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

MEMORIE VAN TOELICHTING

Algemeen deel

1. Inleiding

Dit voorstel voor een Cybersecuritywet (hierna ook: 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 wordt de Wet gegevensverwerking en meldplicht cybersecurity (hierna ook: Wgmc) beleidsneutraal geïncorporeerd in de Csw en ingetrokken.

2. De NIB-richtlijn

Het doel van de NIB-richtlijn is om eenheid en samenhang te brengen in Europees beleid voor netwerk- en informatiebeveiliging, ter ondersteuning van het functioneren van onze samenleving en economie, 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.

Om het beoogde doel te bereiken verplicht de NIB-richtlijn de lidstaten ertoe hun paraatheid te verbeteren en beter met elkaar samen te werken, en door zowel aanbieders van essentiële diensten als digitaledienstverleners ertoe te verplichten adequate maatregelen te nemen om beveiligingsrisico's te beheersen en gevolgen van incidenten te voorkomen en minimaliseren en 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 door de lidstaten aan te wijzen “aanbieders van essentiële diensten” (hierna ook: 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 op “digitaledienstverleners” (hierna ook: DSP’s): aanbieders van onlinemarktplaatsen, onlinezoekmachines en cloudcomputerdiensten. De verplichtingen van de richtlijn gelden niet voor eventuele andere diensten die deze organisaties aanbieden. De richtlijn geldt

[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.

ook voor overheidsorganisaties die essentiële diensten aanbieden.
De richtlijn is niet van toepassing op 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 gelijkwaardig zijn aan de verplichtingen van de NIB-richtlijn.

b) aanwijzing van aanbieders van essentiële diensten
De aanwijzing van de aanbieders van essentiële diensten moet uiterlijk op 9 november 2018 gereed zijn. De richtlijn geeft drie criteria voor de aanwijzing:
1. de dienst is van essentieel belang voor de instandhouding van kritieke maatschappelijke of economische activiteiten,
2. de verlening van de dienst is afhankelijk van netwerk- en informatiesystemen, en
3. een incident zou aanzienlijke verstorende effecten hebben voor de verlening van de dienst.

Ter invulling van dat 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 digitaledienstverleners is niet nodig en niet toegestaan. Zij worden limitatief opgesomd in bijlage III van de richtlijn (zie boven) en gedefinieerd in artikel 4 van de richtlijn.

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 (zie hierna) en legt zo 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 wordt 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 wordt 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-gevoelige) informatie worden uitgewisseld over diensten, activiteiten, samenwerkingscapaciteiten en afzonderlijke incidenten.

f) beveiligingseisen, meldplicht en vrijwillige melding
De aanbieders van essentiële diensten en digitaledienstverleners moeten passende en evenredige technische en organisatorische maatregelen nemen om hun ICT adequaat te beveiligen tegen inbreuken van buitenaf en de gevolgen van incidenten te voorkomen en minimaliseren. Verder moeten zij incidenten met aanzienlijke gevolgen melden bij de bevoegde autoriteit of het CSIRT. 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, de duur van het incident, 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 incidenten met aanzienlijke gevolgen door andere entiteiten dan aanbieders van essentiële diensten en digitaledienstverleners (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 behalve voor wat betreft DSP's gericht op minimumharmonisatie. 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 eisen (artikel 16, tiende lid).

3. Gemaakte implementatiekeuzes op hoofdlijnen

Heel kort samengevat bevat dit wetsvoorstel de volgende keuzes:
1. aanwijzing AED's bij algemene maatregel van bestuur (amvb) of bij nader besluit van een in die amvb te noemen bestuursorgaan;
2. aanwijzing Minister van Veiligheid en Justitie als het centrale contactpunt voor Nederland;
3. aanwijzing Minister van Veiligheid en Justitie als het CSIRT voor AED's;
4. aanwijzing van het CSIRT voor digitale diensten bij algemene maatregel van bestuur;
5. aanwijzing van de vakministers respectievelijk De Nederlandsche Bank (hierna ook: DNB) als de bevoegde autoriteiten (toezicht en sancties);
6. beveiligingseisen: globale norm in de Csw, eventueel sectoraal nader uit te werken;
7. dubbel melden van ernstige ICT-incidenten: zowel bij het CSIRT als bij de bevoegde autoriteit;
8. een-op-een overgenomen uit de Wgmc:
   - aangewezen vitale aanbieders, inclusief AED's, moeten ook inbreuken die ernstige gevolgen kúnnen hebben ("bijna-ongelukken") melden, maar alleen bij (het Nationaal Cyber Security Centrum (NCSC) van) de Minister van Veiligheid en Justitie;
   - voor vitale aanbieders die niet onder de richtlijn vallen, geldt alleen de plicht om incidenten bij het NCSC te melden, en dus geen beveiligingseisen en geen toezicht en sancties.

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. De tweede NCSS heeft als doel een veilig digitaal domein te realiseren waarin kansen van digitalisering worden benut, dreigingen het hoofd wordt geboden en fundamentele rechten worden beschermd. Daarbij wordt gezocht naar een goede wisselwerking tussen veiligheid, vrijheid en maatschappelijke groei met de ambitie dat Nederland tot de wereldtop behoort op het terrein van cybersecurity. In de tweede NCSS zijn strategische doelstellingen en een actieprogramma voor cybersecurity opgenomen. De strategie is opgesteld onder coördinerende verantwoordelijkheid van het Ministerie van Veiligheid en

[3] Zie aanwijzing 332 van de Aanwijzingen voor de regelgeving: "Bepalingen uit bindende EU-rechtshandelingen die verplichten tot feitelijk handelen, worden niet geïmplementeerd."

Justitie, in samenwerking met de betrokken vakdepartementen, private organisaties, kennisinstellingen en maatschappelijke organisaties. Daarnaast is de Cyber Security Raad, bestaande uit vertegenwoordigers van publieke en private partijen en wetenschap, geconsulteerd over de koers van de strategie en is een dialoog met de bredere ICT-gemeenschap gevoerd. Momenteel vindt een doorontwikkeling plaats van de huidige strategie.

4. Verhouding tot de Wet gegevensverwerking en meldplicht cybersecurity

Zoals gezegd incorporeert dit wetsvoorstel de inhoud van de Wet gegevensverwerking en meldplicht cybersecurity en wordt de Wgmc ingetrokken. Implementatie van de NIB-richtlijn in de Wgmc zou hebben geleid tot een, in elk geval optisch, ingrijpende wijziging van de Wgmc, inclusief de citeertitel. In plaats daarvan 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 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 Veiligheid en Justitie 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 rijksorganisaties te waarschuwen en te adviseren. De meldplicht geldt alleen voor bij algemene maatregel van bestuur 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.

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 (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 name voor wat de meldplicht bij het NCSC betreft is met de Wgmc vooruitgelopen op de implementatie van de NIB-richtlijn, met daarin de bepaling dat lidstaten ervoor moeten zorgen dat aanbieders van essentiële diensten ernstige ICT-incidenten bij het bevoegd gezag of het CSIRT melden. 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. Daarbij is er overigens voor gekozen om nog niet te voorzien in toezicht op de naleving van deze meldplicht en regeling daarvan plaats te laten vinden in het kader van de implementatie van alle verplichtingen van de NIB-richtlijn, waarbij het toezicht op de meldplicht in onderlinge samenhang met dat op andere in de richtlijn opgenomen verplichtingen ter hand kan worden genomen. Zoals verderop nader wordt toegelicht wordt met dit wetsvoorstel, voor zover het vitale aanbieders betreft van essentiële diensten als bedoeld in de richtlijn, nu ook toezicht op de naleving van de meldplicht bij het NCSC geregeld. Voor andere vitale aanbieders, die onder de meldplicht bij het NCSC blijven vallen, kan worden bezien of in afzonderlijke nieuwe wetgeving al dan niet op vergelijkbare wijze in toezicht op de naleving van deze meldplicht 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 14 van dit wetsvoorstel. 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 Veiligheid en Justitie wordt aangewezen (centraal contactpunt, CSIRT voor aanbieders van essentiële diensten) 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 16 en 17 van dit wetsvoorstel. De

bepalingen in artikel 9 Wgmc over het verstrekken van vertrouwelijke gegevens met betrekking tot aanbieders worden overgeheveld naar artikel 19 van dit wetsvoorstel. Daarbij is overigens in het derde en vierde lid toegevoegd dat onafhankelijke toezichthouders in dezelfde situaties als andere ministers (en de van hun ministeries deel uitmakende toezichthouders) op de hoogte kunnen worden gebracht van vertrouwelijke herleidbare gegevens met betrekking tot aanbieders.
Het Wgmc-begrip vitale aanbieder komt in aangepaste vorm terug in de Csw: de in de NIB-richtlijn bedoelde aanbieders van essentiële diensten zijn in de Csw een subgroep van de vitale aanbieders. Zo ziet de richtlijn niet op waterkeringen en is de Minister van Infrastructuur en Milieu (hierna ook: IenM) in die zin dus geen aanbieder van een essentiële dienst in de zin van de richtlijn, maar primaire waterkeringen zijn voor Nederland uiteraard wel vitaal, dus de Minister van IenM is voor die waterkeringen wel een vitale aanbieder.
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 (en in het geval van artikel 17 de Algemene verordening gegevensbescherming); zie de artikelsgewijze toelichting.

Nu de Csw in de plaats komt van de Wgmc, trekt dit wetsvoorstel de Wgmc in. In beginsel vervallen daardoor de ministeriële regeling tot aanwijzing van computercrisisteams, bedoeld in 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). Eventueel kunnen zij worden aangepast aan de Csw en worden “omgehangen” (“gehangen” onder de Csw).

5. Relatie met sectorale wetten en bevoegdheden

Ministerie van Economische Zaken

Voor de aan te wijzen aanbieders van essentiële diensten die onder de verantwoordelijkheid van de Minister van Economische Zaken vallen, zal het NCSC de CSIRT-functie gaan vervullen. Voor de DSP’s zal het CSIRT bij een algemene maatregel van bestuur worden aangewezen.
Voor de aan te wijzen aanbieders van essentiële diensten die onder de verantwoordelijkheid van de Minister van Economische Zaken vallen en voor de DSP’s zijn de door de Minister van Economische Zaken aangewezen personen belast met het toezicht op de naleving van de Csw.

De Csw voorziet in een meldplicht en een beveiligingsverplichting op het punt van cybersecurity. Op de aan te wijzen aanbieders van essentiële diensten in de sector energie zijn de Elektriciteitswet 1998 en de Gaswet van toepassing. De Elektriciteitswet 1998 (artikel 16, eerste lid, onderdeel q; let op: onderdeel p door wetsvoorstel VET) en de Gaswet (artikel 10, negende lid; let op: achtste lid door wetsvoorstel VET) 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 algemene maatregel van bestuur kan gezien 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. 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 aanbieders van essentiële diensten in overige sectoren die onder de verantwoordelijkheid van de Minister van Economische Zaken 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 overlap of botsende verplichtingen.

Ministerie van Financiën
Voor de financiële sector geldt dat de aan te wijzen aanbieders van essentiële diensten ook al vallen onder de meldplicht die is opgenomen in de Wgmc. In dit opzicht brengt de Cybersecuritywet geen extra verplichtingen met zich mee.

De Nederlandsche Bank was al belast met het toezien op de operationele continuïteit van het betalingsverkeer. Het ligt daarom voor de hand om DNB aan te wijzen als sectorale toezichthouder. Als CSIRT fungeert de Minister van Veiligheid en Justitie (NCSC).

In de Cybersecuritywet zijn een meldplicht en beveiligingseisen opgenomen. Op grond van de Wet op het financieel toezicht (hierna ook: Wft) en de daarop gebaseerde regelgeving bestaan al meldplichten en beveiligingseisen. De doelstelling van de Wft verschilt op dit punt echter van die van de Cybersecuritywet. 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 Cybersecuritywet zijn er vooral om de operationele risico's rondom cyberincidenten zoveel mogelijk te beperken. 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). Deze meldplicht uit de Cybersecuritywet is dus vooral gericht op het bieden van hulp en het ongedaan maken van (de gevolgen van) het incident. Voor wat betreft de beveiligingseisen geldt dat instellingen die onder beide wetten vallen zowel aan de eisen uit de Wft als de Cybersecuritywet moeten voldoen. Niet wordt verwacht dat deze overlap tot ongewenste gevolgen zal leiden. Mocht dit voor bepaalde soorten aanbieders van essentiële diensten wel het geval zijn, dan biedt het voorgestelde artikel 6 de mogelijkheid om bepaalde bij of krachtens de Cybersecuritywet vastgestelde voorschriften buiten toepassing te laten.

Ministerie van Infrastructuur en Milieu
Voor de aan te wijzen aanbieders van essentiële diensten die onder de verantwoordelijkheid van de Minister van Infrastructuur en Milieu vallen geldt dat het overgrote deel van die aanbieders ook onder de meldplicht van de Wgmc valt. De voorgestelde Cybersecuritywet levert voor die aanbieders op het punt van de meldplicht dus geen extra verplichting op.
Voor de aan te wijzen aanbieders van essentiële diensten die onder de verantwoordelijkheid van de Minister van Infrastructuur en Milieu vallen, geldt voorts dat het gaat om professionele organisaties die alle inspanningen leveren die nodig zijn om de continuïteit van hun dienstverlening te waarborgen. Hoewel er nog geen wettelijke verplichtingen bestaan om hun netwerk- en informatiesystemen adequaat te beveiligen is het voor deze aanbieders vanzelfsprekend om daarin te voorzien. De voorgestelde Cybersecuritywet levert voor deze aanbieders dus wel een nieuwe verplichting op maar dan een waar ze zonder veel problemen aan zullen kunnen voldoen.

Voor de aan te wijzen aanbieders van essentiële diensten die onder de verantwoordelijkheid van de Minister van Infrastructuur en Milieu vallen, zal het NCSC de CSIRT-functie gaan vervullen.

De voorgestelde Cybersecuritywet 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 aan te wijzen aanbieders van essentiële diensten die onder de verantwoordelijkheid van de Minister van Infrastructuur en Milieu vallen. Er is dus geen sprake van overlap of botsende verplichtingen.

Ministerie van Volksgezondheid, Welzijn en Sport (VWS)
Wanneer wordt besloten om aanbieders van essentiële diensten (AED's) aan te wijzen die onder de verantwoordelijkheid van de Minister van VWS vallen, geldt dat de Cybersecuritywet (Csw) voor deze aanbieders een extra melding oplevert bij een CSIRT

(het NCSC), naast melding bij de Inspectie voor de Gezondheidzorg (IGZ) in het kader van kwaliteit van zorg (bijv. klachten en geschillen zorg) en/of de Autoriteit persoonsgegevens (AP) in het kader van bescherming van persoonsgegevens. Daarnaast geldt voor deze AED's, dat dit professionele organisaties betreft die veelal al ruime aandacht hebben voor die zaken die nodig zijn om de continuïteit van hun dienstverlening te waarborgen. T.a.v. vertrouwelijkheid en integriteit bestaan voor de zorgsector al regels en toezicht en handhaving, zoals de meldplicht voor calamiteiten op grond van de Wet kwaliteit, de meldplicht datalekken, de beveiligingsvoorschriften NEN 7510, 7512 en 7513 en het toezicht daarop door de IGZ en de AP.
Voor de eventueel 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 toezichthouder voor de zorg, te weten IGZ.
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 juridische overlap of botsende verplichtingen.

6. Handhaving (toezicht en sancties)

De voorgestelde Cybersecuritywet voorziet in handhaving ten aanzien van de verplichtingen voor de aanbieders van essentiële diensten en digitaledienstverleners (zie hoofdstuk 6 Csw). Hiertoe verplichten de artikelen 14 en 17 van de NIB-richtlijn.

De Csw kent naast verplichtingen voor aanbieders van essentiële diensten en digitaledienstverleners verplichtingen voor andere vitale aanbieders. Die verplichtingen komen overeen met de verplichtingen op grond van de Wgmc. Evenals die wet 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 handhaving is zowel reparatoir als punitief van aard. De handhaving heeft betrekking op verplichtingen voor een beperkt aantal entiteiten. Die entiteiten zijn veelal bekend en behoren in de overige gevallen tot een afgebakende categorie. In alle gevallen gaat het om gereguleerde sectoren, die in andere opzichten opereren binnen specifieke kaders. Daar komt nog bij dat de entiteiten die verplichtingen opgelegd krijgen door de Csw, op verschillende terreinen al te maken hebben met bestuursrechtelijke handhaving. Een en ander is reden om (ook) voor de Csw te kiezen voor bestuursrechtelijke handhaving.

Het toezicht op de verplichtingen van de Csw wordt opgedragen aan door de bevoegde autoriteiten aangewezen personen. Die aangewezen personen zijn toezichthouders in de zin van hoofdstuk 5 van de Algemene wet bestuursrecht. Daarmee beschikken zij over de bevoegdheden die hoofdstuk 5 van de Algemene bestuursrecht toekent aan toezichthouders. Het gaat hier om de bevoegdheden geregeld in de artikelen 5:15 tot en met 5:19 van de Algemene wet bestuursrecht en de verplichting om mee te werken aan het toezicht van artikel 5:20 van die wet. 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 Algemene wet bestuursrecht kunnen uitoefenen, voorziet de Csw voor de bevoegde autoriteiten in de mogelijkheid om aanbieders van essentiële diensten of digitaledienstverleners een bindende aanwijzing op te leggen 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, van de Algemene wet bestuursrecht. 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.

De Csw voorziet in de bevoegdheid voor de bevoegde autoriteit om de aanbieder van essentiële diensten 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 de op grond van de voorgestelde Cybersecuritywet voor die aanbieder van toepassing zijn. De mogelijkheid om een audit op te leggen, is opgenomen om te ondervangen dat de bevoegde autoriteit niet altijd beschikt over voldoende kennis en middelen om zelf zo'n audit te doen. Tenzij bij algemene maatregel van bestuur anders wordt bepaald, draagt de aanbieder van de essentiële dienst zelf de kosten van de audit. Mocht de bevoegde autoriteit in staat zijn om zelf een audit uit te voeren dan kan dat ook, in dat geval op haar kosten.

Indien de aanbieder van essentiële diensten de bij of krachtens de Csw gestelde normen overtreedt, dan voorziet de wet in de mogelijkheid van het opleggen van bestuurlijke herstelsancties, dus last onder dwangsom of last onder bestuursdwang, en bestuurlijke boetes. Zoals hiervoor al opgemerkt is bestuursrechtelijke handhaving de aangewezen weg, daarom is gekozen voor een bestuurlijke boete en niet voor strafrechtelijke handhaving.
Voor de volledigheid wordt erop gewezen dat voor het opleggen van een bestuurlijke sanctie niet altijd vereist is dat er eerst een bindende aanwijzing wordt gegeven. Indien de norm die wordt overtreden voldoende concreet is, kan direct een bestuurlijke sanctie worden opgelegd.
Voor de verschillende sectoren waarin de aanbieders van essentiële diensten waarvoor de Csw, in navolging van de NIB-richtlijn, normen stelt, opereren is vaak al voorzien in de mogelijkheid om voor andere overtredingen 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 Wet op het financieel toezicht. Voor het niet voldoen aan de verplichting om na een melding nadere gegevens te verstrekken alsmede bij het niet verlenen van de gevorderde medewerking is het maximum bepaald op € 1 miljoen. Een bijkomende overweging voor deze hoogte van de maximale bestuurlijke boete voor de overige overtredingen is dat het voor aanbieders van essentiële diensten 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.

7. Transponeringstabel

Artikel, -lid of -onderdeel NIB-richtlijn[4]	**Te implementeren in**[5]	**Bijzonderheden** (zoals beleidskeuzes)
Artikel 1 (onderwerp en toepassingsgebied)	Art. 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. Art. 1 lid 7 (voorrang voor sectorspecifieke EU-regels): art. 6 Csw. Voor het overige behoeft art. 1 geen implementatie want betreft uitleg richtlijn.	
Artikel 2 (bescherming en verwerking persoonsgegevens)	Art. 16 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").	
Artikel 4 (definities)	Art. 1 Csw (voor zover de begrippen in de Csw worden gebruikt).	
Artikel 5 (aanwijzing AED's)	Lid 1-3: artikel 5 Csw. Lid 4-7 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 (aanwijzing bevoegde autoriteit en centraal contactpunt)	Lid 1 en 2 (bevoegde autoriteit): art. 4 lid 1, lid 2 onder a en lid 3 en art. 16 lid 2 Csw. Lid 3 en 4 (centraal contactpunt): art. 2 onder a, art. 3 lid 1 onder a en art. 18 Csw. Lid 5-7 behoeven geen implementatie want betreft feitelijk handelen.	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.

[4] 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).

[5] Gebruikte afkortingen:
AED: aanbieder van een essentiële dienst
amvb: algemene maatregel van bestuur
Awb: Algemene wet bestuursrecht
CSIRT: computer security incident response team
Csw: Cybersecuritywet
DSP: digitaledienstverlener.

Artikel, -lid of -onderdeel NIB-richtlijn[4]	**Te implementeren in**[5]	**Bijzonderheden** (zoals beleidskeuzes)
Artikel 9 (aanwijzing CSIRT)	Lid 1: art. 2 onder b, 3 lid 1 onder b en 16 lid 1 (AED's) en art. 4 lid 2 onder b en lid 4 en 16 lid 3 Csw (DSP's). Lid 2-5 behoeven geen implementatie want betreft feitelijk handelen.	De richtlijn laat het aan de lidstaten om een of meer CSIRT's aan te wijzen. De Csw wijst de MVenJ aan als CSIRT voor AED's. Aanwijzing CSIRT voor DSP's bij amvb.
Artikel 10 (samenwerking nationaal)	Lid 1 behoeft geen implementatie want betreft feitelijk handelen. Lid 2, 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. Lid 3 is voor DSP's omgezet in art. 18 lid 1. Voor AED's behoeft het geen implementatie omdat de MVenJ 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.	
Artikel 13 (internationale samenwerking)	Behoeft geen implementatie want betreft handelen Europese Unie.	
Artikel 14 (beveiligingseisen en meldplicht AED's)	Lid 1 en 2: art. 7-9 Csw. Lid 3 en 4: art. 10 lid 1 onder a en lid 2 en 4, en art. 11 en 12 Csw. Lid 5: art. 18 lid 2 Csw. Laatste volzin: art. 18 lid 3 Csw. Lid 6: art. 20 onder a Csw. Lid 7 behoeft geen implementatie want betreft feitelijk handelen.	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 15 (uitvoering en handhaving AED's)	Lid 1: art. 4 lid 3 en hoofdstuk 6 Csw, in samenhang met hoofdstuk 5 Awb. Lid 2 onder a (informatie verschaffen): art. 22 Csw, in samenhang met titel 5.2 Awb. Lid 2 onder b (beveiligingsaudit): art. 23 Csw.	

Artikel, -lid of -onderdeel NIB-richtlijn[4]	**Te implementeren in**[5]	**Bijzonderheden** (zoals beleidskeuzes)
	Lid 3 (bindende aanwijzing): art. 24 Csw. Lid 4 behoeft geen implementatie want betreft feitelijk handelen.	
Artikel 16 (beveilingseisen en meldplicht DSP's)	Lid 1 en 2: art. 7-9 Csw. Lid 3 en 4: art. 13 Csw. Lid 5: art. 10 lid 3 en lid 5 Csw. Lid 6: art. 18 lid 4 Csw. Lid 7: art. 20 onder b Csw. Lid 8 en 9 (uitvoeringshandelingen EC): art. 9 en 14 Csw. Lid 10 behoeft geen implementatie want betreft verbod om andere eisen op te leggen. Lid 11: omschrijving van *digitaledienstverlener* in art. 1 Csw.	Art. 13 Csw regelt dat een DSP een ernstig incident moet melden bij het CSIRT en bij de bevoegde autoriteit.
Artikel 17 (uitvoering en handhaving DSP's)	Het eerste en tweede lid zijn uitgewerkt in hoofdstuk 6 van de Cybersecuritywet. Het derde lid behoeft geen implementatie want betreft feitelijk handelen. Lid 1 en lid 2 onder b: art. 4 lid 3 en hoofdstuk 6 Csw, in samenhang met hoofdstuk 5 Awb. Lid 2 onder a (informatie verschaffen): art. 22 Csw, in samenhang met titel 5.2 Awb. Lid 3: art. 24 Csw. Lid 4 behoeft geen implementatie want betreft feitelijk handelen.	
Artikel 18 (jurisdictie en territorialiteit DSP's)	Omschrijving van *digitaledienstverlener* in art. 1 Csw.	
Artikel 19 (normalisatie)	Behoeft geen implementatie want betreft feitelijk handelen.	
Artikel 20 (vrijwillige melding)	Art. 15 en 16 lid 4 Csw.	
Artikel 21 (sancties)	Art. 24-26 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.	

Artikelsgewijze toelichting

Artikel 1 (begripsbepalingen)
aanbieder:
- 'overheidsorganisatie of *privaatrechtelijke* rechtspersoon': net als in Wgmc toegevoegd om overlap met overheidsorganisatie te voorkomen.
- ziet (indien als zelfstandige term gebruikt, zoals in de artikelen 15 [vrijwillige meldingen] en 19 [verstrekking vertrouwelijke gegevens door NCSC]) ook op de digitaledienstverlener.

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 NL (artikel 18, eerste lid), ofwel (voor wat betreft DSP van buiten de EU) EU-vertegenwoordiger gevestigd in NL (artikel 18, tweede lid).

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 essentiële diensten)
Dit artikel wijst de Minister van Veiligheid en Justitie aan als het in artikel 8 van de richtlijn bedoelde centrale contactpunt en, voor aanbieders van essentiële diensten, als het in artikel 9 van de richtlijn bedoelde CSIRT.

Artikel 3 (taken van Onze Minister)
Dit artikel is voor een groot deel identiek aan artikel 2 Wgmc en implementeert mede artikel 8 van de richtlijn. Het artikel bevat een opsomming van de taken van de Minister (ingevolge de huidige portefeuilleverdeling de Staatssecretaris) van Veiligheid en Justitie 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 het NCSC als centraal contactpunt voor essentiële én digitale diensten en als CSIRT voor essentiële diensten, 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 het NCSC met de aanwijzing in artikel 2 tot centraal contactpunt en tot CSIRT voor essentiële diensten, 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. Aan de opsomming zijn CSIRT's toegevoegd. Blijkens de omschrijving in artikel 1 zijn dat de CSIRT's die door een lidstaat van de Europese Unie (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. Gegevensuitwisseling met andere CSIRT's dan het NCSC (waartoe uiteraard ook behoort het op grond van artikel 4, tweede lid, onder b, aangewezen CSIRT voor digitale diensten) is derhalve gerechtvaardigd en verantwoord. De toetsing van die belangen op grond van artikel 3, tweede lid, onder c, ziet derhalve op andere computercrisisteams dan CSIRT's in de zin van de richtlijn.

De taakomschrijving van artikel 3 omvat de taken die voortvloeien uit de aanwijzing van de Minister van Veiligheid en Justitie 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 digitale diensten)
Dit artikel implementeert de artikelen 9 (aanwijzing CSIRT voor digitale diensten) en (samen met hoofdstuk 6 Csw en hoofdstuk 5 Awb) 15 en 17 van de richtlijn (handhaving).
Derde lid, 'bestuursrechtelijke handhaving': de term *handhaving* is hier gebruikt in dezelfde brede zin als in hoofdstuk 5 Awb, dwz 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 beveiligingsmaatregel.
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 correspondeeert 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 afgeleid van 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 Besluit meldplicht cybersecurity. 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 NV”) 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,[6] waarin de amvb de aanwijzing delegeert aan een in die amvb te noemen bestuursorgaan, bijvoorbeeld (zie het Besluit meldplicht cybersecurity) de aanwijzing van waterkeringen door de Minister van Infrastructuur en Milieu of de aanwijzing van financiële instellingen als bedoeld in artikel 1:1 Wft 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 NV naar verwachting worden aangewezen als aanbieder van de essentiële dienst ‘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 (gedelegeerde) verordeningen. Het voorgestelde artikel 6 biedt de mogelijkheid om, voor zover nodig om te voldoen aan artikel 1, zevende lid, van de richtlijn, bij algemene maatregel van bestuur (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 aanbieders van essentiële diensten als voor digitaledienstverleners.

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).

Artikel 8 (gevolgen van incidenten voorkomen en minimaliseren)
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 de nadelige gevolgen van incidenten te voorkomen en minimaliseren).

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 algemene maatregel van bestuur (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 digitaledienstverleners mogen alleen nadere regels worden gesteld voor zover dat nodig is ter implementatie van door de Europese Commissie vastgestelde “uitvoeringshandelingen” als bedoeld in artikel 16, achtste lid, van de richtlijn. Het tiende lid van dat artikel verbiedt de lidstaten namelijk om aan digitaledienstverleners

[6] Kamerstukken II 2015/16, 34388, nr. 3, p. 27.

“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.

Arikel 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 aanbieder van een essentiële dienst 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). Die dubbele meldplicht zal technisch zó worden vormgegeven, 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, ook als het gaat om ICT van een ander dan de aanbieder zelf.

De meldplicht van het eerste lid, onder b, correspondeert met 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 veiligheid van een elektronisch informatiesysteem waarvan de dienst afhankelijk is, waarbij de inbreuk nog niet daadwerkelijk heeft geleid tot een belangrijke onderbreking van de beschikbaarheid of betrouwbaarheid 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. De meldplicht geldt bijvoorbeeld ook als de integriteit van de ICT is aangetast, zie de definitie van “beveiliging van netwerk- en informatiesystemen” in artikel 4, onder 2, van de richtlijn.
De “bijna-ongelukken” van het eerste lid, onder b, hoeven alleen gemeld te worden bij het NCSC en niet ook bij de bevoegde autoriteit.

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 digitaledienstverlener 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 digitaledienstverlener 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 digitaledienstverlener 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 toezichthouder en (in afwijking van artikel 10, eerste of derde lid) niet ook bij het NCSC. Voor het geval dat de toezichthouder 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 digitaledienstverlener)
Dit artikel implementeert artikel 16, derde en vierde lid, van de richtlijn.
Eerste lid: Net als voor een incident met aanzienlijke gevolgen voor de continuïteit van een essentiële dienst geldt ook voor een incident met aanzienlijke gevolgen voor een digitale dienst als bedoeld in bijlage III van de richtlijn (onlinemarktplaats, onlinezoekmachine en cloudcomputerdienst, zie ook de definities daarvan in artikel 4 van de richtlijn) dat de aanbieder het incident zowel moet melden bij het CSIRT (eerste lid, onder a) als bij de bevoegde autoriteit (tweede lid). En ook hiervoor geldt dat die dubbele meldplicht technisch zó zal worden vormgegeven, dat de aanbieder desgewenst met één handeling aan beide meldplichten kan voldoen, bijvoorbeeld door op een elektronisch formulier beide instanties aan te vinken.
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 digitaledienstverleners een bepaling zoals artikel 11 (bij de melding te verstrekken gegevens). Zie echter de toelichting bij artikel 14 Csw.

Artikel 14 (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 digitaledienstverleners 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 negende lid van dat artikel (formats en procedures voor meldingseisen). De Europese Commissie is overigens niet verplicht om dergelijke uitvoeringshandelingen vast te stellen.

Artikel 15 (vrijwillige melding van incidenten)
Dit artikel, waarmee artikel 20 van de richtlijn wordt geïmplementeerd, geldt voor niet onder de meldplicht van de artikelen 7 en 9 vallende incidenten met aanzienlijke gevolgen voor:
a. een dienst van een niet op grond van artikel 5 aangewezen aanbieder;
b. een niet aangewezen dienst van een aanbieder die óók een essentiële dienst aanbiedt.
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 16 (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 Algemene verordening gegevensbescherming (AVG). Bij de in dit artikel 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 worden door het NCSC uiteraard verwerkt met inachtneming van de AVG; zie ook paragraaf 6 van het algemeen deel van de memorie van toelichting bij de Wgmc. De Autoriteit persoonsgegevens alsook de departementale functionaris voor de gegevensbescherming houden toezicht op deze verwerkingen door het NCSC. Uit de AVG volgt onder andere dat persoonsgegevens die niet langer noodzakelijk zijn voor de uitoefening van de NCSC-taken zullen worden vernietigd. 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, derde en vierde lid bevatten een met het eerste lid vergelijkbare bepaling voor de sectorale toezichthouders, het CSIRT voor digitale diensten en de instantie voor het verwerken van vrijwillige meldingen.

Artikel 17 (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 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. De taak, genoemd in het tweede lid van artikel 3, ziet alleen op verstrekking van gegevens door het NCSC aan derden en kan dus geen grondslag bieden voor verstrekking van gegevens aan het NCSC. 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 voorkoming of beperking van het uitvallen van de beschikbaarheid of het verlies van integriteit van van netwerk- en informatiesystemen van 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. Artikel 23 AVG biedt echter de mogelijkheid om onder voorwaarden de reikwijdte van de verplichtingen en rechten van artikel 5 te beperken door middel van lidstaatrechtelijke bepalingen die op de verwerkingsverantwoordelijke of de verwerker van toepassing zijn. Het tweede lid van artikel 17 Csw geeft toepassing aan die beperkingsbevoegdheid. Die beperking is noodzakelijk ter waarborging van meerdere in artikel 23, eerste lid, AVG, genoemde belangen, waaronder de nationale veiligheid, de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid, de economische en financiële belangen van Nederland en andere lidstaten van de EU, volksgezondheid en de bescherming van de rechten en vrijheden van anderen. Naar mijn oordeel rechtvaardigt het zwaarwegende algemene belang dat het NCSC zijn wettelijke taken kan vervullen, de voorgestelde beperking van artikel 5 AVG. De vertrouwelijkheid van de gegevens die op grond van artikel 17 worden verstrekt aan het NCSC, wordt beschermd door artikel 19 van dit wetsvoorstel.

Artikel 18 (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.

Artikel 19 (verstrekking van vertrouwelijke gegevens door Onze Minister)
Deze bepaling is voor een groot deel identiek aan artikel 9 Wgmc en regelt de verstrekking door het NCSC aan derden van vertrouwelijke gegevens met betrekking tot aanbieders die het NCSC heeft verkregen, 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 sectorale toezichthouders 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 en aangevuld met een toelichting bij wat in artikel 19 Csw nieuw is. Voor de duidelijkheid worden de verschillen tussen artikel 19 Csw en artikel 9 Wgmc nog eens opgesomd aan het eind.

Artikel 9 ziet op alle vertrouwelijke gegevens met betrekking tot aanbieders die zich bij het NCSC 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. De medewerkers van het NCSC zijn gebonden aan de geheimhoudingsplicht van artikel 272 van het Wetboek van Strafrecht en artikel 2:5 van de Algemene wet bestuursrecht. 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 19 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, van de Wet op het financieel toezicht (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 Wet bescherming persoonsgegevens (en vanaf 25 mei 2018 de Algemene verordening gegevensbescherming), 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,[7] zoals artikel 8:28 Algemene wet bestuursrecht (inlichtingen verstrekken aan de bestuursrechter door partijen in een beroepsprocedure) of artikel 126nc 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), computercrisisteams die bij ministeriële regeling zijn aangewezen en aan de Nederlandse inlichtingen- en veiligheidsdiensten, 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 toezichthouder. Een dergelijke toestemming kan bijvoorbeeld overleg mogelijk maken tussen het NCSC en die toezichthouder om te voorkomen dat de aanbieder geconfronteerd wordt met een aanwijzing van de toezichthouder 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

[7] Vgl. “voor zover enig wettelijk voorschrift hem tot mededeling verplicht” in artikel 2:5 Algemene wet bestuursrecht.

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.[8] 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 Staatssecretaris van Veiligheid en Justitie 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 avies verstrekken aan de voor de betrokken sector verantwoordelijke minister of staatssecretaris of, in het geval van de financiële sector, aan De Nederlandsche Bank (dit laatste is nieuw ten opzichte van artikel 9, derde lid, Wgmc), met inbegrip van de in het advies opgenomen herleidbare gegevens (artikel 19, 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 cybersecurity-aspecten van het incident of de kwetsbaarheid waarop het advies betrekking heeft.

De bevoegdheid van het derde lid kan uiteraard ook betrekking hebben op bij het NCSC gemelde inbreuken als bedoeld in artikel 10, eerste lid, onder b (bijna-ongelukken).

Als het advies betrekking heeft op een rijksoverheidsorganisatie zal in elk geval (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 Algemene wet bestuursrecht 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).

[8] Kamerstukken II 2013/14, 26643, nr. 297, p. 4.

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 formulering “andere organisaties” ziet bijvoorbeeld ook op een toezichthoudende dienst die geen onderdeel is van een ministerie, zoals de Autoriteit Financiële Markten.

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 enige overlap met de ter uitvoering van de NIB-richtlijn in artikel 20 geregelde bevoegdheid van de bevoegde autoriteit om het publiek te informeren. Er zijn situaties denkbaar waarin zowel het NCSC als de bevoegde autoriteit bevoegd is om het publiek te informeren. Dat is een gevolg van de keuze om de Wgmc beleidsneutraal te incorporeren in de Csw. 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. Deze zal er zo nodig op wijzen dat beide instanties openbaarmaking voorbereiden.

Overigens hebben beide bevoegdheden niet hetzelfde bereik. De bevoegdheid van het NCSC om het publiek te informeren, geldt voor alle aanbieders en niet alleen, zoals artikel 20, voor aanbieders van een essentiële of digitale dienst.

Het **zesde lid** (nieuw ten opzichte van artikel 9 Wgmc) strekt ertoe om te voorkomen dat de Minister van Veiligheid en Justitie niet kan voldoen aan zijn verplichtingen als centraal contactpunt. Het gaat daarbij enerzijds om het waarschuwen van het centrale contactpunt van een andere lidstaat voor een bij het NCSC gedane melding van een ernstig incident met gevolgen voor die lidstaat (artikel 18, tweede, derde en vierde lid, Csw), anderzijds om het waarschuwen van de Nederlandse bevoegde autoriteit of het Nederlandse CSIRT voor digitale diensten, voor een elders in de Europese Unie gemeld ernstig incident met gevolgen voor Nederland (artikel 18, vijfde lid, Csw).

Zoals uiteengezet in het algemeen deel van deze memorie bevat artikel 19 een bijzondere openbaarheidsregeling voor vertrouwelijke herleidbare gegevens die afwijkt van de Wet openbaarheid van bestuur. 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 19, bij een ander overheidsorgaan berusten. Een en ander geldt echter niet voor milieu-informatie. Ter uitvoering van het Verdrag van Aarhus[9] en EU-richtlijn 2003/4/EG[10] bevat de Wob voor 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[11] maar relatief,[12] en in plaats van de relatieve weigeringsgrond dat onevenredige bevoordeling of benadeling

[9] Verdrag betreffende toegang tot informatie, inspraak bij besluitvorming en toegang tot de rechter inzake milieuaangelegenheden, Trb. 2001, 73.
[10] 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).
[11] Artikel 10, eerste lid, aanhef en onder c, Wob.
[12] Artikel 10, vierde lid, tweede volzin, Wob.

voorkomen moet worden[13] 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.[14] 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.[15] Om strijdigheid met het genoemde verdrag en de genoemde richtlijn te voorkomen, volgt uit het zevende lid van artikel 19 dat de Wob onverkort van toepassing is op herleidbare gegevens die milieu-informatie inhouden.

Artikel 19, 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 19 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). Van dergelijke "computercrisisteams" moet worden aangenomen dat zij voldoen aan de waarborgen van bijlage I van de NIB-richtlijn en dat Nederland niet bevoegd is om te toetsen (op grond van artikel 19, tweede lid, onder b) of gegevensuitwisseling daarmee gerechtvaardigd en verantwoord is.
2. In het *derde lid* is de bevoegde autoriteit toegevoegd als instantie waaraan de Minister van Veiligheid en Justitie 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 De Nederlandsche Bank, 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 De Nederlandsche Bank.
4. Het zesde lid is nieuw ingevoegd, zie boven.

Artikel 20 (openbaarmaking incidenten)
Het eerste lid (essentiële diensten) implementeert artikel 14, zesde lid, van de richtlijn, het tweede lid (digitale diensten) artikel 16, zevende lid. 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 20.

De zinsnede "Onverminderd artikel 19, vierde lid, onder b," beoogt duidelijk te maken dat artikel 20 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

[13] Artikel 10, tweede lid, aanhef en onder g, Wob.
[14] Artikel 1, onder g, en artikel 10, zesde en zevende lid, Wob.
[15] ABRvS 10 maart 2010, ECLI:NL:RVS:2010:BL7035.

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 20 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 bevatten twee verschillen, die zijn overgenomen in artikel 20:
1. Openbaarmaking van een AED-incident mag alleen “als publieke bewustwording nodig is”, openbaarmaking van een DSP-incident mag óók als dat “anderszins in het algemeen belang is”.
2. Anders dan bij een AED-incident kan de bevoegde autoriteit bij een DSP-incident er ook voor kiezen om te vorderen (“require” in de Engelse tekst van de richtlijn, “imposer” in de Franse tekst) dat de digitaledienstverlener het publiek zelf informeert.

Artikel 21 (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 23 (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 algemene maatregel van bestuur voor daarbij omschreven soorten aanbieders of voor alle aanbieders in een bepaalde sector.

Artikel 24 (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 digitaledienstverlener 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, Wet bescherming persoonsgegevens.

Artikel 26 (bestuurlijke boete)
Lid 1 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.

Lid 2: gekozen is voor de hoogste boetemaxima zoals die zijn opgenomen in de betrokken sectorale wetgeving. Dat biedt de sectorale toezichthouders 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.

Lid 2 onder a, boetemaximum bij niet verstrekken nadere gegevens artikel 12 of niet-meewerken aan vordering toezichthouder: ontleend aan artikel 5 Besluit bestuurlijke boetes financiële sector, in samenhang met artikel 1:81, tweede lid, Wft (categorie 2).

Lid 3, beroep schorst de werking van het boetebesluit: in navolging van artikel 1:85 Wft en artikel 15.12 Telecommunicatiewet (Tw). Vgl. artikel 12p Instellingswet ACM. De formulering is ontleend aan aanwijzing 160 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.

Lid 4, verzet schorst de invordering: in navolging van artikel 15.14 Tw.

Lid 5, niet-meewerken aan vordering toezichthouder 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 27 (samenloop met wetsvoorstel Wet open overheid)
PM: samenloop Woo actualiseren: artikel 9.60a Woo regelt samenloop met artikel 9 lid 6 Wgmc (= artikel 19 lid 7 Csw), door die laatste bepaling toe te voegen aan de bijlage bij artikel 8.8 Woo.

Artikel 28 (intrekking Wet gegevensverwerking en meldplicht cybersecurity)
De Wgmc wordt geïncorporeerd in de Csw en wordt ingetrokken. In beginsel vervallen daardoor de ministeriële regeling tot aanwijzing van computercrisisteams, bedoeld in 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). Eventueel kunnen 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 aanbieders van een essentiële dienst en andere vitale aanbieders)).

De Staatssecretaris van Veiligheid en Justitie,