AED's in de zorg is niet nodig om cybersecurity in de zorgketen goed te organiseren. Samen met de zorgsector zijn en worden immers reeds verschillende maatregelen genomen om de informatieveiligheid en de continuïteit van zorg zo goed mogelijk te waarborgen. Naast de verplichting om datalekken te melden bij de Autoriteit persoonsgegevens gaat het bij deze maatregelen onder meer om protocollen en wettelijk verplichte normen voor informatiebeveiliging in de zorg, specifieke netwerken voor informatiedeling tussen zorgaanbieders, samenwerking van zorgaanbieders in de Zorg-CERT, en toezicht op de informatiebeveiligingsnormen bij de Inspectie gezondheidszorg en jeugd in oprichting.

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 komt in de plaats van de Wgmc, dus het is niet zo dat de betrokken organisaties straks aan beide wetten moeten voldoen. Voor wat betreft AED's en DSP's introduceert de Csw toezicht en sancties.

Verder vragen deze leden of er een aanleiding moet zijn om een audit op te leggen, of dat dit ook periodiek kan. En waarom kan aan een DSP geen audit worden opgelegd?

De bevoegde autoriteit kan een AED verplichten tot een onafhankelijke audit als daar een concrete aanleiding voor is, maar het kan ook periodiek, zonder concrete aanleiding. Beide situaties vallen onder artikel 26, eerste lid, Csw, dat artikel 15, tweede lid, onder b, NIB-richtlijn implementeert. Inderdaad voorziet de Csw niet in een vergelijkbare bevoegdheid jegens een DSP. Dat is een gevolg van de keuze om met dit wetsvoorstel uitsluitend de NIB-richtlijn te implementeren.[6] Artikel 17 NIB-richtlijn zwijgt namelijk over de mogelijkheid om een DSP een audit op te leggen, en de NIB-richtlijn wil voor DSP's alleen «licht en reactief toezicht achteraf» (zie overweging 60). Audits op vrijwillige basis zijn uiteraard altijd mogelijk.
Overigens legt de inmiddels vastgestelde uitvoeringsverordening[7] DSP's wel de verplichting op om maatregelen te treffen op het gebied van toezicht, controle en testen. Het gaat hierbij om bedrijfsinterne beveiligingsmaatregelen zoals het uitvoeren van waarnemingen of metingen om te beoordelen of de netwerk- en informatiesystemen naar behoren werken, en inspectie en verificatie om na te gaan of aan een norm of reeks richtsnoeren wordt voldaan (artikel 2, vierde lid, onder a en b). Daarnaast bepaalt artikel 2, zesde lid, van die uitvoeringsverordening dat DSP's

---

[6] In navolging van aanwijzing 9.4 van de Aanwijzingen voor de regelgeving: «Bij implementatie worden in de implementatieregeling geen andere regels opgenomen dan voor de implementatie noodzakelijk zijn.»

[7] Uitvoeringsverordening (EU) 2018/151 van de Commissie van 30 januari 2018 tot vaststelling van toepassingsbepalingen voor Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad wat betreft de nadere specificatie van de door digitaledienstverleners in aanmerking te nemen elementen voor het beheer van de risico's in verband met de beveiliging van netwerk- en informatiesystemen en van de parameters om te bepalen of een incident aanzienlijke gevolgen heeft (PbEU 2018, L 26).

ervoor zorgen dat zij over passende documentatie beschikken zodat de bevoegde autoriteit kan nagaan of DSP's aan de gestelde beveiligingseisen voldoen. Het herstel van de situatie (het beëindigen van een overtreding of het voorkómen van herhaling van een overtreding) is in de Csw geregeld via de bevoegdheid van de bevoegde autoriteit om een bindende aanwijzing te geven (artikel 27 Csw) en om een last onder bestuursdwang op te leggen (artikel 28 Csw).

Verder lezen de genoemde leden dat de AED zelf de kosten van de audit draagt tenzij bij amvb anders is bepaald. Is de regering voornemens om een dergelijke amvb vast te stellen? In welke gevallen voert de bevoegde autoriteit zelf de audit uit?

Vooralsnog heeft de regering niet het voornemen om toepassing te geven aan artikel 26, derde lid, Csw en op die manier af te wijken van de hoofdregel dat de AED zelf de kosten van de audit draagt.
Doorgaans zal de bevoegde autoriteit de AED opdragen om een audit te laten uitvoeren. De opmerking in de memorie van toelichting (p. 14) dat de bevoegde autoriteit de audit eventueel ook zelf, maar dan op eigen kosten, kan uitvoeren, ziet op uitoefening van de reguliere toezichtsbevoegdheden van de Awb (titel 5.2). De kosten van regulier toezicht komen immers in beginsel ten laste van de overheid.

Ook vragen de leden van de CDA-fractie naar de reden van de grote verschillen tussen de boeteplafonds in sectorale wetgeving. 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?

De verschillen tussen de boetemaxima in sectorale wetgeving kunnen verklaard worden uit de verschillende context of departementale domeinen waarvoor de boetes zijn bedoeld en de diverse motieven voor de bestuurlijke boete. Het maakt bijvoorbeeld uit of de bestuurlijke boete is bedoeld voor eenvoudige of voor complexe zaken. Daarnaast zijn bestuurlijke-boetesystemen in de loop der jaren gegroeid en aangepast, mede onder invloed van Europese regelgeving. Het ligt voor de hand dat de vakministers en DNB voor de boetes die zij als bevoegde autoriteit opleggen op grond van artikel 29 Csw, aansluiting zoeken bij de boetehoogtes die in de betrokken sector gebruikelijk zijn (uiteraard voor zover bestaande sectorale wetgeving hun nu al de bevoegdheid geeft om een bestuurlijke boete op te leggen). Hoe dan ook moeten zij de bestuurlijke boete afstemmen op de ernst van de overtreding en de mate waarin deze aan de overtreder kan worden verweten, en daarbij zo nodig rekening houden met de omstandigheden waaronder de overtreding is gepleegd (artikel 5:46, tweede lid, Awb). Als beroep bij de bestuursrechter wordt ingesteld tegen een boetebesluit, wordt de rechtmatigheid van de bestuurlijke boete doorgaans indringend getoetst door de rechter.

Verder vragen voornoemde leden welke mogelijkheden er zijn 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?

Een bestuurlijke boete mag niet worden opgelegd voor zover de overtreding niet aan de overtreder kan worden verweten (artikel 5:41 Awb). Schadevergoeding op grond van onrechtmatige daad via het civiele recht vereist echter naast toerekenbaarheid (zoals verwijtbaarheid) ook een causaal verband tussen de gedraging en de schade (condicio sine qua

non, artikel 6:98 BW) en vereist ook dat de geschonden norm strekt tot bescherming tegen de schade zoals de benadeelde die heeft geleden (artikel 6:163 BW). Een opgelegde bestuurlijke boete is op zichzelf dus onvoldoende grond voor schadevergoeding, maar kan zeker relevant zijn.

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 SGP-fractie begrijpen dat het de bedoeling is de dubbele meldplicht zo veel mogelijk te kunnen laten plaatsvinden door één handeling. In dit licht vragen zij in hoeverre het waar is dat er inmiddels tientallen meldplichten zijn, afhankelijk van de verschillende sectoren. Zijn er mogelijkheden 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 zo veel mogelijk te beperken?

De vraag welke instantie zal worden aangewezen als het CSIRT voor DSP's, bespreek ik hierna, in paragraaf 9. Ik beschik niet over een overzicht van alle in Nederland geldende wettelijk geregelde meldplichten. Wel is in 2015 een overzicht gemaakt van huidige en toekomstige meldplichten die betrekking hebben op de bedrijfsvoering in de private of publieke sector.[8] In totaal noemt dat overzicht 11 meldplichten, inclusief die van de Wgmc en de NIB-richtlijn.
Hoe dan ook is het denkbaar dat sommige organisaties één incident aan meerdere instanties zullen moeten melden. Die instanties worden vanuit een ander belang en op grond van andere taken en bevoegdheden betrokken bij een incident. De meldplicht bij bijvoorbeeld het NCSC (CSIRT voor AED's) stelt het NCSC in staat om met het oog op het voorkomen van maatschappelijke ontwrichting hulp te verlenen aan de getroffen organisatie en eventuele gevolgen te beperken. Met behulp van de informatie over de melding kan het NCSC bijvoorbeeld ook andere vitale organisaties die een soortgelijk risico lopen informeren en adviseren. Bevoegde autoriteiten gebruiken de informatie op grond van de meldplicht om toezichthoudend en handhavend op te treden. De meldplicht bij de Autoriteit persoonsgegevens ziet specifiek op de bescherming van persoonsgegevens.
Op de vraag of meldingen die betrekking hebben op één incident in één keer gedaan kunnen worden bij de verschillende instanties, is ingegaan in paragraaf 3, in antwoord op vragen van de leden van de fracties van het CDA en D66.

De leden van de SP-fractie merken op dat de Autoriteit persoonsgegevens heeft geadviseerd andere partijen dan vitale aanbieders en DSP's onder het wetsvoorstel te laten vallen. Zij vragen of en hoe de regering verdere invulling wil geven aan dit advies en vragen de regering tevens haar beweegredenen aan te geven indien zij het advies niet opvolgt.

[8] Zie de memorie van antwoord bij het wetsvoorstel meldplicht datalekken, Kamerstukken I 2014/15, 36 662, C, p. 11–14.

In overeenstemming met vast kabinetsbeleid wordt met dit wetsvoorstel uitsluitend de NIB-richtlijn geïmplementeerd en bevat het wetsvoorstel ten opzichte van de Wgmc alleen nieuwe bepalingen over AED's en DSP's.[9] Voor partijen die niet onder dit wetsvoorstel vallen, zijn de inspanningen – los van de implementatie van de NIB-richtlijn – gericht op het tot stand brengen van een stelsel van intermediaire organisaties die hulp kunnen bieden bij bijvoorbeeld incidenten, zie ook in paragraaf 5.3 het antwoord op de vraag van de leden van de SP-fractie waarom de NIB-richtlijn niet geldt voor kleine en micro-DSP's.[10]
Andere partijen dan vitale aanbieders en DSP's vallen in één opzicht overigens wel onder de Csw. Artikel 16 Csw biedt hun namelijk het recht om een niet-meldplichtig incident dat niettemin aanzienlijke gevolgen heeft voor een dienst, te melden bij het Ministerie van Justitie en Veiligheid, dat de melding zelf kan behandelen maar ook ter behandeling kan doorsturen naar een ander CSIRT of naar een ander bij ministeriële regeling aangewezen computercrisisteam (CERT). Deze bepaling implementeert artikel 20 van de NIB-richtlijn.

9. Grondrechtentoets

De leden van de SP-fractie vragen welke organisatie de regering in gedachten heeft voor het CSIRT voor DSP's of welke criteria zij wil hanteren voor het aanwijzen van dat CSIRT.

De voorbereiding van de besluitvorming hierover is momenteel in volle gang. Criteria die in acht worden genomen zijn onder meer de beoogde omvang van taken bij de start, de daarbij benodigde expertise en personele bezetting, de doorgroeimogelijkheden van het CSIRT en kostenefficiëntie.
In het wetsvoorstel zoals oorspronkelijk ingediend, was opgenomen dat het CSIRT voor DSP's zou worden aangewezen bij amvb (artikel 4, tweede lid, onder b, Csw). Om tijd te winnen (zoals gezegd verstrijkt de implementatietermijn voor DSP's op 9 mei 2018), heb ik dat bij nota van wijziging gewijzigd in «bij koninklijk besluit».

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 voorjaarsnota 2018. Is deze dekking inmiddels geregeld? Wat zijn 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?

De thans begrote kosten voor toezicht voor de sectoren energie, digitale infrastructuur en digitale diensten worden gedekt uit de departementale begroting van het Ministerie van Economische Zaken en Klimaat. Over de inrichting en operationalisering van het CSIRT voor DSP's is een besluit in voorbereiding, hiertoe worden nu verschillende scenario's verkend. Binnen het Ministerie van Infrastructuur en Waterstaat is onlangs de uitvoerder van enkele Csw-taken aangewezen. De dekking van de benodigde uitvoeringskosten wordt derhalve op een later moment dan bij voorjaarsnota 2018 binnen dat ministerie zelf geregeld. Omdat uitvoering van de wet voor AED's pas per 9 november 2018 dient te starten, is de

[9] Zie ook aanwijzing 9.4 van de Aanwijzingen voor de regelgeving: «Bij implementatie worden in de implementatieregeling geen andere regels opgenomen dan voor de implementatie noodzakelijk zijn.»
[10] Kamerstukken II 2017/18, 26 643, nr. 488.

verwachting dat er hierdoor geen negatieve gevolgen zijn voor de uitvoering van de Csw-taken.

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?

Het begrip aanbieder van een essentiële dienst is een begrip uit de NIB-richtlijn en ziet alleen op de sectoren en entiteiten die limitatief zijn opgesomd in bijlage II bij de NIB-richtlijn. De richtlijn is het resultaat van een Europees onderhandelingsproces. Waterkeringen staan bijvoorbeeld niet in bijlage II bij de richtlijn, terwijl het goed en continu functioneren van (de ICT van) bepaalde waterkeringen voor Nederland uiteraard wel van vitaal belang is. Daarom is de Minister van IenW in het Bmc, vastgesteld op grond van de Wgmc, aangewezen als meldplichtige vitale aanbieder voor bepaalde (onderdelen van) waterkeringen. In overeenstemming met vast kabinetsbeleid wordt met de Csw uitsluitend de NIB-richtlijn geïmplementeerd. Voor AED's verplicht de NIB-richtlijn niet alleen tot het regelen van een meldplicht voor ernstige ICT-incidenten, maar ook tot het regelen van beveiligingsverplichtingen en toezicht en sancties. Een en ander verklaart waarom in de Csw is vastgehouden aan de eerder in de Wgmc gemaakte keuze om te werken met het overkoepelende begrip vitale aanbieder. In de Csw zijn AED's een subgroep van de vitale aanbieders.[11] Voor ándere vitale aanbieders, dus aanbieders die niet tevens een AED zijn (naast de Minister van IenW als aanbieder van bepaalde waterkeringen gaat het bijvoorbeeld om aanbieders in de sectoren telecom en nucleair), worden in de Csw geen andere regels gesteld dan de regels die al gelden uit hoofde van de Wgmc.
In de tabel in de «opvolger» van het Bmc zal onderscheid worden gemaakt tussen AED's en andere vitale aanbieders.

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?

De AED is zelf verantwoordelijk voor de te treffen maatregelen aan de hand van de open normen in het wetsvoorstel. Het wetsvoorstel voorziet in de mogelijkheid om die open norm door nadere regels te concretiseren. Op dit moment wordt per sector bezien of dat wenselijk is.

---

[11] Zie de definitie van vitale aanbieder in artikel 1 Csw:
– vitale aanbieder:
  a. aanbieder van een essentiële dienst;
  b. aanbieder van een andere dienst waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving.

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. Wat wordt vervolgens met deze verstrekte persoonsgegevens 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 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.

Artikel 18 Csw is afgeleid van artikel 4 Wgmc en alleen aangepast aan de vervanging van de Wet bescherming persoonsgegevens door de Algemene verordening gegevensbescherming (AVG). Voor deze bevoegdheid om rechtspersonen en bestuursorganen de mogelijkheid te bieden persoonsgegevens te verstrekken aan het NCSC, ook wanneer dit niet-verenigbaar is met de doeleinden waarvoor de persoonsgegevens zijn verzameld, is reden gezien omdat een dergelijke verstrekking noodzakelijk kan zijn voor de uitoefening van de taken van het NCSC met het oog op nationale veiligheid, meer specifiek het voorkomen van maatschappelijke ontwrichting. Artikel 18 Csw geldt dan ook alleen als het NCSC de (persoons)gegevens nodig heeft voor de uitvoering van de taken, genoemd in artikel 3, eerste lid, onder a tot en met e. In artikel 6, vierde lid, AVG in combinatie met artikel 23 AVG wordt uitdrukkelijk de mogelijkheid geboden voor een nationale bepaling zoals artikel 18, tweede lid, Csw. De bepaling stelt buiten twijfel dat de organisatie bevoegd is om gevraagde persoonsgegevens te verstrekken. Ik heb tot nu toe geen signalen dat organisaties in dergelijke situaties niet bereid zijn om vrijwillig persoonsgegevens te verstrekken aan het NCSC. Een vorderingsbevoegdheid is daarom niet nodig.
De toegang tot de verstrekte persoonsgegevens is beperkt tot die personen die belast zijn met de uitvoering van de betrokken NCSC-taken. Het NCSC mag deze gegevens enkel delen met andere organisaties voor zover dat krachtens de AVG en de Csw mogelijk is.

Uit de memorie van toelichting maken deze leden op dat de Autoriteit persoonsgegevens (AP) en de krachtens de AVG in te stellen departementale functionaris voor de gegevensbescherming toezicht zullen houden op de verwerkingen. Op welke wijze wordt de AP 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? Worden alle gegevens vernietigd zodra de verwerking ervan niet meer noodzakelijk is voor de uitoefening van die taken?

De AP heeft diverse toezichts- en sanctiebevoegdheden, die zij deels rechtstreeks aan de AVG ontleent en deels aan de Uitvoeringswet AVG (UAVG), in samenhang met de Awb. Een voorbeeld van een toezichtsbevoegdheid is de bevoegdheid om «van de verwerkingsverantwoordelijke en de verwerker toegang te verkrijgen tot alle persoonsgegevens en alle informatie die noodzakelijk is voor de uitvoering van haar taken» (artikel 58, eerste lid, onder e, AVG en artikel 15 UAVG, in samenhang met titel 5.2 Awb). Voorbeelden van sanctiebevoegdheden zijn de bevoegdheid om aan de overtreder een last onder dwangsom (artikel 58, tweede lid, AVG en artikel 5:32, eerste lid, Awb, in samenhang met artikel 16 UAVG) of een

bestuurlijke boete op te leggen (artikel 83 AVG en de artikelen 14, 17 en 18 UAVG; zie ook titel 5.4 Awb).
De reden dat in de door deze leden bedoelde passage in de memorie van toelichting onderscheid wordt gemaakt tussen enerzijds persoonsgegevens en anderzijds andere gegevens zoals vertrouwelijke bedrijfsgegevens, is dat de AP alleen bevoegd is voor zover het gaat om persoonsgegevens. Alle persoonsgegevens en vertrouwelijke bedrijfsgegevens worden door het NCSC vernietigd zodra de verwerking daarvan niet meer noodzakelijk is voor de uitoefening van zijn 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 (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? Is het niet gewenst om de opmerking uit de memorie van toelichting over het vierde lid van artikel 20 dat het «in beginsel slechts in uitzonderlijke gevallen nodig is om herleidbare gegevens te verstrekken» in de wettekst op te nemen?

De artikelen 20, 21 en 22 Csw bieden een verregaande waarborg dat vertrouwelijke gegevens met betrekking tot een aanbieder, ook echt vertrouwelijk blijven. Zo garandeert art. 22 Csw de vertrouwelijkheid bijvoorbeeld ook als het nodig is om dergelijke gegevens op te nemen in een bindende aanwijzing of in een sanctiebesluit. Het blijven dan immers gegevens die de bevoegde autoriteit ingevolge de Csw heeft verkregen. Voor vertrouwelijke gegevens die herleid kunnen worden tot een aanbieder, wordt in de artikelen 20, zevende lid, 21, zesde lid, en 22, tweede lid, Csw afgeweken van de Wob. Voor andere vertrouwelijke gegevens met betrekking tot een aanbieder blijft de Wob onverkort gelden. Beide wetten botsen dus niet maar vullen elkaar juist aan.
Het kan in uitzonderlijke omstandigheden nodig zijn om herleidbare vertrouwelijke bedrijfsgegevens openbaar te maken om het publiek adequaat te kunnen waarschuwen: door het NCSC op grond van artikel 20, vierde lid, onder b, of door de bevoegde autoriteit op grond van artikel 23 Csw. De memorie van toelichting bij de Wgmc bevatte een passage over artikel 9, vierde lid, onder b, Wgmc die ook geldt voor het identieke artikel 20, vierde lid, onder b, Csw:

«In veel gevallen zal volstaan kunnen worden met niet-herleidbare mededelingen, bijvoorbeeld als het publiek moet worden gewaarschuwd voor de risico's van een door internetcriminelen gehanteerde werkwijze. Soms echter zal de voorlichting alleen effectief kunnen zijn als de aanbieder of het product of de dienst concreet wordt aangeduid, bijvoorbeeld als het nodig is om het publiek te waarschuwen dat er grote risico's verbonden zijn aan het gebruik van een bepaald product of een bepaalde dienst. De beslissing om dergelijke voorlichting te geven, vergt een belangenafweging.[12] Zo zal het belang van het publiek om op de hoogte te zijn niet altijd opwegen tegen het belang van de betrokken

[12] Zie ook artikel 3:4 Algemene wet bestuursrecht (Awb). Deze bepaling geldt in beginsel ook voor andere handelingen – van bestuursorganen – dan besluiten, zie artikel 3:1, tweede lid, Awb.

aanbieder. Denkbaar is ook dat de bekendmaking de maatschappelijke schade juist veroorzaakt of vergroot in plaats van voorkomt of beperkt. Vandaar mijn voorstel om hiervoor een streng criterium te hanteren: «voor zover dat noodzakelijk is om ernstige maatschappelijke gevolgen te voorkomen of beperken». Bij «ernstige maatschappelijke gevolgen» moet worden gedacht aan ontwrichting van de Nederlandse samenleving. Het NCSC zal de betrokken organisatie raadplegen bij het maken van bovenvermelde belangenafweging en bij de vorm en inhoud van de concrete publieksmededeling.»[13]

De in dit citaat bedoelde belangenafweging kan ook tot leidraad dienen bij de toepassing van artikel 23 Csw (openbaarmaking van incidenten door de bevoegde autoriteit).
Artikel 20, vierde lid, bevat dus al het strenge criterium «voor zover dat noodzakelijk is om ernstige maatschappelijke gevolgen te voorkomen of beperken». Naar het oordeel van de regering heeft het geen meerwaarde om dat criterium in de wettekst aan te vullen met de opmerking dat het «in beginsel slechts in uitzonderlijke gevallen nodig is om herleidbare gegevens te verstrekken».

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.

Deze suggestie zal worden betrokken bij het overleg tussen de sectorale toezichthouders en het NCSC over de uitvoering en toepassing van de Csw.

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus

[13] Memorie van toelichting Wgmc, algemeen deel, par. 4, Kamerstukken II 2015/16, 34 388, nr. 3, p. 13.