Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2017–2018

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

Nr. 3

MEMORIE VAN TOELICHTING

Algemeen deel

1. Inleiding

Dit voorstel voor een Cybersecuritywet (hierna: Csw) strekt ter uitvoering van de zogenoemde NIB-richtlijn van de Europese Unie (hierna ook: de richtlijn).[1] De lidstaten moeten uiterlijk op 9 mei 2018 aan deze richtlijn voldoen door de richtlijn waar nodig in hun regelgeving om te zetten.[2] De transponeringstabel is opgenomen aan het eind van het algemeen deel van deze memorie. Vanwege de inhoudelijke samenhang en overlap met de Wet gegevensverwerking en meldplicht cybersecurity (Wgmc) wordt de Wgmc beleidsneutraal, zonder materiële wijzigingen, geïncorporeerd in de Csw en ingetrokken.

2. De NIB-richtlijn

Het doel van de NIB-richtlijn is om, ter ondersteuning van het functioneren van onze samenleving en economie, eenheid en samenhang te brengen in Europees beleid voor netwerk- en informatiebeveiliging, door de digitale paraatheid te vergroten en de gevolgen van cyberincidenten te verkleinen. Het niveau van netwerk- en informatiebeveiliging verschilt momenteel per lidstaat. Dit leidt tot een sterk wisselend niveau van paraatheid bij incidenten en een ongelijk niveau van bescherming van consumenten en bedrijven. Deze fragmentatie leidt er mede toe dat informatie over dreigingen en incidenten niet uitgewisseld wordt.

De NIB-richtlijn verplicht de lidstaten hun paraatheid te verbeteren en beter met elkaar samen te werken. Lidstaten moeten zowel aanbieders van essentiële diensten als digitaledienstverleners verplichten om (i)

---

[1] Richtlijn (EU) 2016/1148 van het Europees parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PbEU 2016, L 194).

[2] Voor de aanwijzing van aanbieders van essentiële diensten, en logischerwijs dus ook voor de *inwerkingtreding* (niet de bekendmaking) van de voor hen geldende voorschriften, verstrijkt de implementatietermijn een half jaar later, op 9 november 2018.

kst-34883-3
ISSN 0921 - 7371
's-Gravenhage 2018

adequate maatregelen te nemen om beveiligingsrisico's te beheersen, incidenten te voorkomen en, als zich toch incidenten voordoen, de gevolgen daarvan zo veel mogelijk te beperken en (ii) ernstige incidenten te melden aan de nationale bevoegde autoriteit of het CSIRT (computer security incident response team). De belangrijkste onderdelen van de richtlijn zijn:

a) reikwijdte;
b) aanwijzing van aanbieders van essentiële diensten;
c) nationale strategie;
d) aanwijzing van centraal contactpunt, CSIRT en bevoegde autoriteit;
e) samenwerking op nationaal en Europees niveau;
f) beveiligingseisen, meldplicht en vrijwillige melding;
g) toezicht en sancties.

a) reikwijdte

De NIB-richtlijn is van toepassing op (i) door de lidstaten aan te wijzen «aanbieders van essentiële diensten» (hierna: AED's) binnen de in bijlage II van de richtlijn genoemde sectoren (energie, vervoer, bankwezen, infrastructuur voor de financiële markt, gezondheidszorg, drinkwater en digitale infrastructuur) en (ii) «digitaledienstverleners» (hierna: DSP's): aanbieders van onlinemarktplaatsen, onlinezoekmachines en cloudcomputerdiensten. De verplichtingen van de richtlijn gelden niet voor eventuele andere diensten die deze organisaties aanbieden, zoals bijvoorbeeld de ICT van de winkels op Schiphol. De richtlijn geldt ook voor overheidsorganisaties die essentiële diensten aanbieden.
De beveiligings- en meldingseisen zijn niet van toepassing op openbare elektronische-communicatienetwerken en -diensten (telecomsector) en verleners van elektronische vertrouwensdiensten (zoals een certificaat voor een elektronische handtekening), omdat voor die sectoren al vergelijkbare EU-regels gelden. Meer in het algemeen geeft de richtlijn voorrang aan bestaande en toekomstige sectorspecifieke EU-regels inzake de beveiliging van netwerk- en informatiesystemen of meldplichten voor incidenten, als die regels ten minste gelijkwaardig zijn aan de verplichtingen van de NIB-richtlijn.

b) aanwijzing van AED's

De aanwijzing van de AED's moet uiterlijk op 9 november 2018 gereed zijn. De richtlijn geeft drie criteria voor de aanwijzing:

1. de aanbieder verleent een dienst die van essentieel belang is voor de instandhouding van kritieke maatschappelijke of economische activiteiten,
2. de verlening van die dienst is afhankelijk van netwerk- en informatiesystemen, en
3. een incident zou aanzienlijke verstorende effecten hebben voor de verlening van die dienst.

Ter invulling van het derde criterium geeft de richtlijn een niet-limitatieve opsomming van relevante factoren, zoals het aantal gebruikers dat afhankelijk is van de dienst, de afhankelijkheid van andere in bijlage II genoemde sectoren van de dienst en de gevolgen die incidenten kunnen hebben voor economische en maatschappelijke activiteiten of de openbare veiligheid. De selectie van aanbieders moet regelmatig worden geëvalueerd en geactualiseerd.
Aanwijzing van DSP's is niet nodig en niet toegestaan; de richtlijn is van toepassing op alle DSP's die binnen de definities vallen. De categorieën worden limitatief opgesomd in bijlage III van de richtlijn (zie boven) en gedefinieerd in artikel 4 van de richtlijn, zie nader paragraaf 5 van deze memorie.

c) nationale strategie

Elke lidstaat moet voor de beveiliging van netwerk- en informatiesystemen een nationale strategie vaststellen waarin de strategische doelstellingen en concrete beleidsmaatregelen worden bepaald voor de in bijlage II genoemde sectoren en voor de digitale diensten van bijlage III.

d) aanwijzing van centraal contactpunt, CSIRT en bevoegde autoriteit

Elke lidstaat moet één centraal contactpunt aanwijzen en een of meer CSIRT's en bevoegde autoriteiten:
– het centrale contactpunt heeft een verbindingsfunctie in de samenwerking tussen de lidstaten;
– het CSIRT heeft onder meer tot taak om te waarschuwen voor cyberrisico's en te reageren op incidenten;
– de bevoegde autoriteit ziet toe op de naleving van de beveiligingseisen en de meldplicht en legt indien nodig sancties op.

e) samenwerking op nationaal en Europees niveau

Als de taken van de bevoegde autoriteit, het centrale contactpunt en het CSIRT binnen een lidstaat aan meerdere instanties zijn toegekend, moeten zij samenwerken. Op EU-niveau is een samenwerkingsgroep opgericht om de strategische samenwerking en uitwisseling van informatie tussen de lidstaten te ondersteunen en te faciliteren. De samenwerkingsgroep bestaat uit vertegenwoordigers van de lidstaten, de Europese Commissie en ENISA, het Europese Agentschap voor netwerk- en informatiebeveiliging. De samenwerkingsgroep krijgt elk jaar een verslag van de centrale contactpunten van de lidstaten over de ontvangen incidentmeldingen. Daarnaast is een netwerk van nationale CSIRT's ingesteld, dat bestaat uit vertegenwoordigers van de CSIRT's van de lidstaten en CERT-EU (het computer emergency response team voor de instellingen van de Europese Unie). Dit netwerk moet een snelle en doeltreffende operationele samenwerking tussen de lidstaten bevorderen. Daartoe kan onder meer (niet-vertrouwelijke) informatie worden uitgewisseld over diensten, activiteiten, samenwerkingscapaciteiten en afzonderlijke incidenten.

f) beveiligingseisen, meldplicht en vrijwillige melding

De AED's en DSP's moeten volgens de richtlijn passende en evenredige technische en organisatorische maatregelen nemen om hun ICT adequaat te beveiligen tegen inbreuken van buitenaf. Verder moeten zij passende maatregelen treffen om incidenten te voorkomen en, als zich toch incidenten voordoen, de gevolgen daarvan zo veel mogelijk te beperken. Verder moeten AED's en DSP's incidenten met aanzienlijke gevolgen melden bij de bevoegde autoriteit of het CSIRT. Om te bepalen of een incident aanzienlijke gevolgen heeft, zijn in elk geval de volgende factoren relevant: het aantal getroffen gebruikers, de omvang van het getroffen geografische gebied en de duur van het incident. Voor DSP's voegt de richtlijn daar nog twee factoren aan toe: de omvang van de verstoring van de werking van de dienst en de omvang van de gevolgen voor de economische en maatschappelijke activiteiten.

Verder voorziet de richtlijn ook in de mogelijkheid voor het vrijwillig melden van niet-meldplichtige incidenten met aanzienlijke gevolgen (artikel 20 NIB-richtlijn).

g) toezicht en sancties

Op de naleving van de beveiligingseisen en meldplichten moet toezicht gehouden worden en zo nodig moet handhavend worden opgetreden (artikelen 15, 17 en 21 NIB-richtlijn).

De NIB-richtlijn is gericht op minimumharmonisatie, behalve voor wat betreft DSP's. Dit betekent dat lidstaten aanvullende regels kunnen stellen en een onderwerp uitgebreider kunnen reguleren dan de desbetreffende bepaling(en) in de richtlijn, maar bijvoorbeeld ook dat de richtlijn de lidstaten vrij laat om regels te stellen over cybersecurity voor sectoren die niet onder de richtlijn vallen, zoals waterkeringen en nucleair. Voor wat betreft DSP's verbiedt de richtlijn in beginsel het stellen van andere beveiligings- en meldingseisen (zie artikel 16, tiende lid, van de richtlijn).

3. Gemaakte implementatiekeuzes op hoofdlijnen

Op hoofdlijnen zijn in dit wetsvoorstel de volgende implementatiekeuzes gemaakt:

1. aanwijzing van de AED's bij amvb of bij nader besluit van een in die amvb te noemen bestuursorgaan;
2. aanwijzing van de Minister van Justitie en Veiligheid als het centrale contactpunt voor Nederland;
3. scheiding van de functies van het CSIRT (advies en bijstand) en de bevoegde autoriteit (toezicht en sancties), waarmee wordt aangesloten bij de in Nederland nu ook al voor verschillende sectoren geldende taakverdeling;
4. aanwijzing van de Minister van Justitie en Veiligheid als het CSIRT voor AED's;
5. aanwijzing van het CSIRT voor DSP's bij amvb;
6. aanwijzing van de Minister van Justitie en Veiligheid als het «loket» voor vrijwillige incidentmeldingen;
7. sectoraal toezicht: aanwijzing van de vakministers respectievelijk De Nederlandsche Bank N.V. (hierna: DNB) als de bevoegde autoriteiten;
8. dubbel melden van ernstige ICT-incidenten: zowel bij het CSIRT als bij de bevoegde autoriteit. Er wordt naar gestreefd deze dubbele meldplicht technisch zó in te richten dat het verspreiden van de benodigde informatie maar één handeling vergt;
9. beveiligingseisen: de beveiligingsverplichtingen zijn opgenomen in de artikelen 7 en 8 Csw. Het is in eerste instantie aan de organisaties zelf om te bepalen welke concrete maatregelen voor hen passend en evenredig zijn. Artikel 9 Csw geeft de bevoegdheid om desgewenst, bij of krachtens algemene maatregel van bestuur (amvb), voor AED's of DSP's (of voor bepaalde categorieën daarvan) nadere regels te stellen over de te treffen beveiligingsmaatregelen. Die nadere regels kunnen desgewenst ook worden opgenomen in een bestaande sectorale amvb. Als op Europees niveau richtsnoeren worden opgesteld over de beveiligingsmaatregelen, zullen deze hierbij worden betrokken;
10. een-op-een overgenomen uit de Wgmc:
    – aangewezen vitale aanbieders, inclusief AED's, moeten ook inbreuken melden die aanzienlijke gevolgen kúnnen hebben voor de continuïteit van vitale dienstverlening («bijna-ongelukken»), maar dergelijke inbreuken hoeven alleen te worden gemeld bij (het Nationaal Cyber Security Centrum (NCSC) van) de Minister van Justitie en Veiligheid. Het staat aanbieders vrij om deze inbreuken op vrijwillige basis ook bij de bevoegde autoriteit te melden;

– voor vitale aanbieders die niet onder de richtlijn vallen, geldt alleen de plicht om incidenten bij het NCSC te melden, en gelden op grond van het onderhavige wetsvoorstel dus geen beveiligingseisen en geen toezicht en sancties;

11. implementatie in één centrale wet en niet in sectorale wetten van de vakdepartementen (zoals de Wet op het financieel toezicht (Wft) en de Drinkwaterwet).

Aan de verplichting van artikel 7 van de richtlijn om een nationale strategie vast te stellen, een bepaling die verplicht tot feitelijk handelen, kan worden voldaan zonder omzetting in een wettelijk voorschrift.[3] In 2011 is de eerste Nationale Cybersecurity Strategie (NCSS) verschenen waarmee de basis is gelegd voor de Nederlandse cybersecurity-aanpak. Om tegemoet te kunnen komen aan de snelle ontwikkelingen in het cyberdomein, is in 2013 de tweede NCSS gepubliceerd. Bij de doorontwikkeling van de huidige strategie zal artikel 7 van de richtlijn in acht worden genomen.

4. Verhouding tot de Wgmc

Zoals gezegd incorporeert dit wetsvoorstel de inhoud van de Wgmc en wordt de Wgmc ingetrokken. Reden hiervoor is met name gelegen in de inhoudelijke samenhang en overlap van (onderdelen van) de Wgmc met de bepalingen die ter implementatie van de NIB-richtlijn in dit wetsvoorstel worden opgenomen. Daarbij is ervoor gekozen om de Wgmc-bepalingen beleidsneutraal, zonder materiële wijzigingen, te incorporeren in dit wetsvoorstel. Voorbeelden van de inhoudelijke verwevenheid van de Wgmc en de NIB-richtlijn zijn de huidige CERT-functie van het NCSC en de CSIRT-taken van de richtlijn, en de meldplicht bij het NCSC voor ernstige ICT-incidenten.

De strekking van de Wgmc kan als volgt worden samengevat. Ten eerste regelt de Wgmc (in de artikelen 5 tot en met 8) een meldplicht bij de Minister van Justitie en Veiligheid voor aanbieders van producten of diensten waarvan de beschikbaarheid en betrouwbaarheid van vitaal belang zijn voor de Nederlandse samenleving (vitale aanbieders) van inbreuken op de veiligheid of het verlies van integriteit van hun elektronische informatiesystemen (ICT-inbreuken). Doel van deze meldplicht is in hoofdzaak om het NCSC in staat te stellen om, ter voorkoming of beperking van maatschappelijke ontwrichting, getroffen organisaties hulp te verlenen bij het waarborgen of herstellen van de beschikbaarheid en betrouwbaarheid van hun producten of diensten en waar aangewezen ook andere vitale en rijksoverheidsorganisaties te waarschuwen en te adviseren. De meldplicht geldt alleen voor bij amvb (het Besluit meldplicht cybersecurity) aangewezen (categorieën van) vitale aanbieders voor bij die maatregel eveneens aangewezen producten en diensten. Daarnaast geldt de meldplicht alleen als er sprake is van een inbreuk waardoor de beschikbaarheid of betrouwbaarheid van genoemde producten of diensten in belangrijke mate wordt of kan worden onderbroken. In samenhang met bepalingen over de meldplicht zelf regelt de Wgmc ook de bevoegdheid voor het NCSC om naar aanleiding van een verplichte melding aanvullende gegevens op te vragen voor zover dat noodzakelijk is om bijvoorbeeld de betrokken organisatie bij te staan bij het treffen van herstellende maatregelen.

[3] Zie aanwijzing 9.6 van de Aanwijzingen voor de regelgeving: «Bepalingen uit bindende EU-rechtshandelingen die verplichten tot feitelijk handelen van de centrale overheid zonder dat derden daarop aanspraak hoeven te kunnen maken, worden niet geïmplementeerd.»

Ten tweede voorziet de Wgmc (in de artikelen 2 en 3) in een vastlegging van de taken van het NCSC in het kader waarvan in elk geval ook persoonsgegevens worden verwerkt, en in samenhang hiermee in de grondslag om ten behoeve van de uitoefening van die taken zowel persoons- als andere gegevens te verwerken. Ter voorkoming of beperking van de uitval van de beschikbaarheid of het verlies van integriteit van de systemen van rijks- en vitale organisaties, en ter verdere versterking van de digitale weerbaarheid van de Nederlandse samenleving, gelden krachtens de Wgmc voor het NCSC de volgende taken: het bijstaan van genoemde organisaties bij het treffen van maatregelen om de beschikbaarheid en betrouwbaarheid van hun producten of diensten te waarborgen of te herstellen; het informeren en adviseren van die organisaties en anderen in en buiten Nederland over dreigingen en incidenten met betrekking tot informatiesystemen van die organisaties; het ten behoeve hiervan verrichten van analyses en technisch onderzoek naar aanleiding van (aanwijzingen voor) dreigingen en incidenten; en het aan andere organisaties verstrekken van bij die analyses verkregen informatie over dreigingen en incidenten met betrekking tot andere informatiesystemen. Ook voorziet de Wgmc (in artikel 4) in een wettelijke grondslag om bijvoorbeeld bij andere publiekrechtelijke organisaties de voor bovengenoemde taakuitoefening noodzakelijke gegevens te vragen en in de mogelijkheid van die derden om in reactie daarop zo nodig ook persoonsgegevens te verstrekken aan het NCSC.

Ten slotte bevat de Wgmc (in artikel 9) regels over de voorwaarden waaronder vertrouwelijke gegevens met betrekking tot aanbieders, die bij het NCSC zijn gemeld of anderszins zijn verkregen, verstrekt mogen worden aan derden. Voor deze strikte regeling is aanleiding gezien, omdat het van groot belang is dat de vertrouwelijkheid van deze voor het NCSC beschikbaar gekomen gegevens over incidenten zo veel mogelijk wordt gewaarborgd. De redenen daarvoor zijn gelegen in het zo veel mogelijk voorkomen van schade bij aanbieders, zoals reputatieschade, benadeling van de concurrentiepositie en toegenomen kwetsbaarheid voor aanvallen, en in het door het NCSC voor hulpverlening kunnen gebruiken van deze gegevens zonder daarbij gehinderd te worden door mogelijk vroegtijdig openbaar worden daarvan. Met name als het gaat om niet verplicht te melden gegevens bestaat anders ook het risico dat aanbieders terughoudend worden met het delen van informatie en het NCSC daardoor serieus benadeeld wordt in de uitoefening van zijn taken. Bepaald wordt daarom dat vertrouwelijke gegevens in het kader van de taakuitoefening door het NCSC slechts aan derden worden verstrekt, indien de geheimhouding daar voldoende is gewaarborgd en voldoende is gewaarborgd dat de gegevens uitsluitend worden gebruikt voor het doel waarvoor zij worden verstrekt. Voor verstrekking van vertrouwelijke gegevens die herleid kunnen worden tot een aanbieder, geldt een bijzondere openbaarheidsregeling, die in de plaats treedt van de Wet openbaarheid van bestuur (hierna: Wob). Dergelijke gegevens kunnen slechts in beperkte kring (AIVD, etc.) worden gedeeld (tenzij de aanbieder instemt met bredere verspreiding), met dien verstande dat ik kan beslissen om de betrokken vakminister op de hoogte te stellen van een door het NCSC gegeven advies, inclusief de daarin opgenomen vertrouwelijke herleidbare gegevens, als een aanbieder onvoldoende gevolg aan dat advies heeft gegeven. Verder ben ik verplicht om dergelijke gegevens onverwijld te verstrekken aan de vakminister als dat noodzakelijk is ter voorkoming of beperking van ernstige nadelige maatschappelijke gevolgen. In een dergelijke situatie kan ik dergelijke gegevens ook verstrekken aan andere organisaties of over die gegevens mededelingen doen aan het publiek, maar alleen na raadpleging van de betrokken aanbieder.

Met de meldplicht van de Wgmc is vooruitgelopen op de implementatie van de NIB-richtlijn, die bepaalt dat lidstaten ervoor moeten zorgen dat AED's ernstige ICT-incidenten melden bij de bevoegde autoriteit of het CSIRT. Dit is gerechtvaardigd geacht met het oog op het maatschappelijke belang van een zo spoedig mogelijk geldende wettelijke plicht voor vitale aanbieders om ernstige ICT-inbreuken voor hulpverlening bij het NCSC te melden. Voor wat betreft vitale aanbieders die AED zijn, voorziet de Csw ter implementatie van de NIB-richtlijn in bepalingen ter handhaving van de meldplicht (toezicht en sancties). Voor andere vitale aanbieders dan AED's kan worden bezien of in afzonderlijke nieuwe wetgeving al dan niet op vergelijkbare wijze in die handhaving zal worden voorzien.

De inhoud van de in de Wgmc opgenomen artikelen over de meldplicht (5 tot en met 8) wordt overgeheveld naar de artikelen 5, 10, 11, 12 en 15 Csw. Net als in de Wgmc geldt de plicht voor aangewezen vitale aanbieders om ICT-incidenten te melden bij het NCSC, ook voor incidenten die aanzienlijke gevolgen voor de continuïteit van hun diensten kúnnen hebben.

De in artikel 2 Wgmc beschreven taken van het NCSC worden in dit wetsvoorstel vastgelegd in artikel 3, waarin ook de uit de richtlijn volgende taken waarvoor de Minister van Justitie en Veiligheid wordt aangewezen (centraal contactpunt, CSIRT voor AED's en instantie voor de behandeling van vrijwillige incidentmeldingen) zijn opgenomen. De inhoud van de artikelen 3 en 4 Wgmc (over verwerking van gegevens door en verstrekking van gegevens aan het NCSC) wordt overgeheveld naar de artikelen 17, eerste lid, en 18 Csw. De bepalingen in artikel 9 Wgmc over het verstrekken van vertrouwelijke gegevens met betrekking tot aanbieders worden overgeheveld naar artikel 20 Csw. Daarbij is overigens in het derde en vierde lid toegevoegd dat ook de bevoegde autoriteit op de hoogte kan worden gebracht van vertrouwelijke herleidbare gegevens met betrekking tot aanbieders.

AED's zijn een subgroep van de vitale aanbieders, bedoeld in de Wgmc. Sommige vitale aanbieders zijn geen AED, maar bieden wel een dienst aan waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving. Zo ziet de richtlijn niet op waterkeringen. De Minister van Infrastructuur en Waterstaat is als beheerder van waterkeringen dus geen AED. Maar het goed en continu functioneren van bepaalde waterkeringen is voor Nederland uiteraard wel vitaal. De Minister van Infrastructuur en Waterstaat blijft voor die waterkeringen dus een vitale aanbieder. De verplichtingen in dit wetsvoorstel verschillen voor vitale aanbieders die een AED zijn en vitale aanbieders die geen AED zijn (zie met name de artikelen 7 en 8 Csw). Dat is een gevolg van de keuze[4] om met dit wetsvoorstel uitsluitend de NIB-richtlijn te implementeren. De richtlijn ziet behalve op DSP's immers alleen op AED's en niet op andere voor Nederland vitale aanbieders. Daarom wordt in dit wetsvoorstel zowel het huidige Wgmc-begrip vitale aanbieders als het nieuwe begrip AED gehanteerd.

In navolging van de NIB-richtlijn, die alleen ziet op «diensten», komt de Wgmc-term «product» niet terug in de Csw. Dat verschil heeft geen inhoudelijke betekenis.
Ook in een aantal andere gevallen is de formulering van artikelen uit de Wgmc in dit wetsvoorstel aangepast om daarmee meer aan te sluiten bij de in de richtlijn gebruikte begrippen. Verder is de tekst van de Csw ten opzichte van de Wgmc aangepast aan de Algemene verordening

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

gegevensbescherming (hierna: AVG).[5] Zie nader de artikelsgewijze toelichting.

Nu de Csw in de plaats komt van de Wgmc, trekt dit wetsvoorstel de Wgmc in. In beginsel vervallen daardoor de Regeling aanwijzing computercrisisteams, vastgesteld op grond van de artikelen 2, tweede lid, onder b, en 9, tweede lid, onder a, Wgmc, en het op artikel 5 Wgmc gebaseerde Besluit meldplicht cybersecurity (aanwijzing van de meldplichtige vitale aanbieders, hierna: Bmc). Zoals nu wordt voorzien, zullen zij worden aangepast aan de Csw en worden «omgehangen» («gehangen» onder de Csw).

Het feit dat de Wgmc wordt geïncorporeerd in de Csw neemt overigens niet weg dat de Csw uitsluitend strekt ter uitvoering van de NIB-richtlijn. Voor zover de Csw door die incorporatie regels bevat die niet voortvloeien uit de richtlijn (zoals de verplichting voor vitale aanbieders in de sectoren telecom, waterkeringen en nucleair om ernstige ICT-incidenten te melden bij het NCSC), gelden die regels immers al uit hoofde van de Wgmc.

5. Digitaledienstverleners

In de NIB-richtlijn zijn definities opgenomen van de drie soorten digitale diensten die onder de richtlijn vallen, te weten «onlinemarktplaats» (artikel 4, onder 17), «onlinezoekmachine» (artikel 4, onder 18) en «cloudcomputerdienst» (artikel 4, onder 19). De reikwijdte van deze begrippen wordt verduidelijkt in de overwegingen van de richtlijn. Hierna worden de definities en de overwegingen geciteerd, en worden de begrippen onlinemarktplaats en cloudcomputerdienst nader toegelicht. Het begrip onlinezoekmachine behoeft geen nadere verduidelijking.

Onlinemarktplaats

Artikel 4, onder 17: «een digitale dienst die het consumenten en/of ondernemers, zoals gedefinieerd in artikel 4, lid 1, onder a) respectievelijk onder b), van Richtlijn 2013/11/EU van het Europees Parlement en de Raad, mogelijk maakt om online verkoop- of dienstenovereenkomsten met ondernemers te sluiten op de website van de onlinemarktplaats of op de website van een ondernemer die gebruikmaakt van door de onlinemarktplaats aangeboden informaticadiensten».

Overweging 15: «Een onlinemarktplaats maakt het consumenten en ondernemers mogelijk online verkoop- of dienstenovereenkomsten met ondernemers te sluiten en is de eindbestemming voor het sluiten van deze overeenkomsten. Zij dient geen betrekking te hebben op onlinediensten die slechts als tussenschakel voor diensten van een derde fungeren waarmee uiteindelijk een overeenkomst kan worden gesloten. Derhalve dient zij geen betrekking te hebben op onlinediensten die de prijzen van bepaalde producten of diensten van verschillende ondernemers vergelijken en die de gebruiker vervolgens automatisch naar de geprefereerde ondernemer doorverwijzen om het product te kopen. Tot de computerdiensten die op de onlinemarktplaats worden aangeboden, kunnen de verwerking van transacties, de verzameling van gegevens of de profilering van gebruikers behoren. Applicatiewinkels, die als onlinewinkels de digitale distributie van applicaties of softwareprogramma's van

[5] 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 (algemene verordening gegevensbescherming) (PbEU 2016, L 119).

derden mogelijk maken, moeten als een soort onlinemarktplaats worden beschouwd.»

Nadere uitleg:

Een onlinemarktplaats betreft een digitale dienst die producten of diensten van derden (ondernemers) aanbiedt en namens deze derde partij gedeeltelijk of in zijn geheel fases overneemt die deze derde partij zelf zou uitvoeren (bijvoorbeeld betaling, verzending, of aanbieden van een dienst/product).

In navolging van overweging 15 van de NIB-richtlijn worden diensten die uitsluitend producten of diensten vergelijken of voor een product of dienst doorverwijzen naar een website van een derde, niet gezien als online-marktplaats in de zin van de richtlijn. Het gaat erom dat de onlinemarkt-plaats niet alleen een product of dienst van een derde aanbiedt en de overeenkomst tot stand brengt maar ook andere handelingen verricht die normaliter worden afgehandeld door de aanbiedende derde (betaling, verzending, aanbieden van een dienst /product namens deze derde etc.); het enkel doorlinken naar een derde partij valt hier dus niet onder. Indien een doorverwijzing naar de website van die derde partij plaatsvindt en de gebruiker moet daar opnieuw alle handelingen verrichten om een product of dienst af te nemen (bijvoorbeeld aanvragen offerte, producten selecteren/in het winkelwagentje doen etc.) en de verwijzende website vervult in het verdere traject ook geen enkele rol meer, dan valt die website dus niet onder het begrip DSP.

Onlinezoekmachines

Artikel 4, onder 18: «een digitale dienst die het gebruikers mogelijk maakt zoekacties uit te voeren op in beginsel alle websites of websites in een bepaalde taal op basis van een zoekvraag over om het even welk onderwerp in de vorm van een trefwoord, frase of andere input; het resultaat zijn hyperlinks naar informatie over de opgevraagde inhoud».

Overweging 16: «Een onlinezoekmachine maakt het de gebruiker mogelijk om in principe over elke website een zoekopdracht over elk mogelijk onderwerp uit te voeren. Er kan ook specifiek op websites in een bepaalde taal mee worden gezocht. De definitie van een onlinezoekmachine in deze richtlijn dient geen betrekking te hebben op zoekfuncties die beperkt zijn tot de inhoud van een specifieke website, ongeacht of de zoekfunctie door een externe zoekmachine wordt aangeboden. Zij dient evenmin betrekking te hebben op onlinediensten die de prijzen van bepaalde producten of diensten van andere ondernemers vergelijken en die de gebruiker vervolgens automatisch doorverwijst [lees: doorverwijzen] naar de geprefereerde ondernemer om het product te kopen.»

Cloudcomputerdiensten

Artikel 4, onder 19: «een digitale dienst die toegang mogelijk maakt tot een schaalbare en elastische pool van deelbare computercapaciteit».

Overweging 17: «Cloudcomputerdiensten bestrijken een breed scala aan activiteiten die volgens verschillende modellen kunnen worden verricht. Voor de toepassing van deze richtlijn wordt onder „cloudcomputer-diensten» verstaan: diensten die toegang tot een schaalbare en elastische groep van gedeelde computercapaciteit geven. Die „computercapaciteit» heeft betrekking op capaciteit zoals netwerken, servers en andere infrastructuur, opslag, applicaties en diensten. Met „schaalbaar» wordt bedoeld: computercapaciteit die, ongeacht de geografische locatie van de

capaciteit, op flexibele wijze door aanbieders van cloudcomputerdiensten wordt toegewezen teneinde met schommelingen in de vraag te kunnen omgaan. Met „elastische groep» wordt bedoeld: de computercapaciteit die afhankelijk van de vraag ter beschikking wordt gesteld en wordt vrijgegeven teneinde deze beschikbare capaciteit snel te kunnen verhogen en verlagen naargelang van het werkvolume. Met „gedeeld» wordt bedoeld: de computercapaciteit die ter beschikking wordt gesteld aan meerdere gebruikers die een gemeenschappelijke toegang tot de dienst hebben, maar waarbij de verwerking voor elke gebruiker afzonderlijk plaatsvindt, hoewel de dienst door middel van dezelfde elektronische uitrusting wordt verleend.»

Nadere uitleg:

De NIB-richtlijn hanteert de definitie van cloudcomputerdiensten van het National Institute of Standards and Technology (NIST), die ook wordt gebruikt door het Department of commerce van de Verenigde Staten. Om te bepalen welke cloudcomputerdiensten precies onder de NIB-richtlijn vallen, kan worden gekeken naar verschillende serviceniveaus binnen cloudcomputing. Deze niveaus zijn in te delen in Infrastructure as a Service (IaaS), Platform as a Service (PaaS) en Software as a Service (SaaS). Door het afnemen van een van deze (of soortgelijke) services heeft het inhurende/afnemende bedrijf minder controle over zijn eigen ICT-infrastructuur, platform of software in het geval van storing of uitval. Hoe meer services het bedrijf overdraagt aan cloudcomputerdiensten, des te afhankelijker het wordt van de cloudcomputerdienstverlener en des te groter de gevolgen voor hem zijn bij een verstoring of uitval van deze cloudcomputerdienst. Mogelijke effecten bij uitval treden niet alleen op bij IaaS, dit kan eveneens plaatsvinden bij PaaS en SaaS. Daarom ligt het in de rede om ervan uit te gaan dat deze drie serviceniveaus van cloudcomputerdiensten onder de reikwijdte van de NIB-richtlijn vallen, mits men voldoet aan de omzet- en personeelseisen (zie hierna).

Uit overweging 17 van de richtlijn blijkt dat de richtlijn met gedeelde computercapaciteit (of deelbare computercapaciteit, zie artikel 4, onder 19) (sharable computing resources) doelt op computercapaciteit die door meerdere gebruikers wordt gedeeld. Aangenomen mag worden dat een privécloud (een cloudcomputerdienst die slechts wordt gebruikt door de medewerkers van één organisatie) geen digitale dienst is in de zin van de richtlijn. Als sprake is van enige vorm van een publieke cloudcomputerdienst (volledig of hybride) dan wordt deze verondersteld onder de Csw te vallen.

Onder welke jurisdictie valt een DSP?

Zoals de richtlijn in artikel 18 bepaalt, valt een DSP uitsluitend onder de jurisdictie van de lidstaat waar de DSP zijn hoofdvestiging heeft in de Unie; in beginsel is dat de plaats waar de dienstverlener zijn hoofdkantoor heeft in de Unie. Indien een DSP niet in de Unie is gevestigd, moet een vertegenwoordiger in de Unie worden aangewezen. De vertegenwoordiger is gevestigd in één van de lidstaten waar de diensten worden aangeboden. De DSP wordt geacht te vallen onder de jurisdictie van de lidstaat waar zijn vertegenwoordiger is gevestigd.

Omzet- en personeelseisen DSP's

De beveiligingseisen en de verplichting om ernstige incidenten te melden, gelden voor een DSP pas als hij meer dan 50 medewerkers in dienst heeft en zijn omzet groter is dan 10 miljoen euro per jaar. Dit volgt uit artikel 16, elfde lid, van de richtlijn, waarin wordt verwezen naar aanbeveling

2003/361/EG.[6] Het aantal medewerkers en de omzet van een bedrijf hebben betrekking op de rechtspersoon die de digitale dienst verleent. Deze uitzondering voor zogeheten kleine en micro-ondernemingen is geïmplementeerd in de omschrijving van *digitaledienstverlener* in artikel 1 Csw.

6. Relatie met sectorale wetten en bevoegdheden

Ministerie van Economische Zaken en Klimaat

Voor de aan te wijzen AED's die onder de verantwoordelijkheid van de Minister van Economische Zaken en Klimaat (EZK) vallen, zal het NCSC de CSIRT-functie gaan vervullen. Voor de DSP's zal het CSIRT bij een amvb worden aangewezen.
Voor de aan te wijzen AED's die onder de verantwoordelijkheid van de Minister van EZK vallen en voor de DSP's zijn de door die Minister aangewezen personen belast met het toezicht op de naleving van het bepaalde bij of krachtens de Csw.

Voor netbeheerders van elektriciteit en gas alsmede voor de grotere internetknooppunten geldt dat zij al vallen onder de meldplicht die is opgenomen in de Wgmc.

De Csw voorziet in een meldplicht en een beveiligingsverplichting op het punt van cybersecurity. Op de aan te wijzen AED's in de sector energie zijn de Elektriciteitswet 1998 en de Gaswet van toepassing. De Elektriciteitswet 1998 (artikel 16, eerste lid, onderdeel q) en de Gaswet (artikel 10, negende lid) bevatten de taak voor netbeheerders om hun netten te beschermen tegen invloeden van buitenaf. Cybersecurity is daar onderdeel van. De zorgplicht die dit wetsvoorstel regelt en de eventuele uitwerking daarvan bij amvb kunnen gezien worden als instructie aan de netbeheerders hoe zij op het gebied van cybersecurity invulling geven aan hun taak op grond van de Elektriciteitswet 1998 en de Gaswet. Een meldplicht op het punt van cybersecurity is niet geregeld in deze wetten. Er is dus geen sprake van botsende verplichtingen.
Voor de aan te wijzen AED's in overige sectoren die onder de verantwoordelijkheid van de Minister van EZK vallen en voor de DSP's zijn de meldplichten of beveiligingsverplichtingen op het punt van cybersecurity nog niet geregeld in de wetgeving die op hen van toepassing is. Er is dus geen sprake van botsende verplichtingen.

Zie paragraaf 8.6 voor een nadere toelichting over de samenhang tussen de Csw en de Telecommunicatiewet en de e-IDAS-verordening.[7]

Ministerie van Financiën

Voor de financiële sector geldt dat de aan te wijzen AED's ook al vallen onder de meldplicht die is opgenomen in de Wgmc. De voorgestelde Csw voorziet in een meldplicht bij de sectorale bevoegde autoriteit en een beveiligingsverplichting op het punt van cybersecurity. Omdat dergelijke verplichtingen ten behoeve van een beheerste en integere uitoefening reeds geregeld zijn in de sectorale wetgeving die van toepassing is op aan te wijzen AED's in de financiële sector brengt de Csw in dit opzicht geen extra verplichtingen met zich mee. DNB was al belast met het toezien op

---

[6] Aanbeveling 2003/361/EG van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (PbEG 2003, L 124).
[7] Verordening (EU) nr. 910/2014 van het Europees parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (PbEU 2014, L 257).

de operationele continuïteit van het betalingsverkeer. Het ligt daarom voor de hand om DNB aan te wijzen als sectorale bevoegde autoriteit. Als CSIRT fungeert de Minister van Justitie en Veiligheid (NCSC).

In de Csw zijn een meldplicht en beveiligingseisen opgenomen. Het bankwezen en de infrastructuur voor de financiële markt worden voor het overgrote deel gereguleerd door rechtshandelingen van de Unie waarin reeds meldplichten en beveiligingseisen zijn opgenomen. Afgezien van rechtstreeks werkende verordeningen, zijn deze meldplichten en beveiligingseisen geïmplementeerd in de Wft en de daarop gebaseerde lagere regelgeving. De insteek van de Wft verschilt van die van de NIB-richtlijn en de Csw. De verplichtingen uit de Wft maken, afhankelijk van de soort instelling, deel uit van het *doorlopende prudentiële toezicht* en het gedragstoezicht dat DNB en de Autoriteit Financiële Markten uitoefenen. Het betreft dan het waarborgen van de beheerste en integere uitoefening van het bedrijf. De verplichtingen uit de Csw zijn er vooral om de *operationele risico's* rondom cyberincidenten zo veel mogelijk te beperken. De verplichting om ernstige ICT-incidenten te melden bij het NCSC en bij DNB heeft als doel om risico's tijdig te kunnen inschatten en te helpen bij het duiden van de aard en de ernst van de melding, mede met het oog op mogelijke gevolgen voor andere andere AED's en andere vitale sectoren in Nederland (en daarbuiten). Voor wat betreft de beveiligingseisen geldt dat instellingen zowel moeten voldoen aan de eisen uit de rechtshandelingen van de Unie als aan de Csw-eisen. In een aantal gevallen vormt het (voorkomen van) operationeel risico tevens een onderdeel van de prudentiële regulering en het prudentiële toezicht op het bankwezen en de infrastructuur voor de financiële markt. Om deze reden zal artikel 6 Csw worden toegepast om specifieke Csw- beveiligingseisen bij amvb buiten toepassing te laten indien beveiligingseisen afkomstig van de specifiek voor die sectoren geldende rechtshandelingen van de Unie feitelijk gelijkwaardig zijn aan de beveiligingseisen van de Csw.

Ministerie van Infrastructuur en Waterstaat

Voor de aan te wijzen AED's die onder de verantwoordelijkheid van de Minister van Infrastructuur en Waterstaat vallen geldt dat het overgrote deel van die aanbieders ook onder de meldplicht van de Wgmc valt. De voorgestelde Csw voorziet in een meldplicht bij de sectorale bevoegde autoriteit en een beveiligingsverplichting op het punt van cybersecurity. Dergelijke verplichtingen op het punt van cybersecurity zijn nog niet (expliciet) geregeld in de wetgeving die van toepassing is op de aan te wijzen AED's die onder de verantwoordelijkheid van de Minister van Infrastructuur en Waterstaat vallen. Er is dus geen sprake van botsende verplichtingen.

Voor de aan te wijzen AED's die onder de verantwoordelijkheid van de Minister van Infrastructuur en Waterstaat vallen, zal het NCSC de CSIRT-functie gaan vervullen.

Ministerie van Volksgezondheid, Welzijn en Sport

Vooralsnog wordt niet voorzien dat zorgaanbieders worden aangewezen als AED. Wanneer wordt besloten om AED's aan te wijzen die onder de verantwoordelijkheid van de Minister voor Medische Zorg vallen, geldt dat de Csw voor deze aanbieders een extra melding oplevert bij een CSIRT (het NCSC) en bij de bevoegde autoriteit, naast de al bestaande verplichtingen tot melding van incidenten bij de Inspectie Gezondheidszorg en Jeugd in oprichting (IGJ i.o.) in het kader van kwaliteit van zorg (bijvoorbeeld klachten en geschillen zorg) en/of de Autoriteit persoonsgegevens (AP) in het kader van bescherming van persoonsgegevens. Ten aanzien

van vertrouwelijkheid en integriteit bestaan voor de zorgsector al regels en toezicht en handhaving, zoals de meldplicht voor calamiteiten op grond van de Wet kwaliteit, klachten en geschillen zorg, de meldplicht datalekken, de beveiligingsvoorschriften NEN 7510, 7512 en 7513 en het toezicht daarop door de IGJ i.o. en de AP.
Voor de eventueel in de toekomst aan te wijzen AED's zal in overeenstemming met de Csw het NCSC de CSIRT-functie gaan vervullen. De bevoegde autoriteit voor de zorgsector is de Minister voor Medische Zorg. De Csw voorziet in een meldplicht en een beveiligingsverplichting op het punt van cybersecurity. Dergelijke meldplichten of beveiligingsverplichtingen op het punt van cybersecurity zijn nog niet (expliciet) geregeld in de wetgeving die van toepassing is op de eventueel aan te wijzen AED's. Er is dus geen sprake van botsende verplichtingen.

Mogelijkheid tot voorrang voor sectorspecifieke EU-regels

Indien nodig, biedt artikel 6 de mogelijkheid om bij amvb te bepalen dat daarbij aangewezen, bij of krachtens de Csw gestelde voorschriften, vanwege de aanwezigheid van sectorspecifieke voorschriften als bedoeld in artikel 1, zevende lid, van de NIB-richtlijn, niet gelden voor de bij die amvb omschreven categorieën van AED's of DSP's. Deze bepaling geldt ook voor eventuele toekomstige sectorspecifieke EU-regels, en zelfs voor voorschriften in door de Europese Commissie vastgestelde (gedelegeerde) verordeningen.

7. Handhaving (toezicht en sancties)

De voorgestelde Csw voorziet in handhaving ten aanzien van de verplichtingen voor de AED's en DSP's (zie hoofdstuk 6 Csw). Hiertoe verplichten de artikelen 14 en 17 van de NIB-richtlijn.

De Csw kent naast verplichtingen voor AED's en DSP's ook verplichtingen voor andere vitale aanbieders dan AED's. Die verplichtingen komen overeen met de verplichtingen op grond van de Wgmc. Evenals de Wgmc voorziet de Csw niet in toezicht en sancties jegens die andere vitale aanbieders, zie paragraaf 4.

In dit wetsvoorstel is voorzien in bestuursrechtelijke handhaving, die zowel reparatoir als punitief kan zijn. De handhaving heeft betrekking op verplichtingen voor AED's en DSP's, die op verschillende terreinen al te maken hebben met bestuursrechtelijke handhaving. Het is wenselijk om aan te sluiten bij al bestaande bevoegdheden en instrumenten van de sectorale toezichthouders. Een en ander is reden om (ook) voor de Csw te kiezen voor bestuursrechtelijke handhaving en niet voor strafrechtelijke handhaving.

Het toezicht op de naleving van het bepaalde bij of krachtens de Csw wordt opgedragen aan door de bevoegde autoriteiten aangewezen personen. Die aangewezen personen zijn toezichthouders in de zin van artikel 5:11 van de Algemene wet bestuursrecht (hierna: Awb): «een persoon, bij of krachtens wettelijk voorschrift belast met het houden van toezicht op de naleving van het bepaalde bij of krachtens enig wettelijk voorschrift». Daarmee beschikken zij over de bevoegdheden die titel 5.2 Awb aan hen toekent. Het gaat hier om de bevoegdheden geregeld in de artikelen 5:15 tot en met 5:19 Awb en de verplichting om mee te werken aan het toezicht van artikel 5:20 Awb. De toezichthouders op de Csw-verplichtingen beschikken daarmee met name over de bevoegdheid om plaatsen te betreden, met uitzondering van woningen zonder toestemming van de bewoner, om identificatie van personen te vorderen,

om inzage te vorderen van zakelijke gegevens en bescheiden en daarvan kopieën te maken.

Naast de standaardbevoegdheden die de toezichthouders op grond van de Awb kunnen uitoefenen, voorziet de Csw voor de bevoegde autoriteiten in de mogelijkheid om AED's of DSP's een bindende aanwijzing op te leggen (artikel 27 Csw) bij wijze van concretisering van de globaal geformuleerde verplichtingen (doelvoorschriften) van de artikelen 7 en 8 Csw of verdere concretisering van de nadere regels van artikel 9 Csw. Met deze bevoegdheid wordt invulling gegeven aan de artikelen 15, derde lid, en 17, tweede lid, onderdeel b, van de NIB-richtlijn.
De bindende aanwijzing is een zelfstandige last als bedoeld in artikel 5:2, tweede lid, Awb. Een dergelijke last wordt toegepast om een abstractere norm te concretiseren. Daarmee wordt voor de aanbieder die een bindende aanwijzing krijgt opgelegd duidelijk waaraan moet worden voldaan en heeft de bevoegde autoriteit een norm waarop gehandhaafd kan worden. Te denken valt aan een last onder dwangsom om de aanwijzing op te volgen of zelfs een boete wegens het niet opvolgen van de aanwijzing.

Het is niet uitgesloten dat een getroffen organisatie in een concreet geval wordt geconfronteerd met een aanwijzing van een bevoegde autoriteit die tegenstrijdig is aan het advies van het NCSC, bijvoorbeeld omdat in een concreet geval onvoldoende tijd beschikbaar is voor onderling overleg of omdat de betrokken organisatie voor dat overleg geen toestemming heeft gegeven. In een dergelijk geval prevaleert de aanwijzing van de bevoegde autoriteit. Het NCSC vervult geen toezichthoudende rol en zijn adviezen zijn niet bindend.

De Csw voorziet in de bevoegdheid voor de bevoegde autoriteit om de AED's een zogenoemde audit op te leggen. Zo'n audit door een onafhankelijke ICT-auditor dient om vast te stellen of de aanbieder in kwestie heeft voldaan aan de beveiligingseisen die op grond van de voorgestelde Csw voor die aanbieder van toepassing zijn. De mogelijkheid om een audit op te leggen vloeit voort uit de richtlijn. Tenzij bij amvb anders wordt bepaald, draagt de AED zelf de kosten van de audit. Mocht de bevoegde autoriteit zelf een audit uitvoeren dan kan dat ook, in dat geval op haar kosten.

Voor het geval een AED of DSP de bij of krachtens de Csw gestelde normen overtreedt, voorziet de wet in de mogelijkheid van het opleggen van bestuurlijke herstelsancties, dus last onder dwangsom of last onder bestuursdwang, en bestuurlijke boetes. In sectorale wetgeving, zoals de Wft of de Gaswet, is al voorzien in de mogelijkheid om aan partijen bij een overtreding een bestuurlijke boete op te leggen. De maximale hoogte van die boetes verschilt aanzienlijk. Om de bestuurlijke boete wegens overtreding van de Csw voldoende afschrikkende werking te geven, is gekozen voor aansluiting bij het hoogste maximum van de hiervoor bedoelde boetes, te weten € 5 miljoen zoals geregeld in de Wft. Eveneens in navolging van de Wft is de maximumboete voor het niet voldoen aan de verplichting om na een melding nadere gegevens te verstrekken alsmede bij het niet verlenen van de gevorderde medewerking bepaald op € 1 miljoen. Deze boetemaxima bieden de sectorale bevoegde autoriteit die uit hoofde van bestaande wetgeving al bevoegd is om een bestuurlijke boete op te leggen, de ruimte om voor de boetebedragen aan te sluiten bij de boetehoogtes die in die sector passend zijn. Een bijkomende overweging voor deze hoogte van de maximale bestuurlijke boete voor de overige overtredingen is dat het voor AED's en DSP's niet moet lonen om de norm niet na te komen; met andere woorden: de boete moet hoger zijn dan de te verwachten besparing wegens het niet naleven van de norm.

8. Consultatiereacties

8.1. Inleiding

Een eerdere versie van dit wetsvoorstel is opengesteld voor consultatie op www.internetconsultatie.nl en voor commentaar toegezonden aan belangenorganisaties en vitale aanbieders. Hieronder volgt een globale bespreking van de reacties.

8.2. Reikwijdte van de Csw

Een organisatie vraagt of waterschappen onder de reikwijdte van de Csw (gaan) vallen.

Ten aanzien hiervan wijs ik erop dat de Csw niet alleen ziet op AED's, maar ook op aanbieders van andere diensten waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving. Tot deze laatste categorie behoren enkel waterkeringen die in beheer zijn bij de Minister van Infrastructuur en Waterstaat. Naar de huidige inzichten worden keringen die in beheer zijn bij waterschappen niet aangewezen als vitaal proces. Datzelfde geldt ook voor overige diensten van waterschappen. Voor waterschappen geldt dan ook dat zij niet als vitale aanbieder zullen worden aangewezen. Met regelmaat zal worden getoetst of de aanwijzing van vitale aanbieders nog up-to-date is. Niet uitgesloten is dan ook dat in de toekomst ook andere beheerders van waterkeringen of van zuiveringsinstallaties als vitale aanbieder worden aangewezen.

Een organisatie vraagt of in het kader van de voorgestelde minimumharmonisatie van de NIB-richtlijn, er bewust voor is gekozen dat organisaties wel in de NIB-richtlijn worden genoemd, maar niet in de Nederlandse implementatie in de Csw.

Ten aanzien hiervan merk ik op dat zowel de NIB-richtlijn als de Csw het begrip AED's hanteert. In bijlage II van de richtlijn worden de sectoren en bijbehorende categorieën aanbieders genoemd, waarbinnen lidstaten, aan de hand van de artikelen 5, tweede lid, en 6 van de richtlijn, bepalen welke specifieke aanbieders als AED worden aangewezen. Daarnaast zullen, net als krachtens de huidige Wgmc, andere vitale aanbieders (bijvoorbeeld de Minister van Infrastructuur en Waterstaat als beheerder van bepaalde waterkeringen of onderdelen daarvan) worden aangewezen, waarvoor met name ook de meldplicht bij het NCSC zal komen te gelden (artikel 10, eerste lid, Csw). Aanwijzing van al deze aanbieders zal krachtens artikel 5, eerste lid, Csw bij amvb plaatsvinden, of bij besluit van een bij amvb genoemd bestuursorgaan.

Een andere organisatie vraagt of binnen de zorgsector ook toeleveranciers van AED's onder de Csw komen te vallen. Ten aanzien hiervan merk ik op dat de NIB-richtlijn voor de genoemde sector alleen geldt voor zorgaanbieders. In artikel 3, onder g, van Richtlijn 2011/24/EU[8] wordt een zorgaanbieder gedefinieerd als: *«een natuurlijke of rechtspersoon of een andere instantie die op het grondgebied van een lidstaat wettelijke gezondheidszorg verstrekt»*. Software- en andere toeleveranciers vallen hier dus niet onder. Daarnaast worden zij thans in de Nederlandse situatie ook overigens niet aangemerkt als aanbieders van vitale diensten.

[8] Richtlijn 2011/24/EU van het Europees parlement en de Raad van 9 maart 2011 betreffende de toepassing van de rechten van patiënten bij grensoverschrijdende gezondheidszorg (PbEU 2011, L 88).

8.3. Beveiligingsmaatregelen voor AED's

Microsoft is van mening dat in de Csw de veiligheidsmaatregelen voor AED's in een risico-gebaseerde en uitkomstgerichte benadering moeten voorzien[9]. Daarnaast wijst Microsoft erop dat security baselines zouden moeten worden gehanteerd, standaardprocessen van risicobeheer en monitoring moeten worden ontwikkeld en internationale best practices in overweging moeten worden genomen zoals het *NIST Framework for Improving Critical Infrastructure Cybersecurity*. Ook benadrukt Microsoft het belang van harmonisatie, zowel bij het definiëren van essentiële diensten als door gebruik van *Security Baselines Harmonization* in de gehele EU.

Een andere organisatie vraagt of de globale en specifieke beveiligingseisen waar de AED's aan moeten voldoen, door de betrokken ministeries verder worden uitgewerkt in een sectorale amvb.

In reactie hierop merk ik op dat het in eerste instantie aan de organisaties zelf is om te bepalen welke specifieke maatregelen in het kader van de beveiligingsverplichtingen in de artikelen 7 en 8 Csw voor hen passend en evenredig zijn. Er zal nog worden bezien of bij of krachtens amvb nadere regels over de te treffen beveiligingsmaatregelen zullen worden gesteld (voor alle AED's of voor AED's in bepaalde sectoren). Een eventuele concretisering van de te treffen maatregelen zou ook de vorm kunnen krijgen van beleidsregels of richtsnoeren. Richtsnoeren kunnen ook op Europees niveau worden opgesteld. De verantwoordelijkheid voor eventuele concretisering op nationaal niveau ligt bij het vakdepartement.

8.4. Meldplicht voor incidenten

Een organisatie geeft in haar reactie aan dat zij de inbreuken, bedoeld in artikel 10, eerste lid, onder b, Csw (bijna-ongelukken) graag gemeld wil zien bij zowel het NCSC als bij de sectorale bevoegde autoriteit. Daarbij wordt opgemerkt dat in de desbetreffende sector is afgesproken dat organisaties de bevoegde autoriteit ook zullen informeren over deze inbreuken.

Ten aanzien hiervan merk ik op dat de NIB-richtlijn niet verplicht tot het regelen van een meldplicht (bij bijvoorbeeld de bevoegde autoriteit) voor bijna-ongelukken. De in artikel 10, eerste lid, onder b, opgenomen meldplicht is overgenomen van de Wgmc. Het doel ervan is om het NCSC zo vroeg mogelijk op de hoogte te brengen van inbreuken die aanzienlijke gevolgen kunnen hebben voor de continuïteit van voor de samenleving vitale diensten, en daardoor in staat te stellen om, ter voorkoming of beperking van maatschappelijke ontwrichting, getroffen organisaties al in een vroeg stadium bijstand te verlenen bij het treffen van maatregelen om de continuïteit van hun diensten te waarborgen en waar aangewezen ook andere vitale en rijksoverheidsorganisaties te waarschuwen en te adviseren. Om deze reden hoeven deze inbreuken alleen gemeld te worden bij het NCSC en niet ook bij de bevoegde autoriteit. Het staat aanbieders uiteraard vrij om op vrijwillige basis dit soort inbreuken ook bij de bevoegde autoriteit te melden.

8.5. Verstrekking vertrouwelijke gegevens

Twee organisaties pleiten ervoor om gevoelige gegevens niet aan derden te verstrekken zonder instemming van de betrokken vitale aanbieder.

---

[9] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer

Ten aanzien hiervan merk ik op dat het in beginsel slechts in uitzonderlijke gevallen nodig zal zijn om vertrouwelijke herleidbare gegevens te verstrekken aan derden. Er is voor gekozen in artikel 20, vierde lid, onder b, Csw «na raadpleging» op te nemen in plaats van «na instemming», vanwege de eigen verantwoordelijkheid van het NCSC als het gaat om het voorkomen van nadelige maatschappelijke gevolgen en de uitoefening door de bevoegde autoriteit. Zie in dezelfde zin artikel 23 Csw over het informeren, door de bevoegde autoriteit, van het publiek over een gemeld incident.

8.6. Relatie met aanverwante regelgeving

KPN wijst erop dat de beveiligings- en meldingseisen uit de NIB-richtlijn niet van toepassing zijn op ondernemingen die openbare elektronische communicatienetwerken of -diensten in de zin van Richtlijn 2002/21/EG (Kaderrichtlijn)[10] aanbieden of op verleners van vertrouwensdiensten in de zin van de e-IDAS-verordening. KPN pleit ervoor om in de memorie van toelichting dezelfde formulering te gebruiken als in artikel 1, derde lid, van de NIB-richtlijn[11].

KPN wijst er terecht op dat in de consultatieversie van deze memorie (op p. 2) het woord «openbaar» ontbrak bij elektronische communicatienetwerken en -diensten. Een ander verschil in formulering is dat de letterlijke tekst van artikel 1, derde lid, van de NIB-richtlijn suggereert dat de NIB-richtlijn niet geldt voor een onderneming die een essentiële of digitale dienst aanbiedt náást openbare elektronische communicatienetwerken of -diensten of vertrouwensdiensten. Een dergelijke uitleg ligt echter niet in de rede, aangezien zij tot gevolg zou hebben dat de verlening van de essentiële of digitale dienst in zo'n geval onder geen enkel wettelijk regime met meldings- en beveiligingseisen zou vallen. Bovendien zou dat ook nadelig kunnen zijn voor het level playing field, ten opzichte van ondernemingen die niet met een deel van hun activiteiten onder de Kaderrichtlijn of e-IDAS-verordening vallen. Aan de andere kant is het ongewenst dat één activiteit onder twee vergelijkbare wettelijke regimes valt. Kortom, bij het bepalen van de toepasbaarheid van de NIB-richtlijn gaat het erom in hoeverre een activiteit al onder de Kaderrichtlijn of e-IDAS-verordening valt.

Een organisatie vraagt hoe dit wetsvoorstel zich verhoudt tot de verplichtingen die voortvloeien uit de Elektriciteitswet 1998 en de Gaswet en de bepalingen op het gebied van security in de NTA8120 als invulling daarvan.

Hierover merk ik op dat de zorgplicht die dit wetsvoorstel regelt en de eventuele uitwerking daarvan bij of krachtens amvb, gezien kan worden als instructie aan de netbeheerders hoe zij op het gebied van cybersecurity invulling kunnen geven aan hun taak op grond van de Elektriciteitswet 1998 en de Gaswet. Wanneer de sector en de bevoegde autoriteit specifieke knelpunten signaleren tussen de Csw en sectorale wetgeving, zal worden bezien hoe deze knelpunten weggenomen kunnen worden zonder af te doen aan de intentie van de Europese richtlijnen.

---

[10] Richtlijn 2002/21/EG van het Europees parlement en de Raad van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronische-communicatienetwerken en -diensten (kaderrichtlijn) (PbEG 2002, L 108).

[11] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer

8.7. DSP's

8.7.1. Zwaarte en harmonisatie regelgeving
Meerdere organisaties hebben opmerkingen gemaakt over de zwaarte en harmonisatie van de regelgeving voor de DSP's. Microsoft geeft aan dat digitale diensten in meerdere EU-lidstaten tegelijkertijd actief zijn en dat hierbij een geharmoniseerd regelgevend raamwerk essentieel is voor deze diensten om succesvol over grenzen heen te kunnen opereren. Hierbij wordt ook bepleit om ten aanzien van de verschillende subcategorieën digitale diensten – clouddiensten, zoekmachines en onlinemarktplaatsen – te differentiëren, bijvoorbeeld qua beveiligingseisen.

VNO-NCW en MKB-Nederland bepleiten om het gebruikelijke beveiligingsniveau bij DSP's in Nederland tot inzet te maken van de onderhandelingen in Europa over de uitvoeringshandelingen, zodat de normen voor digitale veiligheid in de EU naar een hoger niveau kunnen worden getild. Tegelijkertijd vinden VNO-NCW en MKB-Nederland dat de zorgplicht significant lichter moet worden dan de zorgplicht voor essentiële diensten vanwege de «light touch approach» die gekozen is voor de DSP's. Andere partijen (waaronder Considerati) wijzen erop dat de richtlijn «licht en reactief toezicht achteraf» beoogt (overweging 60 richtlijn). Tot slot, verwijzen VNO-NCW en MKB-Nederland naar overweging 49 van de NIB-richtlijn, die benadrukt dat DSP's de vrijheid behouden om maatregelen te treffen die zij passend vinden.

Ten aanzien hiervan merk ik op dat de NIB-richtlijn het grensoverschrijdende karakter van deze digitale diensten onderkent door een geharmoniseerde aanpak te hanteren. Ten aanzien van de meldings- en beveiligingseisen voorziet de richtlijn in maximumharmonisatie en de Europese Commissie zal uitvoeringshandelingen vaststellen om de invulling en tenuitvoerlegging van de maatregelen te vergemakkelijken en tevens te zorgen voor een hoge mate van harmonisatie van de beveiligings- en meldingseisen voor DSP's (artikel 16, achtste lid, van de richtlijn). Daarmee is nadrukkelijk gekozen voor een andere aanpak bij DSP's dan bij AED's. De uitvoeringshandelingen zullen uiteindelijk een resultaat zijn van overleg tussen 28 lidstaten en de Europese Commissie, en zullen naar verwachting begin 2018 worden vastgesteld.

De Nederlandse regering vindt het niet noodzakelijk om voor deze drie subcategorieën digitale diensten dezelfde meldings- en beveiligingseisen te stellen; indien gewenst kan worden gedifferentieerd. Dit heeft Nederland ook bij de voorbereiding van deze uitvoeringshandelingen naar voren gebracht. Nederland hecht ook belang aan de «light touch approach» en heeft benadrukt dat de beveiligingsmaatregelen «risicogebaseerd en uitkomstgericht» moeten zijn, waarbij niet in detail wordt voorgeschreven op welke wijze en op welk niveau maatregelen moeten worden getroffen. Op deze manier wordt invulling gegeven aan de hierboven genoemde overweging 49. Het «gebruikelijke beveiligingsniveau» bij Nederlandse DSP's tot Nederlandse inzet van de onderhandelingen maken waarvoor VNO-NCW en MKB Nederland pleiten is lastig uitvoerbaar, omdat er nog geen duidelijk beeld bestaat wat dit «gebruikelijke beveiligingsniveau» eigenlijk is. Door in te zetten op risicogebaseerde en uitkomstgerichte beveiligingsmaatregelen wordt in ieder geval ruimte geboden aan DSP's om «passende» maatregelen te treffen die kunnen aansluiten op hun eigen beveiligingsniveau.

Ten aanzien van het «reactief toezicht» voor DSP's verwijs ik naar overweging 60 van de richtlijn, waarin wordt overwogen dat DSP's moeten worden onderworpen aan licht en reactief toezicht achteraf. De bevoegde autoriteit moet daarom alleen maatregelen nemen als zij over

aanwijzingen beschikt voor een schending van de bepalingen in deze wet. Die aanwijzingen kunnen bijvoorbeeld verstrekt zijn door de DSP zelf, een bevoegde autoriteit van een andere lidstaat of een gebruiker van een dienst.

8.7.2. Definities digitale diensten
Enkele organisaties, waaronder Nederland ICT, VNO-NCW, MKB-Nederland en Considerati[12] missen duidelijke definities van de subcategorieën (1) onlinemarktplaats, (2) onlinezoekmachine en (3) cloudcomputerdiensten.

Microsoft vindt de definitie van cloudcomputerdienst te breed, want er wordt hierbij geen onderscheid gemaakt tussen de verschillende niveaus van criticaliteit, zoals SaaS, PaaS, IaaS en het soort cloud (privaat, gemeenschap, hybride of publiek).

Naar aanleiding van deze reacties is aan deze memorie van toelichting een paragraaf toegevoegd over DSP's (par. 5). Hierin is uitgelegd waarom het begrip cloudcomputerdiensten betrekking heeft op zowel Saas, PaaS als IaaS, en alleen op publieke clouddiensten.

Nederland ICT verzoekt om duidelijkheid te scheppen over welke bedrijven onder deze wet gaan vallen voordat handhaving gaat plaatsvinden. Hierbij wordt gerefereerd aan Denemarken, waar bedrijven per brief op de hoogte worden gesteld dat ze zijn aangemerkt als DSP. Hierover merk ik het volgende op. In par. 5 van deze memorie zijn de definities van de cloudcomputerdiensten en de onlinemarktplaatsen nader uitgewerkt. Dit kan bedrijven helpen om te bepalen in hoeverre ze hieronder vallen. Daarnaast zal het Ministerie van Economische Zaken en Klimaat voordat de Csw in werking treedt – eventueel in samenwerking met betrokken brancheorganisaties – bezien op welke manier aan partijen over de Csw kan worden gecommuniceerd, zodat partijen – bijvoorbeeld aan de hand van een checklist/overzicht – eenvoudiger kunnen nagaan of zij onder de reikwijdte van de Csw vallen. Het landschap met spelers die actief zijn binnen de digitale economie is dusdanig dynamisch dat niet is gekozen voor het aanschrijven van partijen. Of een onderneming kwalificeert als DSP, hangt bijvoorbeeld af van de omzet en personeelsomvang. Bovendien past dit soort aanbieders regelmatig de aard van hun dienstverlening aan waardoor ze plotseling wel of juist niet meer onder de definitie vallen.

Een organisatie vraagt vanaf welk moment de DSP's moeten voldoen aan de verplichtingen uit de Csw.

Ten aanzien hiervan merk ik op dat de verplichtingen voor DSP's vanaf 10 mei 2018 gaan gelden (mits de Csw tijdig in werking treedt), zie artikel 25, eerste lid, van de NIB-richtlijn.

8.8. Advies Autoriteit Persoonsgegevens

De Autoriteit Persoonsgegevens (AP) heeft advies uitgebracht over een eerdere versie van het wetsvoorstel[13]. Waar de nummers van de artikelen verschillen, worden de artikelen van die eerdere versie hierna aangeduid met: ([artikelnummer] oud).

[12] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer
[13] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer

De AP wijst erop dat een meldplichtig Csw-incident tevens een datalek kan zijn, dat uit hoofde van de AVG gemeld moet worden bij de AP. Ook merkt de AP op dat bij een dergelijk incident samengewerkt moet worden tussen de AP, het betrokken CSIRT en de bevoegde autoriteit.

Naar aanleiding daarvan merk ik op dat ernaar zal worden gestreefd om bij de incidentopvolging, met inachtneming van de wettelijke kaders, zo veel mogelijk samen te werken tussen het betrokken CSIRT, de bevoegde autoriteit en andere instanties zoals de AP. Dit kan bijvoorbeeld indien aangewezen in convenanten worden vastgelegd.

De AP adviseert om ook andere partijen dan vitale aanbieders en DSP's onder het wetsvoorstel te laten vallen, in verband met een landelijke dekking bij incidenten.
Hierover merk ik op dat het de aandacht van het kabinet heeft om ook voor andere partijen te voorzien in ondersteuning op het gebied van cybersecurity. De toenmalige Minister van Economische Zaken heeft de Kamer bij brief van 23 september 2017 geïnformeerd over het Digital Trust Center (DTC), dat beoogt, in samenwerking met het NCSC, ook het niet als vitaal aangemerkte bedrijfsleven weerbaarder te maken tegen cyberdreigingen.[14] Zie hierover ook paragraaf 8.9.

De AP adviseert (onderdelen van) de overheid als vitale aanbieder aan te wijzen, vanwege hun kritische functie en belang bij incident management en emergency response.
In reactie hierop kan worden opgemerkt dat krachtens artikel 3 Csw (net als in het huidige artikel 2 Wgmc) alle organisaties die deel uitmaken van de rijksoverheid, ongeacht of zij al dan niet vitaal zijn, tot de doelgroep van het NCSC behoren en dus in aanmerking komen voor bijstand door het NCSC bij dreigingen en incidenten. Daarnaast wordt op dit moment bezien welke organisaties behorende tot de rijksoverheid voor specifieke bepaalde diensten, naast de Minister van Infrastructuur en Waterstaat met betrekking tot de waterkeringen, als vitale aanbieder zullen worden aangemerkt.

Verder merkt de AP op dat de toelichting niet ingaat op de Richtlijn dataprotectie.[15]

In reactie hierop merk ik op dat die richtlijn niet van toepassing is op de Csw, omdat de verwerkingen van persoonsgegevens door de in de Csw genoemde organisaties ten behoeve van de in de Csw vermelde taken niet gericht zijn op het strafrechtelijke traject. Het NCSC en de bevoegde autoriteit zullen geen onderzoek doen naar personen of organisaties die verantwoordelijk zijn voor die dreigingen en incidenten of daar anderszins aan bijdragen of hebben bijgedragen.

De AP merkt op dat persoonsgegevens soms wellicht heen en weer bewegen tussen het domein van cybersecurity naar het domein van politie en justitie, mede omdat het NCSC is ondergebracht bij het Ministerie van Justitie en Veiligheid.
Verstrekking van persoonsgegevens door het NCSC uit eigen beweging aan bijvoorbeeld het OM geschiedt alleen voor zover dat mogelijk is

---

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

[15] Richtlijn (EU) 2016/680 van het Europees parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (PbEU 2016, L 119).

krachtens de Wet bescherming persoonsgegevens (Wbp, vanaf mei 2018 de AVG). Los daarvan geldt dat de officier van justitie persoonsgegevens kan vorderen op grond van artikel 126nd e.v. van het Wetboek van Strafvordering.

Verder merkt de AP op dat de tekst helderder gemaakt kan worden door verschillende begrippen beter toe te lichten. Naar aanleiding hiervan is de toelichting op enkele plaatsen verduidelijkt.

De AP vraagt of er buiten de artikelen 19, 20 en 23 Csw (18–20 oud) nog andere situaties zijn waarin het NCSC persoonsgegevens kan verstrekken aan derden, en zo ja, aan wie.
Ik kan bevestigen dat het NCSC in de gevallen genoemd in artikel 3, eerste en tweede lid, Csw, uiteraard met inachtneming van de AVG, persoonsgegevens kan verstrekken aan andere organisaties. Voor artikel 20 Csw (19 oud) geldt overigens dat het betrekking heeft op de verstrekking van vertrouwelijke gegevens met betrekking tot aanbieders, en dat het daarbij dus vaak niet zozeer zal gaan om persoonsgegevens. En artikel 23 (20 oud) gaat over het informeren van het publiek over incidenten door de bevoegde autoriteit of de aanbieder, en niet door het NCSC.

De AP vraagt of de openbaarmaking in artikel 23 Csw (20 oud) ook persoonsgegevens betreft. Er wordt op dit moment niet voorzien dat dat het geval is. Als dit wel het geval blijkt te zijn, zal dit alleen plaatsvinden voor zover dat mogelijk is krachtens de AVG en het strikt noodzakelijk is gelet op de doeleinden van artikel 23 Csw.

Tot slot vraagt de AP of het NCSC op grond van artikel 20 (19 oud), tweede lid, onder c, Csw ook uit eigen beweging gegevens verstrekt aan de AIVD. Dat kan ik bevestigen; uiteraard vinden dergelijke verstrekkingen uitsluitend plaats met inachtneming van de regels daarvoor gesteld in artikel 20. Overigens ziet artikel 20 alleen op vertrouwelijke gegevens met betrekking tot aanbieders, dus niet op andere vertrouwelijke gegevens, zoals persoonsgegevens die niet herleidbaar zijn tot een aanbieder (zie de artikelsgewijze toelichting bij artikel 20).

8.9. Overige opmerkingen

Naast de bovenstaande thema's zijn er nog verschillende deelvragen gesteld. Hieronder volgt een globale bespreking van een aantal van deze vragen.
Een organisatie geeft aan te maken te hebben met verschillende toezichthouders. Met het oog op het minimaal houden van de toezichtlasten, stelt de organisatie een door het Ministerie van Justitie en Veiligheid geharmoniseerde aanpak van toezicht voor.

Ten aanzien hiervan merk ik op dat in de Csw is gekozen voor een sectorale aanpak van het toezicht. Dat neemt niet weg dat sectorale toezichthouders kennis en ervaring met elkaar kunnen uitwisselen over toezichtkwesties teneinde de kwaliteit van toezicht te optimaliseren.

Nederland ICT dringt erop aan te onderzoeken of het DTC op termijn kan worden gebruikt als CSIRT en is van mening dat het DTC niet moet worden belast met toezicht en handhaving.

Hierover merk ik op dat de Tweede Kamer in juni 2017 een motie[16] heeft aangenomen met het verzoek aan de regering om voor Prinsjesdag 2017 de Kamer te informeren over hoe een DTC kan worden opgericht en

[16] Kamerstukken II 2016/17, 26 643, nr. 474.

vormgegeven. De regering heeft de Kamer hierover bij brief van 23 september 2017 geïnformeerd.[17] Momenteel wordt nader onderzocht hoe de CSIRT-functie voor DSP's moet worden ingericht en welke organisatie daarvoor zal worden aangewezen. Het wetsvoorstel regelt dat het CSIRT voor DSP's wordt aangewezen bij amvb (zie artikel 4, tweede lid, onder b, Csw). Het is in ieder geval niet de bedoeling dat een DTC zal worden belast met toezicht en handhaving.

KPN en een andere organisatie wijzen op het belang van veilige hardware en software voor de veiligheid en continuïteit van hun eigen dienstverlening.

Ten aanzien hiervan wijs ik erop dat hardwareproducenten en softwareontwikkelaars buiten de reikwijdte van de NIB-richtlijn vallen, omdat zij niet als AED's of DSP's worden aangemerkt. Daarnaast worden deze organisaties thans in de Nederlandse situatie ook overigens niet aangemerkt als aanbieders van vitale diensten. Het kabinet erkent echter het belang van veilige hardware en software en zet zich in om kwetsbaarheden te verminderen. Zo worden gebruikers door het NCSC en via de website veiliginternetten.nl (https://veiliginternetten.nl/) geïnformeerd over onveilige apparaten en wat zij daaraan kunnen doen. Verder werkt de sector in de Secure Software Alliance samen aan richtlijnen voor het ontwikkelen van veilige software. Ook onderzoekt het kabinet, in overleg met het bedrijfsleven, op welke wijze de digitale veiligheid van het Internet of Things kan worden versterkt.[18]

Een organisatie vraagt of het klopt dat deze memorie van toelichting, anders dan het Bmc, uitgaat van zowel het elektriciteits- als het gasnetwerk.

Hierover merk ik op dat de Csw, net als de Wgmc en het Bmc, gaat gelden voor beide deelsectoren.

Euronext vraagt in hoeverre rekening wordt gehouden met reeds toepasselijke financiële regelgeving voor gereglementeerde markten[19].

Hierover merk ik op dat er rekening is gehouden met reeds toepasselijke regelgeving voor de aan te wijzen AED's. De meldplicht bij het NCSC heeft als doel om risico's tijdig te kunnen inschatten en helpen bij het duiden van de aard en de ernst van de melding, mede met het oog op mogelijke gevolgen voor andere vitale sectoren in Nederland (en daarbuiten). De instellingen die onder beide wetten vallen, zullen zowel aan de eisen uit de Wft als de Csw moeten voldoen. Niet wordt verwacht dat deze overlap tot ongewenste gevolgen zal leiden. Voor zover de beveiligingseisen afkomstig van de specifiek voor de financiële markten geldende rechtshandelingen van de Unie feitelijk gelijkwaardig zijn aan de beveiligingseisen van de Csw, zal artikel 6 Csw worden toegepast en worden de desbetreffende Csw-eisen bij amvb buiten toepassing gelaten.

Meerdere organisaties verzoeken om te bezien of er een systeem kan komen waardoor bedrijven slechts één keer hoeven te melden. Een van de organisaties doet een voorstel om de uitvoering en naleving van diverse meldplichten te vergemakkelijken met behulp van een zogeheten «Meldplicht Quick Reference Card», waarbij de meldingsvereisten op een overzichtelijke manier worden gepresenteerd.

---

[17] Kamerstukken II 2017/18, 26 643, nr. 488.
[18] Kamerstukken II 2015/16, 29 544, nr. 733, p. 11.
[19] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer

Hierover merk ik op dat ernaar gestreefd wordt de dubbele meldplichten (CSIRT, bevoegde autoriteit) technisch zo in te richten dat het verspreiden van de benodigde informatie maar één handeling vergt. De suggestie van een «Meldplicht Quick Reference Card» zal daarbij ook in overweging worden genomen.

Naar aanleiding van een aantal specifieke vragen en opmerkingen zijn de wettekst en de memorie van toelichting op enkele plaatsen gecorrigeerd of aangevuld.

9. Grondrechtentoets

9.1. Inleiding

In paragraaf 6 en 7 van de memorie van toelichting bij de Wgmc is uitgebreid ingegaan op de grondrechtelijke aspecten vanwege de daarin geregelde verwerking van (persoons)gegevens door het NCSC en het in verband daarmee opgestelde privacy impact assessment (PIA).[20] Voor de taken van het NCSC, die reeds waren geregeld in de Wgmc, en de taken van het CSIRT voor AED's geldt dat daartussen geen noemenswaardige verschillen bestaan. Met het oog daarop wordt niet voorzien dat er krachtens de Csw sprake zal zijn van nieuwe verwerkingen van persoonsgegevens door het NCSC, ook niet in zijn hoedanigheid van «loket» voor vrijwillige incidentmeldingen (artikel 16 Csw). Om die reden is hiervoor geen aanvullend PIA uitgevoerd.

DNB heeft een PIA uitgevoerd voor haar verwerkingen als bevoegde autoriteit, voor wat betreft de meldplicht (nu het doorlopend toezicht ook al geschiedt op basis van de Wft en dit geen nieuwe verwerkingen inhouden). Het is nog niet bekend welke ambtelijke dienst namens de Minister van Infrastructuur en Waterstaat de taken van de bevoegde autoriteit zal uitvoeren, waardoor nog geen PIA kon worden uitgevoerd. In de sector gezondheidszorg wordt vooralsnog niet voorzien dat AED's worden aangewezen. Nu de IGJ i.o. vooralsnog geen taken van bevoegde autoriteit zal uitvoeren namens de Minister voor Medische Zorg, is in dit stadium voor de IGJ i.o. geen PIA uitgevoerd. Agentschap Telecom (AT), onderdeel van het Ministerie van EZK, zal voor de Minister van EZK de taken uitvoeren van de bevoegde autoriteit. Hoe de taken operationeel worden ingericht bij AT, wordt op dit moment nog nader vormgegeven. In dit stadium kan daarom nog geen PIA worden uitgevoerd.
Het CSIRT voor digitale diensten is nog niet aangewezen. Ook wordt nog onderzocht wie namens de Minister van Justitie en Veiligheid de taken van het centrale contactpunt uit zal voeren. Om die reden is ook voor die taken nog geen PIA uitgevoerd.

De tekst hierna is overgenomen van paragraaf 6 van de memorie van toelichting bij de Wgmc, waar mogelijk en aangewezen aangevuld met passages over de gegevensverwerkingen door het centrale contactpunt, het CSIRT voor DSP's, de bevoegde autoriteit en bij de behandeling van vrijwillige meldingen, alsook waar nodig aangepast aan de tekst van de Csw en de AVG.[21]

Het NCSC krijgt vanuit zijn rol als informatieknooppunt in het nationale en internationale netwerk met regelmaat de beschikking over aanzienlijke hoeveelheden data. Deze data komen binnen in het kader van een

[20] Zie voor de tekst daarvan de bijlage bij de nota naar aanleiding van het verslag, Kamerstukken II 2015/16, 34 388, nr. 6.
[21] Zoals toegelicht onder 8.8, is de Richtlijn dataprotectie niet van toepassing op verwerkingen ingevolge dit wetsvoorstel.

signalering van een incident of dreiging met betrekking tot een elektronisch informatiesysteem waarbij Nederlandse vitale aanbieders of niet-vitale aanbieders die onderdeel zijn van de rijksoverheid betrokken kunnen zijn. De Csw voorziet in een bevoegdheid om deze gegevens te verkrijgen en verder te verwerken ter voorkoming of beperking van het uitvallen van de beschikbaarheid of het verlies van integriteit van dergelijke elektronische informatiesystemen en ter verdere versterking van de digitale weerbaarheid van de Nederlandse samenleving. Vaak bevat een dataset IP-adressen, e-mailadressen en domeinnamen. Daarnaast verwerkt het NCSC contactgegevens van medewerkers van aanbieders die voor het NCSC als contactpersoon fungeren en van andere melders van incidenten en kwetsbaarheden. Het is denkbaar dat aan het NCSC een dataset wordt aangeboden die ook bijzondere persoonsgegevens bevat. Vooropgesteld zij dat het voor het NCSC met het oog op de uitoefening van de in artikel 3 Csw bedoelde taken niet nodig is om over bijzondere persoonsgegevens te beschikken. Uitgangspunt is dan ook dat het NCSC geen datasets in ontvangst neemt waarvan bekend is of vermoed wordt dat daarin ook bijzondere persoonsgegevens voorkomen. Degene die een dataset aanbiedt zal in een dergelijk geval worden gevraagd om de dataset te filteren en alleen die gegevens aan het NCSC te verstrekken die noodzakelijk zijn voor het uitvoeren van de NCSC-taken.[22] Voor bijvoorbeeld vitale aanbieders die het NCSC gegevens over dreigingen of incidenten willen verstrekken, geldt overigens uiteraard dat zij ook zelf, zeker ook aangaande bijzondere persoonsgegevens die mogelijkerwijs deel uitmaken van een dataset, de AVG in acht moeten nemen. Mocht pas na ontvangst van een dataset blijken dat daarin toch bijzondere persoonsgegevens voorkomen, dan zullen deze door het NCSC onmiddellijk worden vernietigd.

De Minister van Justitie en Veiligheid heeft krachtens dit wetsvoorstel ook de taak van centraal contactpunt. Het centrale contactpunt vervult ingevolge de NIB-richtlijn een verbindingsfunctie om te zorgen voor grensoverschrijdende samenwerking in EU-verband met de autoriteiten van andere lidstaten, met de samenwerkingsgroep en het CSIRT-netwerk. Bij de uitoefening van deze taak zullen ook persoonsgegevens worden verwerkt, meer in het bijzonder de contactgegevens van de medewerkers van centrale contactpunten van andere lidstaten. Ook is het denkbaar dat in het kader van de uitoefening van deze taak, meer in het bijzonder de verstrekking van incidentinformatie, bedoeld in artikel 19 Csw, andere persoonsgegevens zullen worden verwerkt (zoals de bij incidenten betrokken IP-adressen). Mocht hierbij de beschikking worden verkregen over bijzondere persoonsgegevens, dan zijn die persoonsgegevens ook in dit geval in beginsel niet nodig voor de uitoefening van de taken, en zal hiermee dus op dezelfde wijze worden omgegaan als hierboven beschreven voor de NCSC-taken.

De bevoegde autoriteit zal, voor wat betreft de AED's en DSP's, tot taak hebben om zorg te dragen voor de bestuursrechtelijke handhaving van het bepaalde bij en krachtens de Csw. Dat houdt onder meer in dat toezicht wordt gehouden op de naleving van de bij en krachtens de Csw vastgelegde verplichtingen voor AED's en DSP's (beveiligingsverplichtingen en meldplichten), audits kunnen worden opgelegd en de resultaten daarvan kunnen worden beoordeeld, en aan aanbieders bindende aanwijzingen kunnen worden gegeven. Bij de uitoefening van haar taken zal de bevoegde autoriteit de beschikking kunnen krijgen over persoonsgegevens. Naar verwachting zal het daarbij in hoofdzaak gaan over de contactgegevens van medewerkers van AED's en DSP's. Vooropgesteld zij dat het voor de bevoegde autoriteit, met het oog op de uitoefening van de

[22] Zie bijvoorbeeld de casus Hold Security, Kamerstukken II 2014/15, 26 643, nr. 328.

taken op grond van dit wetsvoorstel, niet nodig is om over bijzondere persoonsgegevens te beschikken. Mocht de bevoegde autoriteit deze desondanks ontvangen, dan zal zij die gegevens onmiddellijk vernietigen.

Dit wetsvoorstel introduceert verder een CSIRT voor DSP's. Hoewel nog niet bekend is welke instantie die taak gaat uitvoeren, ligt het voor de hand dat daarbij in belangrijke mate dezelfde typen persoonsgegevens zullen worden verwerkt als de persoonsgegevens die het NCSC verwerkt in zijn hoedanigheid van CSIRT voor AED's. Hoe dan ook zal het CSIRT voor DSP's alleen (persoons)gegevens verwerken voor zover dat noodzakelijk is ten behoeve van de in artikel 4, vierde lid, bedoelde taken, waarbij ook overigens de wetgeving inzake de bescherming van persoonsgegevens in acht zal worden genomen.

9.2. Inmenging door het openbaar gezag in het recht op respect voor de persoonlijke levenssfeer

De verwerking van persoonsgegevens door het NCSC, het CSIRT voor DSP's, de instantie voor vrijwillige meldingen en de bevoegde autoriteit is een inmenging door het openbaar gezag in het recht op respect voor de persoonlijke levenssfeer (de artikelen 10 Grondwet, 8 EVRM[23] en 17 IVBPR[24]). Artikel 8, eerste lid, EVRM bepaalt dat een ieder recht heeft op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. Het tweede lid staat inmenging in dit recht op respect voor de persoonlijke levenssfeer alleen toe voor zover zij bij wet is voorzien, een geoorloofd, expliciet genoemd doel dient en noodzakelijk is in een democratische samenleving. Het noodzaakcriterium wordt in de jurisprudentie van het Europese Hof voor de rechten van de mens (EHRM) nader ingevuld met de vereisten van een dringende maatschappelijke behoefte, proportionaliteit en subsidiariteit. Het wetsvoorstel is aan deze beginselen getoetst. Die toetsing wordt hieronder besproken. Het wetsvoorstel is ook getoetst aan artikel 10 Grondwet en artikel 17 IVBPR. Die toetsing leidt niet tot andere gezichtspunten.

9.2.1. De beperkende maatregel moet «voorzien bij wet» zijn
Artikel 17, eerste lid, Csw biedt een specifieke wettelijke grondslag voor de verwerking van persoonsgegevens door de Minister van Justitie en Veiligheid, en in de praktijk dus in hoofdzaak het NCSC. Die bepaling beperkt de verwerking van (persoons)gegevens tot de in artikel 3 omschreven doeleinden en taken. Voor een bespreking van de in artikel 3 omschreven taken zij verwezen naar paragraaf 4 (voor zover identiek aan de Wgmc-taken) en voor het overige (centraal contactpunt, CSIRT voor AED's en «loket» voor vrijwillige incidentmeldingen) naar de desbetreffende bepalingen van de NIB-richtlijn (met name artikel 8, derde lid, artikel 20 en bijlage I, onder 2). Specifiek wat betreft de onderzoekstaak (artikel 3, eerste lid, onder e) zij erop gewezen dat analyses en technisch onderzoek naar aanleiding van (aanwijzingen voor) dreigingen en incidenten met betrekking tot vitale elektronische informatiesystemen alleen tot de NCSC-taken behoren als die werkzaamheden in dienst staan van de NCSC-taken om bijstand te verlenen of te informeren en adviseren. Het is derhalve geen NCSC-taak om onderzoek te doen naar personen of organisaties die verantwoordelijk zijn voor die dreigingen en incidenten. Dergelijk onderzoek is voorbehouden aan de inlichtingen- en veiligheidsdiensten, die daartoe beschikken over wettelijk geregelde bijzondere inlichtingenmiddelen, en aan de politie en het OM, die daartoe beschikken over opsporingsbevoegdheden.

---

[23] Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden.
[24] Internationaal Verdrag inzake burgerrechten en politieke rechten.

Artikel 17, tweede lid, Csw biedt een specifieke wettelijke grondslag voor de verwerking van persoonsgegevens door de bevoegde autoriteit. Die bepaling beperkt de verwerking van (persoons)gegevens tot de in artikel 4, derde lid, omschreven taak: de bestuursrechtelijke handhaving van het jegens AED's en DSP's bepaalde bij of krachtens de Csw. Voor een bespreking van die taak zij verwezen naar paragraaf 6 en de artikelsgewijze toelichting bij artikel 4.

Artikel 17, derde lid, Csw biedt een specifieke wettelijke grondslag voor de verwerking van persoonsgegevens door het nog aan te wijzen CSIRT voor DSP's. Die bepaling beperkt de verwerking van (persoons)gegevens tot de in bijlage I, onder 2, van de NIB-richtlijn omschreven taken van een CSIRT.

9.2.2. De beperking moet een legitiem doel dienen en noodzakelijk zijn
Artikel 8, tweede lid, EVRM, bepaalt dat inmenging in het recht op respect voor het privéleven uitsluitend is toegestaan binnen de kaders van de expliciet en limitatief in dat lid opgesomde belangen.

Het NCSC verwerkt persoonsgegevens primair om de beschikbaarheid en de integriteit van informatiesystemen die nodig zijn ten behoeve van overheidsdiensten en andere voor de samenleving vitale producten en diensten, te waarborgen, en zodoende maatschappelijke ontwrichting te voorkomen. Verwerking van persoonsgegevens door het centrale contactpunt strekt tot uitvoering van de taak van centraal contactpunt, zoals omschreven in de NIB-richtlijn. Verwerking van persoonsgegevens door de bevoegde autoriteit strekt tot de bestuursrechtelijke handhaving (toezicht en sancties) van het jegens AED's en DSP's bepaalde bij en krachtens de Csw. Verwerking van persoonsgegevens door het CSIRT voor DSP's en door het NCSC bij de behandeling van vrijwillige incidentmeldingen strekt tot uitvoering van de CSIRT-taken zoals omschreven in de NIB-richtlijn, respectievelijk tot uitvoering van artikel 20 van de NIB-richtlijn. Deze verwerkingen dienen onder meer de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land. Deze belangen staan genoemd in artikel 8, tweede lid, EVRM.

De beperking dient bovendien noodzakelijk te zijn in een democratische samenleving. Het noodzaakcriterium wordt in de jurisprudentie van het EHRM nader ingevuld met de vereisten van een dringende maatschappelijke behoefte, proportionaliteit en subsidiariteit. Staten moeten redenen aandragen die voldoende en relevant zijn en hebben daarbij een eigen beoordelingsruimte.

9.2.2a. Dringende maatschappelijke behoefte
De dringende maatschappelijke behoefte van de verwerking van persoonsgegevens door het NCSC is gelegen in de grote afhankelijkheid van de samenleving van elektronische informatiesystemen, die bovendien onderling verweven zijn. De zorg voor veiligheid is een kerntaak van de overheid. Waarborging van de continuïteit van diensten en producten van vitale aanbieders en andere van de rijksoverheid deel uitmakende aanbieders is dan ook belangrijk om maatschappelijke ontwrichting te voorkomen.
IP-adressen worden door het NCSC verwerkt om de aard en ernst van digitale dreigingen en incidenten te kunnen beoordelen en om derden, met name vitale aanbieders en andere van de rijksoverheid deel uitmakende aanbieders, te kunnen waarschuwen en bijstaan. Enerzijds onderzoekt het NCSC de gegevens die deel uitmaken van een incidentmelding om te achterhalen vanaf welke IP-adressen een digitale aanval wordt uitgevoerd. Die IP-adressen worden verstrekt aan derden (binnen de kaders van de artikelen 3, 19 en 20) om hen in staat te stellen maatregelen te nemen tegen (mogelijke) aanvallen vanaf die adressen. Ander-

zijds onderzoekt het NCSC of de bij het NCSC bekende IP-adressen van vitale aanbieders en andere tot de rijksoverheid behorende aanbieders getroffen of kwetsbaar zijn en waarschuwt zo nodig de betrokken organisaties.
E-mailadressen worden door het NCSC verwerkt om derden te kunnen waarschuwen. Zo kan het voorkomen dat een door het NCSC ontvangen dataset e-mailadressen bevat die zijn buitgemaakt bij een ICT-inbreuk. Deze e-mailadressen kunnen voor malafide doeleinden gebruikt worden, zoals het versturen van spam, of kunnen – doordat zij betrokken zijn bij een ICT-inbreuk – een kwetsbaarheid vormen voor de organisatie waartoe zij behoren. Ook hierover informeert het NCSC derden binnen de kaders van de artikelen 3, 19 en 20 opdat zij maatregelen kunnen nemen om de beschikbaarheid of betrouwbaarheid van hun informatiesystemen te waarborgen. Verder verwerkt het NCSC de e-mailadressen van melders en andere contactpersonen van onder meer aanbieders van producten en diensten. Deze informatie is noodzakelijk om gevolg te kunnen geven aan een melding, het waarschuwen van anderszins gebleken betrokkenheid bij een ICT-inbreuk, of het informeren en adviseren over gebleken digitale dreigingen of kwetsbaarheden.
Domeinnamen worden door het NCSC verwerkt als het NCSC bij een melding informatie krijgt over kwetsbaarheden in websites. Om de digitale weerbaarheid van de Nederlandse samenleving te verhogen en nadelige maatschappelijke gevolgen te beperken of voorkomen is het van belang dat het NCSC ook deze informatie kan analyseren en (binnen de kaders van de artikelen 3, 19 en 20) kan delen met de juiste organisaties. Hoewel het CSIRT voor DSP's nog moet worden aangewezen bij amvb, is voor die instantie te verwachten dat de verwerking van persoonsgegevens in belangrijke mate vergelijkbaar zal zijn met de verwerkingen door het NCSC.

De dringende maatschappelijke behoefte van de verwerking van persoonsgegevens door de Minister van Justitie en Veiligheid in het kader van de uitoefening van de taken van het centrale contactpunt, door de bevoegde autoriteit en door het CSIRT voor DSP's is gelegen in de grote afhankelijkheid van de samenleving van elektronische informatiesystemen, die bovendien onderling verweven zijn. Om economisch welzijn te bevorderen, is van belang dat AED's en DSP's maatregelen nemen om de kans op incidenten te minimaliseren en de impact van eventuele incidenten te mitigeren. Dit wetsvoorstel strekt daartoe. Doordat er via het centrale contactpunt informatie beschikbaar komt die relevant is voor de borging van de continuïteit van de diensten van AED's, draagt dit bovendien bij aan het voorkomen van maatschappelijke ontwrichting.

Handhaving van de Csw-verplichtingen is van belang om voornoemde effectieve maatregelen te verzekeren. Om te kunnen handhaven, zal de bevoegde autoriteit persoonsgegevens moeten verwerken. Het gaat hierbij in hoofdzaak om contactgegevens van de contactpersonen voor de bevoegde autoriteit bij onder meer de organisaties waarop toezicht wordt gehouden.

Ter bevordering van de grensoverschrijdende samenwerking is het nodig dat iedere lidstaat een centraal contactpunt aanwijst dat verantwoordelijk is voor het zorg dragen voor het leggen van verbindingen ten behoeve van die samenwerking op Unieniveau, en meer in het bijzonder het informeren van andere lidstaten in geval van incidenten met grensoverschrijdende consequenties. Om deze taak uit te kunnen voeren is het nodig dat het centrale contactpunt persoonsgegevens verwerkt. Het kan hierbij gaan om informatie uit meldingen die worden doorgegeven aan andere lidstaten om hen in staat te stellen adequaat te reageren op grensoverschrijdende meldingen (denk bijvoorbeeld aan het IP-adres van

een aanvaller) en het spiegelbeeld daarvan (informatie die het centrale contactpunt ontvangt van andere centrale contactpunten), maar ook om bijvoorbeeld contactgegevens van andere centrale contactpunten. Zie artikel 19 Csw.

9.2.2b. Proportionaliteit
Het NCSC verwerkt grote aantallen persoonsgegevens,[25] maar gelet op de aard ervan (bijvoorbeeld IP- en e-mailadressen, contactgegevens van melders), het doel waarvoor zij worden verwerkt en de overige waarborgen waarmee deze gegevens zijn omkleed, gaat het niet om een forse inmenging in het recht op respect voor iemands privéleven. Zo doet het NCSC geen onderzoek naar individuele personen die bij een ICT-inbreuk betrokken zijn. De betrokken gegevens worden door het NCSC verwerkt met inachtneming van de Wbp (vanaf mei 2018 de AVG), onder intern toezicht van de functionaris gegevensbescherming en onder extern toezicht van de Autoriteit Persoonsgegevens. Het NCSC verwerkt slechts gegevens voor zover dat noodzakelijk is voor het uitvoeren van de in artikel 3 genoemde taken. Persoonsgegevens die het NCSC verwerkt ten behoeve van zijn taken worden bovendien niet langer door het NCSC bewaard dan noodzakelijk. Zo worden contactgegevens van de melder bijvoorbeeld na maximaal 13 maanden na het afhandelen van de melding vernietigd en worden andere persoonsgegevens, die benodigd zijn voor de uitoefening van de taken van het NCSC, uiterlijk 18 maanden na het afhandelen van een incident of dreiging vernietigd. Deze bewaartermijnen zijn gebaseerd op de blijkens de huidige NCSC-praktijk gemiddeld benodigde maximale termijn om de NCSC-taken naar behoren te kunnen vervullen. Zo moet ook na enige tijd nog contact kunnen worden gezocht met de melder, bijvoorbeeld voor opvolging (hoe staat het er nu voor? heeft de aanbieder het NCSC-advies gevolgd of zijn er andere maatregelen getroffen?) of om hem te waarschuwen voor kwetsbaarheden die zijn systeem opnieuw in gevaar kunnen brengen. Andere persoonsgegevens in voormelde zin (bijvoorbeeld IP-adressen) kunnen van belang zijn als bijvoorbeeld blijkt dat een bepaald IP-adres opnieuw geraakt wordt of een digitale aanval steeds vanuit dezelfde hoek komt. Dit kan voor het NCSC aanleiding zijn om te onderzoeken of de aanval ook relevant is voor andere recent getroffen IP-adressen. Ook kan uit nieuw onderzoek van een afgehandeld incident blijken dat relevante informatie, zoals een kwetsbaarheid van bepaalde IP-adressen of een bepaalde aanvalstechniek, over het hoofd is gezien. De bewaartermijnen zullen geregeld opnieuw worden beoordeeld en zullen dan zo mogelijk worden verkort en zo nodig worden verlengd. De huidige door het NCSC gehanteerde bewaartermijnen komen overigens overeen met de internationaal door CERT's gehanteerde termijnen.
Hoewel het CSIRT voor DSP's nog moet worden aangewezen bij amvb, is voor die instantie te verwachten dat de verwerking van persoonsgegevens in belangrijke mate vergelijkbaar zal zijn met de verwerkingen door het NCSC.
De bevoegde autoriteit verwerkt slechts persoonsgegevens voor zover dit noodzakelijk is voor het uitoefenen van haar in artikel 4, derde lid, Csw genoemde taak en met inachtneming van de Wbp (vanaf mei 2018 de AVG), onder toezicht van de Autoriteit Persoonsgegevens. Persoonsgegevens die de bevoegde autoriteit verwerkt ten behoeve van haar taak worden niet langer bewaard dan noodzakelijk.

Ter uitvoering van de NIB-richtlijn moet het centrale contactpunt in de gevallen, bedoeld in artikel 19 Csw, informatie doorgeven aan de centrale contactpunten van andere getroffen lidstaten. Hierbij zal telkens de

[25] Zie bijvoorbeeld de getallen, genoemd in de brief van 13 oktober 2014, Kamerstukken II 2014/15, 26 643, nr. 328 (casus Hold Security).

afweging gemaakt moeten worden of het nodig is persoonsgegevens mee te sturen. Ook ontvangt het centrale contactpunt gegevens van andere centrale contactpunten, waaronder persoonsgegevens. Voor die ontvangen persoonsgegevens zal telkens bekeken moeten worden of het, met het oog op de voor het centrale contactpunt in dit wetsvoorstel opgenomen taken, nodig is die te bewaren, en zo ja, voor hoe lang.

9.2.2c. Subsidiariteit
Het NCSC kan zijn taken niet uitoefenen wanneer het niet zou beschikken over de persoonsgegevens die vaak deel uitmaken van datasets die het NCSC verkrijgt bij de melding van een incident. Het NCSC kan niet op een andere wijze de informatie verkrijgen die noodzakelijk is voor het uitoefenen van zijn taken. Ook anonimiseren of pseudonimiseren[26] van de data is voor het NCSC niet mogelijk: als de data niet individualiseerbaar zijn, dan kan het NCSC niet onderzoeken welke partijen zijn geraakt en hen rechtstreeks informeren en dan kan het ook de herkomst en het verdere verloop van de dreiging of het incident niet onderzoeken. Hoewel het CSIRT voor DSP's nog moet worden aangewezen bij amvb, is voor die instantie te verwachten dat de verwerking van persoonsgegevens in belangrijke mate vergelijkbaar zal zijn met de verwerkingen door het NCSC.

Het centrale contactpunt kan zijn taken niet uitvoeren zonder de verwerking van de persoonsgegevens die nodig zijn om contact te leggen met de centrale contactpunten van andere lidstaten. Ter uitvoering van de NIB-richtlijn moet het centrale contactpunt bovendien in de gevallen, bedoeld in artikel 19 Csw, op verzoek van de bevoegde autoriteit of het CSIRT meldingen eventueel ook met daarvan deel uitmakende persoonsgegevens doorsturen aan de centrale contactpunten van andere getroffen lidstaten, inclusief de persoonsgegevens in die melding.

De bevoegde autoriteit op haar beurt kan haar toezichttaken niet uitoefenen zonder de verwerking van de persoonsgegevens die nodig zijn om contact te leggen met de aanbieders waarop zij toezicht houdt.

10. Gevolgen voor de rijksbegroting

Ministerie van Justitie en Veiligheid

De Csw heeft geen gevolgen voor de begroting van het Ministerie van Justitie en Veiligheid. Er vloeien voor dit ministerie nauwelijks nieuwe taken voort uit dit wetsvoorstel. De minimale extra belasting wordt opgevangen binnen de huidige formatie en de lopende begroting.

Ministerie van Economische Zaken en Klimaat

Voor het Ministerie van EZK bedragen de kosten voor de voorbereiding van de Csw-taken in 2017 0,422 miljoen euro. Zij worden gedekt uit artikel 1 van de begroting van dat ministerie. De structurele dekking voor de jaren 2018 en verder wordt geregeld bij voorjaarsnota 2018.

Ministerie van Financiën

Voor het Ministerie van Financiën alsmede voor de bevoegde autoriteit DNB worden de kosten geraamd op 0. Er vloeien voor DNB nauwelijks nieuwe taken voort uit dit wetsvoorstel. De minimale extra belasting wordt opgevangen binnen de huidige formatie van DNB.

[26] Het vervangen, met een bepaald algoritme, van identificerende gegevens door versleutelde gegevens.

Ministerie van Infrastructuur en Waterstaat

Het onderdeel van het Ministerie van Infrastructuur en Waterstaat dat de Csw-taken zal uitvoeren ten behoeve van de betrokken bewindspersoon is uiterlijk mei 2018 bekend. Dat onderdeel stelt vervolgens een formele offerte op. Dekking van de vermoedelijk benodigde bedragen voor 2018 e.v. zal door het Ministerie van Infrastructuur en Waterstaat bij voorjaarsnota 2018 worden geregeld.

Ministerie van Volksgezondheid, Welzijn en Sport

In bijlage II bij de NIB-richtlijn wordt de gezondheidszorg genoemd als sector met potentiële AED's, met als deelsector zorginstellingen. Het is aan de lidstaten om te bepalen welke zorgaanbieders in hun land voldoen aan de criteria voor de aanwijzing van AED's in de artikelen 5, eerste lid, en 6 van de NIB-richtlijn. Vooralsnog wordt niet voorzien dat Nederland zorgaanbieders aanwijst als AED. Indien op een later moment AED's worden aangewezen (bij amvb, zie artikel 5, eerste lid, Csw), zal ten behoeve van de besluitvorming in de ministerraad, in de toelichting bij de amvb expliciet worden ingegaan op de eventuele gevolgen voor de rijksbegroting.

11. Regeldruk

11.1. Inleiding

De door de Csw veroorzaakte regeldruk bestaat uit een bescheiden stijging van de administratieve lasten en inhoudelijke nalevingskosten. De Csw brengt nieuwe verplichtingen met zich mee voor AED's en DSP's. Deze paragraaf bespreekt de meldplicht voor ernstige ICT-incidenten, beveiligingseisen zoals opgenomen in hoofdstuk 4 Csw en eenmalige kennisnamekosten en toezichtlasten. De Csw heeft geen gevolgen voor de regeldruk voor burgers en evenmin voor organisaties die noch worden aangewezen op grond van artikel 5 Csw, noch een DSP zijn in de zin van artikel 1 Csw.

11.2. Meldplicht

De meldplicht is een informatieverplichting en daarmee een administratieve last.

Uit de Csw volgt een meldplicht voor AED's bij zowel het CSIRT als de bevoegde autoriteit. Uitgangspunt is de meldplicht in te richten op een lastenluwe manier. Er wordt naar gestreefd de meldplichten technisch zó in te richten dat het verspreiden van de benodigde informatie maar één handeling vergt, hetgeen de administratieve lasten reduceert. De inrichting van de meldplicht wordt in overleg met betrokken departementen, bevoegde autoriteiten en de sector nader uitgewerkt.

Per categorie aanbieders kan nadere invulling worden gegeven aan de parameters die bepalen wanneer incidenten meldplichtig zijn. Naar verwachting zal deze meldplicht niet leiden tot een groot aantal meldingen voor AED's, daar alleen ernstige incidenten dienen te worden gemeld. Het aantal AED's zal naar schatting 60 organisaties betreffen. Aangezien AED's incidenten dienen te melden met aanzienlijke gevolgen voor de continuïteit van de door hen verleende essentiële diensten is, in lijn met de inschatting zoals vermeld in de toelichting bij het Bmc, de verwachting dat niet meer dan 10 tot 20 ICT-incidenten per jaar onder de meldplicht zullen vallen.

De Csw introduceert een meldplicht voor DSP's voor ICT-incidenten met aanzienlijke gevolgen voor de verlening van de door de DSP verleende dienst in de Europese Unie. Naar verwachting zullen tussen de 100 en 200 DSP's onder de Nederlandse rechtsmacht vallen, dus wordt uitgegaan van een schatting van 150 organisaties. Voor DSP's worden door de Europese Commissie nog nadere parameters uitgewerkt voor wat aanzienlijke gevolgen zijn. Om deze reden valt nog geen accurate inschatting te maken van de hoeveelheid meldplichtige ICT-incidenten per jaar, maar gezien de hoge drempel ga ik uit van maximaal 15 meldplichtige incidenten per jaar. Dit is gebaseerd op een meldplichtig incident bij 10% van 150 DSP's.

Voor het verrichten van een melding zal het veelal gaan om handelingen als het verzamelen van informatie, het schriftelijk en eventueel telefonisch doen van een melding en het eventueel verstrekken van nadere informatie aan het CSIRT en/of de bevoegde autoriteit. De tijd die het organisaties zal kosten om een melding en vervolghandelingen te doen onder de meldplicht zal verschillen per ICT-incident en zal onder andere afhankelijk zijn van hoe ernstig en complex het incident is. De meldplicht geldt alleen voor incidenten met aanzienlijke gevolgen voor de continuïteit van de door de AED of DSP verleende dienst. Daarom wordt uitgegaan van grootschalige en complexe incidenten en zullen de melding en extra vervolghandelingen naar schatting gemiddeld 300 minuten betreffen per incident. Hierbij wordt aangesloten bij de inschatting van 260 minuten, zoals die is vermeld in de toelichting bij het Bmc. De Wgmc bevat enkel een verplichting tot melding aan het NCSC. Onder de Csw kunnen ook vervolghandelingen voor een organisatie ontstaan als gevolg van vragen of optreden van de bevoegde autoriteit naar aanleiding van de melding. Hoewel naar schatting veelal vergelijkbare informatie zal worden opgevraagd door het CSIRT en de bevoegde autoriteit, zullen mogelijk extra handelingen verricht dienen te worden op verzoek van de bevoegde autoriteit. Hiervoor is een opslag van 15% gerekend, zodat de vereiste tijd uitkomt op 300 minuten per melding. Als uurtarief wordt € 60 gehanteerd, een gangbaar tarief voor hoogopgeleide kenniswerkers.[27] Voor DSP's is de meldplicht bij ICT-incidenten nieuw. Een groot deel van de nog aan te wijzen AED's valt daarentegen reeds onder de meldplicht die voortvloeit uit de Wgmc.[28] Daarom bedragen de nieuwe administratieve lasten per melding 300 minuten voor DSP's (€ 300 per melding), en 40 minuten (300 minus 260 minuten) voor AED's (€ 40 per melding). Bijvoorbeeld bij 10 meldingen per jaar, waaronder 4 meldingen voor DSP's en 6 meldingen voor AED's, zou dit neerkomen op ((4 x € 300 = € 1.200) + (6 x € 40 = € 240) =) € 1.440.

11.2.1. Ministerie van Economische Zaken en Klimaat
Voor beheerders van elektriciteits- en gasnetten alsmede voor internet-knooppunten geldt op grond van de Wgmc reeds de verplichting om ICT-incidenten te melden bij het NCSC. Nieuw onder de Csw is de meldplicht bij de bevoegde autoriteit, wat voor deze partijen extra verplichtingen meebrengt. Voor de AED's in overige sectoren die onder de verantwoordelijkheid van de Minister van EZK vallen en voor de DSP's zijn beide meldplichten nieuw. De administratieve lasten zullen voor wat betreft de meldplicht voor deze organisaties dus hoger zijn, zie de hiervoor genoemde berekening.

[27] Handboek meting regeldruk, 1-7-2014, p. 69.
[28] In deze uitwerking zijn de vitale aanbieders die reeds onder de Wgmc vallen buiten beschouwing gelaten, omdat eventuele administratieve lasten voor hen reeds zijn meegenomen bij de Wgmc.

11.2.2. Ministerie van Financiën
Voor de AED's die onder de verantwoordelijkheid vallen van de Minister van Financiën geldt op grond van de Wgmc reeds een verplichting om ICT-incidenten te melden bij het NCSC. Daarnaast gelden voor deze AED's – hoewel vanuit een andere doelstelling – op grond van financiële toezichtwetgeving reeds verplichtingen om incidenten te melden bij de toezichthouder. Met de Csw verandert er dan ook nauwelijks iets aan de feitelijke situatie, waardoor er niet tot nauwelijks sprake zal zijn van een toename van administratieve lasten als gevolg van de in de Csw opgenomen meldplichten.

11.2.3. Ministerie van Infrastructuur en Waterstaat
Voor de aan te wijzen AED's die onder de verantwoordelijkheid van de Minister van Infrastructuur en Waterstaat vallen, geldt op grond van de Wgmc reeds de verplichting om ICT-incidenten te melden bij het NCSC. Nieuw onder de Csw is de meldplicht bij de bevoegde autoriteit, wat voor deze partijen extra verplichtingen meebrengt.

11.2.4. Ministerie van Volksgezondheid, Welzijn en Sport
Vooralsnog wordt niet voorzien dat zorgaanbieders worden aangewezen als AED's. Daarom wordt geen extra regeldruk voor organisaties in de zorg voorzien.

11.3. Beveiligingseisen

Aanbieders moeten passende technische en organisatorische maatregelen treffen ter beveiliging van hun netwerk- en informatiesystemen. In navolging van de NIB-richtlijn is deze zorgplicht in de Csw geformuleerd als een open norm.
Ook zonder wetgeving hebben aanbieders al de nodige beveiligingsmaatregelen getroffen, zijnde een combinatie van organisatorische en technische maatregelen. Immers voor de continuïteit van hun eigen bedrijfsvoering is het cruciaal dat maatregelen worden getroffen op het gebied van netwerk- en informatiebeveiliging. Zonder maatregelen is men zeer kwetsbaar voor tal van dreigingen, zoals cybercrime, stroomstoringen en menselijke fouten. Daarbij zouden aanbieders een reëel risico kunnen lopen waarbij een correcte levering van hun eigen diensten in gevaar komt, zoals de levering van gas, het verrichten van financiële transacties en het vervoeren van personen en goederen door de lucht of over water.
Aanbieders zullen dus al de nodige investeringen hebben gedaan op het gebied van beveiliging van hun ICT-systemen om zodoende incidenten en – als gevolg daarvan – mogelijk grote schadeposten zoveel mogelijk te voorkomen. Indien nadere beveiligingseisen worden gesteld bij of krachtens amvb, zal daarin nader worden ingegaan op eventueel daaruit voortvloeiende nalevingskosten. Dit zal afhankelijk zijn van de mate waarin de beveiligingseisen overeenkomen met wat reeds wordt toegepast. Bij het opstellen van beveiligingseisen is overigens denkbaar dat aansluiting wordt gezocht bij wat gangbaar is in een sector. Om dit te kunnen bereiken zal overleg plaatsvinden tussen de betrokken bevoegde autoriteit en de sector.

11.4. Eenmalige kennisnamekosten en toezichtlasten

AED's en DSP's zullen eenmalig tijd besteden aan het verdiepen in en kennisnemen van de Csw. Organisaties zullen hier naar schatting 16 uur (2 werkdagen) voor nodig hebben. Uitgaande van een uurtarief van € 60[29] komt dit uit op € 960 eenmalige kennisnamekosten per organisatie. Voor

[29] Handboek meting regeldruk, p. 69.

het verrichten van dagelijkse werkzaamheden, zal een bevoegde autoriteit contact zoeken met organisaties die onder haar toezicht vallen. Met het te onderhouden contact en te woord staan van de bevoegde autoriteit gaan administratieve lasten gepaard voor AED's en DSP's. Ook op dit punt zullen organisaties naar schatting 16 uur (2 werkdagen) nodig hebben, uitkomend op € 60[30] x 16 = € 960 per organisatie. Uitgaande van 150 DSP's en 60 AED's, komt dit neer op € 960 x 210 = € 201.600.

De bevoegde autoriteit kan een AED verplichten een beveiligingsaudit uit te voeren door een onafhankelijke deskundige. De kosten voor een volledige audit worden ingeschat op € 50.000. Nu toezicht op cybersecurity nieuw is, is voorafgaand aan inwerkingtreding van de Csw niet vast te stellen hoe vaak de bevoegde autoriteit het nodig zal vinden deze verplichting op te leggen. In bepaalde gevallen zal in ieder geval volstaan kunnen worden met een audit op onderdelen, die een audit aanvult die een AED uit laat voeren in de normale bedrijfsvoering. Naar verwachting wordt deze maatregel gebruikt bij 10% van de aan te wijzen AED's.

11.5. Advies Adviescollege Toetsing Regeldruk

Dit wetsvoorstel is voorgelegd voor advies aan het Adviescollege Toetsing Regeldruk[31]. Naar aanleiding van het advies is deze toelichting op enkele punten aangepast. Op hoofdlijnen houden deze aanpassingen verduidelijkingen in op de onderwerpen DSP's, vormgeving van de meldplicht en berekening van de regeldruk.

12. Transponeringstabel

Bepaling NIB-richtlijn[1]	**Bepaling in Csw of bestaande regeling: Toelichting indien niet geïmplementeerd of naar zijn aard geen implementatie nodig[2]**	**Toelichting op de keuze(n) bij de invulling van de beleidsruimte**
Artikel 1 lid 3 (uitzondering voor richtlijn 2002/21/EG en voor elektronische vertrouwensdiensten)	Wordt omgezet door deze aanbieders niet aan te wijzen o.g.v. art. 5 lid 1 onder a Csw.	
Artikel 1 lid 5 (vertrouwelijkheid)	Art. 20–22 Csw	
Artikel 1 lid 7 (voorrang voor sectorspecifieke EU-regels)	Art. 6 Csw	
Overige leden artikel 1	Behoeven geen implementatie want betreft uitleg richtlijn.	
Artikel 2 (bescherming en verwerking persoonsgegevens)	Art. 17 Csw	
Artikel 3 (minimumharmonisatie)	De bevoegdheid om te kiezen voor een hoger niveau van beveiliging is gebruikt (voor AED's en andere aangewezen vitale aanbieders) in art. 10 lid 1 onder b Csw (overgenomen uit art. 6 lid 1 Wgmc, «of kan worden onderbroken»).	

[30] Handboek meting regeldruk, p. 69.
[31] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer

Bepaling NIB-richtlijn[1]	Bepaling in Csw of bestaande regeling: Toelichting indien niet geïmplementeerd of naar zijn aard geen implementatie nodig[2]	Toelichting op de keuze(n) bij de invulling van de beleidsruimte
Artikel 4 (definities)	Art. 1 Csw (voor zover de begrippen in de Csw worden gebruikt).	
Artikel 5 lid 1–3 (aanwijzing AED's)	Art. 5 Csw	
Overige leden artikel 5	Behoeven geen implementatie, want betreft feitelijk handelen.	
Artikel 6 (criterium AED)	Art. 5 lid 2 Csw	
Artikel 7 (nationale strategie)	Behoeft geen implementatie want betreft feitelijk handelen.	
Artikel 8 lid 1 en 2 (aanwijzing bevoegde autoriteit)	Art. 4 lid 1, lid 2 onder a en lid 3 en art. 16 lid 2 Csw	De richtlijn laat het aan de lidstaten om een of meer bevoegde autoriteiten aan te wijzen. De Csw wijst de vakministers resp. DNB aan als bevoegde autoriteit.
Artikel 8 lid 3 en 4 (aanwijzing centraal contactpunt)	Art. 2 onder a, art. 3 lid 1 onder a en art. 19 Csw	
Overige leden artikel 8	Behoeven geen implementatie want betreft feitelijk handelen.	
Artikel 9 lid 1 (aanwijzing CSIRT)	Voor AED's: art. 2 onder b, 3 lid 1 onder b en 17 lid 1 Voor DSP's: art. 4 lid 2 onder b en lid 4 en 17 lid 3 Csw	De richtlijn laat het aan de lidstaten om een of meer CSIRT's aan te wijzen. De Csw wijst de Minister van Justitie en Veiligheid aan als CSIRT voor AED's. Aanwijzing CSIRT voor DSP's bij amvb.
Overige leden art. 9	Behoeven geen implementatie want betreft feitelijk handelen.	
Artikel 10 lid 1 (samenwerking nationaal)	Art. 20 lid 3, 20 lid 4 onder a en art. 21 lid 3 en 4 Csw	
Artikel 10 lid 2 (bevoegde autoriteit en CSIRT informeren over incidenten)	Eerste volzin: art. 10, 11 en 12 Csw. De tweede volzin is niet van toepassing vanwege de keuze om een incident ook bij het CSIRT te laten melden.	
Artikel 10 lid 3 (centraal contactpunt informeren over incidenten)	Voor DSP's omgezet in art. 19 lid 1 Csw. Voor AED's behoeft lid 3 geen implementatie omdat de Minister van Justitie en Veiligheid zowel het centrale contactpunt is als het CSIRT. De tweede volzin behoeft geen implementatie want betreft feitelijk handelen.	
Artikel 11 (samenwerkingsgroep lidstaten, EC en Enisa)	Behoeft geen implementatie want betreft feitelijk handelen.	
Artikel 12 (CSIRT-netwerk lidstaten)	Behoeft geen implementatie want betreft feitelijk handelen.	

Bepaling NIB-richtlijn[1]	Bepaling in Csw of bestaande regeling: Toelichting indien niet geïmplementeerd of naar zijn aard geen implementatie nodig[2]	Toelichting op de keuze(n) bij de invulling van de beleidsruimte
Artikel 13 (internationale samenwerking)	Behoeft geen implementatie want betreft handelen EU.	
Artikel 14 lid 1 en 2 (beveiligingseisen AED's)	Art. 7–9 Csw	
Artikel 14 lid 3 en 4 (meldplicht AED's)	Art. 10 lid 1 onder a en lid 2 en 4, en art. 11 en 12 Csw	Art. 10 Csw regelt dat een AED een ernstig incident moet melden bij het NCSC en bij de bevoegde autoriteit. Een bijna-ongeluk (zie art. 10 lid 1 onder b) hoeft alleen gemeld te worden bij het NCSC.
Artikel 14 lid 5 (andere lidstaat informeren)	Art. 19 lid 2 Csw. Tweede volzin: art. 20 lid 1 Csw. Laatste volzin: art. 19 lid 3 Csw.	
Artikel 14 lid 6 (publiek informeren)	Art. 23 onder a Csw	
Artikel 14 lid 7 (richtsnoeren)	Behoeft geen implementatie want betreft feitelijk handelen.	
Artikel 15 lid 1 (toezicht op de naleving AED's)	Art. 4 lid 3 en hoofdstuk 6 Csw, in samenhang met hoofdstuk 5 Awb	
Artikel 15 lid 2 onder a (informatie verschaffen)	Art. 25 Csw, in samenhang met titel 5.2 Awb	
Artikel 15 lid 2 onder b (beveiligingsaudit)	Art. 26 Csw	
Artikel 15 lid 3 (bindende aanwijzing)	Art. 27 Csw	
Artikel 15 lid 4 (samenwerken met autoriteiten gegevensbescherming)	Behoeft geen implementatie want betreft feitelijk handelen.	
Artikel 16 lid 1 en 2 (beveilingseisen DSP's)	Art. 7–9 Csw	
Artikel 16 lid 3 en 4 (meldplicht DSP's)	Art. 13 Csw	Art. 13 Csw regelt dat een DSP een ernstig incident moet melden bij het CSIRT en bij de bevoegde autoriteit.
Artikel 16 lid 5 (meldplicht AED bij incident DSP)	Art. 10 lid 3 en lid 5 Csw	
Artikel 16 lid 6 (andere lidstaat informeren)	Eerste volzin: art. 19 lid 4 Csw. Tweede volzin: art. 20 lid 1 Csw.	
Artikel 16 lid 7 (publiek informeren)	Art. 23 onder b Csw	
Artikel 16 lid 8 en 9 (uitvoeringshandelingen EC)	Art. 9 en 15 Csw	
Artikel 16 lid 10 (verbod om andere eisen op te leggen)	Behoeft geen implementatie want betreft feitelijk handelen.	

Bepaling NIB-richtlijn[1]	Bepaling in Csw of bestaande regeling: Toelichting indien niet geïmplementeerd of naar zijn aard geen implementatie nodig[2]	Toelichting op de keuze(n) bij de invulling van de beleidsruimte
Artikel 16 lid 11 (uitzondering kleine en micro-ondernemingen)	Omschrijving van *digitale-dienstverlener* in art. 1 Csw	
Artikel 17 lid 1 en lid 2 onder b (toezicht en sancties DSP's)	Art. 4 lid 3 en hoofdstuk 6 Csw, in samenhang met hoofdstuk 5 Awb	
Artikel 17 lid 2 onder a (informatie verschaffen)	Art. 25 Csw, in samenhang met titel 5.2 Awb	
Artikel 17 lid 3 (samen-werken met bevoegde autoriteit in andere lidstaat)	Behoeft geen implementatie want betreft feitelijk handelen.	
Artikel 18 (jurisdictie en territorialiteit DSP's)	Omschrijving van *digitale-dienstverlener* in art. 1 Csw	
Artikel 19 (normalisatie)	Behoeft geen implementatie want betreft feitelijk handelen.	
Artikel 20 (vrijwillige melding)	Art. 2 onder c, 3 lid 3, 16 en 17 lid 1 Csw	
Artikel 21 (sancties)	Art. 27–29 Csw, in samenhang met titel 5.3 en 5.4 Awb	
Artikel 22–27 (diverse onderwerpen)	Behoeft geen implementatie want betreft feitelijk handelen of handelen EC.	

[1] Richtlijn (EU) 2016/1148 van het Europees parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PbEU 2016, L 194).
[2] Gebruikte afkortingen:
amvb: algemene maatregel van bestuur
Awb: Algemene wet bestuursrecht
AED: aanbieder van een essentiële dienst
CSIRT: computer security incident response team
Csw: Cybersecuritywet
DSP: digitaledienstverlener
Wft: Wet op het financieel toezicht

Artikelsgewijze toelichting

Artikel 1 (begripsbepalingen)

Alleen begrippen die nieuw zijn ten opzichte van de Wgmc, worden toegelicht. Voor het overige zij verwezen naar de memorie van toelichting op de Wgmc.[32]

aanbieder:
– «overheidsorganisatie of *privaatrechtelijke* rechtspersoon»: net als in Wgmc toegevoegd om overlap met overheidsorganisatie te voorkomen.
– ziet (indien als zelfstandige term gebruikt, zoals in artikel 20 [verstrekking vertrouwelijke gegevens door de Minister van Justitie en Veiligheid]) ook op de DSP.

[32] Kamerstukken II 2015/16, 34 388, nr. 3.

incident: een «inbreuk» (artikel 10, eerste lid, onder b) is ook een incident als gedefinieerd in de richtlijn, want ook bij een inbreuk is er daadwerkelijk schadelijk effect op de beveiliging van netwerk- en informatiesystemen.

CSIRT: ziet alleen op CSIRT's die zijn aangewezen door Nederland of een andere lidstaat van de EU en die derhalve geacht worden te voldoen aan de vereisten van de richtlijn (artikel 9, eerste lid, in samenhang met bijlage I, onder 1).

digitaledienstverlener: beperking tot *rechtspersoon* is overgenomen van definitie artikel 4 onder 6 richtlijn; beperking tot jurisdictie Nederland in de zin van artikel 18 richtlijn houdt in: ofwel hoofdvestiging in Nederland (artikel 18, eerste lid), ofwel (voor wat betreft een DSP van buiten de EU) EU-vertegenwoordiger gevestigd in Nederland (artikel 18, tweede lid); de uitzondering voor kleine en micro-ondernemingen volgt uit artikel 16, elfde lid, van de richtlijn. Voor meer achtergrond bij digitale diensten, zie par. 5 van het algemeen deel van deze memorie.

vitale aanbieder: de Wgmc-formulering «beschikbaarheid en betrouwbaarheid» is vervangen door het richtlijn-begrip «continuïteit». Daarmee is geen inhoudelijke wijziging beoogd.

Artikel 2 (centraal contactpunt; CSIRT voor AED's; loket voor vrijwillige incidentmeldingen)

Dit artikel wijst de Minister van Justitie en Veiligheid aan als het in artikel 8 van de richtlijn bedoelde centrale contactpunt en het in artikel 9 van de richtlijn bedoelde CSIRT voor AED's en als het «loket» voor de in artikel 16 Csw (artikel 20 van de richtlijn) bedoelde vrijwillige incidentmeldingen.

Artikel 3 (taken van Onze Minister)

Dit artikel is voor een groot deel identiek aan artikel 2 Wgmc en implementeert mede de artikelen 8 en 20 van de richtlijn. Het artikel bevat een opsomming van de taken van de Minister van Justitie en Veiligheid op het terrein van cybersecurity, ten behoeve waarvan verwerking van gegevens, waaronder persoonsgegevens, aangewezen is, en omschrijft (in de aanhef van het eerste en tweede lid) de doeleinden van die taken.

Afgezien van terminologische aanpassingen (vervanging van *informatiesystemen* door *netwerk- en informatiesystemen* en van *beschikbaarheid en betrouwbaarheid* door *continuïteit)* bevat artikel 3 de volgende wijzigingen ten opzichte van artikel 2 Wgmc:

– Eerste lid:
  a. Aan het slot van de aanhef is toegevoegd: en ter uitvoering van de NIB-richtlijn. De relevantie hiervan is met name dat de Minister van Justitie en Veiligheid mede tot taak heeft om bij te dragen aan samenwerking tussen de lidstaten (zie de artikelen 8, vierde en vijfde lid, en 12, eerste en tweede lid, van de richtlijn).
  b. Aan het begin van de opsomming zijn twee onderdelen toegevoegd om buiten twijfel te stellen dat de Minister van Justitie en Veiligheid met de aanwijzing in artikel 2 tot centraal contactpunt en tot CSIRT voor AED's, ook de taken van die instanties heeft. Er zit enige overlap tussen enerzijds die onderdelen a en b en anderzijds de onderdelen c, d en e.
– Tweede lid:
  a. In de aanhef is na ter voorkoming van nadelige maatschappelijke gevolgen toegevoegd: in en buiten Nederland.

b. De NIB-richtlijn introduceert CSIRT's, wat in feite de nationale computercrisisteams zijn. De Wgmc maakt geen onderscheid tussen CSIRT's en andere computercrisisteams. Daarom zijn CSIRT's aan de opsomming in het tweede lid toegevoegd. Blijkens de omschrijving in artikel 1 zijn dat de CSIRT's die door een lidstaat van de EU (op grond van artikel 9 van de richtlijn) zijn aangewezen. Voor die CSIRT's gelden de vereisten van bijlage I, onder 1, van de richtlijn. Taken van een CSIRT zijn onder andere het monitoren van incidenten op nationaal niveau, reageren op incidenten en zorgen voor een dynamische risico- en incidentanalyse en situatiekennis. Gegevensuitwisseling met andere CSIRT's dan het NCSC (waaronder het op grond van artikel 4, tweede lid, onder b, aangewezen CSIRT voor DSP's) wordt gerechtvaardigd en verantwoord geacht. Hierbij wordt met name ook van betekenis geacht dat uitwisseling van gegevens binnen de Europese Unie zal plaatsvinden en voldoende is gebleken dat de gegevens zullen worden aangewend voor maatregelen ter voorkoming van nadelige maatschappelijke gevolgen. Zie in dit verband ook al in dezelfde zin de huidige Regeling aanwijzing computercrisisteams,[33] gebaseerd op artikel 2, tweede lid, onder b, Wgmc. Na inwerkingtreding van de Csw zullen CSIRT's niet langer onder de Regeling aanwijzing computercrisisteams hoeven te vallen.

c. In samenhang met de toevoeging van CSIRT's onder b, wordt ten aanzien van de aanwijzing bij ministeriële regeling, bedoeld in het tweede lid, onder c, verduidelijkt dat dit andere computercrisisteams dan CSIRT's betreft. Momenteel wordt ook al voor enkele andere computercrisisteams dan de nationale computercrisisteams van de lidstaten van de Europese Unie een beoordeling uitgevoerd of en in hoeverre zij bij ministeriële regeling als zodanig kunnen worden aangewezen. Ook is het goed voorstelbaar dat het in de toekomst aangewezen zal blijken te zijn voor nieuwe computercrisisteams een dergelijke beoordeling uit te voeren.

– Derde lid:
Dit lid is nieuw ten opzichte van artikel 2 Wgmc en volgt uit de aanwijzing – in artikel 2 onder c Csw – van de Minister van Justitie en Veiligheid als het «loket» voor de in artikel 16 Csw (artikel 20 van de richtlijn) bedoelde vrijwillige incidentmeldingen.
De taakomschrijving van artikel 3 omvat de taken die voortvloeien uit de aanwijzing van de Minister van Justitie en Veiligheid in artikel 2, maar is daar niet toe beperkt. De doelgroep van het NCSC omvat immers ook andere vitale aanbieders dan AED's, en ook niet-vitale aanbieders die deel uitmaken van de rijksoverheid.
De formulering «andere aanbieders die onderdeel zijn van de rijksoverheid» in het eerste lid doelt ook op zelfstandige bestuursorganen.

Artikel 4 (bevoegde autoriteit; CSIRT voor DSP's)

Dit artikel implementeert de artikelen 9 (aanwijzing CSIRT voor DSP's) en (samen met hoofdstuk 6 Csw en hoofdstuk 5 Awb) 15 en 17 van de richtlijn (handhaving).
Ten aanzien van het derde lid, «bestuursrechtelijke handhaving»: de term *handhaving* is hier gebruikt in dezelfde brede zin als in hoofdstuk 5 Awb, dat wil zeggen als verzamelterm voor toezicht en sancties, in dit geval inclusief het besluit tot oplegging van een auditverplichting en het besluit (bindende aanwijzing) tot oplegging van een concrete beveiligingsmaat-

[33] Stcrt. 2017, 54242.

regel. Door toezicht te houden op de naleving van het bepaalde bij en krachtens de Csw en door sancties op te leggen bij overtreding, voldoen de bevoegde autoriteiten aan artikel 8, tweede lid, van de NIB-richtlijn («De bevoegde autoriteiten monitoren de toepassing van de NIB-richtlijn op nationaal niveau.»). De plicht tot melding van ernstige incidenten (zie de artikelen 10, tweede lid, en 13, eerste lid, onder b) helpt hen daarbij. De beperking tot AED's en DSP's correspondeert met de reikwijdte van hoofdstuk 6 (Handhaving).
De NIB-richtlijn bevat diverse bepalingen over samenwerking binnen en tussen de lidstaten, bijvoorbeeld in de artikelen 8, zesde lid, 10, eerste lid, 11, en 12. Die bepalingen betreffen feitelijk handelen en behoeven geen omzetting.

Artikel 5 (aanwijzing van vitale aanbieders)

Het eerste lid, onder a, en het tweede lid implementeren de artikelen 5 en 6 van de richtlijn (aanwijzing van AED's). Het eerste lid, onder b, is ontleend aan artikel 5 Wgmc (aanwijzing van andere vitale aanbieders dan AED's).
Het aanwijzen van vitale aanbieders (waaronder AED's) is een gedeelde verantwoordelijkheid van de vakminister en van mij als coördinerend bewindspersoon voor cybersecurity. De primaire verantwoordelijkheid berust bij de vakminister.

Vitale aanbieders kunnen krachtens artikel 5 worden aangewezen in of op grond van één centrale amvb, naar het voorbeeld van het Bmc. Zij kunnen desgewenst echter ook krachtens dit artikel worden aangewezen in of op grond van een bestaande sectorale amvb (bijvoorbeeld voor de sector drinkwater in het Drinkwaterbesluit).

In navolging van artikel 5 Wgmc biedt artikel 5 Csw de keuze tussen de aanwijzing van individuele aanbieders («Royal Schiphol Group N.V.») en de aanwijzing van categorieën van aanbieders («drinkwaterbedrijf als bedoeld in artikel 1, eerste lid, van de Drinkwaterwet»). De formulering «of bij besluit van een bij die maatregel genoemd bestuursorgaan» doelt op de constructie zoals beschreven in de toelichting bij artikel 5 Wgmc,[34] waarin de amvb de aanwijzing delegeert aan een in die amvb te noemen bestuursorgaan, bijvoorbeeld (zie het Bmc) de aanwijzing van waterkeringen door de Minister van Infrastructuur en Waterstaat of de aanwijzing van financiële instellingen door DNB.

Eerste lid: Net als krachtens artikel 5 Wgmc geldt de aanwijzing van een aanbieder alleen voor de daarbij genoemde (categorie van) diensten. Zo zal de Royal Schiphol Group N.V. naar verwachting worden aangewezen als AED voor «een veilige en vlotte vlucht- en vliegtuigafhandeling». Een dergelijke aanwijzing geldt niet voor ICT waarvan de winkels op de luchthaven afhankelijk zijn.

Artikel 6 (voorrang voor sectorspecifieke EU-regels)

Dit artikel strekt ter implementatie van artikel 1, zevende lid, van de richtlijn. Die bepaling geeft voorrang aan sectorspecifieke EU-regels die «ten minste feitelijk gelijkwaardig zijn aan de verplichtingen van deze richtlijn». Het is vooralsnog onduidelijk of deze bepaling concrete relevantie heeft en zo ja, om welke EU-regels en welke essentiële of digitale diensten het gaat. Bovendien geldt de bepaling ook voor eventuele toekomstige sectorspecifieke EU-regels, en zelfs voor voorschriften in door de Europese Commissie vastgestelde (gedele-

[34] Kamerstukken II 2015/16, 34 388, nr. 3, p. 27.

geerde) verordeningen. Het voorgestelde artikel 6 biedt de mogelijkheid om, ter voorkoming van onnodige dubbeling met sectorspecifieke voorschriften als bedoeld in artikel 1, zevende lid, van de NIB-richtlijn, bij amvb te bepalen dat daarbij aangewezen, bij of krachtens de Csw gestelde voorschriften, niet gelden voor de bij die amvb omschreven categorieën van aanbieders. Net als artikel 1, zevende lid, van de richtlijn geldt artikel 6 zowel voor AED's als voor DSP's.

Artikel 7 (risico's beheersen)

Dit artikel implementeert (samen met artikel 9) het eerste lid van de artikelen 14 en 16 van de richtlijn (verplichting voor AED's en DSP's om maatregelen te nemen om de risico's voor de beveiliging te beheersen). Overweging 52 van de richtlijn verduidelijkt dat het hierbij zowel kan gaan om private netwerk- en informatiesystemen die door het interne IT-personeel wordt beheerd, als systemen waarvan de beveiliging is uitbesteed.

Met «toezicht» onder artikel 7, tweede lid, wordt met name het monitoren van de beveiliging van het netwerk- en informatiesysteem bedoeld.

Artikel 8 (incidenten voorkomen en gevolgen van incidenten beperken)

Dit artikel implementeert (samen met artikel 9) het tweede lid van de artikelen 14 en 16 van de richtlijn (verplichting voor AED's en DSP's om maatregelen te nemen om incidenten te voorkomen en de nadelige gevolgen van incidenten te beperken).

Artikel 9 (nadere regels over beveiligingseisen)

Dit artikel biedt de mogelijkheid om de globale beveiligingsnormen van de artikelen 7 en 8 desgewenst te concretiseren bij of krachtens amvb. Doorgaans zullen dat sectorspecifieke nadere regels zijn. Dergelijke regels kunnen desgewenst krachtens dit artikel ook worden opgenomen in een bestaande sectorale amvb (bijvoorbeeld voor de sector drinkwater in het Drinkwaterbesluit). De voordracht voor zo'n sectorspecifieke amvb zal worden gedaan door de eerstverantwoordelijke bewindspersoon.
Wat betreft DSP's mogen alleen nadere regels worden gesteld voor zover dat nodig is ter implementatie van de NIB-richtlijn en de door de Europese Commissie vastgestelde «uitvoeringshandelingen» als bedoeld in artikel 16, achtste lid, van de NIB-richtlijn. Het tiende lid van dat artikel verbiedt de lidstaten namelijk om aan DSP's «andere beveiligings- of meldingseisen» op te leggen (dan de eisen van artikel 16 of van de uitvoeringshandelingen van de Europese Commissie). Wel maakt artikel 1, zesde lid, van de richtlijn op dat verbod een uitzondering voor met name nationale veiligheid en de opsporing en vervolging van strafbare feiten.

Artikel 10 (meldplicht aangewezen vitale aanbieder)

Het eerste lid, onder a, en het tweede en vierde lid implementeren artikel 14, derde en vierde lid, van de richtlijn (meldplicht AED's). Het derde en vijfde lid implementeren artikel 16, vijfde lid, van de richtlijn (meldplicht AED voor incident bij DSP als de AED daarvan afhankelijk is).

Eerste lid, «een incident met aanzienlijke gevolgen voor de continuïteit van de door hem verleende dienst»: de meldplicht geldt alleen voor zover de dienst valt onder de aanwijzing van artikel 5, eerste lid.

Eerste en tweede lid: De AED moet een incident met aanzienlijke gevolgen voor de continuïteit van die dienst zowel melden bij het NCSC (eerste lid, onder a) als bij de bevoegde autoriteit (tweede lid). Het streven is die dubbele meldplicht technisch zó vorm te geven, dat de aanbieder desgewenst met één handeling aan beide meldplichten kan voldoen, bijvoorbeeld door op een elektronisch formulier beide instanties aan te vinken.

De meldplicht van het eerste en tweede lid ziet op aantasting van de beveiliging van ICT waarvan de vitale dienst afhankelijk is. Dit kan dus ook gaan om ICT van een ander dan de aanbieder zelf.

De meldplicht van het eerste lid, onder b, is overgenomen uit artikel 6, eerste lid, Wgmc, voor zover dat lid de vitale aanbieder verplicht tot melding van «een inbreuk op de veiligheid of een verlies van integriteit van zijn informatiesysteem waardoor de beschikbaarheid of betrouwbaarheid van een product of dienst in belangrijke mate […] kan worden onderbroken». Net als die bepaling ziet de meldplicht van artikel 10, eerste lid, onder b, op een daadwerkelijke inbreuk op de beveiliging van een elektronisch informatiesysteem waarvan de dienst afhankelijk is, waarbij de inbreuk nog niet heeft geleid tot een belangrijke onderbreking van de continuïteit van de verlening van een vitale dienst, maar dat gevolg wel alsnog kan hebben. De formulering van het eerste lid, onder b, is aangepast aan de terminologie van de richtlijn. De reikwijdte wijzigt niet. Hierbij zij nog opgemerkt dat de NIB-richtlijn niet verplicht tot het regelen van een meldplicht bij bijvoorbeeld de bevoegde autoriteit voor incidenten die nog niet aanzienlijke gevolgen voor de continuïteit van vitale dienstverlening hebben, maar die gevolgen wel kunnen hebben (bijna-ongelukken). Doel van de in artikel 10, onder b, opgenomen meldplicht is onverminderd om het NCSC zo vroegtijdig mogelijk op de hoogte te brengen van incidenten die aanzienlijke gevolgen kunnen hebben voor de continuïteit van voor de samenleving vitale diensten, en daardoor in staat te stellen om, ter voorkoming of beperking van maatschappelijke ontwrichting, getroffen organisaties al in een vroeg stadium bijstand te verlenen bij het treffen van maatregelen om de continuïteit van hun diensten te waarborgen en waar aangewezen andere vitale en rijksoverheidsorganisaties te waarschuwen en te adviseren. Deze meldplicht betreft overigens, net als nu in de Wgmc, alleen incidenten met mogelijke aanzienlijke gevolgen voor de continuïteit van vitale diensten, waarbij sprake is van een daadwerkelijke inbreuk op de beveiliging van de netwerk- en informatiesystemen van een vitale aanbieder.

Om te bepalen of een incident aanzienlijke gevolgen heeft, zijn in de genoemde artikelen van de richtlijn verschillende parameters opgenomen. Het gaat daarbij om het aantal gebruikers en de omvang van het geografische gebied dat door het incident wordt getroffen en de duur van het incident. Deze parameters kunnen nader in richtsnoeren worden ingevuld door het Ministerie van Justitie en Veiligheid, in overeenstemming met de vakdepartementen en na overleg met de sector. Daarbij zal meer specifiek kunnen worden bepaald wanneer een incident meldplichtig is. In dat geval zullen meldplichtige partijen hiervan op de hoogte worden gesteld.

In navolging van de tekst van de NIB-richtlijn (vgl. het vierde lid van de artikelen 14 en 16) ontbreken in het vierde lid twee parameters die wel genoemd worden in artikel 13, tweede lid, onder d en e, Csw, namelijk de omvang van de verstoring van de werking van de dienst, en de omvang van de gevolgen voor de economische en maatschappelijke activiteiten. Die niet genoemde parameters zijn uiteraard ook relevant voor een incident bij een AED, zie ook artikel 11, onder a en c.

Zoals gezegd implementeren het derde en vijfde lid artikel 16, vijfde lid, van de richtlijn. Die laatste bepaling bevat een meldplicht voor AED's voor een incident bij een DSP als de AED afhankelijk is van die digitale dienst. De richtlijn doelt daarbij niet alleen op een DSP die onder de jurisdictie van Nederland valt. Om dat te regelen wijkt het vijfde lid af van die jurisdictiebeperking in de definitie van DSP in artikel 1 Csw.
De meldplicht van het derde lid zou kunnen samenvallen met die van artikel 13, in die zin dat een incident bij een DSP die onder de jurisdictie van Nederland valt, aanzienlijke gevolgen heeft voor zowel die digitale dienst als voor een essentiële dienst als bedoeld in artikel 10. In dat geval zijn zowel de AED als de DSP meldplichtig, vandaar de formulering «Onverminderd artikel 13» in artikel 10, derde lid.

Artikel 11 (bij de melding te verstrekken gegevens)

Dit artikel is afgeleid van artikel 6, tweede lid, Wgmc. Ten opzichte van die bepaling is in onderdeel c (de mogelijke gevolgen van het incident) voor de duidelijkheid toegevoegd: «in en buiten Nederland».

Artikel 12 (verstrekking nadere gegevens door aangewezen vitale aanbieder)

Het eerste lid is afgeleid van artikel 7 Wgmc. Denkbaar is dat het NCSC naar aanleiding van een melding nadere gegevens nodig heeft om de getroffen organisatie adequaat te kunnen helpen, bijvoorbeeld als deze bij het doen van de melding nog geen zekerheid kon bieden over de gevolgen van de inbreuk of over de te nemen maatregelen. Ook kunnen nadere gegevens nodig zijn om de risico's te kunnen inschatten voor informatiesystemen van de andere aanbieders die tot de doelgroep van het NCSC behoren. Het eerste lid bevat voor dergelijke gevallen een aanvullende informatieplicht, die wordt geactiveerd door een concreet verzoek van het NCSC in reactie op een melding als bedoeld in artikel 10, eerste of derde lid.

Het tweede lid ziet op 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) niet ook bij het NCSC. Voor het geval dat de bevoegde autoriteit de door hem bij de melding ontvangen gegevens al naar het NCSC heeft doorgestuurd, regelt het tweede lid dat de aanbieder ook in dat geval verplicht is om het NCSC desgevraagd de noodzakelijke nadere gegevens te verstrekken.

Artikel 13 (meldplicht DSP)

Dit artikel implementeert artikel 16, derde en vierde lid, van de richtlijn. Eerste lid: Ook een DSP heeft een meldplicht voor een incident met aanzienlijke gevolgen voor een digitale dienst. De aanbieder moet dit incident zowel melden bij het CSIRT (eerste lid, onder a) als bij de bevoegde autoriteit (tweede lid). Er wordt naar gestreefd de dubbele meldplicht technisch zó in te richten dat het verspreiden van de benodigde informatie maar één handeling vergt. ICT-incidenten bij DSP's leiden in de regel niet tot maatschappij-ontwrichtende situaties. In tegenstelling tot de meldplicht bij AED's is die omstandigheid dan ook niet relevant voor de meldplicht voor DSP's. Om strijdigheid te voorkomen met artikel 16 van de richtlijn en met de uitvoeringshandelingen, bedoeld in het negende lid van dat artikel (formats en procedures voor meldingseisen), ontbreekt voor meldingen door DSP's een bepaling zoals artikel 11 (bij de melding te verstrekken gegevens). Zie echter de toelichting bij artikel 15 Csw.

Het tweede lid van artikel 13 Csw (in elk geval relevante parameters voor de vraag of een incident aanzienlijke gevolgen heeft) zal nadere uitwerking krijgen in de uitvoeringshandelingen die de Europese Commissie in 2017 opstelt.

Het derde lid implementeert artikel 16, vierde lid, laatste volzin, van de richtlijn. Het kan voor een DSP in sommige situaties lastig zijn om te beoordelen of een incident aanzienlijke gevolgen heeft. Zo zal een DSP bij uitval van de eigen dienstverlening de duur van het incident makkelijker kunnen vaststellen dan het bepalen van de gevolgen voor economische en maatschappelijke activiteiten, omdat informatie over de duur van het incident naar verwachting in het eigen bedrijf aanwezig zal zijn, maar informatie over de maatschappelijke en economische gevallen niet of in mindere mate.

Artikel 14 (verstrekking nadere gegevens door DSP's)

Om een DSP goed te kunnen bijstaan, kan de situatie zich voordoen dat het CSIRT voor digitale diensten meer informatie nodig heeft dan de informatie die bij de melding is verstrekt. Daarnaast kan het gemelde incident duiden op een kwetsbaarheid in ICT die ook relevant is voor andere gebruikers van die ICT. Meer informatie over de kwetsbaarheid van de getroffen DSP kan noodzakelijk zijn om andere DSP's of – via het NCSC – AED's adequaat te kunnen waarschuwen. Het eerste lid bevat een informatieplicht voor de DSP die een incident heeft gemeld op grond van artikel 13, eerste lid, om op verzoek van het CSIRT voor digitale diensten aanvullende informatie te verstrekken.
De informatieplicht geldt ook in de situatie waarin de DSP een incident alleen heeft gemeld bij de bevoegde autoriteit en niet ook bij het CSIRT voor digitale diensten. Voor het geval dat de bevoegde autoriteit de door haar bij de melding ontvangen gegevens al heeft doorgestuurd naar het CSIRT voor digitale diensten, regelt het tweede lid dat de DSP ook in dat geval verplicht is om het CSIRT voor digitale diensten desgevraagd de noodzakelijke nadere gegevens te verstrekken.

Artikel 15 (nadere regels meldplicht)

Dit artikel is afgeleid van artikel 8 Wgmc. Het bevat de grondslag om, indien nodig, nadere regels te stellen over bijvoorbeeld de gegevens die in het kader van de meldplicht moeten worden verstrekt. De betrokken sectoren zullen over de nadere regels worden geconsulteerd.
Wat betreft de meldplicht voor DSP's mogen alleen nadere regels worden gesteld voor zover artikel 16 van de richtlijn daarvoor ruimte biedt. Dergelijke nadere regels kunnen in elk geval nodig zijn ter implementatie van de uitvoeringshandelingen, bedoeld in het achtste lid van dat artikel. Het gaat daarbij om de parameters voor het bepalen of een incident aanzienlijke gevolgen heeft. Ook kan de Europese Commissie ingevolge het negende lid van artikel 16 uitvoeringshandelingen vaststellen over de formats en procedures voor meldingseisen, maar zij is dat niet verplicht. Voorts kan het noodzakelijk zijn om nadere regels te stellen in het belang van een goede uitvoering van de NIB-richtlijn.

Artikel 16 (vrijwillige melding van incidenten)

Dit artikel, waarmee artikel 20 van de richtlijn wordt geïmplementeerd, geldt voor incidenten met aanzienlijke gevolgen die niet onder de meldplicht van de artikelen 10 en 13 vallen:
a. een dienst van een andere entiteit dan een AED of DSP;
b. een niet onder de meldplicht vallende dienst van een AED of DSP.

Artikel 2 onder c Csw wijst de Minister van Justitie en Veiligheid aan als het «loket» voor deze vrijwillige meldingen. In de praktijk voert het NCSC deze taak uit. Het NCSC zal bij ándere incidenten dan incidenten bij vitale aanbieders of bij andere aanbieders die onderdeel zijn van de rijksoverheid, beoordelen of het de melding kan doorsturen naar een (ander) CSIRT of naar een bij ministeriële regeling aangewezen (ander) computercrisisteam. Dit geschiedt uiteraard met inachtneming van artikel 20 Csw; toestemming van de melder is daarom in de regel vereist. Als er geen geschikt computercrisisteam bestaat of doorzenden om andere redenen niet mogelijk is, dan behandelt het NCSC de melding alleen als dit geen onevenredige of overmatige belasting oplevert.
Gekozen is voor de formulering «de betrokken dienstverlener» omdat de term «aanbieder» alleen ziet op (overheidsorganisaties en) rechtspersonen (zie artikel 1), terwijl artikel 20 van de richtlijn ook ziet op commerciële dienstverleners zonder rechtspersoonlijkheid.

Artikel 17 (verwerking van gegevens door Onze Minister en andere instanties)

Het eerste lid is afgeleid van artikel 3 Wgmc en alleen aangepast aan de terminologie van de AVG. Wel is de reikwijdte breder doordat het eerste lid verwijst naar de in artikel 3 Csw genoemde doeleinden en taken, en artikel 3 Csw ook ziet op de taken van de Minister van Justitie en Veiligheid als centraal contactpunt, CSIRT voor AED's en instantie voor de behandeling van de in artikel 16 Csw (artikel 20 van de richtlijn) bedoelde vrijwillige incidentmeldingen.
Bij de in het eerste lid bedoelde (persoons)gegevens gaat het bijvoorbeeld om bij een incident of dreiging betrokken IP-adressen en om contactgegevens van vitale organisaties of andere organisaties binnen de rijksoverheid en van andere melders van incidenten of kwetsbaarheden. Contactgegevens worden verwerkt om het NCSC onder meer in staat te stellen contact op te nemen met de meldende organisatie teneinde advies en ondersteuning te bieden. IP-adressen maken vaak deel uit van incident-informatie; op basis daarvan kan onderzoek worden gedaan naar de (ernst van de) inbreuk en kan advies over te treffen beveiligingsmaatregelen worden gegeven. Ook is deze kennis van belang ten behoeve van het informeren van derden, waaronder andere aanbieders, daar zij op basis van deze informatie alert kunnen worden gemaakt voor gelijksoortige inbreuken. Persoonsgegevens zullen door het Ministerie van Justitie en Veiligheid worden verwerkt met inachtneming van de AVG, zoals thans met inachtneming van de Wbp. De Autoriteit Persoonsgegevens alsook de departementale functionaris voor de gegevensbescherming houden toezicht op deze verwerkingen. Ten aanzien van deze verwerkingen geldt vanwege het bepaalde in de AVG onder andere dat zij zullen worden vernietigd zodra zij niet langer noodzakelijk zijn voor de uitoefening van de betrokken taken. Ook andere gegevens, zoals vertrouwelijke bedrijfsgegevens, zullen worden vernietigd zodra de verwerking daarvan niet meer noodzakelijk is voor de uitoefening van die taken.
Het tweede en derde lid bevatten een met het eerste lid vergelijkbare bepaling voor de sectorale bevoegde autoriteit en het CSIRT voor DSP's. Zie voor een nadere toelichting over de verwerking van persoonsgegevens die zijn gemoeid met dit wetsvoorstel paragraaf 9 aangaande de grondrechtentoets.

Artikel 18 (verstrekking persoonsgegevens aan Onze Minister)

Dit artikel en de toelichting hierna zijn afgeleid van artikel 4 Wgmc en van de toelichting bij dat artikel en alleen aangepast aan de vervanging van de Wbp door de AVG.

Het eerste lid voorziet in een wettelijke bevoegdheid voor het NCSC om rechtspersonen (overheden of private partijen) of organen daarvan om gegevens te vragen die noodzakelijk zijn voor de uitoefening van de in artikel 3, eerste lid, onder b tot en met e, genoemde taken. Het eerste lid voorziet niet in een bevoegdheid tot het *vorderen* van gegevens: de rechtspersoon of het orgaan waaraan het verzoek is gericht, is niet verplicht tot medewerking. Een dergelijke verplichting acht ik alleen nodig voor een krachtens artikel 5 aangewezen vitale aanbieder die bij het NCSC een meldplichtig incident heeft gemeld; daarin voorziet artikel 12.
Voor de goede uitoefening van zijn taken is het van belang dat het NCSC, met het oog op het belang van de beschikbaarheid en betrouwbaarheid van netwerk- en informatiesystemen van, en daarmee de continuïteit van de dienstverlening door, vitale aanbieders en andere aanbieders die onderdeel zijn van de rijksoverheid, over voldoende gegevens beschikt over incidenten en kwetsbaarheden met betrekking tot informatiesystemen van de rijksoverheid en vitale private partijen. Het kan daarbij ook gaan om persoonsgegevens zoals IP-adressen (zie ook paragraaf 6 van het algemeen deel van de memorie van toelichting bij de Wgmc). Ingevolge het doelbindingsbeginsel van artikel 5, eerste lid, onder b, AVG moeten persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen zij vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt. De AVG biedt echter de mogelijkheid om onder voorwaarden door middel van lidstaatrechtelijke bepalingen de verdere verwerking van persoonsgegevens mogelijk te maken, ook als dat geschiedt voor een doel dat niet verenigbaar is met het doel waarvoor de persoonsgegevens zijn verkregen. Het tweede lid van artikel 18 Csw geeft toepassing aan die bevoegdheid. Dat is een noodzakelijke en evenredige maatregel ter waarborging van meerdere in artikel 23, eerste lid, AVG, genoemde belangen, waaronder onder meer de nationale veiligheid en de openbare veiligheid.

Artikel 19 (verstrekking incidentinformatie aan en door centrale contactpunten)

Dit artikel implementeert de artikelen 10, derde lid, 14, vijfde lid, en 16, zesde lid, van de richtlijn.

Het vijfde lid betreft het doorzenden aan de bevoegde autoriteit of het CSIRT voor DSP's van meldingsinformatie die het centrale contactpunt, bij wijze van spiegelbeeld, van centrale contactpunten van andere lidstaten ontvangt.

Artikel 20 (verstrekking van vertrouwelijke gegevens door Onze Minister)

Deze bepaling is voor een groot deel identiek aan artikel 9 Wgmc en regelt de verstrekking door de Minister van Justitie en Veiligheid, ter uitvoering van de in artikel 3 bedoelde taken, aan derden van vertrouwelijke gegevens met betrekking tot aanbieders, zoals gegevens over de identiteit van een bij een incident betrokken aanbieder of specifieke gegevens over de beveiliging van een elektronisch informatiesysteem van een aanbieder. Artikel 19 staat uiteraard niet in de weg aan verstrekking door het NCSC aan derden van gegevens die niet vertrouwelijk zijn. Zo ligt het voor de hand dat het NCSC en de sectorale bevoegde autoriteit elkaar binnen de wettelijke kaders zo veel mogelijk voorzien van op sectorniveau opgestelde overzichten van (meldingen van) incidenten.

De toelichting hierna is woordelijk overgenomen uit de toelichting bij artikel 9 Wgmc, voor zover nodig met aanpassing van verwijzingen,

aangevuld met een toelichting bij het begrip «vertrouwelijke gegevens» en bij wat in artikel 20 Csw nieuw is. Voor de duidelijkheid worden de verschillen tussen artikel 20 Csw en artikel 9 Wgmc nog eens opgesomd aan het eind.

Artikel 20 ziet op alle vertrouwelijke gegevens met betrekking tot aanbieders die zich bij het Ministerie van Justitie en Veiligheid bevinden, en is dus niet beperkt tot de gegevens die het NCSC heeft verkregen op grond van de meldplicht, bedoeld in artikel 10, eerste lid, bedoelde meldplicht of naar aanleiding van een verzoek als bedoeld in artikel 12. Bij het begrip vertrouwelijke gegevens kan worden gedacht aan informatie over netwerk- en informatiesystemen die een bedrijf gebruikt bij zijn dienstverlening. Het kan ook zien op kwetsbaarheden in die systemen (ongeacht of er sprake is van een concrete dreiging), of op specifieke informatie over dreigingen of incidenten met betrekking tot die systemen. Ook kan worden gedacht aan concrete informatie over de aanbieder die door een dreiging of incident is getroffen waarbij openbaarmaking tot gevolg heeft dat die aanbieder daarvan nadeel ondervindt (bijvoorbeeld omdat klanten weglopen, of omdat gegevens bekend worden waar concurrenten hun voordeel mee kunnen doen). Het is voor de toepassing van artikel 20 niet relevant of het NCSC de gegevens heeft verkregen van de aanbieder zelf of anderszins, zoals door analyse van het NCSC of ontvangst van een andere CSIRT.

De medewerkers van het NCSC zijn gebonden aan de geheimhoudingsplicht van artikel 272 van het Wetboek van Strafrecht en artikel 2:5 Awb. Deze laatste bepaling geldt voor «Een ieder die is betrokken bij de uitvoering van de taak van een bestuursorgaan en daarbij de beschikking krijgt over gegevens waarvan hij het vertrouwelijke karakter kent of redelijkerwijs moet vermoeden». De geheimhoudingsplicht geldt niet «voor zover enig wettelijk voorschrift hem tot mededeling verplicht of uit zijn taak de noodzaak tot mededeling voortvloeit». Uit de NCSC-taken in artikel 3 kan de noodzaak voortvloeien tot mededeling van vertrouwelijke gegevens met betrekking tot aanbieders. Artikel 20 regelt onder welke voorwaarden en aan wie dergelijke gegevens mogen worden verstrekt ter uitvoering van de NCSC-taken.

Het **eerste lid** is mede ontleend aan de artikelen 1:90, eerste lid, onderdelen d en f, en 1:93, tweede lid, onderdelen d en f, Wft (verstrekking van vertrouwelijke gegevens door de toezichthouder). Deze bepaling regelt dat bij het NCSC, bijvoorbeeld naar aanleiding van een melding, berustende vertrouwelijke gegevens slechts ter uitvoering van de in artikel 3 genoemde taken aan derden worden verstrekt, indien aldaar de geheimhouding van de gegevens voldoende is gewaarborgd en voldoende is gewaarborgd dat de gegevens uitsluitend worden gebruikt voor het doel waarvoor zij worden verstrekt.

Het eerste lid ziet op vertrouwelijke gegevens met betrekking tot aanbieders, dus niet op andere vertrouwelijke gegevens, zoals persoonsgegevens die niet herleidbaar zijn tot een aanbieder (bijvoorbeeld de e-mailadressen die op grond van artikel 3, tweede lid, voor verstrekking aan derden in aanmerking komen). Voor de verwerking van laatstbedoelde persoonsgegevens door het NCSC geldt de Wbp (en vanaf 25 mei 2018 de AVG), net als voor de verwerking van andere persoonsgegevens waarover het NCSC beschikt.

Soms zijn gegevens die betrekking hebben op een aanbieder vertrouwelijk zonder dat zij tot die aanbieder herleid kunnen worden. Denk aan een nieuw concurrentiegevoelig bedrijfsprocedé dat buiten de betrokken onderneming nog niet bekend is. Anders dan het tweede, derde en vierde

lid ziet het eerste lid ook op dergelijke vertrouwelijke maar niet-herleidbare gegevens.

Zowel het eerste lid als het tweede lid zien alleen op verstrekking van de daarin bedoelde vertrouwelijke gegevens «ter uitvoering van de in artikel 3 genoemde taken», en dus niet op verplichtingen tot verstrekking door het NCSC van vertrouwelijke gegevens uit hoofde van andere wetten,[35] zoals artikel 8:28 Awb (inlichtingen verstrekken aan de bestuursrechter door partijen in een beroepsprocedure) of artikel 126nd e.v. Wetboek van Strafvordering (vorderen van gegevens door officier van justitie).

Uit het **tweede lid** volgt dat verstrekking, uit hoofde van artikel 3, van vertrouwelijke gegevens die herleid kunnen worden tot een aanbieder, zonder diens instemming alleen mogelijk is aan (andere) CSIRT's (in de zin van artikel 9 NIB-richtlijn; dit is nieuw ten opzichte van artikel 9, tweede lid, Wgmc), andere computercrisisteams die bij ministeriële regeling zijn aangewezen en aan de Nederlandse inlichtingen- en veiligheidsdiensten (zie daarover ook de artikelsgewijze toelichting bij artikel 3), en dan alleen voor zover dat dienstig is voor het bevorderen van maatregelen ter voorkoming of beperking van een verstoring van het maatschappelijk verkeer. Als de aanbieder daar toestemming voor geeft, dan kunnen de gegevens uiteraard ook aan andere organisaties worden verstrekt, bijvoorbeeld aan een sectorale bevoegde autoriteit. Een dergelijke toestemming kan bijvoorbeeld overleg mogelijk maken tussen het NCSC en die bevoegde autoriteit om te voorkomen dat de aanbieder geconfronteerd wordt met een aanwijzing van de bevoegde autoriteit die tegenstrijdig is aan het advies van het NCSC.

De formulering «gegevens die herleid kunnen worden tot een aanbieder» doelt op de naam van een aanbieder en alle andere gegevens waarmee in redelijkheid de identiteit van die aanbieder direct dan wel indirect kan worden vastgesteld.

Gelet op de in artikel 3 genoemde taken heeft het NCSC (mede) tot taak om vitale aanbieders en andere aanbieders die onderdeel zijn van de rijksoverheid te adviseren over maatregelen die zouden kunnen worden genomen vanwege een dreiging of incidenten met betrekking tot hun informatiesystemen. Een dergelijk advies is niet bindend. Het is echter onwenselijk als de betrokken aanbieder zich vrij voelt om het advies zonder goede reden naast zich neer te leggen. Het **derde lid** beoogt dat te voorkomen.[36] Het blijft primair de eigen verantwoordelijkheid van de aanbieder zelf om passende maatregelen te nemen om uitval of verstoring van zijn dienst te voorkomen of te beperken. Ook is het primair aan de aanbieder zelf om, als een wettelijk voorschrift hiertoe verplicht, de eigen toezichthouders of vakdepartementen op de hoogte te stellen. Voor het geval de Minister van Justitie en Veiligheid echter van oordeel is dat de aanbieder onvoldoende gevolg geeft aan het advies, en daardoor het risico op maatschappelijke ontwrichting aanwezig blijft, kan hij het advies verstrekken aan de voor de betrokken sector verantwoordelijke Minister of Staatssecretaris of, in het geval van de financiële sector, aan DNB (dit laatste is nieuw ten opzichte van artikel 9, derde lid, Wgmc), met inbegrip van de in het advies opgenomen herleidbare gegevens (artikel 20, derde lid). Wanneer het voornemen bestaat om in een dergelijk geval een advies door te zenden aan een betrokken bewindspersoon of aan DNB, zal het NCSC daarover in overleg treden met het betrokken ministerie dan wel DNB. Na doorzending zal het NCSC, indien gewenst, het betrokken ministerie dan wel DNB nader informeren en adviseren over de

[35] Vgl. «voor zover enig wettelijk voorschrift hem tot mededeling verplicht» in artikel 2:5 Awb.
[36] Kamerstukken II 2013/14, 26 643, nr. 297, p. 4.

cybersecurity-aspecten van het incident of de kwetsbaarheid waarop het advies betrekking heeft. Indien het advies wordt doorgeleid naar de betrokken bewindspersoon of DNB zal dit uiteraard geschieden binnen een gepaste tijdsperiode, gekoppeld aan het urgentieniveau van het incident.

De bevoegdheid van het derde lid kan bijvoorbeeld ook betrekking hebben op bij het NCSC gemelde inbreuken als bedoeld in artikel 10, eerste lid, onder b.

Als het advies betrekking heeft op een rijksoverheidsorganisatie zal (ook) de Minister van Binnenlandse Zaken en Koninkrijksrelaties worden geïnformeerd, aangezien hij in elk geval «betrokken» (in de zin van het derde lid) is, gezien zijn coördinerende rol voor informatiesystemen van de overheid.

De aanbieder heeft voldoende gevolg gegeven aan het advies als hij het advies weliswaar niet heeft gevolgd, maar de dreiging niettemin in voldoende mate is verdwenen, bijvoorbeeld doordat de organisatie andere dan de geadviseerde maatregelen heeft genomen of door adequate actie van anderen.

De verstrekking van het NCSC-advies aan de eerstverantwoordelijke bewindspersoon is een feitelijke handeling. De beslissing tot verstrekking is geen besluit in de zin van de Awb vanwege het ontbreken van rechtsgevolg: de verstrekking brengt geen wijziging in de rechten of plichten van de betrokken aanbieder en het advies wordt ook niet openbaar gemaakt. Het is aan de eerstverantwoordelijke bewindspersoon om al dan niet actie te ondernemen naar aanleiding van het aan hem verstrekte NCSC-advies. Tegen de (beslissing tot) verstrekking staat dan ook geen bestuursrechtelijke rechtsbescherming open.

Het **vierde lid** ziet op het specifieke geval dat verstrekking van bovenbedoelde herleidbare gegevens nodig is om ernstige maatschappelijke gevolgen te voorkomen of te beperken. In een dergelijk geval is het NCSC verplicht om die gegevens te verstrekken aan de politiek verantwoordelijke bewindspersoon of -personen of, in het geval van de financiële sector, aan DNB (dit laatste is nieuw ten opzichte van artikel 9, vierde lid, Wgmc) (onderdeel a). Daarbij kan bijvoorbeeld worden gedacht aan een dreigende crisissituatie ten aanzien waarvan het nemen van crisisbeheersingsmaatregelen aangewezen kan zijn. De verplichting tot verstrekking kan ook betrekking hebben op bij het NCSC gemelde inbreuken als bedoeld in artikel 10, eerste lid, onder b (bijna-ongelukken).

Bij een incident zal niet in alle situaties even duidelijk zijn of en in hoeverre ernstige maatschappelijke gevolgen in het geding kunnen zijn. Het NCSC zal ook dan op basis van bij het NCSC beschikbare informatie hiervan een inschatting moeten maken. Vanuit haar rol kan het NCSC bij die afweging in overleg treden met anderen die beschikken over relevante kennis, om haar beeld zo volledig mogelijk te maken. Denk bijvoorbeeld aan de situatie dat sectorkennis nodig is, en het NCSC in gesprek gaat met de bevoegde autoriteit (waarbij het NCSC de niet tot de betrokken aanbieder herleidbare gegevens kan delen). Uiteindelijk maakt het NCSC op basis van de beschikbare informatie de inschatting of er sprake is van mogelijke ernstige maatschappelijke gevolgen, ter voorkoming waarvan herleidbare gegevens betreffende een aanbieder gedeeld moeten (met de betrokken Minister of de bevoegde autoriteit) of kunnen (met andere organisaties of het publiek) worden. Het kan voorkomen dat het NCSC, na het besluit om herleidbare gegevens te delen met de betrokken Minister of de bevoegde autoriteit om ernstige maatschappelijke gevolgen te

voorkomen, op basis van bijvoorbeeld verder overleg aan de hand van die herleidbare gegevens tot de conclusie komt dat de beoordeling van de ernst van de gevolgen bijgesteld wordt.

Aan andere organisaties of aan het publiek mogen dergelijke gegevens met toepassing van het vierde lid slechts worden verstrekt na raadpleging van de betrokken aanbieder (onderdeel b). Daarbij spreekt het voor zich dat deze informatieverstrekking niet verder gaat dan strikt noodzakelijk is om die organisaties of het publiek in staat te stellen om te bepalen of en welke maatregelen zij in dit verband dienen te nemen. Voor dit doel zal het in beginsel slechts in uitzonderlijke gevallen nodig zijn om herleidbare gegevens te verstrekken.

De verstrekking, op grond van het vierde lid, van herleidbare gegevens aan het publiek gaat naar haar aard niet samen met geheimhouding en doelbinding. Daarom bepaalt het **vijfde lid** dat het eerste lid op die mededelingen niet van toepassing is.

De uit de Wgmc overgenomen bevoegdheid van het NCSC om het publiek te informeren, bevat overigens enige overlap met de ter uitvoering van de NIB-richtlijn in artikel 23 geregelde bevoegdheid van de bevoegde autoriteit om het publiek te informeren, namelijk in geval van verplichte meldingen van incidenten die zijn gedaan door AED's of DSP's. Dat vereist dat beide instanties de voorgenomen toepassing van hun bevoegdheid met elkaar afstemmen. Hoe dan ook geldt voor beide bevoegdheden dat de aanbieder vooraf geraadpleegd moet worden, waarbij laatstgenoemde er zo nodig op zal kunnen wijzen dat beide instanties openbaarmaking voorbereiden.

Het **zesde lid** (nieuw ten opzichte van artikel 9 Wgmc) strekt ertoe om te voorkomen dat de Minister van Justitie en Veiligheid niet kan voldoen aan zijn verplichtingen als centraal contactpunt, een nieuwe taak die voortvloeit uit de richtlijn. Als de Minister vanuit die rol en in de in artikel 19 genoemde situaties informatie moet verstrekken, kan die verstrekking, in afwijking van het tweede lid, ook vertrouwelijke herleidbare informatie over aanbieders betreffen. Het gaat daarbij enerzijds om het waarschuwen en informeren van het centrale contactpunt van een andere lidstaat met betrekking tot een melding van een ernstig incident met gevolgen voor die lidstaat (artikel 19, tweede, derde en vierde lid) en anderzijds om het waarschuwen en informeren van een Nederlandse bevoegde autoriteit of het Nederlandse CSIRT voor DSP's met betrekking tot een in een andere lidstaat gemeld ernstig incident met gevolgen voor diensten in Nederland (artikel 19, vijfde lid).

Zoals uiteengezet in het algemeen deel van deze memorie bevat artikel 20 een bijzondere openbaarheidsregeling voor vertrouwelijke herleidbare gegevens die afwijkt van de Wob. Het **zevende lid** stelt dit buiten twijfel. Deze afwijking geldt niet alleen zolang die gegevens bij het NCSC berusten, maar ook nadat zij, na verstrekking door het NCSC op grond van artikel 20, bij een ander overheidsorgaan berusten. Ten opzichte van de Wgmc is dit nu expliciet opgenomen in het zevende lid. Hiermee is geen inhoudelijke wijziging beoogd.
Een en ander geldt echter niet voor milieu-informatie. Ter uitvoering van het Verdrag van Aarhus[37] en EU-richtlijn 2003/4/EG[38] bevat de Wob voor

[37] Verdrag betreffende toegang tot informatie, inspraak bij besluitvorming en toegang tot de rechter inzake milieuaangelegenheden, Trb. 2001, 73.
[38] Richtlijn 2003/4/EG van het Europees Parlement en de Raad van 28 januari 2003 inzake de toegang van het publiek tot milieu-informatie en tot intrekking van Richtlijn 90/313/EEG van de Raad, PbEU 2003, L 41).

het verstrekken van milieu-informatie diverse afwijkende bepalingen. Zo is de weigeringsgrond voor bedrijfs- en fabricagegegevens die vertrouwelijk aan de overheid zijn meegedeeld in het geval van milieu-informatie niet absoluut[39] maar relatief,[40] en in plaats van de relatieve weigeringsgrond dat onevenredige bevoordeling of benadeling voorkomen moet worden[41] geldt voor milieu-informatie dat verstrekking achterwege blijft voor zover het belang daarvan niet opweegt tegen de bescherming van het milieu waarop de informatie betrekking heeft of de beveiliging van bedrijven en het voorkomen van sabotage.[42] Hoewel herleidbare gegevens in de meeste gevallen zelf geen informatie over het milieu bevatten, blijkt uit de rechtspraak dat namen van ondernemingen milieu-informatie kunnen inhouden als zij onlosmakelijk verbonden zijn met maatregelen en activiteiten ter bescherming van elementen van het milieu.[43] Om strijdigheid met het genoemde verdrag en de genoemde richtlijn te voorkomen, volgt uit het zevende lid van artikel 20 dat de Wob onverkort van toepassing is op herleidbare gegevens die milieu-informatie inhouden.

Artikel 20, en dan met name het eerste lid, staat er niet aan in de weg dat het NCSC vertrouwelijke gegevens die niet herleidbaar zijn, uit eigen beweging verstrekt aan bijvoorbeeld de politie en het Openbaar Ministerie in de reeds bestaande overlegstructuren. Wél herleidbare gegevens kunnen door het NCSC aan politie en OM worden verstrekt als de betrokken aanbieder daarmee instemt. Beide vormen van verstrekking kunnen voor de officier van justitie vervolgens aanleiding zijn om gebruik te maken van zijn wettelijke bevoegdheid om bij het NCSC gegevens te vorderen.

Samengevat bevat artikel 20 Csw de volgende verschillen ten opzichte van artikel 9 Wgmc:

1. In het tweede lid zijn CSIRT's toegevoegd (als bedoeld in artikel 9 NIB-richtlijn, zie de begripsomschrijving in artikel 1 Csw). In dit verband is mede van betekenis dat de geheimhouding, bedoeld in het eerste lid, bij CSIRT's voldoende gewaarborgd wordt geacht te zijn, en dat voldoende is gebleken dat hieraan verstrekte gegevens zullen worden aangewend voor maatregelen ter voorkoming of beperking van een verstoring van het maatschappelijk verkeer. Dit is ook in lijn met de huidige Regeling aanwijzing computercrisisteams onder de Wgmc.
2. In het derde lid is de bevoegde autoriteit toegevoegd als instantie waaraan de Minister van Justitie en Veiligheid een door het NCSC gegeven advies, inclusief de daarin opgenomen vertrouwelijke herleidbare gegevens, kan verstrekken als de aanbieder onvoldoende gevolg geeft aan het advies. Materieel heeft dat alleen betekenis voor DNB, aangezien de andere in artikel 4 Csw aangewezen bevoegde autoriteiten ministers zijn en dus al vielen onder de reikwijdte van het hier overgenomen artikel 9, derde lid, Wgmc («aan onze betrokken Minister»).
3. Ook in het vierde lid, onder a, is de bevoegde autoriteit toegevoegd. Ook die verruiming heeft alleen betekenis voor DNB.
4. Het zesde lid is nieuw ingevoegd, zie boven.
5. In het zevende lid is expliciet bepaald dat de afwijking van de Wob ook geldt als de gegevens, na verstrekking door het NCSC op grond van artikel 20, bij een ander overheidsorgaan berusten.

---

[39] Artikel 10, eerste lid, aanhef en onder c, Wob.
[40] Artikel 10, vierde lid, tweede volzin, Wob.
[41] Artikel 10, tweede lid, aanhef en onder g, Wob.
[42] Artikel 1, onder g, en artikel 10, zesde en zevende lid, Wob.
[43] ABRvS 10 maart 2010, ECLI:NL:RVS:2010:BL7035.

Daarnaast verschilt artikel 20 Csw ook in die zin van artikel 9 Wgmc, dat artikel 20 Csw, doordat het eerste en tweede lid verwijzen naar artikel 3 Csw, tevens betrekking heeft op de taken van de Minister van Justitie en Veiligheid als het centrale contactpunt, het CSIRT voor AED's en het «loket» voor vrijwillige incidentmeldingen.

Artikel 21 (verstrekking van vertrouwelijke gegevens door het CSIRT voor digitale diensten)

Dit artikel regelt de verstrekking van vertrouwelijke gegevens met betrekking tot DSP's aan derden door het CSIRT voor digitale diensten. De taken die het CSIRT voor digitale diensten op grond van dit wetsvoorstel vervult zijn vergelijkbaar met de CSIRT-taken van het NCSC, zoals het monitoren van en reageren op incidenten en zorgen voor een risico- en incidentanalyse en deelnemen aan het CSIRT-netwerk (zie bijlage 1, onderdeel 2, onder a, NIB-richtlijn). Daarom is ervoor gekozen om een vergelijkbare regeling op te nemen voor de verstrekking van vertrouwelijke gegevens door het CSIRT voor digitale diensten. Voor de toelichting op dit artikel zij dan ook verwezen naar de toelichting op artikel 20.
Twee leden van artikel 21 behoeven enige aanvullende toelichting. Het vierde lid verschilt van het vierde lid van artikel 20 vanwege de aard van de gevolgen van de incidenten bij een DSP. Het gaat bij DSP's niet om maatschappelijke ontwrichting, dat is vooral aan de orde bij AED's, maar er kunnen zich wel degelijk ernstige economische of sociale gevolgen voordoen. In hoeverre die gevolgen optreden hangt af van de aard en omvang van het incident. Een incident zal in de eerste plaats gevolgen hebben voor de DSP zelf. Het kan hierbij gaan om grote digitale spelers die belangrijk zijn voor de Nederlandse economie. Daarnaast zal het incident de consumenten en ondernemingen treffen die gebruikmaken van de digitale dienst. De gevolgen voor gebruikers van de digitale dienst hangen onder meer af van in hoeverre zij (snel) kunnen overschakelen op een alternatieve dienst of in hoeverre het ook een effect heeft op de continuïteit en veiligheid van de eigen dienstverlening aan derden. Ook zouden geconstateerde ICT-kwetsbaarheden zich kunnen voordoen bij andere partijen die dezelfde soort ICT-producten of -diensten gebruiken. Als het CSIRT voor digitale diensten de inschatting maakt dat dergelijke ernstige economische of sociale gevolgen zich in een bepaalde mate zouden kunnen voordoen dan wel dat de vakminister in het kader van de uitoefening van crisistaken ernstige gevolgen kan helpen voorkomen of verminderen, dan is het van belang dat de vakminister hierover wordt geïnformeerd. Het kan hierbij gaan om de Minister van Economische Zaken en Klimaat maar ook om de andere vakministers. Zo worden clouddiensten in tal van sectoren toegepast; als er veiligheids- of integriteitsproblemen ontstaan met clouddiensten, dan kan dit gevolgen hebben voor de dienstverlening in verschillende sectoren.

Het zesde lid, waarin artikel 20, zevende lid, «van overeenkomstige toepassing» wordt verklaard, ziet op verstrekking door het CSIRT voor digitale diensten van vertrouwelijke gegevens die herleid kunnen worden tot een DSP.

Artikel 22 (verstrekking vertrouwelijke gegevens door de bevoegde autoriteit)

Het draagt bij aan de uniformiteit in het cyberdomein als gegevens bij zowel het CSIRT als de bevoegde autoriteit onder de bijzondere openbaarheidsregeling vallen. Daarom is een soortgelijke regeling opgenomen voor vertrouwelijke herleidbare gegevens met betrekking tot een AED of een DSP die een bevoegde autoriteit ingevolge de Csw verkrijgt.

Artikel 23 (openbaarmaking incidenten)

Het eerste lid, onder a, (essentiële diensten) implementeert artikel 14, zesde lid, van de richtlijn, het eerste lid, onder b, (digitale diensten) artikel 16, zevende lid van de richtlijn. Voor beide soorten diensten bepaalt de richtlijn dat de bevoegde autoriteit of het CSIRT het publiek kan informeren over een gemeld incident. Het ligt in de rede om die bepalingen zó uit te leggen dat de lidstaten verplicht zijn om de bevoegde autoriteit of het CSIRT, of desgewenst beide instanties, de bevoegdheid te geven om het publiek te informeren. Die uitleg is gevolgd bij de formulering van artikel 23, eerste lid.

De zinsnede «Onverminderd artikel 20, vierde lid, onder b,» beoogt duidelijk te maken dat artikel 23, eerste lid, geen lex specialis is ten opzichte van de bevoegdheid van het NCSC om het publiek te informeren: beide bevoegdheden gelden naast elkaar. Als in een concrete situatie zowel het NCSC als de bevoegde autoriteit bevoegd is om het publiek te informeren, dienen beide instanties de voorgenomen toepassing van hun bevoegdheid met elkaar af te stemmen. Hoe dan ook geldt voor beide bevoegdheden dat de aanbieder vooraf geraadpleegd moet worden. Deze zal er zo nodig op wijzen dat beide instanties openbaarmaking voorbereiden.

Artikel 23, eerste lid, ziet alleen op uit hoofde van de meldplicht gemelde incidenten, dus niet op vrijwillig gemelde incidenten of niet-meldplichtige incidenten die op andere manier ter kennis van de bevoegde autoriteit zijn gekomen.

De genoemde twee richtlijnbepalingen, en daarmee de twee onderdelen van artikel 23, eerste lid, verschillen in die zin dat openbaarmaking van een incident bij een AED alleen mag «als publieke bewustwording nodig is» en openbaarmaking van een DSP-incident óók mag als dat «anderszins in het algemeen belang is».

In beide onderdelen van dit lid is vastgelegd dat de bevoegde autoriteit de bevoegdheid heeft om, in plaats van zelf het publiek te informeren, te vorderen dat de betrokken aanbieder dat zelf doet.

Artikel 24 (reikwijdte hoofdstuk 6)

Hoofdstuk 6 strekt, in combinatie met hoofdstuk 5 Awb, ter implementatie van de artikelen 15 (AED's), 17 (DSP's) en 21 (AED's en DSP's) van de richtlijn. Daarom gelden de bevoegdheden van hoofdstuk 6 alleen jegens AED's en DSP's.

Artikel 26 (beveiligingsaudit)

Dit artikel implementeert artikel 15, tweede lid, onder b, van de richtlijn en geldt alleen voor AED's.
Derde lid: De aanbieder draagt zelf de kosten van een door de bevoegde autoriteit opgedragen externe audit. Van die hoofdregel kan worden afgeweken bij amvb voor daarbij omschreven soorten aanbieders of voor alle aanbieders in een bepaalde sector.

Artikel 27 (bindende aanwijzing)

Dit artikel implementeert artikel 15, derde lid, en 17, tweede lid, onder b, van de richtlijn en geldt voor AED's en DSP's. De bepaling is met name bedoeld om de globale norm van de artikelen 7 en 8 op bindende wijze te concretiseren, maar ook bij de nadere regels van artikel 9 kan er behoefte

zijn aan een dergelijke (verdere) concretisering, bijvoorbeeld toegespitst op de betrokken aanbieder. Aan een DSP mag alleen een aanwijzing worden gegeven voor zover artikel 16 van de richtlijn daarvoor ruimte biedt, zie ook de toelichting bij artikel 9.
De aanwijzing kan ook inhouden dat de aanbieder een bepaalde gedraging moet staken of nalaten.
Een vergelijkbare bevoegdheid is te vinden in artikel 1:75 Wft, artikel 12j Instellingswet Autoriteit Consument en Markt (ACM) en artikel 66, derde lid, Wbp.

Artikel 29 (bestuurlijke boete)

Eerste lid, onder b, bestuurlijke boete bij overtreding van artikel 5:20, eerste lid, Awb: in navolging van artikel 1:80, onder d, Wft en artikel 12m, eerste lid, onder c, Instellingswet ACM.

Tweede lid: gekozen is voor de hoogste boetemaxima zoals die zijn opgenomen in de betrokken sectorale wetgeving. Dat biedt de sectorale bevoegde autoriteit die uit hoofde van bestaande wetgeving al bevoegd zijn om een bestuurlijke boete op te leggen, de ruimte om voor de boetebedragen aan te sluiten bij de boetehoogtes die in die sector passend zijn.
Tweede lid, onder a, boetemaximum bij niet verstrekken nadere gegevens artikel 12 of niet-meewerken aan vordering bevoegde autoriteit: ontleend aan artikel 5 Besluit bestuurlijke boetes financiële sector, in samenhang met artikel 1:81, tweede lid, Wft (categorie 2).

Derde lid, beroep schorst de werking van het boetebesluit: in navolging van artikel 1:85 Wft en artikel 15.12 Telecommunicatiewet. Vgl. artikel 12p Instellingswet ACM. De formulering is ontleend aan aanwijzing 5.55 van de Aanwijzingen voor de regelgeving. Uit de Awb volgt dat ook het maken van bezwaar de werking van het besluit opschort. De beroepstermijn gaat immers pas lopen na de bezwaarfase.

Vierde lid, verzet schorst de invordering: in navolging van artikel 15.14 Telecommunicatiewet.

Vijfde lid: niet-meewerken aan vordering van de bevoegde autoriteit is alleen bestuurlijk beboetbaar, niet ook nog een strafbaar feit op grond van artikel 184 Wetboek van Strafrecht (niet opvolgen ambtelijk bevel). Het vijfde lid is ontleend aan artikel 12m, vierde lid, Instellingswet ACM en artikel 18.16q, tweede lid, Wet milieubeheer.

Artikel 30 (wijziging Awb)

In artikel 7 van bijlage 2 bij de Awb wordt de rechtbank Rotterdam aangewezen als bevoegde rechtbank voor beroep in eerste instantie. In artikel 11 van die bijlage wordt het College van Beroep voor het bedrijfsleven aangewezen als hoger beroepsinstantie.
Voor de sectoren bankwezen, infrastructuur voor de financiële markt en spoor geldt al dat de rechtbank Rotterdam en het College van Beroep voor het bedrijfsleven zijn aangewezen als bevoegde rechters. Dat geldt evenzeer voor de deelsectoren gas en elektriciteit. Voor de sector gezondheidszorg is in eerste aanleg de rechtbank Rotterdam aangewezen als bevoegde rechter.
Het is aannemelijk dat besluiten op grond van de Csw in veel gevallen in samenhang met besluiten op grond van betrokken sectorale wet- en regelgeving zullen worden genomen. In die gevallen is het niet wenselijk dat voor besluiten op grond van sectorale wetten een bijzondere bestuursrechter bevoegd is, terwijl voor besluiten op grond van de Csw

de gewone bevoegdheidsregeling zou gelden. Voorts zal in het algemeen een goed oordeel over besluiten op grond van de Csw niet gevormd kunnen worden zonder inzicht in de betrokken sector. Indien voor die sector een bijzondere bestuursrechter bevoegd is verklaard, zal die rechter inhoudelijke deskundigheid hebben opgebouwd ten aanzien van die sector. Het ligt dan voor de hand die rechter ook te laten oordelen over besluiten ten aanzien van die sector op grond van de Csw. Dit geldt voor de sectoren energie (met uitzondering van aardolie), bankwezen, infrastructuur voor de financiële markt, gezondheidszorg (alleen in eerste instantie bij de rechtbank Rotterdam) en spoor.
Voor de deelsectoren aardolie en digitale infrastructuur en voor DSP's geldt dat er nog weinig wetgeving is en evenmin een bijzondere bevoegdheidsregeling. Omwille van de eenduidigheid is ervoor gekozen voor deze (deel)sectoren en dienstverleners aan te sluiten bij de verwante (deel)sectoren waarvoor reeds een bijzondere bevoegdheidsregeling geldt. Voor aardolie zijn dat de deelsectoren elektriciteit en gas en voor digitale infrastructuur en DSP's is dat de telecomsector.

Artikel 31 (samenloop met wetsvoorstel Wet bekostiging financieel toezicht 2019)

Het toezicht op de Csw valt niet onder de bekostiging van het financieel toezicht omdat het toezicht op de Csw wordt uitgevoerd in het kader van de centralebank-taak van DNB in de context van de bescherming van vitale infrastructuren. De bevoegdheden die DNB krijgt toebedeeld in de Csw worden toegepast ter bevordering van de goede werking van het betalingsverkeer (als bedoeld in artikel 4, eerste lid, onderdeel b, van de Bankwet 1998). Deze taak wordt onderscheiden van het uitoefenen van toezicht op financiële instellingen als bedoeld in artikel 4, eerste lid, onderdeel a, Bankwet 1998.

In de Wet bekostiging financieel toezicht is geregeld welke taken onder het financieel toezicht vallen. Zolang de Csw niet in die wet genoemd wordt, vallen de taken van DNB op grond van de Csw niet onder het financieel toezicht. Op dit moment is een wetsvoorstel in procedure waarmee de Wet bekostiging financieel toezicht wordt vervangen (Kamerstukken 34 870). In dat voorstel voor een Wet bekostiging financieel toezicht 2019 is niet langer een lijst met taken opgenomen die onder het financieel toezicht vallen, maar is geregeld dat alle taken van DNB onder het financieel toezicht in de zin van die wet vallen, tenzij de taken zijn uitgezonderd. Een wijziging van dat wetsvoorstel is nodig om de Csw buiten de reikwijdte van de Wet bekostiging financieel toezicht 2019 te houden. Artikel 31 voorziet hierin.

Artikel 34 (intrekking Wgmc)

De Wgmc wordt geïncorporeerd in de Csw en wordt ingetrokken. In beginsel vervallen daardoor de Regeling aanwijzing computercrisisteams, vastgesteld op grond van de artikelen 2, tweede lid, onder b, en 9, tweede lid, onder a, Wgmc, en het op artikel 5 Wgmc gebaseerde Bmc (aanwijzing van de meldplichtige vitale aanbieders). Zoals nu wordt voorzien, zullen zij worden aangepast aan de Csw en worden «omgehangen» («gehangen» onder de Csw: onder de artikelen 3, tweede lid, onder c, en 19, tweede lid, onder b [aanwijzing computercrisisteams] en onder artikel 5, eerste lid [aanwijzing AED's en andere vitale aanbieders]).

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