concept 22 januari 2015 www.internetconsultatie.nl/cybersecurity

Wet houdende regels over het verwerken van gegevens ter bevordering van de veiligheid en de integriteit van elektronische informatiesystemen die van vitaal belang zijn voor de Nederlandse samenleving en regels over het melden van ernstige inbreuken (Wet gegevensverwerking en meldplicht cybersecurity)

MEMORIE VAN TOELICHTING

ALGEMEEN

1. Inleiding

Dit wetsvoorstel introduceert een meldplicht voor een inbreuk op de veiligheid of een verlies van integriteit van elektronische informatiesystemen (hierna ook: ICT-inbreuken) en stelt regels over het verwerken van gegevens ten behoeve van de taken van de Minister van Veiligheid en Justitie op het terrein van cybersecurity.

De meldplicht geldt alleen voor aanbieders van producten of diensten waarvan de beschikbaarheid of betrouwbaarheid van vitaal belang is voor de Nederlandse samenleving, en slechts als de inbreuk tot gevolg heeft of kan hebben dat de beschikbaarheid of betrouwbaarheid van dergelijke producten of diensten in belangrijke mate wordt of kan worden onderbroken. De meldplicht geldt uitsluitend voor bij algemene maatregel van bestuur aan te wijzen aanbieders van daarbij aan te wijzen producten of diensten. De melding moet worden gedaan aan de Minister van Veiligheid en Justitie. De melding wordt behandeld door het Nationaal Cyber Security Centrum (NCSC), een onderdeel van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), die deel uitmaakt van het ministerie. De melding stelt het NCSC in staat om hulp te verlenen aan de getroffen aanbieder en om andere aanbieders te waarschuwen, met als uiteindelijke doel om het risico van maatschappelijke ontwrichting in te schatten en die ontwrichting te voorkomen of in elk geval zo veel mogelijk te beperken.

Deze meldplicht voor ICT-inbreuken is aangekondigd in een brief aan de Tweede Kamer van 6 juli 2012, naar aanleiding van een verzoek van de Kamer om te komen tot de wettelijke vastlegging van een ‘security breach notification’ bij het NCSC voor organisaties die betrokken zijn bij voor de samenleving vitale informatiesystemen. Aanleiding voor dat verzoek was de elektronische inbraak bij het bedrijf DigiNotar in het najaar van 2011. Deze ICT-inbreuk heeft het toegenomen belang en de onderlinge verwevenheid van ICT-systemen bij de overheid en (overige) vitale sectoren zichtbaar gemaakt. De meldplicht sluit aan bij het voorstel van de Europese Commissie om EU-breed te komen tot een meldplicht voor overheden en vitale marktpartijen die bijdraagt aan het verhogen van de digitale veiligheid.

Naar aanleiding van het Pobelka-incident in 2013 heb ik onderzocht of er voldoende rechtsbasis is voor de verwerking van gegevens door het NCSC. In mijn brief van 12 december 2013 heb ik de Tweede Kamer bericht dat voor de huidige verwerking van (persoons)gegevens door het NCSC een afdoende wettelijke grondslag voorhanden is, maar dat het, juist ook met het oog op de toekomst, aangewezen is om de taken van het NCSC in het kader waarvan persoonsgegevens worden verwerkt, alsook de daaraan gekoppelde bevoegdheid tot verwerking daarvan, van een steviger wettelijke grondslag te voorzien. Daartoe strekken met name de artikelen 2 en 3 van dit wetsvoorstel. In dezelfde brief ben ik tevens ingegaan op het belang van de vertrouwelijkheid van aan het NCSC verstrekte gegevens. Om die vertrouwelijkheid te waarborgen, bevat het voorgestelde artikel 9 een strikte regeling over de verstrekking aan derden van door het NCSC verkregen vertrouwelijke gegevens.

Waar in deze memorie van toelichting wordt gesproken van vitale aanbieders, kan dit zowel (rijks)overheidsorganisaties als private partijen omvatten, wanneer deze aanbieders van vitale producten of diensten zijn. Het begrip vitale aanbieder is, tenzij uit de context anders volgt, niet beperkt tot vitale aanbieders die onder de meldplicht vallen.

2. Meldplicht

2.1. Inleiding

Doel van de in dit wetsvoorstel vervatte meldplicht voor vitale aanbieders aan het NCSC is tweeledig. Een melding van een ernstige ICT-inbreuk bij een vitale aanbieder aan het NCSC is enerzijds bedoeld om tijdig te kunnen inschatten hoe groot de impact en daarmee de potentiële maatschappelijke ontwrichting van een ICT-inbreuk is. Anderzijds stelt de melding het NCSC in staat om hulp aan de getroffen organisatie te verlenen en om te anticiperen op de mogelijk bredere effecten van een dergelijke inbreuk, met name ook door andere vitale organisaties te waarschuwen en te adviseren. De hulp door het NCSC aan de getroffen organisatie behelst het bieden van handelingsperspectief door het geven van advies en informatie en waar noodzakelijk het bieden van technische ondersteuning om de gevolgen van een ICT-inbreuk te beperken en een volgende ICT-inbreuk te voorkomen.

Belangrijk bij de in dit wetsvoorstel vervatte meldplicht is ook dat deze een cultuur tracht te realiseren waarin het gezamenlijk bijdragen aan veiligheid centraal staat. In de luchtvaartsector bestaat bijvoorbeeld ruime ervaring met deze praktijk onder de noemer van het werken aan een *just culture*. Om een dergelijke cultuur te bevorderen is het bij het doen van de melding van belang dat deze in vertrouwen gedaan kan worden om kwetsbaarheden te beperken dan wel in de toekomst te vermijden. De meldplicht past qua karakter daarbij in het bredere kader van privaat-publieke samenwerking met betrekking tot het realiseren van cybersecurity binnen de overheid en de vitale sectoren zoals uiteengezet in de tweede Nationale Cyber Security Strategie.

Om het NCSC een ondersteunende rol te laten vervullen bij het voorkomen en beperken van onderbrekingen van de beschikbaarheid of betrouwbaarheid van voor de samenleving vitale diensten en producten én te zorgen voor een veiligheidscultuur waarbij meldingen gedaan worden om daar lering uit te trekken, is het voorts van belang om de drempel om meldingen te doen zo laag mogelijk te maken. Mede in verband hiermee stel ik voor om het NCSC niet te belasten met de handhaving van de meldplicht (toezicht en sancties, zie ook de paragrafen 2.7 en 2.9). De meldplicht is primair gericht op het bieden van hulp. Het NCSC kan daarbij functioneren als informatieknooppunt om partijen te informeren en te adviseren over de te ondernemen acties. Het NCSC kan daarbij putten uit een omvangrijk nationaal en internationaal netwerk van o.a. publieke en private Computer Emergency Response Teams (computercrisisteams, CERT's). Binnen de CERT's is veel kennis beschikbaar over de wijze van omgaan met en het leveren van response bij ICT-inbreuken.

2.2. Inhoud van de melding

Met het oog op het bijstaan van vitale aanbieders bij het treffen van maatregelen, het informeren en adviseren van vitale aanbieders en anderen in en buiten Nederland over dreigingen en incidenten en het verrichten van onderzoek ten behoeve van de hiervoor genoemde taken naar dreigingen en incidenten met betrekking tot informatiesystemen, is het van belang dat de melding aan het NCSC bestaat uit voldoende informatie. Om het NCSC daadwerkelijk invulling aan deze taken te laten kunnen geven en uit dien hoofde een inschatting te kunnen laten maken van de risico's van een inbreuk en de in verband daarmee benodigde maatregelen, is het van belang dat de melding, hoewel deze qua aard per vitale sector verschilt, in elk geval bestaat uit een aantal elementen.

Ten eerste dient de melding inzicht te geven in de aard en omvang van de ICT-inbreuk. Op basis van deze informatie kan onder meer gericht in het nationale en internationale netwerk gezocht worden naar relevante informatie en kennis die voor de getroffen partij van belang is. Een specificatie van het soort getroffen systemen is in dit verband bijvoorbeeld van belang. Ten tweede dient, wanneer bekend, bij de melding aangegeven te worden wat het tijdstip van aanvang van de betrokken ICT-inbreuk is. Ten derde dient de melding, voor zover aan de orde, in te gaan op de reeds getroffen of te nemen maatregelen, zodat mede op basis daarvan geadviseerd kan worden over de eventuele nog te treffen aanvullende maatregelen. Ook is het van belang dat de melding ingaat op de te verwachten hersteltijd én dat de melding contactgegevens van de betrokken partij bevat, zodat desgewenst in nader contact kan worden getreden in het kader van de hulpverlening. De initiële melding kan beknopt zijn: liever een snelle melding die zo nodig later kan worden aangevuld, dan een uitvoerige melding die daardoor op zich laat wachten. Het voorgestelde artikel 7 biedt de mogelijkheid om ad hoc te bepalen of de inbreuk ernstig genoeg is voor (nadere) betrokkenheid van het NCSC, daar op grond hiervan zo nodig nadere informatie aan het NCSC moet worden verstrekt.

Bij de formulering van het voorgestelde artikel 6 is aansluiting gezocht bij reeds bestaande meldplichten, teneinde de (administratieve) lasten voor vitale aanbieders die moeten voldoen aan meerdere meldplichten zo veel mogelijk te beperken. Zie hierover ook paragraaf 2.5.

2.3. Meldplichtige partijen

Dit wetsvoorstel bevat een meldplicht voor vitale aanbieders, waarbij een ICT-inbreuk direct of indirect (cascade-effect) kan leiden tot maatschappelijke ontwrichting. De vitale aanbieders en hun concrete producten en diensten waarvoor de meldplicht gaat gelden, zullen worden aangewezen bij algemene maatregel van bestuur. In overeenstemming met mijn brief van 6 juli 2012 zal de aanwijzing in ieder geval zien op partijen uit de sectoren: elektriciteit, gas, drinkwater, telecom, financiën, overheid (waaronder in ieder geval keren en beheren oppervlaktewater) en transport (mainports Rotterdam en Schiphol). Te denken valt daarbij aan vitale aanbieders zoals energienetwerkbeheerders, drinkwaterbedrijven, telecombedrijven, beheerders van hoofdwaterkeringen of banken.

Voor certificaatdienstverleners, waartoe in het verleden bijvoorbeeld DigiNotar behoorde, geldt dat de melding van ICT-inbreuken langs andere weg vorm wordt gegeven. Voor certificaatdienstverleners die gekwalificeerde certificaten aanbieden geldt nu reeds de plicht om veiligheidsinbreuken of integriteitsverlies te melden bij toezichthouder ACM en het NCSC. Zie hiervoor ook paragraaf 2.8.

2.4. Te melden ICT-inbreuken

De meldplicht in dit wetsvoorstel ziet alleen op een daadwerkelijke inbreuk op de veiligheid of een daadwerkelijk verlies van integriteit van een elektronisch informatiesysteem. Van een inbreuk op de veiligheid kan bijvoorbeeld worden gesproken in het geval een niet-geautoriseerd persoon zich ongeoorloofd toegang heeft verschaft, of zelfs onopzettelijk toegang heeft verkregen, tot het computersysteem of netwerk van de vitale aanbieder. Van een verlies van integriteit kan bijvoorbeeld worden gesproken wanneer een derde in staat is geweest om, ongeoorloofd, informatie die een belangrijke rol speelt in een vitale dienst of een vitaal product toe te voegen, aan te passen of te verwijderen.

De aan te wijzen organisaties in de vitale sectoren zijn niet verplicht om elke ICT-inbreuk aan het NCSC te melden. De verplichting tot melden geldt alleen als de inbreuk tot gevolg heeft of kan hebben dat de beschikbaarheid of betrouwbaarheid van het aangewezen product of de aangewezen dienst in belangrijke mate wordt of kan worden onderbroken. Dit zou namelijk kunnen leiden tot maatschappelijke ontwrichting. In

overleg met de betrokken sectoren en departementen zal nader worden uitgewerkt wat voor de verschillende betrokken producten en diensten moet worden verstaan onder "in belangrijke mate", zo mogelijk in de vorm van meetbare drempelwaarden. Daarbij zal mede bepalend zijn onder welke omstandigheden sprake is of kan zijn van maatschappelijke ontwrichting. Deze criteria kunnen bijvoorbeeld worden vastgelegd in beleidsregels.

De in dit wetsvoorstel geïntroduceerde meldplicht ziet niet op verstoringen waarbij geen sprake is van een daadwerkelijke ICT-inbreuk, zoals DDoS-aanvallen (Distributed Denial of Service). Het is wenselijk om de meldplicht te beperken tot (potentieel) ontwrichtende situaties waarbij rechtstreekse betrokkenheid van het NCSC voldoende meerwaarde heeft. Dit is niet het geval bij een DDoS-aanval, gezien het relatief eenvoudige karakter daarvan. Bij een DDoS-aanval wordt de bereikbaarheid van een online-dienst aangetast zonder aantasting van de systemen die in dat verband worden gebruikt. Veelal zal het bij deze aanvallen om een tijdelijke beperking van de bereikbaarheid gaan. Hierdoor is de maatschappelijk ontwrichtende werking in deze gevallen in het algemeen veel beperkter dan in geval van daadwerkelijke ICT-inbreuken. Een en ander laat overigens onverlet dat partijen de mogelijkheid hebben om ook deze verstoringen van de bereikbaarheid op basis van vrijwilligheid aan het NCSC te melden.

2.5. Verhouding tot sectorale meldplichten

Voor enkele sectoren geldt thans voor ICT-inbreuken al een verplichting tot melding aan de sectorale toezichthouder. Een voorbeeld hiervan is de plicht voor vitale aanbieders van openbare elektronische communicatienetwerken en -diensten om een inbreuk op de veiligheid en een verlies van integriteit te melden aan de Minister van Economische Zaken bij het Agentschap Telecom op grond van artikel 11a.2 van de Telecommunicatiewet, als door die inbreuk of dat verlies de continuïteit van het netwerk of de dienst in belangrijke mate werd onderbroken.

Gegeven het karakter van de meldplicht aan het NCSC, waarbij het doel van de melding ligt in het mogelijk maken van hulpverlening aan getroffen vitale aanbieders en het op die wijze voorkomen of beperken van maatschappelijke ontwrichting ten gevolge van de ICT-inbreuk, verschilt de aard en strekking van de meldplicht aan het NCSC wezenlijk van de aard en strekking van meldplichten aan toezichthouders, waarbij immers de naleving van wettelijke zorgplichten of veiligheidseisen centraal staat. Ook als een vitale aanbieder een ICT-inbreuk op basis van andere wetgeving reeds moet melden bij een ander overheidsorgaan, is het cruciaal dat het bedrijf de inbreuk óók onverwijld en rechtstreeks aan het NCSC meldt, om vertraging in het daar waar nodig bieden van hulp zo veel mogelijk te beperken en om het delen van informatie over de kwetsbaarheid met andere mogelijk getroffenen te bespoedigen. Bovendien heb ik als coördinerend bewindspersoon voor cybersecurity een eigen verantwoordelijkheid om de digitale weerbaarheid van de Nederlandse samenleving te versterken en maatschappelijke ontwrichting door het uitvallen van vitale systemen te voorkomen, zonder filtering (eigen beoordeling) door een toezichthouder.

Een toename van de administratieve lasten voor genoemde vitale aanbieders, die zowel op basis van huidige wetgeving als op grond van dit wetsvoorstel tot melding verplicht zullen zijn, zal zo veel mogelijk worden voorkomen door de meldplicht te beperken tot ICT-inbreuken die een serieuze bedreiging voor de Nederlandse samenleving inhouden, door stroomlijning van de wijze van melden en van de gegevens die daarbij verstrekt moeten worden, door maatwerk en door efficiënte inrichting van processen. Om dat laatste mogelijk te maken, verplicht het voorgestelde artikel 7 de vitale aanbieder die een inbreuk heeft gemeld, om desgevraagd nadere gegevens te verstrekken die nodig zijn om de risico's in te schatten en de vitale aanbieder bij te staan. Dankzij die bepaling kan de initiële melding beknopt zijn (liever een snelle melding die zo nodig later kan worden aangevuld, dan een uitvoerige melding die daardoor op zich laat wachten), en

wordt ad hoc bepaald of de inbreuk ernstig genoeg is voor (nadere) betrokkenheid van het NCSC (zie ook paragraaf 2.2). Daarnaast zal, waar mogelijk en wanneer de betrokken vitale aanbieder hier toestemming voor geeft, overleg plaatsvinden met toezichthouders om adviezen van het NCSC en aanwijzingen of ander handhavend optreden van de toezichthouder zo veel als mogelijk op elkaar af te stemmen.

Het voorgaande sluit niet uit dat een vitale aanbieder in een concreet geval kan worden geconfronteerd met een aanwijzing van een toezichthouder die tegenstrijdig is aan het advies van het NCSC, bijvoorbeeld omdat in een concreet geval onvoldoende tijd beschikbaar staat voor onderling overleg of omdat de betrokken vitale aanbieder voor dat overleg geen toestemming heeft gegeven. In een dergelijk geval prevaleert het handhavende optreden van de toezichthouder omdat het NCSC geen toezichthoudende rol vervult, zie paragraaf 2.1. In dit geval kan de vitale aanbieder volstaan met een mededeling aan het NCSC van het besluit van de toezichthouder. De voorgestelde meldplicht sluit hiermee aan op het bestaande stelsel van sectorale meldplichten en treedt niet in de thans geldende sectorale bevoegdheden. Daarmee laat de voorgestelde meldplicht ook de bestaande crisisbeheersingsstructuren onverlet.

2.6. Verhouding tot wetsvoorstel meldplicht datalekken

Bij het parlement is een wetsvoorstel aanhangig tot wijziging van de Wet bescherming persoonsgegevens (Wbp) en de Telecommunicatiewet in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens ('meldplicht datalekken'). De in dat wetsvoorstel bedoelde melding moet worden gedaan aan het College bescherming persoonsgegevens (Cbp). Die melding ziet op inbreuken op de in de Wbp voorgeschreven beveiliging van persoonsgegevens tegen verlies en onrechtmatige verwerking (artikel 13 Wbp). Een vergelijkbare meldplicht voor inbreuken op de beveiliging van persoonsgegevens is reeds opgenomen in artikel 11.3a van de Telecommunicatiewet.

Bij een inbreuk op de veiligheid of een verlies van integriteit waarop het onderhavige wetsvoorstel ziet, is er weliswaar sprake van een inbreuk op de beveiliging van een informatiesysteem van een organisatie, maar daarbij hoeven niet noodzakelijkerwijs ook persoonsgegevens in het geding te zijn, bijvoorbeeld als het elektronisch informatiesysteem een fysiek proces aanstuurt. De meldplicht in dit wetsvoorstel heeft daarmee een bredere reikwijdte dan de voorgestelde meldplicht op grond van de Wbp. Wanneer echter óók persoonsgegevens in het geding zijn door de ICT-inbreuk, zal de vitale aanbieder de inbreuk zowel bij het NCSC als bij het Cbp moeten melden. Ook hiervoor geldt dat nodeloze administratieve lasten zullen worden voorkomen door middel van onderlinge afstemming van de wijze waarop moet worden gemeld en van de gegevens die dienen te worden verstrekt en door processen efficiënt in te richten.

2.7. Verhouding tot EU-richtlijn netwerk- en informatiebeveiliging

In februari 2013 publiceerde de Europese Commissie een Europese Cyber Security Strategie en een voorstel voor een EU-richtlijn over netwerk- en informatiebeveiliging (NIB-richtlijn). De Europese onderhandelingen over deze richtlijn zijn gaande. De richtlijn strekt tot geven van een impuls aan het waarborgen van een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging. De Europese Commissie wil de beveiliging van het internet en de particuliere netwerken en informatiesystemen verbeteren door de lidstaten ertoe te verplichten hun paraatheid te verbeteren, beter met elkaar samen te werken en door vitale partijen te verplichten adequate beveiligingsmaatregelen te nemen en ernstige incidenten aan de nationale bevoegde autoriteiten te rapporteren. Voorts introduceert de NIB-richtlijn een stelsel van toezicht en handhaving op deze zorgplichten en meldplicht.
Bij de onderhandelingen wordt er door Nederland op gelet dat de richtlijn voldoende ruimte laat voor het kunnen aanwijzen van, met verschillende deeltaken belaste

bevoegde autoriteiten op nationaal niveau, de gewenste mate van operationele samenwerking, alsmede een toepassingsbereik tot overheids- en marktpartijen dat met dit wetsvoorstel wordt beoogd.
Hoewel de onderhandelingen nog gaande zijn en de uiteindelijke tekst van de richtlijn zich op dit moment niet laat voorspellen, kan niet worden uitgesloten dat de Nederlandse meldplicht te zijner tijd op onderdelen zal moeten worden aangepast en aangevuld. Wat dat laatste betreft valt bijvoorbeeld te denken aan het stellen van beveiligingseisen aan informatiesystemen en aan de handhaving van die eisen en van de meldplicht. In lijn met mijn brief van 6 juli 2012 zullen die onderwerpen worden geregeld in sectorale wetten. Een en ander is geen reden om de invoering van de Nederlandse meldplicht uit te stellen. De samenleving wordt steeds afhankelijker van elektronische informatiesystemen, die bovendien onderling verweven zijn. Om cascade-effecten te voorkomen is het cruciaal dat vitale aanbieders het NCSC tijdig op de hoogte stellen van ernstige ICT-inbreuken. Het belang van de meldplicht voor de Nederlandse samenleving rechtvaardigt derhalve om niet te wachten op de Europese besluitvorming. Dit volgt ook uit de aanvaarding door de Tweede Kamer, eind 2011, van de motie-Hennis-Plasschaert c.s., die de concrete aanleiding voor het opstellen van dit wetsvoorstel vormt.
Uiteraard zal Nederland zich houden aan zijn Europeesrechtelijke verplichtingen, waaronder de tijdige implementatie van de NIB-richtlijn en het verbod om tijdens de implementatietermijn nationale maatregelen vast te stellen die afwijken van het met de richtlijn beoogde resultaat.

2.8 Verhouding tot EU-Verordening elektronische identificatie en vertrouwensdiensten voor elektronische transacties

Voor certificaatdienstverleners en vitale aanbieders van niet gekwalificeerde vertrouwensdiensten, waartoe in het verleden bijvoorbeeld DigiNotar behoorde, geldt dat de melding van ICT-inbreuken langs andere weg vorm wordt gegeven.

Voor gekwalificeerde certificaatdienstverleners geldt op dit moment al een meldplicht op grond van het Besluit elektronische handtekeningen (artikel 2, eerste lid, onder t). Voor zowel gekwalificeerde als niet-gekwalificeerde certificaatdienstverleners treedt op 1 juli 2016 de EU-verordening over elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt in werking. De verordening bevat onder meer een - rechtstreeks werkende - plicht tot melding van inbreuken op de veiligheid van elektronische vertrouwensdiensten (artikel 19, tweede lid) aan de toezichthouder en, waar passend, andere relevante organen zoals het bevoegde nationale orgaan voor informatieveiligheid of de gegevensbeschermingsautoriteit. Veiligheidsinbreuken in de systemen van dienstverleners van gekwalificeerde certificaten en niet gekwalificeerde vertrouwensdiensten zullen gemeld moeten worden bij zowel de (sectorale) toezichthouder als het NCSC.

Een toename van de administratieve lasten voor genoemde dienstverleners zal zo veel mogelijk worden voorkomen, door de wijze waarop moet worden gemeld en de gegevens die dienen te worden verstrekt aan de te onderscheiden instanties waarbij gemeld wordt, waar mogelijk op elkaar af te stemmen en processen efficiënt in te richten, waarbij er naast het NCSC niet een ander orgaan zal worden aangemerkt als nationaal orgaan voor informatieveiligheid zoals bedoeld in de verordening.

2.9. Naleving

Zoals ik in paragraaf 2.1 al heb opgemerkt, stel ik voor om het NCSC niet te belasten met de handhaving van de meldplicht (toezicht en sancties). Mede vanwege de aansluiting bij de bestaande publiek-private samenwerking verwacht ik dat de meldplicht goed wordt nageleefd. De doelgroep is beperkt tot vitale aanbieders. Het nut en de noodzaak van het delen van vertrouwelijke gegevens met betrekking tot ICT-inbreuken die ernstige gevolgen hebben of kunnen krijgen, wordt binnen die doelgroep breed

gedragen. Voornoemde partijen zijn zich bewust van hun verantwoordelijkheid. Met de voorgestelde inrichting van de meldplicht die in samenwerking met de betrokken vitale aanbieders nader gestalte wordt gegeven, worden gunstige voorwaarden geschapen voor spontane naleving. Tegenover de bescheiden kosten van melding voor de betrokken organisaties staan hoge baten in de vorm van schadebeperking en probleemoplossing. Gegevens die ter uitvoering van de meldplicht worden verstrekt, worden door het NCSC zo vertrouwelijk mogelijk behandeld teneinde onder meer schade aan reputatie of concurrentiepositie van de getroffen vitale aanbieder zo veel als mogelijk te voorkomen, zie artikel 9.

In uitzonderlijke gevallen kan ik, wanneer mocht blijken dat een getroffen organisatie op grond van het door het NCSC verstrekte advies geen of onvoldoende maatregelen treft om (verdere) verstoring van de betrouwbaarheid of beschikbaarheid van de getroffen producten of diensten te voorkomen, onder meezending van het advies van het NCSC, het voor de betreffende sector verantwoordelijke ministerie, met het oog op diens wettelijke verantwoordelijkheid daarvan op de hoogte stellen, teneinde deze in staat te stellen daar waar nodig passend invulling te geven aan de sectorale verantwoordelijkheid van het betrokken vakdepartement. Zie in dit verband ook artikel 9.

In paragraaf 2.7 besprak ik al dat de concept-NIB-richtlijn verplicht tot handhaving van de meldplicht (toezicht en sancties). Dat betekent dat als de definitieve richtlijn in dit opzicht ongewijzigd blijft, bij de implementatie ervan alsnog zal worden voorzien in de handhaving van de meldplicht, waarbij de bevoegdheid zal komen te liggen bij sectorale toezichthouders.

3. Wettelijke grondslag voor taken en gegevensverwerking NCSC

Het NCSC ontwikkelt zich door zijn rol als nationaal kennis- en expertisecentrum op het gebied van digitale veiligheid steeds verder tot kennis-knooppunt over en centraal meldpunt voor cyberincidenten. Het NCSC groeit gestaag door van nationale CERT tot Nationaal Cybersecurity Operations Centre (NCSOC). Ontwikkelingen zoals de facilitering van Information Sharing and Analysis Centres (ISAC's) en de opzet van een nationaal responsnetwerk laten zien dat het NCSC een steeds belangrijkere rol speelt in het bevorderen van de vitale digitale infrastructuren in Nederland.

Bij de uitvoering van zijn taken verwerkt het NCSC een veelheid aan gegevens, waaronder ook persoonsgegevens. Bij de verwerking van persoonsgegevens gaat het daarbij, met het oog op de algemene taak van het NCSC om de veiligheid en integriteit van informatiesystemen van vitale aanbieders te bevorderen, om een beperkt aantal categorieën persoonsgegevens, meer in het bijzonder de bij een incident of dreiging betrokken IP-adressen, e-mailadressen en domeinnamen, alsook contactgegevens van overheids- en vitale private partijen. Op de verwerking van genoemde persoonsgegevens door het NCSC is de Wet bescherming persoonsgegevens (Wbp) van toepassing. De Wbp vereist voor iedere verwerking van persoonsgegevens dat deze kan worden gebaseerd op een van de grondslagen van artikel 8 Wbp. Zoals ik in de brief van 12 december 2013 heb uiteengezet is het wenselijk om de wettelijke grondslag voor gegevensverwerking door het NCSC, gelet op het groeiend belang en de ontwikkeling van het NCSC, te verstevigen.

Ten behoeve van die versteviging voorziet dit wetsvoorstel in een vastlegging van de NCSC-taken in het kader waarvan verwerking van persoonsgegevens geschiedt (zoals de analyse ten behoeve van advisering en ondersteuning bij incidenten of dreigingen, zie hierna), alsook in samenhang hiermee in een steviger wettelijke grondslag voor de bevoegdheid tot die verwerking (artikelen 2 en 3). Voorts voorziet dit wetsvoorstel volledigheidshalve met het oog op dezelfde taken ook in een concrete wettelijke basis voor het verwerken van andere gegevens (bijvoorbeeld over 'malware' (kwaadaardige software) of kwetsbaarheden, eveneens in de artikelen 2 en 3). Ook voorziet dit

wetsvoorstel in een wettelijke grondslag om bijvoorbeeld bij andere publiekrechtelijke organisaties de voor bovengenoemde taakuitoefening benodigde gegevens te vragen en in de mogelijkheid van die derden om in reactie daarop zo nodig ook persoonsgegevens te verstrekken aan het NCSC (artikel 4). Ten slotte regelt dit wetsvoorstel de voorwaarden waaronder vertrouwelijke gegevens, die bij het NCSC berusten, verstrekt mogen worden aan derden (artikel 9).

De taak van het NCSC om de veiligheid en integriteit van elektronische informatiesystemen te bevorderen, waarbij het NCSC zich richt op vitale aanbieders, valt uiteen in verschillende deeltaken waarbij onder meer persoonsgegevens worden verwerkt. Het gaat hierbij allereerst om het bijstaan van vitale aanbieders van producten of diensten bij het treffen van maatregelen om de beschikbaarheid en betrouwbaarheid van die producten of diensten te waarborgen of te herstellen én om het informeren en adviseren van diezelfde aanbieders en anderen in en buiten Nederland over dreigingen en incidenten met betrekking tot informatiesystemen van die aanbieders (artikel 2, eerste lid, onder a en b). Daarnaast heeft het NCSC als taak om onderzoek te doen naar dreigingen en incidenten met betrekking tot vitale informatiesystemen (artikel 2, eerste lid, onder c). Daarbij gaat het met name om het verrichten van analyses op basis van aan het NCSC verstrekte gegevens, teneinde de aard en ernst van dreigingen en incidenten in relatie tot vitale aanbieders te kunnen bepalen en op basis daarvan die aanbieders te kunnen waarschuwen en adviseren. Ook worden technische activiteiten verricht die nodig zijn om die analyses te kunnen verrichten. Denk hierbij bijvoorbeeld aan de situatie waarin het NCSC een gegevensdrager met mogelijk relevante gegevens over dreigingen en incidenten krijgt aangeleverd en zich eerst in technische zin toegang moet zien te verschaffen tot de inhoud daarvan alvorens een analyse daarop te kunnen verrichten. Onderzoek door het NCSC geschiedt in hoofdzaak op basis van gegevens die anderen, zoals vitale aanbieders die incidenten melden of computercrisisteams in andere landen, aan het NCSC verstrekken.
Wel voorziet het wetsvoorstel nog in de mogelijkheid om bij andere organisaties ook zelf informatie op te vragen, zonder dat daarvoor overigens een medewerkingsplicht voor de aangezochte organisatie geldt (artikel 4). Daarbij kan het bijvoorbeeld gaan om de kenmerken van een digitale aanval, om een voorbeeld van aangetroffen malware, om gegevens over de interne verspreiding van malware en om de IP-adressen die daarbij betrokken zijn. Met dergelijke gegevens kan een dreiging of incident worden geanalyseerd en kan aan organisaties advies worden gegeven over beveiliging tegen digitale aanvallen. Overige activiteiten tot actieve verwerving van voor analyse bestemde gegevens worden niet door het NCSC verricht.
Onderzoek naar dreigingen en incidenten met betrekking tot vitale elektronische informatiesystemen behoort alleen tot de NCSC-taken als het in dienst staat van de NCSC-taken om bijstand te verlenen of te informeren en adviseren. Ook is vastgelegd dat het geen NCSC-taak is 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 en, bij mogelijke strafbare feiten, aan het openbaar ministerie.

Bij het onderzoek naar dreigingen en incidenten met betrekking tot vitale informatiesystemen kunnen ook gegevens aan het licht komen over dreigingen of incidenten met betrekking tot andere informatiesystemen. Naar mijn oordeel is het niet gewenst als het NCSC in zo'n geval niet bevoegd zou zijn om dergelijke 'bijvangst', ter voorkoming van nadelige maatschappelijke gevolgen, te delen met een beperkte kring van derden, bestaande uit: organisaties die tot taak hebben om andere organisaties of het publiek over die dreigingen of incidenten te informeren, bij ministeriële regeling aangewezen computercrisisteams, en aanbieders van internettoegangs- of internetcommunicatiediensten ten behoeve van het informeren van gebruikers van die diensten. Het voorgestelde tweede lid van artikel 2, waarin deze gegevensverstrekking als taak is vastgelegd, beoogt het bestaan van die bevoegdheid buiten twijfel te stellen. De gegevens zullen alleen worden verstrekt wanneer de aard of omvang van de

gegevens die het NCSC heeft verkregen hiertoe noodzaakt. Denk bijvoorbeeld aan grote hoeveelheden e-mailadressen die door een ICT-inbreuk kwetsbaar zijn geworden; het NCSC kan in een dergelijk geval bijvoorbeeld de betrokken internetaanbieders waarschuwen, die dan op hun beurt hun klanten kunnen voorlichten.

Het NCSC komt bij de uitoefening van zijn taken niet in het vaarwater van de inlichtingen- en veiligheidsdiensten. Zo zijn, zoals hierboven reeds vermeld, onderzoeken naar personen of organisaties die (als actor) betrokken zijn bij digitale spionage of sabotage en waarbij sprake is van een bedreiging voor de nationale veiligheid, voorbehouden aan de AIVD en de MIVD. De hierboven genoemde NCSC-taken worden thans reeds door het NCSC, complementair aan die van genoemde diensten, vervuld en worden met dit wetsvoorstel slechts van een steviger wettelijke grondslag voorzien. Soms raakt de uitoefening van de NCSC-taken aan die van de inlichtingen- en veiligheidsdiensten. De uitoefening door genoemde organisaties van de taken op het terrein van cybersecurity vult echter elkaar aan, door de verschillende wijzen waarop daaraan invulling wordt gegeven en verantwoordelijkheden waarop de nadruk wordt gelegd. Zo ligt de nadruk bij de werkzaamheden van het NCSC bijvoorbeeld op het adviseren van de rijksoverheid en vitale private organisaties in geval van concrete incidenten of generieke kwetsbaarheden met betrekking tot hun informatiesystemen teneinde op die wijze maatschappelijke ontwrichting te voorkomen. Voor de AIVD ligt bij de werkzaamheden de nadruk bijvoorbeeld op de bevordering van maatregelen ter beveiliging van gegevens waarvan geheimhouding door de nationale veiligheid wordt geboden en van de voor het maatschappelijk leven vitale onderdelen van de overheid en het bedrijfsleven. Voor de MIVD ligt de nadruk op de taak, genoemd in artikel 7, tweede lid, onder d, van de Wet op de inlichtingen- en veiligheidsdiensten 2002, waaronder het bevorderen van maatregelen ter beveiliging van gegevens betreffende de krijgsmacht waarvan geheimhouding is geboden. Door samenwerking tussen het NCSC en de inlichtingen- en veiligheidsdiensten wordt ieders taakuitoefening juist ook versterkt: zo kunnen zich situaties voordoen waarbij de uitoefening van de (wettelijke) taken van enerzijds inlichtingen- en veiligheidsdiensten en anderzijds het NCSC complementair aan elkaar is. Hierbij kan gedacht worden aan het binnen de daarvoor geldende wettelijke kaders delen van informatie ten aanzien van specifieke cybersecurity-thema's (bijvoorbeeld geavanceerde malware) die van belang is voor ieders taakuitvoering.

4. Verstrekking van vertrouwelijke gegevens

Het is om twee redenen van groot belang dat de vertrouwelijkheid van bij het NCSC gemelde of anderszins verkregen gegevens over incidenten en kwetsbaarheden betreffende ICT-systemen zo veel mogelijk gewaarborgd is. Ten eerste is dit van belang om te garanderen dat deze gegevens kunnen worden gebruikt door het NCSC voor het adviseren en anderszins ondersteunen van vitale aanbieders bij incidenten en kwetsbaarheden, en het doen van onderzoek daartoe, teneinde, in goed overleg met die aanbieders, incidenten te verhelpen en risico's te beperken en zo maatschappelijke ontwrichting te voorkomen, zonder daarbij gehinderd te worden door mogelijk vroegtijdig openbaar worden van deze gegevens. Ten tweede is het van belang om schade bij betrokken aanbieders, zoals reputatieschade, benadeling van de concurrentiepositie en toegenomen kwetsbaarheid voor gerichte aanvallen, zo veel mogelijk te voorkomen of te beperken. Wanneer aanbieders terughoudend worden met het delen van vertrouwelijke informatie met het NCSC, benadeelt dat het NCSC in ernstige mate in het goed kunnen uitvoeren van zijn bovenvermelde taken in het belang van de nationale veiligheid. Voor het NCSC, waaraan geen taken betreffende toezicht of handhaving zijn toebedeeld, is het zonder deling van gegevens door vitale aanbieders over incidenten en kwetsbaarheden, zeker ook als het meldingen betreft die onverplicht zijn, immers niet goed mogelijk om de rol van kennis- en expertisecentrum te vervullen en vanuit die rol onder meer te adviseren en hulp te verlenen bij het verhelpen van incidenten of kwetsbaarheden en zo met name ook de uitval van de beschikbaarheid of betrouwbaarheid van voor de samenleving vitale producten en diensten te voorkomen of te beperken.

Vanwege het bovenstaande bevat het voorgestelde artikel 9 een strikte regeling over het verstrekken van vertrouwelijke gegevens door het NCSC aan derden. Dergelijke gegevens worden slechts aan derden verstrekt (behoudens verplichtingen tot verstrekking uit hoofde van andere wetten), als aldaar de geheimhouding van de gegevens in voldoende mate is gewaarborgd en voldoende gewaarborgd is dat de gegevens uitsluitend worden gebruikt voor het doel waarvoor zij worden verstrekt. Voor de verstrekking van vertrouwelijke gegevens die bovendien herleid kunnen worden tot een afzonderlijke aanbieder (naam van de aanbieder, etc.) bevat artikel 9 een bijzondere openbaarheidsregeling, die in de plaats treedt van de Wet openbaarheid van bestuur (Wob). Dergelijke gegevens kunnen slechts worden verstrekt aan de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en aan daartoe bij ministeriële regeling aangewezen computercrisisteams (CERT's), voor zover dat dienstig is voor het bevorderen van maatregelen ter voorkoming of beperking van een verstoring van het maatschappelijk verkeer, of aan andere ministers, indien een vitale aanbieder onvoldoende gevolg geeft aan een advies van het NCSC (zie artikel 9, tweede en derde lid). Aan andere dan de hiervoor genoemde organisaties of aan het publiek mogen dergelijke gegevens slechts worden verstrekt voor zover dat noodzakelijk is om ernstige maatschappelijke gevolgen te voorkomen of te beperken (artikel 9, vierde lid). In veel gevallen zal volstaan kunnen worden met niet-herleidbare mededelingen, bijvoorbeeld als het publiek moet worden gewaarschuwd voor de risico's van een door internetcriminelen gehanteerde werkwijze. Soms echter zal de voorlichting alleen effectief kunnen zijn als de vitale aanbieder of het product of de dienst concreet wordt aangeduid, bijvoorbeeld als het nodig is om het publiek te waarschuwen dat er grote risico's verbonden zijn aan het gebruik van een bepaald product of een bepaalde dienst. De beslissing om dergelijke voorlichting te geven, vergt een belangenafweging. Zo zal het belang van het publiek om op de hoogte te zijn niet altijd opwegen tegen het belang van de betrokken vitale aanbieder. Denkbaar is ook dat de bekendmaking de maatschappelijke schade juist veroorzaakt of vergroot in plaats van voorkomt of beperkt. Vandaar mijn voorstel om hiervoor een streng criterium te hanteren: "voor zover dat noodzakelijk is om ernstige maatschappelijke gevolgen te voorkomen of beperken". Bij "ernstige maatschappelijke gevolgen" moet worden gedacht aan ontwrichting van de Nederlandse samenleving. Het NCSC zal zo mogelijk (dat wil zeggen: tenzij wachten onverantwoord is) de betrokken vitale aanbieder en toezichthouder(s) betrekken bij deze belangenafweging en bij de vorm en inhoud van de concrete publieksmededeling.

Verstrekking van herleidbare gegevens aan andere organisaties dan genoemd in artikel 9, tweede en derde lid, geschiedt niet dan na raadpleging van de betrokken aanbieder.

Daarnaast ben ik echter ook van mening dat openheid en transparantie van beleid bij overheidsorganisaties ook in het geval van NCSC zo veel als mogelijk gewaarborgd moeten zijn. Ten aanzien van bij het NCSC berustende gegevens die niet vertrouwelijk zijn, hecht ik daarom bijvoorbeeld aan periodieke publieksmededelingen door het NCSC over bijvoorbeeld voor sectoren geldende aantallen meldingen en typen incidenten. Dergelijke mededelingen beogen de samenleving een beeld te geven van digitale dreigingen en de digitale veiligheid te bevorderen.

Het voorgestelde artikel 9 ziet op alle vertrouwelijke gegevens waarover het NCSC beschikt, en dus niet alleen op vertrouwelijke gegevens die het NCSC heeft verkregen uit verplichte meldingen, maar ook op dergelijke gegevens die zijn verkregen door onverplichte meldingen, eigen onderzoek of mededelingen van derden.

Met bovenstaande regeling wordt naar mijn oordeel voorzien in een goede balans tussen enerzijds het waar nodig ten behoeve van de taakuitoefening van het NCSC, alsook met het oog op belangen van betrokken aanbieders, waarborgen van de vertrouwelijkheid van bij het NCSC berustende informatie over incidenten en kwetsbaarheden, en

anderzijds het met inachtneming daarvan zo veel als mogelijk kunnen blijven informeren van onder meer het publiek over die incidenten en kwetsbaarheden.

5. Totstandkoming van dit wetsvoorstel

5.1. Inleiding
Eerdere versies van dit wetsvoorstel zijn twee keer opengesteld voor consultatie op www.internetconsultatie.nl en voor commentaar toegezonden aan belangenorganisaties, vitale aanbieders en toezichthoudende diensten. Gekozen is voor twee consultatierondes omdat het wetsvoorstel bij de eerste consultatie alleen regels bevatte over de meldplicht voor ICT-inbreuken en nadien is uitgebreid met regels over het verwerken van gegevens ten behoeve van de NCSC-taken.
5.2. Eerste consultatieronde (meldplicht)
Op het concept voor een 'Wet melding inbreuken elektronische informatiesystemen' is inhoudelijk gereageerd door onder meer VNO-NCW en MKB-Nederland, Nederland ICT, Netbeheer Nederland, Bits of Freedom, Business Communication Providers Alliance (BCPA), Schiphol Group, Vereniging van waterbedrijven in Nederland (Vewin), Nederlandse Vereniging van Banken (NVB), De Nederlandsche Bank (DNB) en Autoriteit Financiële Markten (AFM).
Bespreking van de reacties op hoofdlijnen:
5.2.1. 'Just culture', handhaving en rol NCSC
VNO-NCW, MKB-Nederland en de **NVB** vinden dat een wettelijke meldplicht in strijd is met de in de toelichting gepropageerde *just culture:* een veiligheidscultuur waarin het leren van incidenten vooropstaat. Zij en ook **Nederland ICT** wijzen op het gevaar dat een wettelijke meldplicht het NCSC een meer toezichthoudende rol geeft, waardoor de huidige samenwerking tussen bedrijven onderling en met de overheid, waarbij informeel en op basis van vertrouwen veel kennis wordt gedeeld om risico's en inbreuken beter te kunnen inschatten en daarnaar te handelen, negatief wordt beïnvloed. Als niettemin gekozen wordt voor een wettelijke meldplicht, dan pleit de **NVB** voor een getrapte melding via de sectorale toezichthouder.
Bits of Freedom vindt een wettelijke meldplicht juist belangrijk voor het creëren van een *just culture*, en mist in dat kader waarborgen voor naleving van de meldplicht, zoals de aanwijzing van een organisatie die gaat toezien op de naleving en de mogelijkheid van sancties bij niet-melden.
DNB en AFM merken op, reagerend op het ontbreken van sancties, dat zij het niet hun taak achten om een financiële onderneming in een crisissituatie erop te wijzen dat zij een inbreuk (ook) aan het NCSC moet melden, noch om het NCSC namens een financiële onderneming in een crisissituatie zelf te betrekken.
Vewin constateert dat drinkwaterbedrijven met dit wetsvoorstel een dubbele meldplicht krijgen: aan het NCSC en (op grond van de Drinkwaterwet) aan de sectorale toezichthouder, de Inspectie voor Leefomgeving en Transport (ILT). Vewin vindt dat melden en toezicht onlosmakelijk verbonden zijn en in één hand moeten (blijven) liggen. Zij wijst erop dat melding rechtstreeks aan het NCSC niet in lijn is met mijn brief van 6 juli 2012 aan de Tweede Kamer, waarin staat: "Zoveel mogelijk zal worden aangesloten bij bestaande meldplichten waardoor organisaties slechts op één plek hoeven te melden en administratieve lasten worden beperkt." Vewin pleit ervoor om de melding via de ILT te laten lopen, die de inbreuk na overleg met het drinkwaterbedrijf zo nodig doorgeeft aan het NCSC. Vewin wil ook niet dat het NCSC een eigen interventiebevoegdheid krijgt.
De bestaande meldplicht voor 'voorvallen' in de luchtvaart (artikel 7.1 Wet luchtvaart (Wlv)) laat zien dat een wettelijke meldplicht goed te verenigen is met het nastreven van een *just culture,* mits de vertrouwelijkheid van de melding wordt beschermd en de mogelijkheid van het opleggen van sancties naar aanleiding van een gedane melding wordt beperkt. Eerder in deze memorie heb ik uitgelegd waarom ik voorstel om het NCSC niet te belasten met de handhaving van de meldplicht (toezicht en sancties). Daar heb ik ook aangekondigd dat als ook de definitieve NIB-richtlijn verplicht tot handhaving van de meldplicht, de bevoegdheid daartoe bij de implementatie van de richtlijn zal worden

opgenomen in sectorale wetten en zal worden toegekend aan sectorale toezichthouders. Wel heb ik als coördinerend bewindspersoon voor cybersecurity een eigen verantwoordelijkheid om de digitale weerbaarheid van de Nederlandse samenleving te versterken en maatschappelijke ontwrichting door het uitvallen van vitale systemen te voorkomen. Daarom vind ik het belangrijk dat de betrokken vitale aanbieders hun ICT-inbreuken rechtstreeks melden bij het NCSC, zonder filtering (eigen beoordeling) door een toezichthouder en het risico van tijdverlies bij getrapt melden. Wel heb ik mede naar aanleiding van de hier besproken consultatiereacties (en de in paragraaf 5.2.5 besproken reacties) het wetsvoorstel op enkele punten aangepast (zie ook paragraaf 4. Verstrekking van vertrouwelijke gegevens):

1. ter uitvoering van de NCSC-taken worden aan derden geen vertrouwelijke gegevens verstrekt als de geheimhouding van de gegevens onvoldoende is gewaarborgd of onvoldoende is gewaarborgd dat de gegevens uitsluitend worden gebruikt voor het doel waarvoor zij worden verstrekt (artikel 9, eerste lid);
2. een vrij ruime bevoegdheid om vertrouwelijke herleidbare gegevens te verstrekken aan de Nederlandse inlichtingendiensten en aan aangewezen CERT's (artikel 9, tweede lid);
3. een expliciete bevoegdheid om een NCSC-advies inclusief vertrouwelijke herleidbare gegevens te verstrekken aan de eerstverantwoordelijke bewindspersoon als de vitale aanbieder onvoldoende gevolg geeft aan het advies (artikel 9, derde lid);
4. een zeer beperkte bevoegdheid om vertrouwelijke herleidbare gegevens te verstrekken in andere gevallen, zoals het informeren van verzelfstandigde sectorale toezichthouders (zoals DNB en AFM) of van het publiek (artikel 9, vierde lid)
5. een expliciete afwijking van de Wob voor wat betreft vertrouwelijke gegevens die herleid kunnen worden tot een afzonderlijke aanbieder (artikel 9, zesde lid).

5.2.2. Reikwijdte van de meldplicht

In veel reacties zijn vragen gesteld over de reikwijdte van de meldplicht, zoals: voor welke vitale aanbieders, producten en diensten gaat de meldplicht gelden en wanneer is voldaan aan het criterium 'in belangrijke mate'? En moet de meldplicht niet ook gaan gelden voor DDoS-aanvallen?

De meldplicht ziet op de situatie dat de beschikbaarheid of betrouwbaarheid van een aangewezen product of dienst in belangrijke mate onderbroken wordt of kan worden, maar alleen als dat gepaard gaat met een daadwerkelijke inbreuk op de veiligheid of een verlies van integriteit van een elektronisch informatiesysteem. Het gaat dus om cumulatieve voorwaarden; in de artikelsgewijze toelichting bij artikel 6, eerste lid, is dat verduidelijkt.

Anders dan **Bits of Freedom** betoogt, kan het louter onbereikbaar-zijn van een online-dienst zoals bij een DDos-aanval, niet worden aangemerkt als een inbreuk. Het is wenselijk om de meldplicht te beperken tot (potentieel) maatschappelijk ontwrichtende situaties waarbij rechtstreekse betrokkenheid van het NCSC voldoende meerwaarde heeft. Onbereikbaarheid door een DDos-aanval is meestal van korte duur. Overigens vallen ook DDos-aanvallen die tot langdurige onbereikbaarheid leiden, niet onder de meldplicht, dit in reactie op een opmerking van **BCPA**. Wel staat het vitale aanbieders vrij om ook dergelijke incidenten vrijwillig bij het NCSC te melden.

Om de meldplicht nader in te vullen, is en wordt de wenselijke reikwijdte van de meldplicht besproken met betrokken partijen uit de vitale sectoren (financiën, drinkwater, energie, telecom, haven Rotterdam, Schiphol, 'keren en beheren oppervlaktewater' en overheid). Vervolgens zullen de vitale aanbieders, producten en diensten die onder de meldplicht gaan vallen, worden aangewezen bij algemene maatregel van bestuur. Het overleg met de vitale sectoren dient ook om te bespreken wat voor de verschillende producten en diensten moet worden verstaan onder 'in belangrijke mate'. Het is de bedoeling om dat in te vullen met een goed hanteerbaar, objectief criterium, waar mogelijk in de vorm van drempelwaarden. Dit leidt per sector of onderdeel van een sector tot een specifieke uitwerking, die in overleg met de sector plaatsvindt.

5.2.3. Dubbele meldplichten, administratieve lasten

In diverse reacties wordt bezorgdheid uitgesproken over de administratieve lasten door het bestaan van deels overlappende verplichtingen tot melding van incidenten bij meerdere instanties. Zo merkt **Nederland ICT** op: "Voorkomen dient te worden dat bedrijven meer bezig zijn met het informeren van toezichthouders dan het oplossen van het incident. Nederland ICT vreest een juridische lappendeken van meldplichten, doublures en onnodige administratieve lasten. De meldplicht dient inhoudelijk zoveel mogelijk met andere meldplichten te worden gestroomlijnd. De wet dient daarvoor een duidelijke grondslag te bieden." Ook pleit deze organisatie voor de inrichting van één nationaal loket voor alle meldplichten.

Om de lasten voor bedrijven te beperken, pleiten **VNO-NCW** en **MKB-Nederland** juist voor een getrapte melding, via de sectorale toezichthouder.

Bij de vormgeving van de meldplicht is het beperken van de administratieve lasten een belangrijk uitgangspunt. Hoewel ik hecht aan rechtstreekse melding bij het NCSC wordt een toename van administratieve lasten zo veel mogelijk voorkomen. Zie hiervoor de toelichting bij paragraaf 2.5.

5.2.4. Relatie met NIB-richtlijn

VNO-NCW, **MKB-Nederland** en **Nederland ICT** pleiten voor uitstel van de meldplicht totdat de tekst van de NIB-richtlijn vaststaat, om te voorkomen dat de nu voorgestelde meldplicht al na korte tijd moet worden gewijzigd.

Naar aanleiding van deze opmerkingen ben ik in paragraaf 2.7 uitgebreider ingegaan op de keuze om met dit wetsvoorstel niet te wachten op de definitieve tekst van de NIB-richtlijn.

5.2.5. Vertrouwelijkheid van de aan het NCSC verstrekte gegevens

De **NVB** vindt de vertrouwelijkheid van aan het NCSC verstrekte informatie een groot punt van zorg, in het wetsvoorstel maar ook al in de huidige situatie. Vertrouwelijke mededelingen van banken aan DNB vallen onder de geheimhoudingsplicht van de Wet op het financieel toezicht en buiten de Wob. Incidentgegevens die aan het NCSC worden verstrekt, zoals over de wijze waarop het ICT-systeem van een bank wordt aangevallen, zullen wellicht niet altijd kwalificeren als bedrijfs- en fabricagegegevens in de zin van artikel 10 Wob, aldus de NVB. Ook is onduidelijk hoe de vertrouwelijkheid moet worden gegarandeerd als sprake is van een keten van partijen, waar de melder een schakel in vormt. Informatie over andere partijen in de keten valt wellicht niet onder de weigeringsgronden van de Wob waarop de melder een beroep kan doen. Daarnaast vindt de NVB het niet wenselijk dat het NCSC zonder instemming van de melder zeer gevoelige en vertrouwelijke gegevens nationaal en internationaal kan gebruiken voor het geven van advies.

Ook **DNB** en **AFM** pleiten voor beperking van de bevoegdheid van het NCSC om gevoelige gegevens aan derden te verstrekken. Zij menen dat het de informatieverstrekking aan het NCSC door vitale aanbieders uit de sector financiën ten goede zou komen als voor het NCSC een geheimhoudingsplicht zou gelden die vergelijkbaar is met de geheimhoudingsplicht van de sectorale toezichthouders. Daarnaast adviseren zij om wettelijk vast te leggen dat de sectorale toezichthouders beslissen, met ondersteuning van het NCSC, over het verstrekken van gegevens aan derden in een crisissituatie.

Netbeheer Nederland mist in de toelichting aandacht voor de verhouding van artikel 6 van het wetsvoorstel (versie eerste consultatie) met sectorale geheimhoudingsbepalingen

zoals artikel 79, eerste lid, van de Elektriciteitswet 1998. Zij is van oordeel dat artikel 6 (oud) met deze bepalingen op gespannen voet staat.

Nederland ICT vindt dat artikel 6 (oud) onvoldoende rekening houdt met de belangen van de betrokken vitale aanbieder. In elk geval zou de bepaling moeten voorschrijven dat vertrouwelijke bedrijfsgegevens niet zonder overleg worden verstrekt aan derden. Naar aanleiding van de zinsnede "Onverminderd andere wetten" (artikel 6, derde lid (oud)) merkt Nederland ICT op, het onwenselijk te vinden als het NCSC informatie kan of desgevraagd moet verstrekken aan de Autoriteit Consument en Markt (ACM) op basis van artikel 7 van de Instellingswet Autoriteit Consument en Markt. Het NCSC is immers geen "bestuursorgaan, dienst, toezichthouder en andere persoon, belast met de opsporing van strafbare feiten, onderscheidenlijk het toezicht op de naleving van wettelijke voorschriften".

BCPA meent dat alleen gegevens die evident noodzakelijk zijn in het kader van de voorlichtende taken van het NCSC onder het bereik van artikel 6 (oud) moeten vallen. En ook voor de verstrekking van gegevens aan andere vitale aanbieders zou moeten gelden dat zij in beginsel geen herleidbare gegevens ontvangen.

Schiphol Group vraagt wie bepaalt of "het maatschappelijke belang vergt" dat herleidbare gegevens mogen worden verstrekt aan het publiek (artikel 6, tweede lid (oud)): is dat de minister of het NCSC?

Vewin pleit voor een bepaling naar het voorbeeld van artikel 37, vierde lid, van de Drinkwaterwet: "De in het leveringsplan opgenomen gegevens, die betrekking hebben op het voorkomen van een verstoring, de voorbereiding op een verstoring dan wel het optreden in geval van een verstoring, zijn informatie als bedoeld in artikel 10, eerste lid, aanhef en onderdeel b, van de Wet openbaarheid van bestuur." Hiermee worden de betrokken gegevens aangemerkt als vertrouwelijk aan de overheid meegedeelde bedrijfs- en fabricagegegevens in de zin van de Wob en vallen zij (tenzij sprake is van milieu-informatie) onder de daarvoor geldende absolute weigeringsgrond.

Volgens **Bits of Freedom** leidt transparantie juist tot meer cybersecurity, doordat het zorgt voor vertrouwen in de organisatie, het onderzoek naar cyberdreigingen ten goede komt en leidt tot bewustwording bij andere organisaties en bij de consument. Het imago van een organisatie wordt meer beschadigd door geheimzinnigheid dan door openheid. De organisatie pleit voor het periodiek, bijvoorbeeld per kwartaal, openbaar maken van het aantal inbreuken per sector, de aard en de gevolgen daarvan, en de opvolging naar aanleiding van deze meldingen, een en ander overigens zonder herleidbare gegevens.

Zoals moge blijken uit het voorgestelde artikel 9, dat in de plaats komt van artikel 6 uit de eerste consultatieversie, heb ik gehoor gegeven aan de zorgen die tot uitdrukking komen in veel van deze reacties. Zo mag het NCSC vertrouwelijke gegevens die herleid kunnen worden tot een afzonderlijke aanbieder slechts verstrekken aan andere aanbieders, verzelfstandigde toezichthouders of het publiek als dat nodig is om ernstige maatschappelijke gevolgen te voorkomen of te beperken en alleen na raadpleging van de betrokken aanbieder (artikel 9, vierde lid). Deze verstrekking ziet op een situatie waarin geheimhouding grote schade zou (kunnen) toebrengen aan de Nederlandse samenleving.

Aan toezichthoudende diensten die deel uitmaken van andere ministeries mag het NCSC dergelijke herleidbare gegevens slechts verstrekken als een vitale aanbieder onvoldoende gevolg geeft aan een NCSC-advies (artikel 9, derde lid), ten einde hen in staat te stellen daar waar nodig passend invulling te geven aan de verantwoordelijkheid van het betrokken vakdepartement. Dit is alleen het geval wanneer het risico op maatschappelijke ontwrichting aanwezig blijft. Dit om te voorkomen dat een advies van het NCSC een te vrijblijvend karakter heeft. Zie ook de artikelsgewijze toelichting bij artikel 9.

De wettekst bepaalt expliciet dat de Wob niet van toepassing is op vertrouwelijke gegevens die herleid kunnen worden tot een afzonderlijke aanbieder (behoudens milieu-informatie, artikel 9, zesde lid), waarmee een vergelijkbaar resultaat wordt bereikt als met de suggestie van **Vewin** voor een bepaling zoals in de Drinkwaterwet. Een en ander leidt ertoe dat voor het NCSC inderdaad, zoals **DNB en AFM** bepleiten, een geheimhoudingsplicht gaat gelden die vergelijkbaar is met de geheimhoudingsplicht van (deze) sectorale toezichthouders. En doordat artikel 9 zich beperkt tot vertrouwelijke gegevens, is duidelijker dan bij artikel 6 (oud) dat artikel 9 niet in de weg staat aan actieve openbaarmaking van bijvoorbeeld aantallen meldingen en typen incidenten, zoals bepleit door **Bits of Freedom**.

Reactie op de overige opmerkingen over vertrouwelijkheid:

1. Gevoelige gegevens niet aan derden verstrekken zonder instemming van **(NVB)** dan wel overleg met **(Nederland ICT)** de betrokken vitale aanbieder? Sectorale toezichthouders laten beslissen over verstrekking van gegevens aan derden **(DNB en AFM)**?

   Artikel 6 (oud) gaf het NCSC een vrij ruime bevoegdheid om gevoelige gegevens te verstrekken aan derden. Zo konden herleidbare gegevens over aan het NCSC gemelde ICT-inbreuken aan andere vitale aanbieders worden verstrekt "ter voorkoming of beperking van schadelijke maatschappelijke gevolgen in of buiten Nederland". In artikel 9 is de drempel voor een dergelijke verstrekking verhoogd naar: "voor zover dat noodzakelijk is om ernstige maatschappelijke gevolgen te voorkomen of te beperken" (vierde lid). Dit criterium geldt ook voor verstrekking aan derden van vertrouwelijke herleidbare gegevens over incidenten en kwetsbaarheden die niet onder de meldplicht vallen. Als voldaan is aan dit criterium, dus als verstrekking van vertrouwelijke herleidbare gegevens inderdaad nodig is om ernstige maatschappelijke gevolgen te voorkomen of te beperken, dan zou het onjuist zijn als een afzonderlijke aanbieder de verstrekking niettemin zou kunnen tegenhouden. Ook een vetorecht van een toezichthouder zou in dat geval geen recht doen aan de eigen verantwoordelijkheid en expertise van het NCSC. Intussen zal het NCSC de betrokken aanbieder en zo mogelijk ook de toezichthouder wel raadplegen over de voorgenomen verstrekking, teneinde de nodige kennis te vergaren over de relevante feiten en de af te wegen belangen.

2. Hoe verhoudt artikel 6 (oud) zich met sectorale geheimhoudingsbepalingen zoals artikel 79, eerste lid, van de Elektriciteitswet 1998 **(Netbeheer Nederland)**?

   De bepaling die door Netbeheer Nederland wordt aangehaald luidt: "Een netbeheerder die bij de uitvoering van zijn taak de beschikking krijgt over gegevens waarvan hij het vertrouwelijke karakter kent of redelijkerwijs moet vermoeden, is verplicht tot geheimhouding van die gegevens, behoudens voor zover enig wettelijk voorschrift hem tot mededeling verplicht, of uit zijn taak de noodzaak tot mededeling voortvloeit." Deze bepaling richt zich tot de netbeheerder en niet, zoals artikel 6 (oud) en artikel 9 (nieuw), tot de Minister van Veiligheid en Justitie. Bovendien voorziet de bepaling er zelf al in dat andere wettelijke voorschriften, zoals de artikelen 6 en 7 (nieuw) van dit wetsvoorstel, de netbeheerder juist verplichten tot verstrekking van vertrouwelijke gegevens. De netbeheerder handelt niet in strijd met de Elektriciteitswet 1998 als hij, gevolg gevend aan de meldplicht van artikel 6 van dit wetsvoorstel of aan de informatieplicht van artikel 7, aan het NCSC herleidbare gegevens verstrekt en het NCSC die gegevens vervolgens, met toepassing van artikel 9, aan derden verstrekt.

3. Geen verstrekking van gegevens door het NCSC aan de ACM op basis van artikel 7 Instellingswet Autoriteit Consument en Markt **(Nederland ICT)**?

De door Nederland ICT aangehaalde bepaling ziet op verstrekking van gegevens door de ACM en niet aan de ACM.
Dit wetsvoorstel bevat geen verplichting voor een toezichthouder om gegevens te verstrekken aan het NCSC, noch een verplichting voor het NCSC om aan een sectorale toezichthouder gegevens te verstrekken. Wel kan het NCSC zich op grond van artikel 4 wenden tot de ACM met het verzoek gegevens te verstrekken. Het staat de ACM echter vrij dit verzoek af te wijzen.

Net als artikel 6 (oud) beoogt het voorgestelde artikel 9, afgezien van de Wet openbaarheid van bestuur, geen afwijking van verplichtingen tot verstrekking van herleidbare gegevens uit hoofde van andere wetten (zie de voorbeelden van dergelijke bepalingen in de artikelsgewijze toelichting bij artikel 9).
De ACM is bevoegd om aan het NCSC gegevens te verstrekken ten behoeve van het opsporen en bestrijden van computercriminaliteit; het NCSC is daartoe aangewezen in artikel 2, eerste lid, onder k, van de Regeling gegevensverstrekking ACM, op grond van artikel 7, derde lid, onder a, van de Instellingswet Autoriteit Consument en Markt.

4. Bepaalt de minister of het NCSC of "het maatschappelijke belang vergt" dat herleidbare gegevens mogen worden verstrekt aan het publiek **(Schiphol Group)**?

   Dit criterium uit artikel 6 (oud) komt niet meer voor in het voorgestelde artikel 9. De uitvoering van de Wet gegevensverwerking en meldplicht cybersecurity, dus ook de toepassing van de in artikel 9 gehanteerde criteria, valt binnen de omschrijving van de taken van het NCSC. Het NCSC voert zijn taken in beginsel zelfstandig uit krachtens mandaat, volmacht en machtiging. Het is dus in beginsel aan het NCSC om de in artikel 9 gehanteerde criteria uit te leggen. Wel zal de Minister van Veiligheid en Justitie zelf beslissen over het al dan niet toezenden van een NCSC-advies (uiteraard inclusief herleidbare gegevens) aan een andere bewindspersoon indien de betrokken vitale aanbieder onvoldoende gevolg geeft aan het advies. Het NCSC zal dus niet zelf beslissen over de toepassing van het derde lid van artikel 9.

5.2.6. Overige reacties op www.internetconsultatie.nl/meldplicht_ict_inbreuken

1. Twee inzenders pleiten voor (al dan niet verplicht te stellen) 'intrusion detection software', programmatuur die ICT-inbreuken detecteert.

   Het NCSC kan in een concreet geval adviseren om dergelijke programmatuur te installeren. Met het oog op de positionering van het NCSC als centrum van publiek-private samenwerking voorziet dit wetsvoorstel niet in interventiebevoegdheden zoals de mogelijkheid om een organisatie te verplichten om een bepaalde beveiligingsmaatregel te nemen. De noodzaak van (het creëren van) dergelijke bevoegdheden zal waarschijnlijk aan de orde komen bij de implementatie van de NIB-richtlijn. (zie paragraaf 2.7).

2. Een inzender vindt dat de meldplicht ook moet gaan gelden voor de gezondheidszorg.

   Uit de omschrijving van "vitale aanbieder" in het voorgestelde artikel 1 volgt dat de meldplicht alleen kan gaan gelden voor producten en diensten waarvan de beschikbaarheid en betrouwbaarheid van vitaal belang zijn voor de Nederlandse maatschappij. De sector gezondheidszorg is op grond van de 'tweede inhoudelijke analyse bescherming vitale infrastructuren van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2009' wel opgenomen in de sector vitaal en valt daarmee binnen de NCSC-taken. Echter, deze sector wordt niet als een zogenaamde 'randvoorwaardelijke' vitale sector bestempeld, vanwege het geringere risico van cascade-effecten.

De vitale aanbieders en hun producten en diensten die onder de meldplicht komen te vallen worden aangewezen bij algemene maatregel van bestuur. Het gaat om een inschatting van het risico dat uitval direct of indirect tot maatschappelijke ontwrichting leidt.

3. Een inzender vraagt welke criteria gelden voor de aanwijzing van meldplichtige vitale aanbieders, producten en diensten, welke mogelijkheid van beroep er is en welke juridische kaders.

   Zoals hierboven opgemerkt kan de meldplicht alleen gaan gelden voor producten en diensten waarvan de beschikbaarheid en betrouwbaarheid van vitaal belang zijn voor de Nederlandse maatschappij. Over de in artikel 5 bedoelde algemene maatregel van bestuur (amvb) zullen de betrokken partijen en de belangenorganisaties worden geraadpleegd en de tekst zal ook op www.internetconsultatie.nl voor inspraak worden opengesteld. Tegen de amvb staat geen bestuursrechtelijke rechtsbescherming open. Om dat buiten twijfel te stellen, is een bepaling aan het wetsvoorstel toegevoegd waarin artikel 5 wordt toegevoegd aan de opsomming van niet-appellabele besluiten in artikel 1 van bijlage 2 bij de Algemene wet bestuursrecht (zie artikel 10).

4. Een inzender vindt de meldplicht onnodig specifiek: elke situatie die cruciale dienstverlening in gevaar brengt, zou meldingsplichtig moeten zijn.

   Een dergelijke uitbreiding van de reikwijdte van de meldplicht zou ook situaties die buiten de reikwijdte van de taken, de expertise en kennis van het NCSC vallen onder de meldplicht scharen. Om rechtszekerheid voor meldplichtige partijen te bewerkstelligen moet de reikwijdte van de meldplicht worden afgebakend.

5.3. Tweede consultatieronde

PM

6. Grondrechtentoets

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 signalering van een incident of dreiging met betrekking tot een elektronisch informatiesysteem waarbij Nederlandse (rijks)overheids- of vitale partijen betrokken kunnen zijn. Dit wetsvoorstel 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 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, contactgegevens van melders van incidenten en kwetsbaarheden of e-mailadressen van bij een ICT-inbreuk betrokken personen. De verwerking van persoonsgegevens door het NCSC is een inmenging door het openbaar gezag in het recht op respect voor de persoonlijke levenssfeer (de artikelen 10 Grondwet, 8 EVRM en 17 IVBPR).

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.

1. De beperkende maatregel moet "voorzien bij wet" zijn

De voorgestelde artikelen 2 en 3 bieden een specifieke wettelijke grondslag voor de verwerking van persoonsgegevens door het NCSC. Artikel 3 beperkt de verwerking van (persoons)gegevens tot de in artikel 2 omschreven doeleinden en taken.

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. De verwerking van persoonsgegevens door het NCSC dient de nationale veiligheid, de openbare veiligheid, het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid en de bescherming van de rechten en vrijheden van anderen. Al 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 Europese Hof voor de rechten van de mens (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.

2a. Dringende maatschappelijke behoefte
De dringende maatschappelijke behoefte van de verwerking van persoonsgegevens door het NCSC is geleden 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 beschikbaarheid en betrouwbaarheid van diensten en producten van vitale aanbieders is dan ook uitermate 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, 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 2 en 9) om hen in staat te stellen maatregelen te nemen tegen een aanval vanaf die adressen. Anderzijds onderzoekt het NCSC of de bij het NCSC bekende IP-adressen van met name vitale 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 2 en 9 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 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 kan delen met de juiste organisaties.

2b. Proportionaliteit
Het NCSC verwerkt grote aantallen persoonsgegevens, maar gelet op de aard ervan (IP- en e-mailadressen en domeinnamen) gaat het niet om een forse inmenging in het recht op respect voor iemands privéleven. De betrokken gegevens worden door het NCSC verwerkt met inachtneming van de Wet bescherming persoonsgegevens. Zo wordt voorafgaand aan het aanleggen van (nieuwe) specifieke verzamelingen van persoonsgegevens een vaste procedure van 'checks and balances' gevolgd. Controle op het creëren en bijhouden van verzamelingen persoonsgegevens vindt daarmee voorafgaand aan deze nieuwe verwerking plaats. De functionaris gegevensbescherming van het Ministerie van Veiligheid en Justitie ziet daarop toe. Er wordt bijvoorbeeld voor gezorgd dat het NCSC niet meer gegevens verwerkt dan vereist is voor het uitvoeren van zijn taken en dat gegevens worden verwijderd zodra zij niet meer noodzakelijk zijn voor het doel waarvoor zij zijn verkregen. Persoonsgegevens die het NCSC verwerkt die noodzakelijk zijn voor de uitvoering van zijn taken worden niet langer door het NCSC bewaard dan noodzakelijk. Zo worden contactgegevens van de melder bijvoorbeeld niet langer dan 13 maanden na het afhandelen van de melding bewaard en worden andere persoonsgegevens uiterlijk 18 maanden na het afhandelen van een incident of dreiging verwijderd of geanonimiseerd. Ook in ander opzicht blijft de inbreuk beperkt: het NCSC doet geen onderzoek naar individuele personen die bij een ICT-inbreuk betrokken zijn.

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 andere wijze de informatie verkrijgen die noodzakelijk is voor het uitoefenen van zijn taken. Ook anonimiseren of pseudonimiseren 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.

3. Conclusie
De verwerking van persoonsgegevens door het NCSC is een gerechtvaardigde beperking van de persoonlijke levenssfeer met het oog op het waarborgen van de digitale veiligheid. De voorgestelde bevoegdheden zijn omkleed met voldoende waarborgen, zoals hierboven is uiteengezet.

7. Privacy impact assessment

Gezien de aard van dit wetsvoorstel is in de fase van beleidsontwikkeling een Privacy Impact Assessment uitgevoerd (zie ook Kamerstukken I 2010/11, 31 051, D, motie-Franken). Met behulp hiervan is de noodzaak van de gegevensverwerking bekeken, en zijn op gestructureerde wijze de implicaties in kaart gebracht. Hierbij is in het bijzonder aandacht besteed aan de beginselen van gegevensminimalisering en doelbinding, het vereiste van een goede beveiliging en de rechten van de betrokkenen. De gezichtspunten die relevant zijn voor de eerste twee beginselen zijn voldoende aan de orde gekomen in paragraaf 6.

Beveiliging
Voor het NCSC staat het waarborgen van de kwaliteit en veiligheid van gegevens voorop. Zo neemt het NCSC uitvoerige maatregelen om de gegevens te beveiligen die zijn opgeslagen op zijn servers. Verder vindt strikte fysieke en digitale toegangscontrole plaats, waarmee toegang door onbevoegden of verlies van de gegevens zo veel mogelijk wordt beperkt.

Rechten betrokkene
Wanneer een betrokkene inzicht wil verkrijgen in de persoonsgegevens die het NCSC over hem of haar verwerkt, deze gegevens wil wijzigen of aanpassen, kan de betrokkene hiertoe een verzoek indienen bij het Ministerie van Veiligheid en Justitie. De gegevens worden daarnaast verwijderd zodra deze niet langer noodzakelijk zijn voor het verwezenlijken van het doel van de verwerking.

Voor de verwerking van persoonsgegevens door het NCSC is de Minister van Veiligheid en Justitie verantwoordelijk. De functionaris voor de gegevensbescherming van het ministerie houdt toezicht op de verwerking van persoonsgegevens door het NCSC.

8. Regeldruk

De door dit wetsvoorstel veroorzaakte regeldruk bestaat uit een bescheiden stijging van de administratieve lasten voor de organisaties die onder de meldplicht vallen. Een definitieve raming kan pas worden gemaakt als vaststaat voor welke vitale aanbieders en voor welke producten en diensten de meldplicht zal gelden (aan te wijzen bij algemene maatregel van bestuur (amvb)), welke gegevens verstrekt moeten worden en op welke wijze dat moet gebeuren (nader te regelen bij of krachtens amvb). In de nota van toelichting bij de amvb (en in de toelichting van de krachtens die amvb eventueel vast te stellen ministeriële regeling) zal hierop nader worden ingegaan. Bovendien ben ik voornemens om samen met de betrokken sectoren en departementen nader uit te werken, zo mogelijk per sector, bijvoorbeeld bij of krachtens algemene maatregel van bestuur of in beleidsregels, welke inbreuken ernstig genoeg zijn om onder de meldplicht te vallen (nadere uitwerking van "in belangrijke mate" in artikel 6, eerste lid). Ook die nadere uitwerking bepaalt voor een deel de omvang van de administratieve lasten.

Intussen mag wellicht een eerste indicatie van de te verwachten administratieve lasten worden ontleend aan de hierboven al besproken meldplicht voor de aanbieder van een openbaar elektronisch communicatienetwerk of een openbare elektronische communicatiedienst (artikel 11a.2 Telecommunicatiewet). De totale administratieve lasten van die meldplicht zijn geraamd op circa € 277 000 per jaar, uitgaande van 10 meldingen per aanbieder per jaar en van 486 aanbieders. Naar verwachting zal in elk geval het aantal aanbieders waarvoor de in dit wetsvoorstel geregelde meldplicht voor ICT-inbreuken zal gelden, aanzienlijk kleiner zijn (alleen vitale aanbieders).

Zoals gezegd zullen voor elkaar overlappende meldplichten de wijze waarop moet worden gemeld en de gegevens die dienen te worden verstrekt, zo veel mogelijk onderling worden afgestemd.

Voor het overige heeft dit wetsvoorstel geen gevolgen voor de regeldruk voor burgers of het bedrijfsleven.

Artikelsgewijze toelichting
Artikel 1

De omschrijving van 'aanbieder' is (afgezien van het element 'bouwen') afgeleid van de definitie van 'aanbieden' in artikel 1.1, onder i, van de Telecommunicatiewet. Een aanbieder kan een rechtspersoon zijn, een samenwerkingsverband zonder rechtspersoonlijkheid (vennootschap onder firma, commanditaire vennootschap of maatschap) of een natuurlijke persoon.

Het begrip 'vitale aanbieder' slaat alleen op aanbieders van voor de Nederlandse samenleving vitale producten of diensten. De meldplicht kan alleen gelden voor vitale aanbieders (zie artikel 5), maar hoeft niet per se voor alle vitale aanbieders te gelden.

Voor de toepassing van de artikelen 2, tweede lid, en 9, tweede lid, zullen bij ministeriële regeling CERT's worden aangewezen ('computercrisisteams'), na toetsing of gegevensuitwisseling daarmee gerechtvaardigd en verantwoord is. Het kan gaan om een aanwijzing van een individuele CERT of van een categorie van CERT's. De term computercrisisteam is ontleend aan artikel 7 van de concept-NIB-richtlijn.

Bij informatiesystemen zal het vaak gaan om systemen die van internet afhankelijk zijn, maar dat is geen vereiste.

De begrippen persoonsgegevens, verwerking van persoonsgegevens en verantwoordelijke hebben dezelfde betekenis als in de Wet bescherming persoonsgegevens (Wbp). Onder persoonsgegevens verstaat artikel 1 Wbp "elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon". In het kader van dit wetsvoorstel betreft het bij de verwerking van persoonsgegevens door het NCSC bijvoorbeeld bij incidenten of dreigingen betrokken IP-adressen (nummers waarmee een individuele computer, en daarmee vaak ook de gebruiker daarvan, geïdentificeerd kan worden) en contactgegevens van bijvoorbeeld overheids- en vitale private partijen. Zie ook artikel 3.

Onder verwerking van persoonsgegevens verstaat de Wbp "elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens".

Onder verantwoordelijke verstaat de Wbp "de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te zamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt". In het kader van dit wetsvoorstel gaat het om de Minister van Veiligheid en Justitie, zie artikel 3.

Artikel 2

Dit artikel bevat een opsomming van de taken van de Minister van Veiligheid en Justitie op het terrein van cybersecurity, ten behoeve waarvan verwerking van onder meer persoonsgegevens aangewezen is, en omschrijft de doeleinden van die taken. Zie voor een nadere toelichting hierop paragraaf 3 van het algemeen deel van deze memorie.
De in het eerste lid vastgelegde taken hebben als doel de uitval van informatiesystemen van aanbieders van voor de Nederlandse samenleving vitale producten of diensten te beperken en te voorkomen, alsook de digitale weerbaarheid van de Nederlandse samenleving te bevorderen. Daarbij gaat het niet alleen om vitale aanbieders en producten en diensten die onder de meldplicht vallen.
Bij het onderzoek door het NCSC van dreigingen en incidenten met betrekking tot vitale informatiesystemen kunnen ook gegevens aan het licht komen over dreigingen of incidenten met betrekking tot andere informatiesystemen. Ter voorkoming van nadelige maatschappelijke gevolgen regelt het tweede lid dat het NCSC ook als taak heeft laatstbedoelde gegevens in voorkomende gevallen in een beperkte kring van derden te delen ten behoeve van de informatievoorziening van andere organisaties of het publiek. Hierbij kan het ook gaan om persoonsgegevens, zoals e-mailadressen die door een ICT-inbreuk kwetsbaar zijn geworden. Een voorbeeld van een organisatie als bedoeld in onderdeel a is SIDN, de Stichting Internet Domeinnaamregistratie Nederland (www.sidn.nl).
Het begrip 'aangewezen computercrisisteams' in onderdeel b van het tweede lid duidt op de CERT's die bij ministeriële regeling zijn aangewezen, zie de definitie in artikel 1.

Artikel 3

Bij de in dit artikel bedoelde (persoons)gegevens gaat het bijvoorbeeld om bij een incident of dreiging betrokken IP-adressen en contactgegevens van vitale organisaties en 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 Wbp; zie ook paragraaf 6 van het algemeen deel van deze memorie.

Artikel 4

Het eerste lid voorziet in een wettelijke bevoegdheid voor het NCSC om eenieder, bijvoorbeeld overheidsorganisaties of private partijen, om gegevens te vragen ten behoeve van de in artikel 2 genoemde doeleinden en taken. Artikel 4, eerste lid, voorziet niet in een bevoegdheid om gegevens te vorderen; degene tot wie het verzoek is gericht, is dus niet verplicht tot medewerking. Een dergelijke verplichting acht ik alleen nodig voor een vitale aanbieder die bij het NCSC een meldplichtige ICT-inbreuk heeft gemeld; daarin voorziet artikel 7. Voor de goede uitoefening van zijn taken is het van belang dat het NCSC over voldoende gegevens beschikt over incidenten en kwetsbaarheden, waaronder zo nodig ook persoonsgegevens zoals IP-adressen, met betrekking tot informatiesystemen van met name de rijksoverheid en vitale private partijen. Omdat deze gegevens juist ook ter voorkoming van maatschappelijke ontwrichting, van grote betekenis kunnen zijn, regelt het tweede lid dat artikel 9 Wbp, waarin onder meer wordt geregeld dat persoonsgegevens niet verder mogen worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor zij zijn verkregen en dat verwerking achterwege blijft voor zover een geheimhoudingsplicht uit hoofde van ambt, beroep of wettelijk voorschrift daaraan in de weg staat, niet van toepassing is op een verzoek als bedoeld in het eerste lid. Deze afwijking van de Wbp verdraagt zich met de Europese privacyrichtlijn, omdat die richtlijn niet van toepassing is op verwerkingen die betrekking hebben op de openbare veiligheid (artikel 3, tweede lid, eerste streepje).

Artikel 5

Dit artikel geeft een grondslag voor aanwijzing bij algemene maatregel van bestuur van de aanbieders en de producten en diensten waarvoor de in artikel 6 opgenomen meldplicht geldt en de in artikel 7 opgenomen verplichting om na een verplichte melding desgevraagd nadere gegevens te verstrekken. Het moet gaan om voor de Nederlandse samenleving vitale producten of diensten, zie de omschrijving van 'vitale aanbieder' in artikel 1. Een aanbieder kan ook buiten Nederland gevestigd zijn; het gaat erom dat hij producten of diensten aanbiedt die vitaal zijn voor de Nederlandse samenleving.
De voordracht voor de algemene maatregel van bestuur zal worden gedaan in overeenstemming met de andere betrokken bewindspersonen.

Artikel 6

De meldplicht geldt alleen als voldaan is aan de volgende cumulatieve voorwaarden:
1. Het gaat om een krachtens artikel 5 aangewezen product of dienst van een aangewezen vitale aanbieder.
2. Er is of was een daadwerkelijke inbreuk op de veiligheid of een daadwerkelijk verlies van integriteit van een elektronisch informatiesysteem waarvan het product of de dienst afhankelijk is.
3. Die inbreuk of dat verlies heeft geleid, of kan leiden tot een onderbreking van de beschikbaarheid of de betrouwbaarheid van het product of de dienst.

4. Die feitelijke of potentiële onderbreking moet belangrijk zijn, dus substantieel.

Doordat de meldplicht alleen geldt als de onderbreking van de beschikbaarheid of de betrouwbaarheid wordt veroorzaakt door een inbreuk op de veiligheid of door een verlies van integriteit, valt een onderbreking van de beschikbaarheid door een DDos-aanval buiten de meldplicht. Een dergelijke aanval gaat immers niet gepaard met een inbreuk op de veiligheid of een verlies van integriteit.

Mede op basis van overleg met de betrokken sectoren en departementen zal nader worden uitgewerkt, en bijvoorbeeld in beleidsregels worden vastgelegd, wat voor de verschillende betrokken producten en diensten moet worden verstaan onder "in belangrijke mate". Daarbij zal mede bepalend zijn onder welke omstandigheden sprake is of kan zijn van maatschappelijke ontwrichting. Hierbij gaat het bijvoorbeeld om criteria zoals de langdurigheid van de uitval van een vitaal proces of vitale dienst waardoor zowel de vitale aanbieder als andere partijen geconfronteerd worden met de gevolgen van de uitval. Tevens valt daarbij te denken aan de ernst en omvang van de inbreuk, waaronder de mate waarin ook andere organisaties of het publiek schade hiervan ondervinden.

De meldplicht geldt dus ook als de ICT-inbreuk nog niet daadwerkelijk heeft geleid tot een belangrijke onderbreking van de beschikbaarheid of betrouwbaarheid van een vitaal product of vitale dienst, maar dat gevolg wel alsnog kan hebben. Dit is immers evenzeer informatie die van groot belang is met het oog op het beperken of voorkomen van schadelijke maatschappelijke gevolgen. Bovendien kan ook van dergelijke inbreuken veel worden geleerd.

Van belang is het dat de melding van een ICT-inbreuk waarvoor de meldplicht geldt zo spoedig mogelijk wordt gedaan. Daarbij dient in aanmerking genomen te worden dat soms enige tijd zal verstrijken tussen de feitelijke inbreuk en de constatering (van de ernst) daarvan door de vitale aanbieder. Het is belangrijk dat het NCSC zo snel als mogelijk in de gelegenheid wordt gebracht om de risico's voor de beschikbaarheid of betrouwbaarheid van een vitaal product of vitale dienst te kunnen bepalen en hulp te verlenen bij het treffen van maatregelen om de beschikbaarheid of betrouwbaarheid te waarborgen of herstellen.

De initiële melding kan beknopt zijn: liever een snelle melding die zo nodig later kan worden aangevuld, dan een uitvoerige melding die daardoor op zich laat wachten. Zie ook paragraaf 2.2.

De omschrijving van de bij de melding te verstrekken gegevens is zo veel mogelijk identiek aan de omschrijving in artikel 7, tweede lid, van het Besluit continuïteit openbare elektronische communicatienetwerken en -diensten en aan de omschrijving die voor verleners van gekwalificeerde certificaten is opgenomen in artikel 2, eerste lid, onder q, van het Besluit elektronische handtekeningen. Het gaat hierbij om gegevens die het NCSC in ieder geval nodig heeft voor een goede uitoefening van zijn taken.

Artikel 7

Denkbaar is dat het NCSC naar aanleiding van een melding nadere gegevens nodig heeft om de aard en de ernst van de ICT-inbreuk te kunnen inschatten en de aanbieder adequaat te kunnen helpen, bijvoorbeeld als de aanbieder bij het doen van de melding nog geen volledige zekerheid kan bieden over de gevolgen van de inbreuk of over de te nemen maatregelen. Dit artikel bevat voor dergelijke gevallen een aanvullende informatieplicht, die wordt geactiveerd door een concreet verzoek van het NCSC in reactie op een in artikel 6 bedoelde melding.

Artikel 8

De hier bedoelde nadere regels dienen onder meer om te concretiseren welke gegevens voor de verschillende aangewezen producten en diensten ingevolge de meldplicht verstrekt moeten worden en de wijze waarop de gegevens verstrekt moeten worden. De nadere regels kunnen bijvoorbeeld ook gebruikt worden om te verduidelijken wat voor de verschillende aangewezen producten en diensten bij de toepassing van artikel 6, eerste lid, moet worden verstaan onder "in belangrijke mate".

Artikel 9

Dit artikel regelt de verstrekking door het NCSC aan derden van vertrouwelijke gegevens 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. Zie hierover ook paragraaf 4 van het algemeen van deze memorie.

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 2 kan de noodzaak voortvloeien tot mededeling van vertrouwelijke gegevens. Artikel 9 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 AFM of DNB). Deze bepaling regelt dat bij het NCSC, bijvoorbeeld naar aanleiding van een melding, berustende vertrouwelijke gegevens slechts ter uitvoering van de in artikel 2 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 alleen op verstrekking van vertrouwelijke gegevens "ter uitvoering van de in artikel 2 genoemde taken", dus niet op verplichtingen tot verstrekking door het NCSC van vertrouwelijke gegevens uit hoofde van andere wetten, zoals artikel 8:28 Algemene wet bestuursrecht (inlichtingen verstrekken aan de bestuursrechter door partijen in een beroepsprocedure), artikel 126nc e.v. Wetboek van Strafvordering (vorderen van gegevens door officier van justitie), de Wet openbaarheid van bestuur en de Wet op de inlichtingen- en veiligheidsdiensten 2002.

Het tweede lid regelt dat verstrekking van vertrouwelijke gegevens die herleid kunnen worden tot een afzonderlijke aanbieder alleen mogelijk is aan door de minister op grond van artikel 1 aangewezen computercrisisteams (CERT's) en aan de Nederlandse inlichtingen- en veiligheidsdiensten, voor zover dat dienstig is voor het bevorderen van maatregelen ter voorkoming of beperking van een verstoring van het maatschappelijk verkeer. De formulering "gegevens die herleid kunnen worden tot een afzonderlijke 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.

Het derde lid beoogt te voorkomen dat de reactie van vitale aanbieders op NCSC-adviezen een te vrijblijvend karakter heeft. Het gaat om de situatie dat het NCSC, al dan niet naar aanleiding van een melding, aan een vitale aanbieder advies heeft gegeven, waarin maatregelen worden genoemd waarmee een ICT-kwetsbaarheid zou kunnen

worden weggenomen met betrekking tot een product of dienst. Het blijft primair de eigen verantwoordelijkheid van de vitale aanbieder om passende maatregelen te nemen om uitval of verstoring van het product of de dienst te voorkomen of te beperken. Ook is het primair aan de vitale aanbieder om, als daar aanleiding toe is, de eigen toezichthouder(s) of vakdepartementen op de hoogte te stellen. Voor het geval de Minister van Veiligheid en Justitie echter van oordeel is dat de vitale aanbieder onvoldoende gevolg geeft aan het advies, en daardoor het risico op maatschappelijke ontwrichting aanwezig blijft, kan hij de voor de betrokken sector verantwoordelijke minister of staatssecretaris een kopie van het advies verstrekken. Die bewindspersoon kan daarmee dan bijvoorbeeld een onder hem ressorterende inspectiedienst waarschuwen. De hier bedoelde verstrekking aan de eerstverantwoordelijke bewindspersoon is alleen zinvol mét de in het advies opgenomen herleidbare gegevens. Daarom regelt het derde lid dat ook in dat geval die gegevens verstrekt mogen worden. Als het advies betrekking heeft op de (rijks)overheid zal overigens 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.
Wat betreft verstrekking van herleidbare gegevens aan sectorale toezichthouders ziet het derde lid uitsluitend op toezichthoudende diensten die onderdeel zijn van een ministerie. Verstrekking aan andere toezichthouders kan alleen op grond van het vierde lid.

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

Het vierde lid ziet op het specifieke geval dat verstrekking van bovenbedoelde herleidbare gegevens noodzakelijk is om ernstige maatschappelijke gevolgen te voorkomen of te beperken. In dat geval kunnen deze gegevens ook met andere dan de hierboven genoemde organisaties, zoals andere aanbieders, of het publiek worden gedeeld. Daarbij spreekt het voor zich dat deze informatieverstrekking niet verder gaat dan strikt noodzakelijk is om anderen 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 dan de in het tweede en derde lid genoemde organisaties" ziet bijvoorbeeld ook op een toezichthoudende dienst die geen onderdeel is van een ministerie, zoals De Nederlandse Bank of de Autoriteit Financiële Markten.

Het derde en vierde lid staan niet in de weg aan overleg met toezichthouders teneinde advies van het NCSC en handhavend optreden van toezichthouders op elkaar af te stemmen, mits de betrokken vitale aanbieder hier toestemming voor geeft.

Op de verstrekking, op grond van het vierde lid, van herleidbare gegevens aan het publiek is reeds ingegaan in het algemeen deel van deze memorie (paragraaf 4. Verstrekking van vertrouwelijke gegevens). Omdat dergelijke mededelingen naar hun aard niet samengaan met geheimhouding en doelbinding, bepaalt het vijfde lid dat het eerste lid op die mededelingen niet van toepassing is.

Zoals uiteengezet in het algemeen deel van deze memorie bevat artikel 9 een bijzondere openbaarheidsregeling voor vertrouwelijke herleidbare gegevens die afwijkt van de Wet openbaarheid van bestuur. Het zesde lid stelt dit buiten twijfel, waarbij een uitzondering wordt gemaakt voor milieu-informatie. Ter uitvoering van het Verdrag van Aarhus en EU-richtlijn 2003/4/EG 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 maar relatief, en in plaats van de relatieve weigeringsgrond dat onevenredige bevoordeling of benadeling voorkomen moet worden 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. 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. Om strijdigheid met het genoemde verdrag en de genoemde richtlijn te voorkomen, volgt uit het zesde lid van artikel 9 dat de Wob onverkort van toepassing is op herleidbare gegevens die milieu-informatie inhouden.

Het kan wenselijk blijken om nadere regels te stellen over het eerste tot en met vierde lid van artikel 9, bijvoorbeeld nadere voorwaarden voor de verstrekking van vertrouwelijke gegevens aan aangewezen CERT's (tweede lid, onder a). In die mogelijkheid voorziet het zevende lid.

Artikel 10

Tegen een besluit, inhoudende een algemeen verbindend voorschrift, staat ingevolge artikel 8:3, eerste lid, onder a, Algemene wet bestuursrecht (Awb) geen bestuursrechtelijke rechtsbescherming open. Het is echter niet zeker of de in artikel 5 bedoelde algemene maatregel van bestuur (amvb) moet worden aangemerkt als een algemeen verbindend voorschrift, aangezien de amvb slechts een opsomming zal bevatten van de vitale aanbieders, producten en diensten waarvoor de wettelijke meldplicht geldt. Als die lijst in de wet zelf zou staan, zou daartegen hoe dan ook geen bestuursrechtelijke rechtsbescherming openstaan, omdat de wetgevende macht geen bestuursorgaan is in de zin van de Awb (zie artikel 1:1, tweede lid, onder a). Dan is het vreemd als tegen diezelfde lijst, maar dan opgenomen in een amvb, wél bezwaar en beroep zouden openstaan. Daarnaast kunnen door het openstellen van bezwaar en beroep tegen een amvb complicaties ontstaan als gevolg van de betrokkenheid van zowel de Afdeling advisering als de Afdeling bestuursrechtspraak van de Raad van State. Artikel 1 van bijlage 2 Awb somt de besluiten op waartegen geen beroep openstaat, en daarmee ook geen bezwaar. Toevoeging van artikel 5 aan die opsomming stelt buiten twijfel dat tegen de amvb geen bezwaar en beroep openstaan.

Artikel 11

Hoewel het in de bedoeling ligt om deze wet als één geheel in werking te laten treden, is de mogelijkheid van gedifferentieerde inwerkingtreding opengehouden. De bepaling is overigens niet bedoeld om de meldplicht van artikel 6, eerste lid, voor afzonderlijke vitale aanbieders, producten of diensten op verschillende tijdstippen in werking te kunnen laten treden. Mocht een dergelijke differentiatie nodig zijn, dan kan zij eventueel worden vormgegeven in de algemene maatregel van bestuur, bedoeld in artikel 5.

De Minister van Veiligheid en Justitie,