INTERNETCONSULTATIE
WET GEGEVENSVERWERKING EN MELDPLICHT CYBERSECURITY

Status per 20150306

1.	INLEIDING / HISTORIE	Datalekken en Cybersecurity incidenten komen sinds een aantal jaren steeds vaker en heftiger voor. In de media wordt regelmatig bericht over beveiligingsincidenten en over nieuwe voorstellen ter aanscherping van de regelgeving met betrekking tot de bescherming van digitale informatie. Dit heeft geleid tot de vraag naar de noodzaak voor en de mogelijkheid van effectieve, technisch onafhankelijke reguleringsinstrumenten die de integriteit van informatiesystemen waarborgen. Het wetsvoorstel Gegevensverwerking en Meldplicht Cybersecurity *('Wetsvoorstel')* sluit aan bij deze actualiteit en de gestelde beveiligingseisen voor een informatiemaatschappij die in het leven zijn geroepen vanuit zowel Europese *('NIB-Richtlijn')* als nationale wetgeving. Het Wetsvoorstel introduceert een meldplicht bij het Nationaal Cyber Security Centrum ('*NCSC*'). Aanleiding voor deze wet zijn de gebeurtenissen bij DigiNotar of een meer recent voorbeeld; de miljarden euro's die van banken zijn gestolen via Malware, waardoor het belang van ICT beveiliging bij de overheid en andere vitale sectoren is toegenomen.
2.	MELDPLICHT	De meldplicht geldt als er sprake is van een (mogelijke) inbreuk op veiligheid en daadwerkelijk verlies van integriteit van een elektronisch informatiesysteem. Hierbij gaat het om alle soorten data inclusief persoonsgegevens. Tijdelijke verstoringen zoals DDoS aanvallen vallen niet onder de meldplicht. De verplichting tot melden bestaat voorts alleen indien de inbreuk gevolgen heeft of kan hebben op de beschikbaarheid of betrouwbaarheid een dienst of product en dit tevens in belangrijke mate kan leiden tot maatschappelijk ontwrichting. De meldplicht heeft alleen betrekking op aanbieders van vitale producten of diensten uit o.a. de volgende sectoren: elektriciteit, gas, drinkwater, telecom, keren en beheren van oppervlaktewater, financiën, overheid en transport (Haven Rotterdam en Schiphol).
3.	DOEL MELDPLICHT	Het NCSC heeft als rol het waarborgen en zorgen voor een hoog kennisniveau van netwerk- en informatiebeveiliging. De meldplicht zorgt voor de benodigde informatie waarmee de NCSC (i) een tijdige inschatting kan maken van de impact van een mogelijke ICT inbreuk en of er sprake is van maatschappelijke ontwrichting, en (ii) hulp kan bieden aan de getroffen organisatie en anticiperen op mogelijk bredere effecten van een dergelijke inbreuk. Deze hulp kan bestaan uit (a) advies en informatie en (b) technische ondersteuning. De doelstelling van het Wetsvoorstel is maatschappelijke ontwrichting door ICT-inbreuken te beperken of te voorkomen. Echter het NCSC houdt (nog) geen toezicht op de naleving van de meldplicht, bijvoorbeeld doormiddel van audits en andere handhavingsbevoegdheden. In de loop der tijd zullen deze bevoegdheden worden uitgebreid op basis van de NIB-Richtlijn doormiddel van periodieke audits en kan het toezicht via sectorale wetgeving worden aangescherpt.

4.	**RELATIE MET ANDERE WETGEVING**	**Europese wetgeving** De meldplicht van de NIB ziet op de marktdeelnemers van stroomafwaartse diensten van de informatiemaatschappij, die anders gezegd dus andere (vitale) diensten mogelijk maken. Voorbeelden zijn platforms voor elektronische handel, gateways voor internetbetalingen, sociale netwerk sites, zoekmachines en cloud computing-diensten (SaaS, PaaS, IaaS). Verstoring van deze ondersteunende diensten belemmert het aanbod van de hierop volgende diensten. Naast regels voor marktdeelnemers schrijft de NIB-Richtlijn regels voor aan overheden en exploitanten van kritieke maatschappelijke diensten die sterk afhankelijk zijn van vitale maatschappelijke voorzieningen als gas, gezondheidszorg, transport, elektriciteit en kredietverlening. Deze exploitanten zijn verantwoordelijk voor de beveiliging van de door deze sectoren gebruikte netwerken en informatiesystemen, los van de vragen wie het onderhoud verricht en of het aanbieden van communicatie de kern van de dienstverlening is. Op dit laatste punt overlappen het Wetsvoorstel en de NIB-richtlijn elkaar. **Nationale wetgeving** Het wetsvoorstel voor de meldplicht datalekken van de Wet bescherming persoonsgegevens *('Wbp')* en de Telecommunicatiewet *('Tw')* ziet op de beveiliging van persoonsgegevens tegen verlies en onrechtmatige verwerking. Het Wbp wetsvoorstel voorziet op veel meer punten in een beter systeem voor het melden van datalekken dan de meldplicht voor ICT inbreuken. Waaronder extra voorzorgsmaatregelen met betrekking tot de via deze wet verkregen persoonsgegevens en maatregelen met betrekking tot handhaving van de wet. Beveiligingsmaatregelen dienen schriftelijk te worden vastgelegd en een enkele melding van een datalek is niet voldoende om onder de verantwoordelijkheden van eventuele burgerrechtelijke aansprakelijkheid voor schade uit te komen. Wanneer er bij een ICT inbreuk persoonsgegevens gemoeid zijn, dan moet er bij beide toezichthoudende organisaties een melding worden gedaan, wat leidt tot een dubbele meldplicht.
5.	**RELATIE MET PRIVACY & SECURITY**	Het is algemeen bekend dat dataprotectie en informatiebeveiliging met elkaar verbonden rechtsgebieden zijn. De Europese Toezichthouder voor Gegevensbescherming ("EDPS") publiceerde op 17 juni 2013 zijn advies over de NIB Richtlijn dat ziet op informatiebeveiliging. In dat advies is de toezichthouder zeer positief over het voorstel, maar tegelijkertijd kritisch over de bescherming van persoonsgegevens. 'Cyberbeveiliging mag in geen geval een excuus zijn voor de onbeperkte monitoring en analyse van persoonsgegevens', aldus EDPS. Het Wetsvoorstel besteedt nauwelijks aandacht aan de bescherming van persoonsgegevens, omdat het niet per se noodzakelijk is dat er persoonsgegevens in het geding zijn bij een ICT inbreuk. Echter, zoals we hierboven al eerder zagen kunnen er wel persoonsgegevens bij gemoeid zijn, waarvoor onvoldoende beschermingswaarborgen in het Wetsvoorstel zijn opgenomen.

		Ondanks dat er een vertrouwelijkheidsclausule in het Wetsvoorstel is opgenomen, kan de NCSC deze bedrijfsgevoelige informatie wel degelijk aan derden overdragen in het kader van het bieden van hulp en overleg voeren met soortgelijke diensten. Met name de 'bijvangst' van deze meldingen kan de NCSC delen met een beperkte kring van derden, dat wordt door dit Wetsvoorstel mogelijk gemaakt, zoals (internationale) inlichtingendiensten. Dergelijke bijvangst is niet nodig om ICT inbreuken te voorkomen en niet noodzakelijk met derden te delen. De Minister kan via dit kanaal ongehinderd meeluisteren en cross-over data gebruiken via deze nieuwe bevoegdheden. Een van de grootste zorgen binnen de private sector. Het massaal verzamelen van bedrijfsgevoelige informatie door NCSC dient van geval tot geval bekeken te worden en alleen strikt noodzakelijk te zijn. Daarnaast dient de verzameling van data beperkt te worden tot een minimum (data minimization) voor een duidelijk en nauwkeurig omschreven doel, en de verzamelde gegevens dienen zo snel mogelijk vernietigd te worden. Dit zou gebaseerd moeten worden op dezelfde waarborgen waar de Wbp wel in voorziet zoals: proportionaliteit, beschikbaarheid, toegang, dataretentie, gebruik en geheimhouding van gegevens, ook wel aangeduid als de Data Life Cycle. Dit verzamelbegrip is in 2014 mede opgenomen in de, in samenspraak met de Europese Commissie (in het bijzonder DG Connect en DG Justice) en ENISA, door de Drafting Group van de EC Cloud Select Industry Group, opgestelde Cloud Service Level Agreement Standardisation Guidelines, en wordt eveneens verwerkt in de nieuwe ISO/IEC 19086 normen. Ons kantoor, Arthur's Legal is een van de experts van voornoemde Drafting Group, en is mede-auteur van voornoemde Guidelines en ISO/IEC normen. Kort gezegd dient het gebruik van informatie door NCSC getoetst en gedefinieerd te worden als onderdeel van de Data Life Cycle. Voor alsnog volgen de beveiligingswaarborgen voor de informatie verzameling onvoldoende uit het Wetsvoorstel. Alleen het noemen van de vertrouwelijkheid en verwijzen naar de Wbp is niet voldoende als men wil zorgen dat ICT inbreuken worden gemeld. Het spanningsveld tussen security en privacy wordt niet door de wetgeving weggenomen.
6.	**OVERHEID VS BEDRIJFSLEVEN**	De meldplicht ICT inbreuken dient gedragen te worden door de privaat-publieke samenwerking, waarbij gezocht wordt naar een goede balans tussen het melden en het vertrouwelijk omgaan met de informatie door NCSC. Door het intensiveren van deze samenwerking wordt de informatiepositie en de rol als kennis- en expertisecentrum van het NCSC verder versterkt, aldus de minister. Maar is een dergelijke overheidsinterventie wel te rechtvaardigen als dit om bedrijfsvertrouwelijke gegevens gaat en kan er dan wel worden gesproken over een samenwerking? De meeste aanbieders van vitale producten of diensten hebben al een verplichte sectorale meldplicht, bijvoorbeeld op basis van DNB of AFM. De minister beroept zich echter op zijn verantwoordelijkheid om de digitale weerbaarheid van de Nederlandse samenleving te versterken en maatschappelijke ontwrichting door uitvallen van vitale systemen te voorkomen, zonder 'filtering' door een toezichthouder. De minister wordt hierdoor als enige bevoegd in het kader van nationale veiligheid, waarbij er geen sprake is van een toetsing van de gegevens en data door een onafhankelijk orgaan. Dit is onwenselijk. Geen

		enkele wet mag natuurlijk nieuwe (Nederlandse) Prism/ Patriot Act en dataretentie issues veroorzaken. De grootste zorgen in de private sector voor cloudsecurity en cloud adoptie zijn dat de overheid ongehinderd kan mee-/afluisteren en het cross-over data gebruik van de overheid (nationaal en internationaal). Bovendien zijn de gevolgen voor reputatieschade, de benadeling van concurrentiepositie en de toegenomen kwetsbaarheid voor gerichte aanvallen aanzienlijk groot. Het is ook nog eens onvoorspelbaar of een meldplicht juist leidt tot het ontstaan van geruchten over de security en daardoor onnodig aanleiding geeft tot vermindering van vertrouwen van het publiek of de relevante markt. Dergelijke verstrekkende gevolgen in relatie tot de meldplicht kunnen verder impact hebben op de ondernemersvrijheid voor een aanbieder en andere markt- en bedrijfsbelangen. De vraag is dan ook of de Wetswijziging op deze manier wel het gewenste effect zal bereiken. De verwachting is bovendien dat de private sector de meldplicht wellicht niet eens zal nakomen. Kijkend naar een oplossing zijn er in omringende landen al verschillende best practices onderzocht, ontwikkeld en getest rondom dergelijke vraagstukken. Zo kent men in Canada een anonieme meldplicht voor datalekken en ICT inbreuken. Met als resultaat dat er meer inbreuken worden gemeld en daardoor al enkele ICT inbreuken zijn voorkomen. Hiermee worden de gevolgen van de meldplicht, zoals reputatieschade en het benadelen van de concurrentiepositie, beperkt. In de Verenigde Staten heeft Obama in de zomer van 2014 een onafhankelijk comité ingeschakeld, wat heeft onderzocht in hoeverre het post-9/11 staatsveiligheidbeleid zich verhoudt tot de Amerikaanse en universele grondrechten. Een groot deel van de aanbevelingen in het rapport over verbetering van de drempel voor het verzamelen van data, verbetering van de gerechtelijke toetsing van verzoeken, minimalisatie van data retentie, duur van dataretentie en transparantie is begin 2014 al doorgevoerd in wet- en regelgeving. Daarnaast is de Europese Commissie flink bezig met het standaardiseren van security normeringen voor ondersteunende elektronische diensten als cloud computing, en andere platforms. Voorbeelden als NIST, ISO/IEC, en de Cloud Service Level Agreement Standardisation Guidelines van de Europese Commissie zijn hiervoor een mooi uitgangspunt. Een andere oplossing is sectorale zelfregulering. Bijvoorbeeld de recente Automotive Privacy en data Security Principles, opgesteld door de marktleiders in de auto-industrie.
8.	CONCLUSIE	Cybersecurity is een complex samenspel van vraagstukken, overlappende spanningsvelden en conflicterende rechten en plichten. Het gaat hier niet alleen om de techniek, maar ook om menselijk gedrag, om de manier waarop organisaties met hun cybersecurity omgaan en om de psychische impact van cyberdreiging op maatschappelijk niveau. Deze spanningsvelden hebben, namelijk security, privacy, markt- en bedrijfsbelangen, andere (branche of andere) compliance regelgevingen, en natuurlijk scheiding der machten. Kortom, het gaat over een combinatie van mens, organisatie, techniek, proces en besturing.

		Het delen van best practices en de daarbij gemoeide inbreuken is van belang om een zo veilig mogelijk digitale maatschappij te kunnen waarborgen. Dit is echter op meerdere manieren in te kleden en hoeft niet altijd te worden opgelost door middel van wetgeving. Los van het feit dat dit niet de meest effectieve manier is, is het ook nog eens de meest ingrijpende manier kijkende naar het spanningsveld tussen security en privacy. Cyberbeveiliging mag in geen geval een excuus zijn voor de onbeperkte monitoring en analyse van persoonsgegevens zonder enige onafhankelijke toetsing op proportionaliteit, data minimization en geheimhouding daarvan. Dusdanige overheidsinterventie onder het mom van security en veiligheid van de maatschappij is niet rechtvaardig als de privacy waarborgen en de markt- en bedrijfsbelangen achterwege worden gelaten.

BCPA

Ministerie van Veiligheid en Justitie
Directie Wetgeving en Juridische Zaken
Postbus 20301
2500 EH Den Haag

Amsterdam, 4 maart 2015

Betreft: consultatie Wet gegevensverwerking en meldplicht cybersecurity

Geachte dames en heren,

Hierbij reageer ik namens BCPA naar aanleiding van het op 22 januari jl. gepubliceerde wetsvoorstel gegevensverwerking en meldplicht cybersecurity[1].

BCPA is een samenwerkingsverband van de in Nederland actieve dochterondernemingen van BT Group, Colt Technology Services en Verizon Enterprise Solutions. Deze aanbieders leveren wereldwijd netwerk- en IT-oplossingen aan multinationals, overheidsinstellingen en grote ondernemingen.

BCPA waardeert de uitbreiding van het wetsvoorstel met regels over de verwerking van persoonsgegevens door het NCSC en met regels over de verstrekking door het NCSC van vertrouwelijke gegevens aan derden. De aangebrachte verbeteringen hebben de kritiek van BCPA op het wetsvoorstel echter niet volledig kunnen wegnemen.

[1] 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

BCPA (Business Communication Providers Alliance) is een samenwerkingsverband tussen
BT Nederland N.V., COLT Technology Services B.V. en Verizon Nederland B.V.
op het gebied van regelgeving en toezicht.
Contact: mr N.C. van Veen, vanveen@bcpa.nl | + 31 (0)6 26 046900

De kritiek van BCPA betreft de volgende drie onderwerpen:

1. de onduidelijke reikwijdte van de meldplicht,
2. de lappendeken van meldplichten, en:
3. het nut van meldplichten in het algemeen.

Hieronder volgt een bespreking van deze onderwerpen.

1. De reikwijdte van de meldplicht

Wie moet melden?

De vitale aanbieders en de concrete producten en diensten, die onder het bereik van de verplichting komen te vallen, zullen worden aangewezen bij algemene maatregel van bestuur. BCPA wordt graag in de gelegenheid gesteld om zich uit te laten over de vraag welke producten en diensten in dit verband als vitaal moeten worden aangemerkt. De toelichting bij artikel 1 stelt terecht dat de meldplicht niet per se voor alle vitale aanbieders hoeft te gelden.

Wat moet worden gemeld?

De meldplicht ziet op een daadwerkelijke inbreuk op de veiligheid of een daadwerkelijk verlies van integriteit van een elektronisch informatiesysteem. De gekozen formulering biedt onvoldoende inzicht in de reikwijdte van de meldplicht. In de toelichting wordt een uitwerking aangekondigd. Zonder uitwerking hangt deze meldplicht in de lucht. BCPA stelt het op prijs dat de telecomsector bij de uitwerking zal worden betrokken. Gezien de haast die de minister kennelijk ervaart begrijpt BCPA niet goed waarom de uitwerking op zich laat wachten. Wij komen hier op terug.

2. Lappendeken van meldplichten

In de telecomsector is een wildgroei van meldplichten ontstaan. De toelichting stelt een efficiënte inrichting van processen in het vooruitzicht. Verschillende processen zullen worden gestroomlijnd. Een eerste bezwaar in dit verband is dat niet duidelijk wordt gemaakt hoe deze processen in de praktijk zullen worden vormgegeven. Aanbieders hebben behoefte aan heldere regels en processen. Zij moeten in een crisissituatie snel kunnen handelen. Het wetsvoorstel voorziet niet in deze behoefte.

Een tweede bezwaar is dat vooruit wordt gelopen op de EU-richtlijn over netwerk- en informatiebeveiliging (NIB-richtlijn). De noodzaak van een Nederlandse regeling, vooruitlopend op de EU-richtlijn, was van meet af aan afwezig. Volgens de minister kan niet worden gewacht op Europese besluitvorming. De haast die de minister kennelijk ervaart blijkt echter niet uit zijn tempo. Er zijn bijna vier jaren verstreken sinds de motie Hennis-Plasschaert werd aangenomen door de Tweede Kamer. De uitwerking van dit wetsvoorstel laat nog altijd op zich wachten. Kennelijk is de urgentie toch niet zo hoog. De urgentie is zeker niet zo hoog dat de EU-richtlijn niet kan worden afgewacht.

BCPA ziet een goede reden om wel te wachten op de EU-richtlijn: het belang van geharmoniseerde wetgeving binnen de Europese Unie. Dit belang wordt sterk gevoeld door aanbieders die internationaal opereren, zoals BT, Colt en Verizon. Wanneer dit belang uit het oog wordt verloren moeten deze aanbieders wegwijs proberen te worden in een lappendeken van verschillende cybersecurity meldplichten in verschillende EU-lidstaten. In Nederland was al een lappendeken van meldplichten inzake cybersecurity, continuïteit en datalekken ontstaan. Het wordt op deze manier steeds lastiger voor internationale aanbieders om te kunnen voldoen aan de vele verplichtingen.

BCPA pleit voor uitstel van de onderhavige meldplicht totdat de NIB-richtlijn van kracht zal zijn. Voorkomen moet worden dat de nu voorgestelde meldplicht al na korte tijd dient te worden gewijzigd.

3. Het nut van meldplichten

BCPA waardeert de ambitie van de rijksoverheid om de digitale veiligheid te vergroten. Het nut en de effectiviteit van de verschillende meldplichten zijn echter niet evident. BCPA pleit daarom voor een verplichte evaluatie van meldplichten en van de onderhavige meldplicht in het bijzonder. Op basis van de resultaten van een evaluatie moet worden besloten over de toekomst van meldplichten.

4. Conclusie

BCPA deelt de zorg van de overheid met betrekking tot de digitale veiligheid. De bevoegdheid om (aanvullende) meldplichten op te leggen moet niettemin terughoudend worden aangewend, met oog voor de effectiviteit van de verplichtingen. De vraag in hoeverre meldplichten daadwerkelijk effectief zijn moet nog worden beantwoord. Harmonisatie van verplichtingen binnen de EU is van groot belang.

Ik vertrouw erop u met het bovenstaande voldoende te hebben geïnformeerd. Deze reactie bevat geen vertrouwelijke informatie.

Met vriendelijke groet,

Niels van Veen,
secretaris BCPA

BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

Post Bits of Freedom
Postbus 10746
1001 ES Amsterdam

Bank 55 47 06 512
KvK 34 12 12 86

M
E
W https://www.bof.nl

Ivo Opstelten
Minister van Veiligheid en Justitie
Postbus 20301
2500 EH DEN HAAG

Betreft
Reactie op consultatie Wet gegevensverwerking en meldplicht cybersecurity

Amsterdam
6 maart 2015

Geachte minister Opstelten,

1. Graag reageert stichting Bits of Freedom op het wetsvoorstel voor gegevensverwerking en meldplicht cybersecurity.

2. Bits of Freedom ziet met vreugde dat dit wetsvoorstel op een aantal punten is verbeterd ten opzichte van het vorige wetsvoorstel over een meldplicht voor inbreuken op ICT-systemen dat werd voorgelegd ter consultatie.

3. In het bijzonder is het goed om te kunnen constateren dat de minister meerwaarde ziet in periodieke openbaring van meldingen over inbreuken op ICT-systemen.

4. Daarnaast is het goed dat het Nationaal Cyber Security Centrum (NCSC) nu ook de mogelijkheid krijgt om adequaat te handelen in situaties waarbij het NCSC de beschikking krijgt over (persoons)gegevens. Het NCSC is een organisatie die een grote meerwaarde heeft voor het verhogen van de Nederlandse digitale veiligheid. Daar hoort bij dat het NCSC ook voldoende is toegerust voor haar taken en dat het juridisch kader voor het NCSC wordt aangepast.

5. Bovenstaande neemt niet weg dat het voorstel op een aantal punten verbetering behoeft. In het vervolg zal Bits of Freedom deze punten behandelen

6. Het betreft daarbij met betrekking tot de meldplicht het openbaar maken van informatie over meldingen, de noodzaak van sanctie en toezicht op naleving van de meldplicht door het NCSC en het verruimen van de

reikwijdte van de meldplicht. Voor de gegevensverwerking door het NCSC zal worden ingegaan op een beperking van het verzoeken om persoonsgegevens door het NCSC. Daarbij zal eerst worden ingegaan op de meldplicht en vervolgens op de gegevensverwerking door het NCSC.

Meldplicht

Transparantie over meldingen is essentieel

7. Om goed inzicht te kunnen verkrijgen in de feitelijke dreigingen voor de ICT-systemen in de vitale sectoren is transparantie over het aantal meldingen, type incidenten, de impact daarvan en de opvolging naar aanleiding van deze meldingen van essentieel belang.

8. Deze cijfers leveren daarnaast een bijdrage aan een vergroot bewustzijn bij burger, bedrijf en de overheid. Deze cijfers kunnen inzichtelijk maken of de digitale weerbaarheid van de aanbieders in vitale sectoren is gegroeid. Mocht er sprake zijn van een daling van de digitale weerbaarheid, dan kunnen deze cijfers aanleiding geven tot versterking van die weerbaarheid door overheid of bedrijfsleven. Op deze wijze wordt er door het openbaar maken van informatie over de meldplicht bijgedragen aan een betere bescherming van de ICT-systemen in vitale sectoren en daarmee wordt ook het belang van de burger beter gediend.

9. De minister gaat in de toelichting op het wetsvoorstel in op onze eerdere aanbeveling[1] om informatie over de meldingen actief openbaar te maken.[2] Daarbij geeft hij aan dat artikel 9 van het wetsvoorsel, over de verstrekking van vertrouwelijke gegevens, daar niet aan in de weg staat. Ook geeft hij een positieve reactie op periodieke en gespecificeerde openbaarmaking, overigens zonder dat daarbij herleidbare informatie geopenbaard wordt[3] Bits of Freedom is blij met deze opmerkingen. Deze opmerkingen krijgen echter ten onrechte geen vervolg in het wetsvoorstel zelf.

10. Zoals hierboven aangegeven levert een actieve openbaarmaking een effectieve bijdrage aan bewustwording en verbetering van de bescherming van ICT-systemen. Het is daarom belangrijk om in het wetsvoorstel een bepaling op te nemen over het actief periodiek, bijvoorbeeld per kwartaal, openbaarmaken van informatie over de meldplicht.

> Bits of Freedom adviseert om een bepaling in het wetsvoorstel op te nemen over periodieke openbaarmaking van gegevens over het aantal inbreuken per sector, de aard en de impact daarvan, en de opvolging naar aanleiding van deze meldingen.

1 Zie de reactie van Bits of Freedom op de consultatie Wetsvoorstel melding inbreuken elektronische informatiesystemen, p. 5.
2 Toelichting op het voorliggende wetsvoorstel, p. 10.
3 Toelichting op het voorliggende wetsvoorstel, p. 15.

Toezicht en sanctionering is noodzakelijk

11. Het belang van de meldplicht is groot. Het is dan ook van wezenlijk belang dat aan de meldplicht wordt voldaan. Om een effectieve meldplicht te garanderen is toezicht op en sanctionering van het niet nakomen van die meldplicht volgens Bits of Freedom noodzakelijk.[4] De minister is echter van mening dat sanctie en toezicht niet noodzakelijk is, mede omdat de noodzaak van delen van incidenten op dit moment kennelijk breed gedragen wordt.[5]

12. Toezicht op het nakomen van de meldplicht en eventuele sanctionering hoeft geen verandering te brengen in de bestaande praktijk. Voor de bedrijven die nu al de noodzaak van de meldplicht zien en zich aan de meldplicht houden, zal niets veranderen. Het is daarentegen wel een noodzakelijke drijfveer voor de bedrijven die de meldplicht niet op prijs stellen en voor bedrijven die de beveiliging van hun ICT-systemen niet op orde hebben.

13. Daarnaast zijn er, mocht in de toekomst de noodzaak van delen niet meer breed gedragen worden, voldoende waarborgen aanwezig zijn om de meldplicht effectief te laten functioneren. Wetgeving hoeft immers niet alleen gebaseerd te zijn op de praktijk van vandaag, maar moet rekening houden met gewijzigde situaties in de toekomst. Dat geldt zeker voor wetgeving over aanbieders van vitale diensten.

14. Een ander argument om nu toezicht en sanctionering op naleving van de meldplicht mogelijk te maken, hangt samen met de NIB-richtlijn. Zoals de minister zelf al aangeeft, is het mogelijk dat op grond van de NIB-richtlijn toezicht en sanctionering op naleving van de meldplicht moet worden ingevoerd. Nederland zou vooruit zou lopen op toekomstige Europese verplichtingen door nu vast toezicht en sanctionering toe te voegen aan dit wetsvoorstel. Het zou tevens consistent zijn; bij de meldplicht datalekken is bewust gekozen om vooruit te lopen op mogelijke Europese verplichtingen. Er is geen reden om dat hier niet ook te doen.

15. Vooruitlopen op Europese ontwikkelingen heeft in dit geval nog een extra voordeel: door toezicht en sanctionering nu bij dit wetsvoorstel integraal te regelen, worden implementatiekosten voor overheid en bedrijfsleven in de toekomst een stuk lager.

4 Zie de reactie van Bits of Freedom op de consultatie Wetsvoorstel melding inbreuken elektronische informatiesystemen, p. 1 en 2.
5 Aldus de minister op p. 8 van de toelichting bij deze wet.

Het toezicht moet bij het NCSC komen

16. Zoals Bits of Freedom eerder al bepleitte, moet toezicht op de naleving en de mogelijkheid om sancties op te leggen bij niet-naleving van de meldplicht bij het NCSC belegd worden.[6]

17. De minister geeft in de toelichting bij deze wet aan dat als op grond van de NIB-richtlijn een meldplicht en sanctie bij niet nakoming van de meldplicht verplicht wordt gesteld, hij voornemens is toezicht op naleving van de meldplicht en sanctionering bij de sectorale toezichthouders neer te leggen.[7]

18. Hier ontstaat de vreemde situatie dat de organisatie die de melding moet ontvangen niet kan controleren of de meldplicht is nageleefd en niet kan sanctioneren bij niet-naleving. Tegelijkertijd ontstaat ook voor de sectorale toezichthouder een vreemde situatie. Deze zal toezicht moeten houden op een meldplicht terwijl de melding niet bij hem ingediend hoeft te worden.

19. Deze situatie is onwenselijk. Meldplicht, toezicht en sanctie zouden in één hand moeten liggen. Als het NCSC verantwoordelijk is voor het ontvangen van de melding, dan moet het NCSC ook toezicht kunnen houden en eventueel sancties kunnen uitdelen als de meldplicht niet wordt nageleefd.

> Bits of Freedom adviseert om een sanctie op te nemen voor het niet nakomen van de meldplicht. Daarnaast moet het NCSC worden aangewezen als toezichthouder op het naleven van de meldplicht.

Reikwijdte meldplicht moet ruimer worden

20. Het ministerie heeft, anders dan Bits of Freedom eerder bepleitte[8], ten onrechte ervoor gekozen om DDoS-aanvallen niet onder de meldplicht te brengen. De meldplicht moet bijdragen aan het "voorkomen of beperken van onderbrekingen van de beschikbaarheid of betrouwbaarheid"[9] van diensten van aanbieders in vitale sectoren. DDoS-aanvallen kunnen die beschikbaarheid eveneens ernstig inperken.

21. Wanneer een DDoS-aanval plaatsvindt bij een dienst in een vitale sector, kan dat grote consequenties hebben en eventueel kunnen leiden tot maatschappelijke ontwrichting. Bij de recente DDoS-aanval op bedrijf Prolocation is de site van de Rijksoverheid vrijwel de hele dag platgelegd. In de toekomst zal nog veel meer dienstverlening alleen nog digitaal verlopen. Dat zal ook gelden voor diensten uit vitale sectoren. Een DDoS-aanval kan

6 Zie de reactie van Bits of Freedom op de consultatie Wetsvoorstel melding inbreuken elektronische informatiesystemen, p. 2 en 3.
7 Toelichting op het voorliggende wetsvoorstel, p. 6.
8 Zie de reactie van Bits of Freedom op de consultatie Wetsvoorstel melding inbreuken elektronische informatiesystemen, p. 3.
9 Toelichting op het voorliggende wetsvoorstel, p. 2.

dan grote, ontwrichtende schade aanrichten als die dienst niet bereikbaar is. Een snelle, verplichte melding kan dan cruciaal zijn.

22. Het verdient daarom aanbeveling om die DDoS-aanvallen die wel tot maatschappelijke ontwrichting kunnen leiden wel onder de meldplicht te brengen, zodat het NCSC desgewenst ondersteuning kan bieden en een bijdrage kan leveren aan het beperken van eventuele maatschappelijke ontwrichting.

> Bits of Freedom adviseert om DDoS-aanvallen die zorgen voor beperkingen in de beschikbaarheid van een dienst op te nemen in de meldplicht.

Gegevensverwerking

23. Het is goed dat de wettelijke grondslag voor de taken van het NCSC en de grondslag voor gegevensverwerking door het NCSC beter verankerd wordt, zeker wanneer die gegevensverwerking betrekking heeft op persoonsgegevens. Toch is er een aantal onduidelijkheden die Bits of Freedom graag opgehelderd ziet.

24. Het is niet duidelijk waar de grenzen liggen van de voorgestelde bevoegdheid voor het NCSC om te verzoeken om gegevens te verstrekken. Artikel 4 van het wetsvoorstel geeft het NCSC de mogelijkheid om "eenieder" te verzoeken gegevens te verstrekken. Daaronder moeten ook persoonsgegevens worden verstaan.[10] Artikel 4 is dus niet beperkt tot verzoeken aan vitale aanbieders of publiekrechtelijke organisaties. Uit de toelichting blijkt niet duidelijk waarom het verzoek om gegevens te verstrekken aan eenieder gericht zou moeten kunnen worden. Daarnaast is er geen begrenzing in de aard van de gegevens die opgevraagd zouden kunnen worden.

25. Bits of Freedom acht het voor de controleerbaarheid noodzakelijk dat het beleid voor verzoeken op basis van artikel 4 zo wordt ingericht dat onder meer inzichtelijk is hoeveel verzoeken er door het NCSC wordt gedaan en aan wie die verzoeken zijn gericht. Dat is extra belangrijk omdat ontvangers van het verzoek weliswaar niet verplicht zijn mee te werken, maar daar mogelijk niet van op de hoogte zijn en zich toch verplicht voelen om mee te werken.

26. Daarnaast wordt uit het wetsvoorstel en de toelichting niet duidelijk hoe de verstrekking van deze verkregen informatie aan derden ingeperkt gaat

10 Toelichting op het voorliggende wetsvoorstel, p. 8.

worden. Zoals Bits of Freedom het begrijpt, valt verdere verwerking van de verkregen informatie niet noodzakelijkerwijs onder artikel 9 van het wetsvoorstel. Het zou goed zijn om nader aandacht te besteden aan de inperking van de verdere verspreiding van de op grond van artikel 4 van het wetsvoorstel verkregen informatie.

> Bits of Freedom adviseert om de reikwijdte van artikel 4 van het wetsvoorstel in te perken.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd. Uiteraard ben ik graag bereid om het bovenstaande nader toe te lichten, mocht daaraan behoefte bestaan.

Hoogachtend,

Ton Siedsma

COLLEGE BESCHERMING PERSOONSGEGEVENS

POSTADRES Postbus 93374, 2509 AJ Den Haag BEZOEKADRES Juliana van Stolberglaan 4-10
TEL 070 - 88 88 500 FAX 070 - 88 88 501 INTERNET www.cbpweb.nl www.mijnprivacy.nl

AAN De minister van Veiligheid en Justitie
De heer mr. G.A. van der Steur
Postbus 20301
2500 EH DEN HAAG

DATUM 18 mei 2015
ONS KENMERK z2015-00056
CONTACTPERSOON

UW BRIEF VAN 22 januari 2015
UW KENMERK 609292

ONDERWERP Advies conceptwetsvoorstel gegevensverwerking en meldplicht cybersecurity

Geachte heer Van der Steur,

Bij brief van 22 januari 2015 heeft het Ministerie van Veiligheid en Justitie het College bescherming persoonsgegevens (CBP) gevraagd, op grond van het bepaalde in artikel 51, tweede lid van de Wet bescherming persoonsgegevens (Wbp) te adviseren over het concept wetsvoorstel gegevensverwerking en meldplicht cybersecurity. Op dat moment stond het wetsvoorstel ook open voor commentaar op het internet.

Het CBP voldoet hiermee aan uw verzoek en heeft het naar aanleiding van de tweede internetconsultatie gewijzigde concept wetsvoorstel, dat het CBP op 1 mei jl. van u heeft ontvangen, daarbij als uitgangspunt genomen.

(Korte) inhoud van het wetsvoorstel

De adviesaanvraag betreft het volgende voorstel:

- De meldplicht voor ernstige ICT-inbreuken (artikel 5 tot en met 8).
- De omschrijving van de taken van de minister van Veiligheid en Justitie "ter voorkoming of beperking van het uitvallen van de beschikbaarheid of het verlies van integriteit van informatiesystemen van vitale aanbieders, en van andere aanbieders die onderdeel zijn van de rijksoverheid, en ter verdere versterking van de digitale weerbaarheid van de Nederlandse samenleving" (artikel 2, eerste lid) en "ter voorkoming van nadelige maatschappelijke gevolgen" (artikel 2, tweede lid).
- Algemene bepalingen met betrekking tot de verwerking van persoonsgegevens ten behoeve van de in artikel 2 genoemde doeleinden en taken (artikel 3).
- De bevoegdheid tot het verzoeken om verstrekking van gegevens: "Onze Minister kan een rechtspersoon of een orgaan daarvan verzoeken om gegevens te verstrekken die redelijkerwijs nodig zijn voor de vervulling van de in artikel 2 genoemde taken" (artikel 4, eerste lid) waarbij artikel 9 Wbp niet van toepassing is op het verstrekken van persoonsgegevens ingevolge een dergelijk verzoek (artikel 4, tweede lid).
- Regels voor (door)verstrekking van vertrouwelijke informatie door de minister van Veiligheid en Justitie (artikel 9).

BIJLAGEN 1
BLAD 1

COLLEGE BESCHERMING PERSOONSGEGEVENS

DATUM 18 mei 2015
ONS KENMERK z2015-00056

Samenvatting van het advies

Bovengenoemd concept wetsvoorstel geeft het CBP aanleiding tot het maken van de volgende op- en aanmerkingen.

1. ***De 'grondrechtentoets' is onvoldoende onderbouwd, en het voorstel bevat onvoldoende passende waarborgen***

De memorie van toelichting stelt dat het NCSC weliswaar grote aantallen persoonsgegevens verwerkt, maar dat het gelet op de aard daarvan (IP- en e-mailadressen en domeinnamen) niet gaat om een forse inmenging in het respect voor iemands privéleven. Echter: ook op het verwerken van IP- en e-mailadressen en domeinnamen zijn de regels uit de Wbp van toepassing. Verder kan het NCSC wel degelijk de beschikking krijgen over (omvangrijke hoeveelheden) bijzondere persoonsgegevens. Een dergelijke gebeurtenis (de verkrijging van een omvangrijke hoeveelheid gegevens die afkomstig was uit het Pobelka-botnet) was mede aanleiding voor het opstellen van dit voorstel. Deze omstandigheid dient niet alleen betrokken te worden in de grondrechtentoets, maar stelt bovendien zwaardere eisen aan de te treffen waarborgen.

Bij de belangenafweging wordt niet voldoende inzichtelijk gemaakt welke passende waarborgen er met betrekking tot de bescherming van de persoonlijke levenssfeer in acht worden genomen. Het voorstel creëert slechts enkele waarborgen met betrekking tot de verstrekking door het NCSC van vertrouwelijke gegevens, en dan met name vertrouwelijke gegevens die tot een afzonderlijke aanbieder kunnen worden herleid. Voor het overige wordt er verwezen naar algemene gegevensbeschermingsbeginselen uit de Wbp die worden gevolgd bij het verwerken van persoonsgegevens, naar het toezicht door de Functionaris voor de Gegevensbescherming (FG) van het ministerie van Veiligheid en Justitie en het externe toezicht door het CBP.

Gelet op de verwerking van bijzondere persoonsgegevens alsmede het buiten toepassing verklaren van het doelbindingsbeginsel en de geheimhoudingsplicht uit de Wbp, is het treffen van extra waarborgen in dit kader essentieel.

2. ***Het voorstel is onvoldoende bepaald***

Relevante begrippen zoals 'vertrouwelijke gegevens', 'vitaal belang', 'vitale aanbieder', 'onverwijld kennis [geven]' en 'in belangrijke mate' worden in het voorstel niet (voldoende) gedefinieerd. De reikwijdte van het voorstel is onduidelijk, aangezien zowel de groep van 'vitale aanbieders' waarop de meldplicht betrekking heeft als de te verstrekken gegevens bij Algemene Maatregel van Bestuur (AMvB) worden aangewezen (waarbij de aanbieders ook kunnen behoren tot een categorie die bij AMvB wordt aangewezen).
Ook (een deel van) de groep van ontvangers van de gegevens is onbepaald. In dit licht verdient artikel 2, lid 2 van het voorstel de aandacht. De minister kan gegevens verstrekken ter

voorkoming van nadelige maatschappelijke gevolgen aan niet nader omschreven "organisaties die tot taak hebben om andere organisaties of het publiek daarover te informeren".

3. ***Het buiten toepassing verklaren van artikel 9 Wbp creëert in de praktijk onduidelijkheden en dilemma's, en noodzakelijke randvoorwaarden ontbreken***

Artikel 9 Wbp heeft betrekking op twee gegevensbeschermingsbeginselen: het doelbindingsbeginsel en de geheimhoudingsplicht. Artikel 43 Wbp voorziet op dit moment al in een mogelijkheid om het doelbindingsbeginsel buiten toepassing te laten voor zover een zwaarwegend algemeen belang dit noodzakelijk maakt. Dit hoeft dus niet in het voorstel te worden geregeld.

Een specifieke onderbouwing voor het buiten toepassing verklaren van artikel 9 Wbp ontbreekt. Bovendien kan artikel 9 Wbp vanzelfsprekend alleen maar buiten toepassing worden gelaten als daaraan een concrete belangenafweging voorafgaat, en ook deze belangenafweging ontbreekt in het wetsvoorstel. De bevoegdheid tot het verzoeken om verstrekking van gegevens uit artikel 4, eerste lid, van het voorstel is vrijblijvend. Dit maakt het buiten toepassing verklaren van artikel 9 Wbp vrijwel betekenisloos: de rechtspersonen (overheden of private partijen) of organen daarvan die om gegevens worden gevraagd, kunnen zonder opgaaf van redenen weigeren om deze te verstrekken. Wel kan het buiten toepassing verklaren van artikel 9 Wbp de indruk wekken dat deze informatie-'plicht' dwingender is dan deze in feite is.

Het is de vraag of het voorstel in zijn huidige vorm voldoende basis biedt aan verantwoordelijken en bewerkers om het NCSC toegang te geven tot persoonsgegevens, of om persoonsgegevens te verstrekken aan het NCSC. Naast de geheimhoudingsplicht uit hoofde van ambt, beroep of wettelijk voorschrift uit het vierde lid van artikel 9 Wbp, is ook de geheimhoudingsplicht uit artikel 12 Wbp van toepassing.

Dictum

Het CBP heeft bezwaar tegen het concept voorstel van wet en adviseert u dit niet aldus in te dienen.

Aanvullende opmerking

De memorie van toelichting bij het voorstel geeft aan dat er een samenloop kan ontstaan tussen de meldplicht uit het voorstel en de meldplicht datalekken. Daarbij wordt opgemerkt 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 de processen efficiënt in te richten."
Het gaat hier om ongelijksoortige meldplichten met uiteenlopende doelstellingen, waarbij de meldingen moeten worden gedaan bij verschillende instanties die ieder hun eigen rol en taak hebben. Het is dan ook zeer de vraag in hoeverre nodeloze administratieve lasten op de hierboven

beschreven wijze daadwerkelijk kunnen worden voorkomen. Met name voor de telecomsector kan er een samenloop van meldplichten ontstaan.

Het volledige advies treft u in de bijlage aan. Het CBP verneemt graag op welke wijze u gevolg geeft aan het advies. Het CBP is beschikbaar indien nadere toelichting is vereist.

Het CBP vertrouwt erop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,
Het College bescherming persoonsgegevens,
Voor het College,

Mr. W.B.M. Tomesen
Lid van het College

Bijlage bij de brief van het College bescherming persoonsgegevens van 18 mei 2015

Advies van het College bescherming persoonsgegevens (CBP) over het concept wetsvoorstel gegevensverwerking en meldplicht cybersecurity.

Bij brief van 22 januari 2015 heeft uw ambtsvoorganger, de minister van Veiligheid en Justitie de heer mr. I.W. Opstelten, het College bescherming persoonsgegevens (CBP) gevraagd op grond van het bepaalde in artikel 51, tweede lid van de Wet bescherming persoonsgegevens (Wbp) te adviseren over het conceptwetsvoorstel gegevensverwerking en meldplicht cybersecurity (hierna: het voorstel).[1]

Tot en met 6 maart 2015 was het voorstel opengesteld voor consultatie op het internet. Op 1 mei 2015 heeft het CBP het gewijzigde wetsvoorstel en de memorie van toelichting ontvangen. Deze gewijzigde versie is als uitgangspunt genomen bij onderstaande advisering.

Het voorstel introduceert een meldplicht voor ernstige ICT-inbreuken. Deze meldplicht geldt alleen voor aanbieders van producten of diensten waarvan de beschikbaarheid of betrouwbaarheid van vitaal belang is voor de Nederlandse samenleving. In de versie van 22 januari 2015 zijn deze aanbieders niet nader omschreven. In de versie van het wetsvoorstel van 1 mei 2015 wordt in artikel 1 nader gespecificeerd dat het bij een aanbieder kan gaan om een overheidsorganisaties of om een privaatrechtelijke rechtspersoon.
Ook stelt het voorstel regels over het verwerken van gegevens ten behoeve van de in het wetsvoorstel nader omschreven taken van de minister van Veiligheid en Justitie op het terrein van cybersecurity. In de versie van 22 januari 2015 wordt de doelgroep van het NCSC niet expliciet omschreven. In de aangepaste versie van 1 mei 2015 omschrijft de memorie van toelichting op p. 8 de doelgroep als de vitale aanbieders (overheid en private sector) en alle aanbieders (vitaal en niet-vitaal) die deel uitmaken van de rijksoverheid.

1. Voorgeschiedenis

In 2011 werd in de motie Hennis-Plasschaert c.s. gevraagd om een meldplicht voor organisaties die betrokken zijn bij voor de samenleving vitale informatiesystemen. Aanleiding was de elektronische inbraak bij het bedrijf DigiNotar. In de motie werd de regering gevraagd om ervoor te zorgen dat de melding bij het Nationaal Cyber Security Centrum (NCSC) zou worden gedaan, en het NCSC vervolgens ook aan te wijzen als verantwoordelijke voor de coördinatie van de opvolging van de melding.[2] In een brief aan de Tweede Kamer van 6 juli 2012 zegde de minister dit toe.[3]

---

[1] http://www.internetconsultatie.nl/cybersecurity.
[2] Kamerstukken II 2011/12, 26643, nr. 202. Het NCSC valt organisatorisch onder de Nationaal Coördinator Terrorismebestrijding en Veiligheid van het ministerie van Veiligheid en Justitie en is gestoeld op publiek-private samenwerking.
[3] Kamerstukken II 2011/12, 26643, nr. 247.

In 2012 kreeg het ICT-beveiligingsbedrijf Digital Investigation via een hosting provider de beschikking over een omvangrijke hoeveelheid gegevens, die afkomstig was uit het zogenoemde Pobelka-botnet. Het gedeelte van de dataset dat nodig was om respons naar de Rijksoverheid en de vitale sectoren mogelijk te maken, bestaande uit de IP-adressen, de computernamen en de tijdstippen waarop de geïnfecteerde computers actief waren binnen het botnet, is doorgegeven aan het NCSC. In een brief aan de Tweede Kamer schrijft de minister hierover: "Het NCSC had geen rechtsbasis om de resterende inhoudelijke en mogelijk gevoelige gegevens in te zien en te verwerken. De informatie was immers oorspronkelijk afkomstig van een misdrijf en bevatte persoonlijke gegevens en informatie waarvan de betrouwbaarheid en herkomst niet kon worden vastgesteld. Tevens stond niet vast stond hoe Digital Investigation deze informatie had verkregen." In dezelfde brief kondigt de minister aan dat zal worden verkend "hoe het NCSC op een zorgvuldige wijze kan omgaan met de informatie die het NCSC vanuit de ICT-community bereikt. Daarbij zal worden gekeken hoe en op welke rechtsbasis het NCSC gegevens kan verwerken om de impact van dreigingen in het digitale domein op de nationale veiligheid te beperken. Het betreft daarbij informatie die mogelijk de persoonlijke levenssfeer raakt."[4] In een brief aan de Tweede Kamer uit december 2013 geeft de minister de uitkomsten van de toegezegde juridische verkenning weer. Uitkomst is enerzijds dat er voor de huidige verwerking van persoonsgegevens een afdoende wettelijke grondslag voorhanden is, maar dat het anderzijds, met het oog op de toekomst, aangewezen is om de taken in het kader waarvan persoonsgegevens worden verwerkt alsmede de bevoegdheid tot die verwerking van een steviger wettelijke grondslag te gaan voorzien. In dezelfde brief gaat de minister ook in op het waarborgen van de vertrouwelijkheid van de gegevens die aan het NCSC worden verstrekt, en op de naleving van de adviezen die door het NCSC worden gegeven. Deze onderwerpen worden in de brief beschreven en in het voorstel nader geconcretiseerd[5]

Voor een eerdere versie van het voorstel werd in de tweede helft van 2013 een internetconsultatie uitgevoerd.[6] Deze eerdere versie, toen bekend als de 'Wet melding inbreuken elektronische informatiesystemen', had uitsluitend betrekking op een meldplicht voor ernstige ICT-inbreuken. Aangezien deze versie slechts zijdelings betrekking had op de verwerking van persoonsgegevens heeft het CBP over deze versie geen advies uitgebracht.

2. Inhoud

De belangrijkste elementen uit het voorstel zijn:

- De meldplicht voor ernstige ICT-inbreuken (artikel 5 tot en met 8).
- De omschrijving van de taken van de minister van Veiligheid en Justitie "ter voorkoming of beperking van het uitvallen van de beschikbaarheid of het verlies van integriteit van

[4] Kamerstukken II 2012/13, 26643, nr. 268.
[5] Kamerstukken II 2013/14, 26643, nr. 297.
[6] http://www.internetconsultatie.nl/meldplicht_ict_inbreuken.

informatiesystemen van vitale aanbieders, en van andere aanbieders die onderdeel zijn van de rijksoverheid, en ter verdere versterking van de digitale weerbaarheid van de Nederlandse samenleving" (artikel 2, eerste lid) en "ter voorkoming van nadelige maatschappelijke gevolgen" (artikel 2, tweede lid).
- Algemene bepalingen met betrekking tot de verwerking van persoonsgegevens ten behoeve van de in artikel 2 genoemde doeleinden en taken (artikel 3).
- De bevoegdheid tot het verzoeken om verstrekking van gegevens: "Onze Minister kan een rechtspersoon of een orgaan daarvan verzoeken om gegevens te verstrekken die redelijkerwijs nodig zijn voor de vervulling van de in artikel 2 genoemde taken" (artikel 4, eerste lid) waarbij artikel 9 Wbp niet van toepassing is op het verstrekken van persoonsgegevens ingevolge een dergelijk verzoek (artikel 4, tweede lid).
- Regels voor (door)verstrekking van vertrouwelijke informatie door de minister van Veiligheid en Justitie (artikel 9).

3. Algemene opmerkingen

Het voorstel is in een aantal opzichten onbepaald. In de Aanwijzingen voor de regelgeving (Circulaire van de Minister President van 19 november 1992) zijn hiervoor nadere regels gesteld, zie met name Aanwijzing 22, 54 en 121.

- Een belangrijk begrip in het wetsvoorstel is de zogenoemde "vitale aanbieder", die in het conceptwetsvoorstel wordt gedefinieerd als een "aanbieder van een product of dienst waarvan de beschikbaarheid en betrouwbaarheid van vitaal belang zijn voor de Nederlandse samenleving".[7] Een nadere definiëring ontbreekt.[8]
- De (categorieën van) vitale aanbieders voor wie de meldplicht geldt zullen bij algemene maatregel van bestuur worden aangewezen, met daarbij de (categorieën van) producten en diensten waarvoor de meldplicht geldt.[9] De memorie van toelichting geeft daarbij aan dat de aanwijzing in ieder geval zal 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), en dat daarbij te denken valt aan vitale aanbieders zoals energienetwerkbeheerders, drinkwaterbedrijven, telecombedrijven, beheerders van hoofdwaterkeringen of banken.[10] Het voorgaande betekent dat de groep van vitale aanbieders voor wie de meldplicht geldt op dit moment nog niet definitief is vastgesteld.

---

[7] Artikel 1 van het voorstel.

[8] Het CBP gaat er van uit dat hier wordt gerefereerd aan het gedachtegoed rond de vitale infrastructuur, waarbinnen een aantal vitale sectoren / producten en diensten worden aangewezen met daarbij een verantwoordelijke minister, zoals weergegeven in de brochure 'Vitale sectoren infrastructuur', http://www.rijksoverheid.nl/documenten-en-publicaties/brochures/2010/06/25/vitale-sectoren-infrastructuur.html.

[9] Artikel 5 van het voorstel.

[10] Memorie van toelichting bij het voorstel, pagina 3.

- Een vitale aanbieder voor wie de meldplicht geldt wordt geacht "onverwijld kennis [te geven] van een inbreuk op de veiligheid of een verlies van integriteit van zijn informatiesysteem waardoor de beschikbaarheid of betrouwbaarheid van een product of dienst in belangrijke mate wordt of kan worden onderbroken."[11] De kwalificatie "onverwijld" wordt in het voorstel of in de memorie van toelichting niet nader toegelicht. Met betrekking tot "in belangrijke mate" geeft de memorie van toelichting aan dat op basis van overleg met de betrokken sectoren en departementen nader zal worden uitgewerkt, en bijvoorbeeld in beleidsregels vastgelegd, wat hier voor de verschillende betrokken producten en diensten onder moet worden verstaan.[12]
- Het voorstel 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 memorie van toelichting van 22 januari en 1 mei 2015 geven beiden aan dat het NCSC deze taken uitvoert. De wetsteksten van 22 januari 2015 en 1 mei 2015 vermelden daartoe 'onze minister [van Veiligheid en Justitie]'. De aangepaste memorie van toelichting van 1 mei 2015 vermeldt dat ingevolge de huidige portefeuilleverdeling het de staatssecretaris betreft en dat waar de memorie van toelichting de rol van het NCSC bespreekt, gedoeld wordt op de uitvoering van de taken en bevoegdheden van de staatssecretaris. Uit de voorgestelde wetstekst blijkt dit echter niet.

De regels die het voorstel stelt zijn in een aantal opzichten vrijblijvend:

- Er staan geen sancties op het niet nakomen van de meldplicht. Verwacht wordt dat de doelgroep nut en noodzaak van de meldplicht inziet en deze spontaan na zal leven.[13]
- Behalve een meldplicht omvat het voorstel ook een informatie-'plicht': het voorstel voorziet in een wettelijke bevoegdheid voor het NCSC om rechtspersonen (overheden of private partijen) of organen daarvan om gegevens te vragen die nodig zijn voor de uitoefening van de in het voorstel genoemde taken. Het voorstel voorziet niet in een bevoegdheid om gegevens te vorderen, en de organisatie of het orgaan waaraan het verzoek is gericht is niet verplicht tot medewerking.[14]

4. Beoordeling

Het wetsvoorstel geeft het CBP aanleiding tot het maken van de volgende op- en aanmerkingen.

[11] Artikel 6, eerste lid, van het voorstel.
[12] Memorie van toelichting bij het voorstel, pagina 26.
[13] Memorie van toelichting bij het voorstel, pagina 7.
[14] Memorie van toelichting bij het voorstel, pagina 25.

1. *De 'grondrechtentoets' is onvoldoende onderbouwd, en het voorstel bevat onvoldoende passende waarborgen*

Artikel 8 van het Europees verdrag voor de Rechten van de Mens (EVRM) staat inmenging van enig openbaar gezag in het recht op respect voor iemands privé-, familie- en gezinsleven uitsluitend toe voor zover deze "bij wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen."[15]
Artikel 10 van de Grondwet scherpt deze bepaling aan en verlangt voor elke beperking een grondslag in de formele wet. Voor een wettelijke beperking van het voornoemde grondrecht gelden ook materiële eisen. Het voorschrift zal voldoende nauwkeurig moeten zijn en adequate en effectieve waarborgen moeten bevatten tegen ongeoorloofde inbreuken. Voorts is een beperking van het recht op privacy slechts toegestaan indien deze in een democratische samenleving noodzakelijk is in het belang van "de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen."
Volgens vaste jurisprudentie van het Europese Hof voor de rechten van de mens betekent dit dat de beperking moet worden gerechtvaardigd door een zwaarwegend algemeen belang en in overeenstemming moet zijn met de beginselen van proportionaliteit (de beperking mag niet onevenredig zijn in verhouding tot het nagestreefde doel) en subsidiariteit (het nagestreefde doel moet niet op een voor de burger minder ingrijpende wijze kunnen worden bereikt).
In dit licht verdient de (door)verstrekking door de minister aan de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en aan de aangewezen computercrisisteams uit het tweede lid van artikel 9 de aandacht. Deze verstrekking kan al plaatsvinden indien dat ter uitvoering van de in artikel 2 genoemde taken "dienstig" is. In het licht van artikel 8 EVRM dient het te gaan om een dringend publiek belang.
Bovengenoemde vereisten moeten in hun onderlinge samenhang gelezen worden. Het proportionaliteitsvereiste is hierbij van wezenlijk belang. Naarmate de inbreuk op de privacy groter is - bijvoorbeeld doordat het gaat om gevoelige gegevens of tussen de taken van de verstrekker en de ontvanger slechts een beperkte verwantschap bestaat (inbreuk op het principe van doelbinding) - zal het belang van de gegevensverstrekking in het licht van het doel van de betrokken regeling concreter moeten worden aangetoond.

De memorie van toelichting stelt dat het NCSC weliswaar grote aantallen persoonsgegevens verwerkt, maar dat het gelet op de aard daarvan (IP- en e-mailadressen en domeinnamen) niet gaat om een forse inmenging in het respect voor iemands privéleven.[16] Echter: ook op het verwerken van IP- en e-mailadressen en domeinnamen zijn de regels uit de Wbp van toepassing.

---

[15] Artikel 8, tweede lid, EVRM.

[16] Memorie van toelichting bij het voorstel, pagina 22.

Verder kan het NCSC wel degelijk de beschikking krijgen over (omvangrijke hoeveelheden) bijzondere persoonsgegevens. Een dergelijke gebeurtenis (de verkrijging van een omvangrijke hoeveelheid gegevens die afkomstig was uit het Pobelka-botnet) was mede aanleiding voor het opstellen van dit voorstel.[17] Deze omstandigheid dient niet alleen betrokken te worden in de grondrechtentoets, maar stelt bovendien zwaardere eisen aan de te treffen waarborgen.
Bij de belangenafweging wordt niet voldoende inzichtelijk gemaakt welke passende waarborgen er met betrekking tot de persoonlijke levenssfeer in acht worden genomen. Het voorstel creëert slechts enkele waarborgen met betrekking tot de verstrekking door het NCSC van vertrouwelijke gegevens, en dan met name vertrouwelijke gegevens die tot een afzonderlijke aanbieder kunnen worden herleid. Voor het overige wordt er verwezen naar algemene gegevensbeschermingsbeginselen uit de Wbp die worden gevolgd bij het verwerken van persoonsgegevens, naar het toezicht door de Functionaris voor de Gegevensbescherming (FG) van het ministerie van Veiligheid en Justitie en het externe toezicht door het CBP.[18] Gelet op de verwerking van bijzondere persoonsgegevens alsmede het buiten toepassing verklaren van het doelbindingsbeginsel en de geheimhoudingsplicht uit de Wbp, is het treffen van extra waarborgen in dit kader essentieel.

2. *Het voorstel is onvoldoende bepaald*

Relevante begrippen zoals 'vertrouwelijke gegevens', 'vitaal belang' en 'vitale aanbieder' worden in het voorstel niet (voldoende) gedefinieerd. De reikwijdte van het voorstel is onduidelijk, aangezien zowel de groep van 'vitale aanbieders' waarop de meldplicht betrekking heeft als de te verstrekken gegevens bij Algemene Maatregel van Bestuur (AMvB) worden aangewezen (waarbij de aanbieders ook kunnen behoren tot een categorie die bij AMvB wordt aangewezen).
Ook (een deel van) de groep van ontvangers van de gegevens is onbepaald. In dit licht verdient artikel 2, lid 2 van het voorstel de aandacht. De minister kan gegevens verstrekken ter

---

[17] In zijn 'Nadere analyse Pobelka botnet' van 18 maart 2013 schreef het NCSC hierover het volgende: "De buitgemaakte gegevens zijn heel divers. Persoonidentificerende gegevens, bedrijfsinformatie (zoals concurrentiegevoelige informatie), informatie over de computer en kwetsbaarheden in software gebruikt door de getroffen organisatie of persoon hebben voor verschillende actoren een grote waarde en worden soms voor grote bedragen verhandeld. Kant-en-klare informatieverzamelingen die relatief eenvoudig te verhandelen zijn, zijn op deze manier steeds vaker te koop, zoals bijvoorbeeld creditcardgegevens. Persoonsidentificerende gegevens kunnen op eenzelfde manier verhandeld worden maar ook gebruikt worden voor identiteitsfraude of voor het misleiden van mensen, bijvoorbeeld met behulp van 'social engineering'. [...] Omdat de malafide software alle gegevens verzamelt die via de webbrowser verstuurd worden, worden ook alle inloggegevens verzameld die worden gebruikt in invoervelden op webpagina's. In veel bedrijfsomgevingen wordt er gebruik gemaakt van Outlook Web Access (OWA) om op een gemakkelijker manier via internet toegang te hebben tot de zakelijke e-mail omgeving. Bij de analyse is er specifiek gegevens naar dit verkeer. Het botnet heeft, naast de inloggegevens, 206.221 verschillende e-mailberichten verzameld. Het is belangrijk om hierbij op te merken dat berichten die in een mailbox zijn opgeslagen in veel gevallen zeer vertrouwelijk van aard zijn."
[18] Memorie van toelichting bij het voorstel, pagina 22.

voorkoming van nadelige maatschappelijke gevolgen aan niet nader omschreven "organisaties die tot taak hebben om andere organisaties of het publiek daarover te informeren". Tevens blijkt uit de wetstekst niet dat de in het voorstel omschreven taken zullen worden uitgevoerd door het NCSC.

3. ***Het buiten toepassing verklaren van artikel 9 Wbp creëert in de praktijk onduidelijkheden en dilemma's, en noodzakelijke randvoorwaarden ontbreken***

Het voorstel voorziet in een vrijblijvende informatie-'plicht' (artikel 4, eerste lid), waarbij artikel 9 Wbp niet van toepassing is op het verstrekken van persoonsgegevens (artikel 4, tweede lid).

Artikel 9 Wbp heeft betrekking op twee gegevensbeschermingsbeginselen: het doelbindingsbeginsel en de geheimhoudingsplicht. Artikel 43 Wbp voorziet op dit moment al in een mogelijkheid om het doelbindingsbeginsel buiten toepassing te laten voor zover een zwaarwegend algemeen belang dit noodzakelijk maakt. Dit hoeft dus niet in het voorstel te worden geregeld. Wettelijke uitzonderingen op de geheimhoudingsplicht zijn uitsluitend mogelijk voor zover een zwaarwegend algemeen belang deze noodzakelijk maakt, en er passende waarborgen met betrekking tot de persoonlijke levenssfeer in acht worden genomen.

Een specifieke onderbouwing voor het buiten toepassing verklaren van artikel 9 Wbp ontbreekt. Bovendien kan artikel 9 Wbp vanzelfsprekend alleen maar buiten toepassing worden gelaten als daaraan een concrete belangenafweging voorafgaat, en ook deze belangenafweging ontbreekt in het wetsvoorstel. Het buiten toepassing verklaren van artikel 9 Wbp heeft betrekking op de informatie-'plicht' uit artikel 4, eerste lid, van het voorstel. Zoals eerder aangegeven is deze informatie-'plicht' vrijblijvend, en is het NCSC niet bevoegd tot het vorderen van gegevens in dat kader. Dit maakt het buiten toepassing verklaren van artikel 9 Wbp bijna betekenisloos: de rechtspersonen (overheden of private partijen) of organen daarvan die om gegevens worden gevraagd, kunnen zonder opgaaf van redenen weigeren om deze te verstrekken. Wel kan het buiten toepassing verklaren van artikel 9 Wbp de indruk wekken dat deze informatie-'plicht' dwingender is dan deze in feite is.

Verder is het de vraag of het voorstel in zijn huidige vorm voldoende basis biedt aan verantwoordelijken en bewerkers om het NCSC toegang te geven tot persoonsgegevens, of om persoonsgegevens te verstrekken aan het NCSC. Naast de geheimhoudingsplicht uit hoofde van ambt, beroep of wettelijk voorschrift uit het vierde lid van artikel 9 Wbp, is er ook de geheimhoudingsplicht uit artikel 12 Wbp. Weliswaar mag op deze geheimhoudingsplicht een uitzondering worden gemaakt voor zover enig wettelijk voorschrift daartoe verplicht, maar de (vrijblijvende) informatie-'plicht' uit het eerste lid van artikel 4 van het voorstel kan niet als een dergelijke wettelijke verplichting worden gezien.

4. **Dictum**

Het CBP heeft bezwaar tegen het voorstel van wet en adviseert u dit niet aldus in te dienen.

5. Aanvullende opmerking

De memorie van toelichting bij het voorstel geeft aan dat er een samenloop kan ontstaan tussen de meldplicht uit het voorstel en de meldplicht datalekken. Daarbij wordt opgemerkt 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."[19]

Het gaat hier om ongelijksoortige meldplichten met uiteenlopende doelstellingen, waarbij de meldingen moeten worden gedaan bij verschillende instanties die ieder hun eigen rol en taak hebben. Het is dan ook zeer de vraag in hoeverre nodeloze administratieve lasten op de hierboven beschreven wijze daadwerkelijk kunnen worden voorkomen.

Met name voor de telecomsector kan er een samenloop van meldplichten ontstaan. De memorie van toelichting bij het voorstel wijst de telecombedrijven aan als vitale aanbieders op wie de meldplicht mogelijk van toepassing zal zijn.[20] Voor telecombedrijven gelden er reeds twee andere meldplichten, de verplichting tot het melden van continuïteitsverstoringen op grond van artikel 11a.2 Tw en de verplichting tot het melden van datalekken op grond van artikel 11.3a Tw. De wijze waarop de meldingen op grond van artikel 11.3a Tw moeten worden gedaan en de gegevens die daarbij moeten worden verstrekt, worden in hoge mate bepaald door de regels die daaraan worden gesteld in de Europese verordening 611/2013. Deze regels bieden weinig tot geen ruimte voor "onderlinge afstemming van de wijze waarop moet worden gemeld en de gegevens die dienen te worden verstrekt". Daarnaast kan er voor telecombedrijven, evenals voor de overige sectoren, samenloop ontstaan met de voorgestelde meldplicht die is opgenomen in het nieuwe artikel 34a Wbp.

[19] Memorie van toelichting bij het voorstel, pagina 5.
[20] Memorie van toelichting bij het voorstel, pagina 3.

N.V. Nederlandse Gasunie

gasunie

Ministerie van Veiligheid en Justitie
T.a.v. Mr. I. Opstelten
Turfmarkt 147
2311 DP Den Haag

N.V. Nederlandse Gasunie
Postbus 19
9700 MA Groningen
Concourslaan 17
T (050) 521 91 11
F (050) 521 19 99
E communicatie@gasunie.nl
Handelsregister Groningen 02029700
www.gasunie.nl

Datum
3 maart 2015

Doorkiesnummer

Ons kenmerk
J 15.B.09

Uw kenmerk
609274

Onderwerp
Meldplicht

Geachte heer Opstelten,

In uw brief van 22 januari jl. verzocht u N.V. Nederlandse Gasunie om een reactie in het kader van de consultatie wetsvoorstel gegevensverwerking en meldplicht cybersecurity. Wij geven graag gehoor aan dit verzoek. Wij zijn van mening dat het huidige wetsvoorstel op een aantal punten duidelijk verbeterd is ten opzichte van de eerdere versie en dat onze inbreng geleid heeft tot belangrijke aanpassingen hierin. Desalniettemin zijn niet al onze zorgen volledig weggenomen en derhalve treft u hieronder een aantal aandachtpunten van Gasunie (nogmaals) aan.

Noodzaak wetgeving

Gasunie was en is nog steeds de mening toegedaan dat een wettelijke meldplicht niet nodig is, maar dat in plaats daarvan aansluiting zou moeten worden gezocht bij reeds bestaande initiatieven van vitale aanbieders waarbinnen op vrijwillige basis informatie over belangrijke ICT-inbreuken wordt uitgewisseld. Als voorbeeld noemen wij het NDN-netwerk, waarbij het NCSC eveneens een belangrijke rol speelt. Wij denken dat het realiseren van een zogeheten 'just culture', een cultuur waarin het gezamenlijk bijdragen aan veiligheid centraal staat, het best gediend is met samenwerking op basis van vrijwilligheid in plaats van deze samenwerking af te dwingen op basis van wettelijke regels. Gasunie is zich heel goed bewust van haar verantwoordelijkheid ten opzichte van de samenleving en dit geldt ook voor de andere vitale aanbieders. In de Memorie van toelichting wordt dit door u terecht onderkend. Gasunie heeft daarnaast op basis van de Gaswet de wettelijke taak om haar gastransportnet te beschermen tegen invloeden van buitenaf. Dit omvat ook bescherming tegen cyberincidenten. Een wettelijke regeling voor een plicht tot melden lijkt in dat licht bezien overbodig. Niet voor niets is het NCSC een publiek private partnership.

Meerdere meldplichten ondoelmatig

De wettelijke meldplicht achten wij niet alleen overbodig maar ook ondoelmatig. De ACM ziet toe op de naleving van de Gaswet door Gasunie. Voor veel vitale aanbieders geldt dat zij al sectorale meldplichten hebben. Het introduceren van een nieuwe meldplicht bij een ander dan het toezichthoudende orgaan bezorgt de betrokken vitale diensten extra administratieve lasten en navenante kosten.

Bovendien kan dit leiden tot onduidelijkheid en overlap in de taakverdeling tussen de sectorale toezichthouder en het NCSC en tot het krijgen van tegenstrijdige aanwijzingen. Deze problemen kunnen alleen worden voorkomen door alle meldplichten en de processen daaromheen goed op elkaar af te stemmen en te stroomlijnen. In de toelichting bij het wetsvoorstel wordt niet overtuigend uitgelegd dat deze complexe situatie in de praktijk geen problemen zal opleveren. Het risico bestaat dat vitale diensten bij invoering van de meldplicht veel tijd en resources kwijt zijn aan het managen van de processen in plaats van het oplossen van de echte problemen. Wij hebben de indruk dat de kosten en de complexiteit van de meldingen en de opvolging daarvan nu nog onvoldoende worden onderkend en dringen er op aan het wetsvoorstel op dit punt nog eens kritisch tegen het licht te houden en te heroverwegen.

Alleen meldplicht majeure incidenten

Indien het kabinet toch besluit tot invoering van een wettelijke meldplicht dan zou deze alleen moeten gelden voor incidenten die grote maatschappelijke en economische gevolgen kunnen hebben. Enerzijds ter beperking van de administratieve lasten en kosten van de vitale aanbieders en anderzijds om te voorkomen dat, naar achteraf blijkt, onnodig vertrouwelijke informatie wordt uitgewisseld. Dit lijkt ook de insteek van het wetsvoorstel te zijn maar een en ander moet nog uitgewerkt worden in sectorale AmvB's. Wij achten het van belang dat dit uitgangspunt helder en duidelijk in die AmvB's wordt neergelegd en verwerkt.

Vertrouwelijkheid en openbaarheid

1. Volgens artikel 9, lid 1a verstrekt de Minister geen vertrouwelijke gegevens aan derden indien de geheimhouding onvoldoende is gewaarborgd. Hoe beoordeelt de Minister of dat inderdaad zo is ? Wordt in dit oordeel mede betrokken dat de betreffende vertrouwelijke informatie wellicht alsnog openbaar kan worden op basis van de Wet openbaarheid van bestuur ? Volgens de eerste regel van artikel 9, lid 1 gelden de beperkingen ten aanzien van het verstrekken van vertrouwelijke informatie alleen voor de uitvoering van de in artikel 2 genoemde taken. Wat zijn de waarborgen als de vertrouwelijke gegevens ter uitvoering van een andere wettelijke regeling verstrekt moeten worden ? Wat zijn de eventuele consequenties van de invoering van de Wet open overheid ten aanzien van de in artikel 9 genoemde waarborgen ten aanzien van de vertrouwelijkheid ? Graag zouden we een antwoord op deze vragen hebben in de Memorie van Toelichting en zouden wij in het wetsvoorstel geregeld zien dat de in het kader van de meldplicht verstrekte vertrouwelijke gegevens niet onbedoeld openbaar gemaakt moeten worden .

2. In artikel 9, lid 2 wordt aangegeven dat de Minister herleidbare gegevens alleen zal verstrekken aan aangewezen computercrisisteams. Wij vragen wij ons af of hiermee de vertrouwelijkheid voldoende is gewaarborgd, bijvoorbeeld omdat onduidelijk is of deze computercrisisteams wob-baar zijn.

Naar onze mening zou dat niet zo moeten zijn. Dit geldt ook voor de in artikel 9, lid 4 genoemde andere organisaties (zolang geen mededelingen worden gedaan aan het publiek).

Mocht u naar aanleiding van het bovenstaande behoefte hebben aan een nadere toelichting, dan zijn wij daartoe gaarne bereid.

Hoogachtend,

Mr. Drs. C.S. Pisuisse
Directeur Juridische Zaken, Regulering & Communicatie

Luchtverkeersleiding Nederland
Air Traffic Control the Netherlands

Postbus 75200
1117 ZT Luchthaven Schiphol
Nederland

Tel: +31(0) 20 40 62 000
Fax: +31(0) 20 64 84 999
E-mail: atc.nl@lvnl.nl

Ministerie van Veiligheid en Justitie
Directie Wetgeving en Juridische Zaken

uw brief van: 22 januari 2015	**schiphol-o:** 6 maart 2015	**contactpersoon:**
uw kenmerk: 609266	**ons kenmerk:** CS/GM/12035	**toestelnummer:**
onderwerp: Reactie consultatie wetsvoorstel meldplicht cybersecurity	**bijlage(n):** -	**faxnummer:** -

Geachte

Hierbij reageren wij, Luchtverkeersleiding Nederland (hierna: LVNL) op uw brief van 22 januari 2015 met kenmerk 609266, waarin u LVNL in de gelegenheid stelt een reactie te geven op het nieuwe concept-wetsvoorstel "gegevensverwerking en meldplicht cybersecurity".

Het is LVNL opgevallen dat het wetsvoorstel aanzienlijk verbeterd is ten opzichte van de vorige versie. De aangebrachte wijzigingen kunnen de zorg van LVNL echter niet geheel wegnemen. Hieronder staan de vier aandachtspunten die LVNL aan u kenbaar wil maken.

In het wetsvoorstel wordt onvoldoende duidelijk of de gegevens als bedoeld in artikel 4 beschermd zijn wat betreft de **Wob** (relatie tussen artikel 9 en artikel 4). Partijen zullen minder snel genegen zijn informatie te verstrekken als deze informatie op het moment dat deze beschikbaar is bij het Ministerie opvraagbaar is op grond van de Wob. LVNL pleit dan ook voor een zo ruim mogelijke beperking van de Wob in dit kader.

Daarnaast is LVNL van mening dat in artikel 1 een definitie van de term **"inbreuk"** op zijn plaats zou zijn. Deze term is essentieel voor het gehele wetsvoorstel. Hierdoor wordt duidelijk dat het moet gaan om een actie van een derde en dat systeemonderbrekingen door bijvoorbeeld een technische storing (die wel kunnen leiden tot het aantasten van een vitaal product of dienst) hier niet mee worden bedoeld.

Verder is het LVNL onduidelijk wat de status van een **advies** is als bedoeld in artikel 9, derde lid. Wat kunnen partijen ondernemen als zij het niet eens zijn met een dergelijk advies?

Bezoekadres:
Stationsplein Zuid-West 1001
1117 CV Schiphol-Oost

FABEC

Tot slot blijft de **praktische invulling** van onder meer de termen 'in belangrijke mate' en 'producten en diensten' middels AMvB en/of regeling van essentieel belang om een volledig beeld te krijgen van de reikwijdte van dit wetsvoorstel. Gelet op de mogelijke impact voor onze organisatie, blijft LVNL graag direct betrokken bij deze praktische invulling.

Hoogachtend,

Het Bestuur van Luchtverkeersleiding Nederland,
In deze vertegenwoordigd door,

A.Verheijen
Information Security Manager

Nederlandse Vereniging van Banken

Betaalvereniging Nederland

Gustav Mahlerplein 33-35
1082 MS Amsterdam
Postbus 83073
1080 AB Amsterdam
www.betaalvereniging.nl

T 020 305 19 00
F 020 305 19 12

Ministerie van Veiligheid en Justitie

Directeur Wetgeving en Jurdische Zaken
Postbus 20301
2500 EH Den Haag

0 BD

Datum
5 maart 2015

Telefoon
-

Kenmerk
PM/MS/006-2015

E-mail

Betreft
Reactie op concept wetsvoorstel gegevensverwerking en meldplicht cybersecurity

Namens de sector wil ik u bedanken voor de mogelijkheid om op de consultatie van het wetsvoorstel gegevensverwerking en meldplicht cybersecurity te mogen reageren.

In grote lijnen kunnen we ons vinden in het wetsvoorstel. We zien dat veel van onze eerdere zorgen zijn verwerkt in deze versie van het wetsvoorstel. Toch willen we nog een aantal zorgpunten en suggesties met u delen, met het verzoek het wetsvoorstel op deze punten te heroverwegen en aan te passen. Daarnaast hebben wij ook enkele vragen over het wetsvoorstel.

1. *De rol van het NCSC om hulp te geven bij een ernstige ICT inbreuk*
   In het algemeen kunnen we instemmen met de voorgestelde, aanvullende, rol van het NCSC. Echter het wetsvoorstel wekt de indruk, in het bijzonder in artikel 7, dat bij een ernstige ICT inbreuk het NCSC leidend is. Zij kunnen bepalen welke gegevens de betreffende vitale aanbieder moet aanleveren zodat het NCSC deze kan bijstaan. Deze gegevens kan het NCSC dan ook gebruiken om andere vitale aanbieders en andere sectoren te informeren. Zo lijkt het of het NCSC de eindverantwoordelijke voor de afhandeling van dit soort incidenten is. Dat kan onzes inziens niet de bedoeling zijn.
   De Betaalvereniging Nederland (BVN) en de Nederlandse Vereniging van Banken (NVB) willen vooral de samenwerking met het NCSC en het wederzijds vertrouwen borgen. Wij stemmen in met de wens om gegevens aan te leveren, ook waar dit nodig is om andere sectoren adequaat te informeren, echter onder voorwaarden. De behoefte van het NCSC om "bij te staan" kan en moet in goed overleg worden vastgesteld.

KvK 54048370

De financiële sector is dan ook van mening dat te allen tijde de sector/ de vitale aanbieder zelf regie moet voeren. De informatiebehoefte van het NCSC kan worden vastgesteld in overleg met de vitale aanbieder/de sector en de informatiebehoefte moet ook reëel zijn (tenminste kosten/baten gerelateerd). De sector blijft leidend bij het oplossen van het cybersecurity incident. Overigens is het de minister bekend dat de samenwerking in FI-ISAC verband van de financiële sector met de overheid intensief is.

2. *Artikel 9.4 Verstrekking van vertrouwelijke gegevens*
Dit artikel stelt "Na raadpleging van de betrokken aanbieder kan Onze Minister gegevens als bedoeld in het tweede lid voorts verstrekken aan andere dan de in het tweede en derde lid genoemde organisaties of over die gegevens mededelingen doen aan het publiek, voor zover dat noodzakelijk is om ernstige maatschappelijke gevolgen te voorkomen of te beperken."
Dergelijke beslissingen zouden alleen mogen worden genomen in overleg met en na akkoord van de vitale aanbieder. De eigen sector (in ons geval de bancaire sector) dient uit oogpunt van vertrouwelijkheid van de gegevens en vanuit de eigen verantwoordelijkheid te bepalen wanneer bepaalde informatie met het publiek of andere derden mag worden gedeeld en als dit gebeurt, wat mogelijk de gevolgen daarvan zijn.

3. *Kosten van melden*
We delen de mening van het wetsvoorstel niet (zie o.a. punt 2.9 naleving in de memorie van toelichting) dat de kosten van melding beperkt zijn. Dit kan het geval zijn, als bepaalde beschikbare gegevens uit één bron moeten worden gemeld. Als echter gegevens moeten worden verzameld uit meerdere bronnen, dan kan dit arbeidsintensief en dus kostbaar zijn.
Ook hier geldt: de sector doet dat "graag" als de verwachting is dat de schade daardoor aanzienlijk wordt beperkt. Dit vraagt echter overleg tussen de bevraagde sector en het NCSC.
Het toevoegen van een extra meldplicht kan alleen worden verdedigd als dit inhoudelijk toegevoegde waarde heeft. Een aantal sectoren – waaronder de financiële sector – zal al in geval van grote(re) incidenten, deze moeten melden aan de eigen toezichthouder(s). De taak van het NCSC is een andere dan die van een toezichthouder.
De informatiebehoefte van het NCSC zal dan ook zo moeten zijn, dat deze kosten/baten efficiënt is. Dat kan alleen maar in overleg tussen een sector en het NCSC worden vastgesteld.
Wij stellen voor dat artikel 7 wordt aangepast, ter bescherming van de administratieve lasten van de betreffende vitale aanbieder. De aanpassing betreft de constatering, dat de minister in overleg met de betreffende vitale aanbieder afspraken maakt over aan te leveren gegevens.
Dit in plaats van het geformuleerde nu, namelijk "Desgevraagd verstrekt de vitale aanbieder die een kennisgeving als bedoeld in artikel 6 heeft gedaan, Onze Minister onverwijld alle overige gegevens ...".

4. *Wanneer moet een sector melden?*
De hele wet en de memorie van toelichting gaan over de meldplicht waarbij een "ICT-inbreuk direct of indirect (cascade-effect) kan leiden tot maatschappelijke ontwrichting" (quote uit 2.3).
De omschrijving en de voorwaarden waaronder een sector moet melden zijn vaag. In potentie kunnen relatief kleine incidenten uitgroeien tot incidenten met maatschappelijke ontwrichting tot gevolg. Het is wenselijk alleen bij daadwerkelijke ontwrichting een meldplicht voor te schrijven.
De wet, zoals nu beschreven, geeft erg veel ruimte om hier over teveel relatief kleine incidenten sectoren te gaan bevragen.
Belangrijke mate is in deze wet o.i. gekoppeld aan de vitale functies van vitale instellingen, in

ons geval bij de banken: het betalings- en effectenverkeer. Het NCSC heeft, in overleg met de sector, beschreven wanneer "in belangrijke mate" sprake is van een inbreuk op deze veiligheid. De veronderstelling is dat deze beschrijving gehandhaafd blijft in een AMvB. De vraag is dan wel, hoe partijen moeten omgegaan met de term "kan leiden". De invulling mag niet leiden tot veel meldingen die in tweede instantie blijken "mee te vallen".
Zoals hierboven ook al gesteld: de financiële sector is van mening dat de wet zich moet beperken tot het melden als er feitelijk van maatschappelijke ontwrichting sprake is.

5. *WOB-baarheid informatie*
Het wetsvoorstel komt tegemoet aan de door de sectoren en ook door de financiële sector gewenste bescherming tegen het ongewenst openbaren van informatie.
Wij vragen u of dit deel van de wet ook geldt voor informatie die op vrijwillige basis tussen een sector en het NCSC wordt gedeeld.
Ook willen we graag weten of derde partijen waar het NCSC wel informatie aan kan doorgeven (met name betreft dit "aan daartoe bij ministeriële regeling aangewezen computercrisisteams") eveneens niet WOB-baar zijn. Dit geldt uiteraard al voor organisaties als de AIVD en de MIVD.

6. *Artikelsgewijze suggesties en commentaar*
Primair vanuit privacy-optiek worden onderstaande concrete voorstellen gedaan. Wijzigingen zijn ***vet- en schuingedrukt*** aangegeven.
In de bijlage van het document staat een toelichting op de voorgestelde aanpassingen.

Artikel 3
Ten behoeve van de in artikel 2 genoemde doeleinden en taken worden gegevens verwerkt, waaronder persoonsgegevens ***voor zover deze gegevens noodzakelijk zijn om deze doeleinden te bereiken en taken uit te oefenen en in overeenstemming met de op de verwerking van persoonsgegevens toepasselijke wet- en regelgeving (waaronder de Wet Bescherming Persoonsgegevens).*** Onze Minister is verantwoordelijke voor deze verwerking.

Artikel 4
1. Onze Minister kan ~~eenieder~~ verzoeken om gegevens te verstrekken ten behoeve van de in artikel 2 genoemde doeleinden en taken, ***voor zover de gegevens noodzakelijk zijn voor het bereiken van deze doeleinden en uitoefenen van deze taken.***
2. Artikel 9 van de Wet bescherming persoonsgegevens is niet van toepassing op het verstrekken van persoonsgegevens aan Onze Minister ingevolge een verzoek als bedoeld in het eerste lid.

Artikel 5 en toelichting
Wij vinden het van groot belang dat de onderliggende AMvB in nauw overleg met de sector zal worden vastgesteld. In de toelichting staat thans dat de voordracht van de AMvB zal worden gedaan in overeenstemming met de andere betrokken bewindspersonen. Om vast te stellen welke producten en diensten vitaal zijn in een bepaalde sector dient de betreffende sector zelf te worden betrokken.

Artikel 7
Desgevraagd verstrekt de vitale aanbieder die een kennisgeving als bedoeld in artikel 6 heeft gedaan, Onze Minister onverwijld alle overige gegevens die ~~nodig~~ ***noodzakelijk*** zijn om:

Nederlandse Vereniging van Banken

Betaalvereniging Nederland

a. de risico's voor de beschikbaarheid of betrouwbaarheid van producten of diensten in te schatten;
b. de vitale aanbieder bij te staan bij het treffen van maatregelen om de beschikbaarheid en betrouwbaarheid van het product of de dienst te waarborgen of te herstellen.

Artikel 9
1. Ter uitvoering van de in artikel 2 genoemde taken verstrekt Onze Minister geen vertrouwelijke gegevens indien:
a. hun geheimhouding onvoldoende is gewaarborgd, of
b. onvoldoende is gewaarborgd dat zij uitsluitend worden gebruikt voor het doel waarvoor zij worden verstrekt.
2. Onze Minister kan vertrouwelijke gegevens die herleid kunnen worden tot een afzonderlijke aanbieder, uitsluitend verstrekken voor zover dat ***~~dienstig~~ noodzakelijk*** is voor het bevorderen van maatregelen ter voorkoming of beperking van een verstoring van het maatschappelijk verkeer. Ingevolge de eerste volzin worden uitsluitend gegevens verstrekt aan:
a. aangewezen computercrisisteams;
b. de inlichtingen- en veiligheidsdiensten, bedoeld in de Wet op de inlichtingen- en veiligheidsdiensten 2002.
3. ***Indien een vitale aanbieder geen ~~onvoldoende~~*** gevolg geeft aan een door Onze Minister gegeven advies, ***geldt voor vitale aanbieder het comply-or-explain beginsel ~~en kan Onze Minister in het advies opgenomen gegevens als bedoeld in het tweede lid verstrekken aan Onze betrokken Minister~~***).
4. Na ***~~raadpleging~~ instemming*** van de betrokken aanbieder kan Onze Minister *de vitale aanbieder adviseren* gegevens als bedoeld in het tweede lid voorts *te* verstrekken aan andere dan de in het tweede en derde lid genoemde organisaties of over die gegevens mededelingen *te* doen aan het publiek, voor zover dat noodzakelijk is om ernstige maatschappelijke gevolgen te voorkomen of te beperken.
5. Het eerste lid geldt niet voor de in het vierde lid bedoelde mededelingen aan het publiek.
6. De Wet openbaarheid van bestuur is niet van toepassing op de verstrekking van gegevens als bedoeld in het tweede lid, behalve voor zover die gegevens milieu-informatie inhouden als bedoeld in artikel 19.1a van de Wet milieubeheer.
7. Bij of krachtens algemene maatregel van bestuur kunnen nadere regels worden gesteld over het eerste tot en met vierde lid.

Wij gaan ervan uit dat u onze zorg- en aandachtspunten meeneemt in het definitieve wetsvoorstel en daarmee onze zorgen kunt wegnemen.

Uiteraard zijn we bereid verdere vragen van u te beantwoorden.

Hoogachtend,
Betaalvereniging Nederland

PM Mallekoote

Drs. P.M. Mallekoote
Directeur Betaalvereniging

Nederlandse Vereniging van Banken

Drs. E. Dubbeling
Directeur NVB

Nederlandse Vereniging van Banken

Betaalvereniging Nederland

Bijlage: toelichting op 6 artikelsgewijze suggesties

Toelichting bij artikel 3
Het noodzakelijkheidscriterium is toegevoegd om te waarborgen dat alleen die persoonsgegevens worden opgevraagd die het NCSC nodig heeft om zijn doeleinden te bereiken en zijn taken uit te oefenen. Deze proportionaliteitseis vloeit voort uit de Wet Bescherming Persoonsgegevens. Teneinde duidelijk te maken dat het NCSC zich dient te houden aan wet- en regelgeving inzake bescherming persoonsgegevens is opgenomen dat het NCSC in overeenstemming met deze wet- en regelgeving moet handelen. Indien geen verwijzing in de wetstekst wordt opgenomen naar de toepasselijke wet- en regelgeving inzake persoonsgegevens, dan zou de Memorie van Toelichting in ieder geval moeten verduidelijken dat het NCSC persoonsgegevens in overeenstemming met de Wet Bescherming Persoonsgegevens verwerkt.

Toelichting bij artikel 4
Voor zover het persoonsgegevens betreft verwijzen wij naar de toelichting bij Art 3. Echter, ook indien het geen persoonsgegevens betreft zal het NCSC zich eveneens aan de eis van proportionaliteit moeten houden en alleen die gegevens opvragen die het nodig heeft voor het bereiken van zijn doeleinden c.q. vervulling van zijn taak. Het kan niet zo zijn dat het NCSC eenieder kan verzoeken welke gegevens dan ook te verstrekken, ongeacht de relevantie van deze gegevens voor de uitoefening van de taak van het NCSC. Voorts vragen wij ons af of de personen en organisaties waaraan het NCSC gegevens kan vragen niet beperkt moeten worden tot overheidspartijen en vitale private partijen. Het NCSC zal met name gegevens moeten verkrijgen over de informatiesystemen van de rijksoverheid en vitale private partijen, zoals is aangegeven in Memorie van Toelichting bij artikel 4. Wij zien niet in waarom het NCSC gegevens bij 'eenieder' zou mogen opvragen. Dit zou betekenen dat ook individuele burgers informatieverzoeken van het NCSC kunnen ontvangen.

Toelichting bij artikel 7
Ook hier geldt dat duidelijk moet zijn dat het NCSC alleen die gegevens kan opvragen bij vitale aanbieders die noodzakelijk zijn voor het bereiken van zijn doelen. Het gebruik van het woord 'nodig' vinden wij hiervoor te zwak, aangezien dit niet voldoende uitdrukt dat sommige gegevens allicht handig zijn voor het NCSC, maar niet noodzakelijk om zijn taak te kunnen uitoefenen. Om die reden stellen wij voor 'nodig' te vervangen door 'noodzakelijk'. Verder vinden wij het nog niet voldoende expliciet gemaakt wat er nu allemaal onder de "vitale aanbieders" moet worden verstaan.

Toelichting bij artikel 9
Lid 1a. Het is niet duidelijk wat wordt bedoeld met 'onvoldoende gewaarborgd'. Wij sluiten ons aan bij de opmerking van het DNB- consultatiedocument (blz.15 MvT) voor wat betreft de geheimhoudingsplicht van het NCSC.
Lid 3. Wij stellen voor dat het comply-or-explain beginsel hier toepasselijk is, zodat duidelijker wordt dat i) het advies niet bindend is, en ii) er een motivatieplicht geldt voor de vitale instelling waarmee de instelling duidelijk kan maken waarom zij gekozen heeft voor een andere aanpak dan voorgesteld in het advies van het NCSC is gekozen. Voorts valt uit de MvT (blz. 27) op te maken dat de verantwoordelijke minister of staatssecretaris een onder hem ressorterende inspectiedienst kan waarschuwen. Het is echter onduidelijk i) om welke inspectiediensten het hier gaat in geval van betaaldienstverleners, en ii) welke bevoegdheden deze inspectiediensten hebben in het kader van de naleving van de bij dit wetsvoorstel gestelde regels hebben.

Lid 4. Wij zijn van mening dat de rol van het NSCS hier uitsluitend een adviserende kan zijn. Het is aan de vitale dienstverlener zelf om te beslissen over het informeren van andere partijen dan wel het publiek over een inbreuk op de veiligheid en over de inhoud van die mededeling. Een belangrijke reden om deze verantwoordelijkheid bij de vitale dienstverlener te laten is gelegen in het feit dat het zeer waarschijnlijk is dat deze dienstverleners op grond van andere wet- en regelgeving eveneens meldingen en/of mededelingen zullen moeten doen over de inbreuk op de veiligheid. Hierbij valt onder meer te denken aan de verplichting van beursgenoteerde ondernemingen om koersgevoelige informatie openbaar te maken. Voorts hebben sommige vitale aanbieders al meldingsplichten zoals telecomaanbieders aan de ACM op grond van artikel 11 van de Telecommunicatiewet en banken aan de DNB op grond van de Wft. In de nabije toekomst komen hier de meldingsplichten inzake datalekken bij, die aan het CBP en in voorkomend geval aan de getroffen natuurlijke personen moeten worden gemeld. De vitale dienstverlener dient te allen tijde zelf de controle te houden over deze communicaties teneinde te voorkomen dat er tegenstrijdige informatie naar buiten komt, die niet alleen schadelijk voor de vitale aanbieder kan zijn maar ook voor de personen die getroffen worden door een inbreuk op de veiligheid.

Alternatief lid 4: Na *instemming* van de betrokken aanbieder…etc.

Toelichting: in aanvulling op bovenstaande toelichting kan het initiatief tot het informeren van andere partijen dan wel het publiek over een inbreuk op de veiligheid en over de inhoud van die mededeling in dergelijke gevallen wel degelijk komen van het NCSC, maar uiteindelijk dient het de aanbieder zelf te zijn die hier akkoord mee gaat.

0 BD

Schiphol
Amsterdam Airport

Intern

Ministerie van Veiligheid en Justitie
Directie Wetgeving en Juridische Zaken
Sector Staats en bestuursrecht

Postbus 20301
2500 EH Den Haag

Telefoonnummer	Briefnummer	Bijlage	
		-	
Faxnummer	Behandeld door	Uw schrijven d.d.	Schiphol,
		22-01-2015	5 maart 2015

Betreft: Reactie consultatie wetsvoorstel [Uw Kenmerk 609075]

In reactie op uw schrijven dd. 22-01-2015 in welke wij, Schiphol Group, de mogelijk geboden krijgen te reageren op het tweede voorstel 'Wet gegevensverwerking en meldplicht Cyber Security', wil ik u navolgende reactie doen toekomen:

Schiphol Group kan zich vinden in de 2e versie van het aangeboden wetsvoorstel zoals wij deze hebben mogen ontvangen.
Schiphol Group blijft graag direct betrokken bij de praktische invulling zoals bedoeld in Art.5 van het voorstel, alsmede paragraaf 5.2.2 uit de Memorie van Toelichting inzake de termen 'in belangrijke mate' en 'producten en diensten' per sector. Dit aangezien sprake kan zijn van een aanzienlijke interne organisatorische impact.

Hoogachtend,
Directeur Safety, Security & Environment
namens deze,

Hans Aldenkamp
Information Security Advisor

Schiphol Group Postbus 7501 1118 ZG Schiphol Telefoon (020) 601 91 11 Fax (020) 604 14 75
Schiphol Nederland BV K.v.K. Amsterdam nr 34166584
BIC ABNANL2A IBAN NL08ABNA0545610478
BIC ABNANL2A IBAN NL20ABNA0486749304
BIC INGBNL2A IBAN NL03INGB0597660729

T-Mobile

Ministerie van Veiligheid en Justitie
T.a.v. de heer I.W. Opstelten
Postbus 20301
2500 EH Den Haag

Verstuurd: via internetconsultatie.nl

Betreft: Zienswijze T-Mobile Netherlands B.V. Wet gegevensverwerking en meldplicht cybersecurity (openbare versie)

Den Haag, 5 maart 2015

Geachte heer Opstelten,

Op 22 januari 2015 heeft u het wetsvoorstel Wet gegevensverwerking en meldplicht cybersecurity ter (internet)consultatie voorgelegd. T-Mobile Netherlands B.V. (hierna T-Mobile) waardeert dat u de mogelijkheid biedt om haar zienswijze op het wetsvoorstel te geven.

In 2009 is de Telecom-sectordoor de rijksoverheid als 'randvoorwaardelijke vitale sector' aangewezen. Als aanbieder van een openbaar mobiel telecommunicatie netwerk wordt T-Mobile derhalve beschouwd als een vitale infrastructuur. T-Mobile zal daarom een actieve rol spelen in de operationele tenuitvoerlegging van de in het wetsvoorstel opgenomen meldplicht en heeft er om deze reden behoefte aan om op deze tweede consultatie haar zienswijze met u delen.
In de eerste consultatie ronde heeft T-Mobile op 17 september 2013 een zienswijze op het wetsvoorstel ingediend via Nederland ICT, welke optrad namens de bij haar aangesloten telecomaanbieders, waar T-Mobile deel van uitmaakt.
T-Mobile waardeert het dat nu voorliggende tweede wetsvoorstel op enkele voor haar belangrijke onderdelen is aangepast. Er zijn haars inziens echter nog een paar punten welke nadere toelichting of aanpassing behoeven.

Algemeen

Allereerst wil T-Mobile aangeven dat zij het doel van de wetgeving van harte ondersteunt waar het gaat om het leren van elkaars ervaringen, het uitwisselen van best practices en, waar mogelijk en noodzakelijk, het ontvangen van ondersteuning vanuit het Nationaal Cyber Security Centrum (hierna: NCSC). Ook het uitgangspunt van de wet dat het NCSC geen toezichthoudende rol dient te krijgen en het bieden van hulp voorop stelt steunt T-Mobile van harte.
Wil de in dit wetsvoorstel voorgestelde meldplicht nuttig en effectief zijn, dan dient de meldplicht zo min mogelijk drempels te kennen ten aanzien van de melding en tevens zo laag mogelijke administratieve lasten. Ook is het belangrijk om de vertrouwelijkheid van de meldingen en de daarbij verstrekte gegevens te borgen.
Het melden van veiligheidsinbreuken echter wordt reeds in artikel 11a.2 uit hoofdstuk 11a van de Telecommunicatiewet geregeld. T-Mobile ziet een extra meldplicht met een soortgelijk doel daarom als lasten verhogend en weinig effectief.
Graag ziet T-Mobile een plan hoe de in de Memorie van Toelichting aangegeven efficiënte inrichting van processen zal worden vormgegeven. Als er sprake is van een ernstige ICT-inbreuk zal T-Mobile snel willen acteren op het oplossen van het probleem en heeft daarom behoefte aan snelle en vooraf duidelijk neergelegde processen.

T-Mobile Netherlands BV
Adres Wattdorpstraat 60 2521 CC Den Haag
Postadres Postbus 16272, 2500 BG Den Haag
Telefoon +31 (0)6 1109 5000
Fax +31 (0)6 1109 5024
Internet www.t-mobile.nl
Bank Commerzbank Amsterdam 73 31 69 71
KvK Den Haag 33265073

T-Mobile

Opmerkingen bij artikelen van het Wetsontwerp

Artikel 6.1 van het wetsontwerp spreekt van 'onverwijld' kennis geven van een inbreuk. In de Memorie van Toelichting wordt aangegeven dat het van belang is dat de melding van de ICT-inbreuk zo spoedig mogelijk wordt gedaan. Graag zouden we de wetstekst aangepast zien in 'zo snel als redelijkerwijs mogelijk'. Dit om hiermee tegemoet te komen aan het eerste element van de meldplicht die wordt genoemd in de Memorie van Toelichting: het inzicht geven in aard en omvang van de inbreuk.
Als ondersteuning ten aanzien van het voorgaande voorstel om de wetstekst aan te passen het volgende: in de tekst op pagina 23 van de Memorie van Toelichting wordt aangegeven dat er liever een snelle melding moet worden gedaan die later kan worden aangevuld, dan een uitvoerige melding die daardoor op zich laat wachten. In eerste instantie lijkt dit lastenverlagend en efficiënt, echter het doen van een dergelijke 'snelle melding' brengt ook haken en ogen met zich mee: bij een door u voorgestelde beknopte melding zal op basis van artikel 4.1 jo artikel 2 van het wetsvoorstel nadere informatie (kunnen) worden opgevraagd hetgeen de administratieve lasten en efficiëntie niet ten goede zal komen. Zeker niet als eenzelfde melding bij meerdere instanties zal moeten worden gemaakt. Hier pleit T-Mobile dan ook naast helderheid door aanpassing van de wettekst voor één nationaal meldingsloket.
In de Memorie van Toelichting op pagina 4 wordt aangegeven dat het NCSC ongefilterd en met een eigen beoordeling de informatie wil ontvangen en derhalve geen voorstander is van één meldloket. T-Mobile is van mening dat het een het ander niet uitsluit: als met meldloket slechts een doorgeefluik is die bij de diverse instanties zelf terechtkomt kan elke instantie vanuit zijn of haar eigen expertise de situatie beoordelen en is dit efficiënter en lastenverlagend naar de melders toe.

T-Mobile heeft in inmiddels enige ervaring opgedaan met wettelijke meldplichten en wil opmerken dat het nut en de noodzaak van deze verplichtingen voor haar niet altijd duidelijk zijn noch worden. Graag pleit zij dan ook voor een evaluatie ten aanzien van deze meldplicht binnen een termijn van 18 maanden na inwerkingtreding van deze wetgeving.

Openbaarmaking

T-Mobile is van mening dat een uitzondering van door haar gedeelde gegevens inzake opvraagbaarheid van de WOB een noodzakelijke randvoorwaarde is. In artikel 9 van het wetsvoorstel is geregeld dat vertrouwelijke gegevens worden gedeeld, maar niet openbaar mogen worden gemaakt en tot bedrijven herleidbare gegevens alleen maar te verstrekken aan de zgn. CERT's en de inlichtingen- en veiligheidsdiensten. T-Mobile is verheugd over deze verbreding van de geheimhouding. Dit zal deling van gegevens, in het kader van deze meldplicht of zonder plicht tot melding, binnen het NCSC bevorderen. De uitgewisselde informatie betreft immers bedrijfsvertrouwelijke en gevoelige informatie waarvan openbaarmaking onbedoelde economische of maatschappelijke ontwrichting op (inter)nationale schaal zou kunnen veroorzaken.
T-Mobile ziet mede hierom graag een verdere uitwerking van beveiligingseisen ten aanzien van de gegevensverwerking en welke personen toegang hebben tot de vertrouwelijke gegevens.

Ik hoop u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groeten,
namens T-Mobile Netherlands B.V.

Joepke van der Linden
Sr. Regulatory Affairs Counsel

0 BD

VNO NCW

MKB Nederland

Ministerie van Veiligheid en Justitie
De heer mr. I.W. Opstelten
Turfmarkt 147
2511 DP DEN HAAG

Briefnummer
15/10.282/Ma/Ven

Den Haag
3 maart 2015

Onderwerp
Reactie wetsvoorstel gegevensverwerking en meldplicht cybersecurity

Telefoonnummer

E-mail

Excellentie,

In uw brief van 22 januari 2015 heeft u VNO-NCW en MKB-Nederland gevraagd te reageren op de consultatie van het wetsvoorstel gegevensverwerking en meldplicht cybersecurity. Graag maken VNO-NCW en MKB-Nederland van deze mogelijkheid gebruik.
VNO-NCW en MKB-Nederland ondersteunen de ambitie van het kabinet om de digitale veiligheid te vergroten. Met de immer toenemende digitalisering en afhankelijkheid van ICT neemt het belang hiervan alleen maar toe.
In de eerdere consultatie over dit wetsvoorstel hebben VNO-NCW en MKB-Nederland nadrukkelijk gepleit voor het realiseren van een zogenaamde *just culture*, i.e. een dusdanige cultuur die aanmoedigt om cyberincidenten vrijwillig te melden, met als enig doel het verbeteren van de veiligheid van het gehele systeem. Introductie van een wettelijke meldplicht bevordert de opbouw van een *just culture* niet.
Mocht het kabinet desondanks besluiten tot introductie van een wettelijke meldplicht, dan drongen VNO-NCW en MKB-Nederland in hun eerdere reactie onder meer aan op een beperking van de reikwijdte hiervan tot incidenten met een grote impact, en tot enkele vitale sectoren die van essentieel belang zijn voor onze samenleving.
Een ander cruciaal punt waarvoor wij expliciet de aandacht hebben gevraagd betreft de noodzaak om vertrouwelijke omgang met de in het kader van de meldplicht gedeelde informatie te waarborgen. De in dit kader uitgewisselde informatie behelst immers bedrijfsvertrouwelijke en anderszins gevoelige informatie, waarvan openbaarmaking zou kunnen leiden tot gerichte aanvallen en daarmee maatschappelijke ontwrichting.

VNO NCW

MKB Nederland

Met het huidige wetsvoorstel wordt op verschillende punten tegemoet gekomen aan onze bezwaren.

VNO-NCW en MKB-Nederland zijn tevreden met de gekozen insteek om het NCSC geen toezichthoudende rol te geven en het bieden van hulp voorop te stellen. Dit is in lijn met de Kamerbreed gesteunde motie Hennis-Plasschaert, past in de intensieve publiek-private samenwerking die steeds verder vorm krijgt binnen het NCSC en draagt bij aan het creëren voor voornoemde *just culture*.
VNO-NCW en MKB-Nederland zijn eveneens positief over de intentie van het kabinet om vertrouwelijke gegevens die in het kader van deze meldplicht worden uitgewisseld te beschermen tegen ongewenste openbaarmaking.
Op enkele punten blijven echter zorgen bestaan en/of geeft de tekst aanleiding tot vragen. Wij vragen u het wetsvoorstel op deze punten aan te passen dan wel bij de verdere sectorale uitwerking met deze punten rekening te houden:

- Hoewel de intentie van het wetsvoorstel lijkt te zijn de meldplicht te beperken tot incidenten met een grote impact, roept de gekozen formulering dat alle incidenten die *potentieel* maatschappij-ontwrichtend onverwijld dienen te worden gemeld, vragen op. Met deze formulering worden feitelijk alle inbreuken onder de werkingssfeer van de meldplicht gebracht.
  Wij dringen er op aan in de sectorale AMvB's een heldere omschrijving op te nemen van te melden incidenten, waarbij wordt voorkomen dat té veel inbreuken in eerste instantie onder deze meldplicht worden gebracht, waarvan de ernst bij nader inzien blijkt mee te vallen.
  Wij zetten overigens ook vraagtekens bij de capaciteit van het NCSC om daadwerkelijk hulp te bieden bij een te grote stroom aan meldingen.

- Het eerste lid van artikel 9, stelt dat de Minister ter uitvoering van zijn in artikel 2 genoemde taken, geen vertrouwelijke gegevens verstrekt indien hun geheimhouding onvoldoende is gewaarborgd. Het is ons niet helder hoe deze beoordeling plaatsvindt. Wij zien een nadere toelichting op dit punt graag terug in de Memorie van Toelichting.

- Artikel 7 bepaalt dat de vitale aanbieder desgevraagd alle overige informatie verstrekt die nodig is om de risico's in te schatten en de vitale aanbieder bij te staan. Artikel 9, derde lid, geeft de Minister de bevoegdheid om de sectorale toezichthouders te informeren indien het NCSC advies niet of onvoldoende wordt opgevolgd. Vooropgesteld zij dat er bij het bedrijfsleven veel waardering bestaat voor het NCSC en de kennis en expertise die hier aanwezig is. Tegelijkertijd wijzen wij erop dat ook bij de bedrijven in de vitale sectoren zelf veel kennis en expertise aanwezig is, in ieder geval over de eigen ICT-netwerken en systemen.
  De primaire verantwoordelijkheid om maatregelen te nemen om uitval of verstoring van het product of de dienst te voorkomen of te beperken, ligt bij de bedrijven zelf. Goed onderbouwde adviezen van het NCSC zullen zij zeker niet lichtvaardig naast zich neer leggen.
  Publiek-private samenwerking, waarbij partijen vertrouwen hebben in elkaars optreden, is van groot belang. VNO-NCW en MKB-Nederland dringen er daarom

op aan om in nauw overleg met de betrokken sectoren te verkennen hoe de behoefte van het NCSC tot het bieden van hulp en tot het doorsluizen van informatie als deze hulp niet wordt overgenomen, wordt afgebakend.

- Artikel 9, zesde lid, voorziet in een bijzondere openbaarheidsregeling voor herleidbare gegevens. De Wet openbaarheid van bestuur is op deze gegevens niet van toepassing. In de Memorie van Toelichting wordt vermeld dat het hierbij niet alleen gaat om vertrouwelijke gegevens voortkomend uit deze meldplicht, maar ook om gegevens die zijn verkregen door onverplichte meldingen. VNO-NCW en MKB-Nederland onderstrepen het belang van deze regeling. Wel vragen zij zich af of de aangewezen computercrisisteams evenmin Wob-baar zijn. Dit zelfde geldt voor de in lid 4 genoemde 'andere dan de in het tweede en derde lid genoemde organisaties', niet zijnde het publiek.

- Een zorgpunt betreft de mogelijke samenloop van hetzelfde incident en de daarmee gepaard gaande administratieve lasten van diverse meldplichten. Enkele sectoren kennen immers al een meldplicht voor ICT-inbreuken bij hun sectorale toezichthouder. Daarnaast is een brede meldplicht datalekken aanstaande.
  De Memorie van Toelichting spreekt van bescheiden kosten, waar tegenover hoge baten in de vorm van schadebeperking en probleemoplossing staan.
  VNO-NCW en MKB-Nederland zijn van mening dat de kosten voor het bedrijfsleven substantieel kunnen zijn, vooral als de te verstrekken informatie niet eenvoudig verzameld kan worden. Zij wijzen er verder op dat sommige vitale aanbieders die onder dit wetsvoorstel vallen, beursgenoteerd zijn en een kwalificerende inbreuk mogelijk moeten melden aan de beurs. Het coördineren van de vele meldplichten is complex en leidt tot hoge kosten. VNO-NCW en MKB-Nederland vragen uw aandacht hiervoor.
  Een goede regeling over de te verstrekken informatie is in ieder geval essentieel. Wij dringen dan ook aan op nauw overleg tussen de sectoren en het NCSC hierover.

- In de Memorie van Toelichting wordt expliciet aangegeven dat het advies van het NCSC ondergeschikt is aan het advies van de sectorale toezichthouder.
  Het verdient aanbeveling dit expliciet in de Wettekst zelf op te nemen.

- Zoals aangegeven zijn VNO-NCW en MKB-Nederland voorstander van de ontwikkeling van een *just culture*, waarin op basis van vrijwilligheid informatie over incidenten wordt gedeeld met het doel het gehele systeem te versterken. Het is wenselijk dat de effectiviteit van deze meldplicht wordt geëvalueerd.
  Op basis van de resultaten hiervan kan worden besloten over het in stand houden of het afschaffen van deze meldplicht.

Uiteraard tot nadere toelichting bereid.
Met vriendelijke groet,

drs. C. Oudshoorn
directeur beleid

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Microsoft

Wet gegevensverwerking en meldplicht cybersecurity
Inbreng *Microsoft Corporation*
6 maart 2015

Microsoft is verheugd haar visie te kunnen geven op de wet gegevensverwerking en meldplicht cybersecurity. Dat de Nederlandse regering hiertoe het initiatief heeft genomen is van groot belang voor het borgen van de veiligheid van het online ecosysteem van Nederland. Met belangstelling heeft Microsoft de ontwikkeling van vergelijkbare initiatieven op Europees en internationale niveaus gevolgd, en complimenteert de Nederlandse regering dan ook met haar wetsvoorstel, dat een stevig fundament biedt voor het beveiligen van de meest kritieke nationale infrastructuur van Nederland. In het bijzonder verwelkomt Microsoft de vrijwillige aanpak met betrekking tot het melden van inbreuken waar Nederland voor heeft gekozen, omdat dat in onze ervaring de meest effectieve manier is van het beveiligen van informatiesystemen. De redenen daarvoor zetten we in deze reactie kort uiteen.

Microsoft heeft gedurende de afgelopen 20 jaar standaarden en processen ontwikkeld voor gedegen veiligheidsbescherming van onze producten en diensten, waardoor we hebben geleerd om onszelf continue te verbeteren. We hebben een unieke blik op cyberdreigingen omdat we elke maand dreigingsinformatie ontvangen van meer dan 600 miljoen systemen in meer dan 100 landen en regio's. We gebruiken die kennis om netwerk en informatiebeveiliging te versterken, wereldwijd, in Europa en in Nederland. Om dat te bereiken werken we nauw samen met overheden, bedrijven en gebruikers overal ter wereld om te anticiperen op cybersecurity risico's en daar goed op te reageren. Een belangrijke les die we hebben getrokken uit onze samenwerking met overheden is dat de meest effectieve methodes om de algehele cyberveiligheid van online ecosystemen te borgen altijd proportioneel en risico-gebaseerd zijn. Deze aanpak – vaak met beperkte middelen – gaat uit van een focus op de bescherming van wat daadwerkelijk kritieke infrastructuur is voor de economie, veiligheid en gezondheid van een gegeven land. We zijn verheugd dat die denktrant geborgd is in het wetsvoorstel, dat haar focus richt op vitale aanbieders van energie, telecom, financiele diensten en transport.

We begrijpen dat de Nederlandse regering nog een nader besluit zal publiceren dat meer details geeft over de reikweidte van het wetsvoorstel. Die stap verwelkomen we, omdat we weten dat het prioriteren van systemen kan leiden tot lastige belangenafwegingen in de verantwoordelijkheden die de overheid draagt voor het beschermen van burgers en de nationale veiligheid. Voor succesvolle implementatie is het daarom cruciaal een helder proces te hebben dat niet alle systemen, netwerken, infrastructuur of gegevens identificeert als 'hoge prioriteit'. Daarbij is het ook van belang te onderstrepen dat een dergelijke aanpak bijdraagt aan het internationaal harmoniseren van de bescherming van kritieke infrastructuren, en essentieel is voor het garanderen van de continuiteit van informatie over de grenzen heen, net als voor het vermogen van lokale partijen om makkelijker internationaal te kunnen concurreren.

Eveneens is het van belang te onderstrepen dat niet alle vitale aanbieders die vallen onder het wetsvoorstel zich noodzakelijkerwijs in Nederland zullen bevinden. Meer in het bijzonder zullen niet alle vitale aanbieders een in Nederland gebaseerd team beschikbaar hebben dat de cybersecurity van systemen en diensten in Nederland, dan wel systemen buiten Nederland in de gaten kan houden. Daarom stellen wij voor het wetsvoorstel zo aan te passen dat het niet vereist is dat contactgegevens van een zich in Nederland bevindend persoon dienen te worden overhandigd bij de melding van een ICT inbreuk, maar simpelweg de meest daartoe geëigende persoon (Artikel 6.2). Daarbij zouden we aanbevelen dat de regering overweegt een systeem te introduceren dat ook de anonieme melding van incidenten mogelijk maakt.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Microsoft

Zoals al hierboven vermeld zien we de vrijwillige aanpak zoals door Nederland voorgesteld als de juiste weg. Uit ervaring weten we dat een van de belangrijkste elementen voor het aanmoedigen van de uitwisseling van informatie tussen publieke en private partners in cybersecurity *vertrouwen* is. Vertrouwde relaties zorgen voor het vertrouwen dat gedeelde informatie daadwerkelijk zal worden gebruikt en dat deze zal worden beschermd, dan wel met zorg gedeeld. Het is echter onmogelijk om vertrouwen effectief in wetgeving te vangen. Gezien de complexiteit van cybersecurity dreigingen is een aanpak gebaseerd op gedegen publiek-private samenwerking daarom van cruciaal belang. Wetten die het rapporteren van incidenten verplicht stellen vergroten niet noodzakelijkerwijs vertrouwen en samenwerking, noch verminderen ze risico's. Sterker, het tegenovergestelde kan daarvan het resultaat zijn.

Daarnaast zou een meldplicht van incidenten niet moeten worden gebruikt voor meer situationele bewustzijn en analyse, twee van de doelstellingen zoals door Nederland geidentificeerd. Dit zou zelfs contraproductief kunnen werken. Een meldplicht is inherent éénrichtingsverkeer en draagt *an sich* niet bij aan operationele veiligheid of response. Vaak komt de focus te liggen op de melding zelf en niet op hoe de verzamelde informatie zal worden gebruikt, waarmee de fundamentale doelstellingen van de meldplicht kunnen worden ondermijnd. In relatie tot dit laatste punt bevelen we daarom ook aan dat de Nederlandse regering een proces toepast dat evalueert of strategische analyses daadwerkelijk worden gedaan op basis van gedeelde informatie die bijdraagt aan *nieuwe* lessen of responsecapaciteit voor partijen. Het ontwikkelen van een 'levende' aanpak van informatiedeling borgt dat gezochte informatie ook daadwerkelijk wordt gebruikt.

Microsoft vindt dat meldingen een duidelijke focus moeten hebben om te garanderen dat de verzamelde gegevens worden gebruikt om veiligheid te verbeteren en privacy te beschermen. De drempels moeten daarom heel precies worden gedefinieerd zodat vitale aanbieders ze makkelijk kunnen begrijpen en snel procedures kunnen volgen in crisissituaties. De drempels moeten ook de hoeveelheid meldingen beperken tot daadwerkelijk essentiele informatie, zodat het National Cybersecurity Centrum niet wordt overbelast. Wat ons betreft is de *Technical Guideline on Incident Reporting*[1] in Artikel 13a van de European Network and Information Security Agency (ENISA) nuttig in deze context, omdat het een logische aanpak voorschrijft gericht op de impact van beschikbaarheid en hoeveelheid gebruikers die worden geraakt. Hoewel de huidige *Guideline* gericht is op telecomaanbieders, zou deze makkelijk kunnen worden aangepast voor dit doeleinde. Een andere drempel om te overwegen is het beperken van meldingen tot nieuwe aanvallers of methodes, waarmee veel meer praktisch bruikbare informatie wordt verzameld, of voor incidenten waarbij persoonlijke gegevens zijn gemoeid, wat reeds een juridisch vereiste is.

Wat het uiteindelijke besluit ook zal zijn, Microsoft is van mening dat de navolgende principes als uitgangspunt voor de Nederlandse regering zou moeten dienen:

- Rapportage van incidenten moeten worden gedaan op basis van helder gedefinieerde uitkomsten, zoals het beschermen van privacy, publieke veiligheid, coördinatie van response, of het verbeteren van veiligheidsdefensie.

- Rapportage van incidenten moet flexibel en commercieel acceptabel zijn, moeten passen binnen algemeen geaccepteerde internationale standaarden, en waar mogelijk incompatibiliteit vermijden.

[1] https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/technical-guideline-on-incident-reporting-v-2-0

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Microsoft

- Rapportage van incidenten moeten rekening houden met de balans tussen de risico's en voordelen die met het publiceren van details van incidenten zijn geassocieerd.

- Rapportage van incidenten moeten worden vertaald naar specifieke uitkomsten en niet arbitrair worden gekozen met tijdlijnen voor het melden van incidenten.

- Rapportage van incidenten moeten worden ondersteund door onderzoek en ontwikkeling in zowel de publieke als private sector.

Als laatste bevelen we aan dat de regering Artikel 9 van het wetsvoorstel aanpast zodat het verder delen van door de overheid verzamelde informatie strikt beperkt blijft tot een zeer kleine en scherp gedefinieerd aantal omstandigheden. Dat is essentieel voor vitale aanbieders om informatie vrijwillig te willen delen, gezien de verplichtingen die wij met onze klanten aangaan om hun privacy en veiligheid zo goed als mogelijk te borgen. We raden de regering daarom aan dat het een vermelding in het wetsvoorstel opneemt waarmee het National Cybersecurity Centrum wordt verplicht alléén informatie te delen na consultatie met de vitale aanbieder, en ook om specifiek te definieren met wie het National Cybersecurity Centre informatie kan delen. Wij geloven dat informatie alleen breed mag worden gedeeld als is besloten dat publiek bewustzijn noodzakelijk is om een incident te voorkomen of een bestaand incident te mitigeren. Wij zij ook van mening dat de informatie niet moet worden gedeeld met opsporings- of veiligheidsdiensten buiten de bestaande wetgeving en procedures. Voor aanvullende informatie kunt u altijd direct contact met mij opnemen. Ik ben graag bereid om meer details te geven over onze reactie op het wetsvoorstel, vragen te beantwoorden, of het bespreken van nauwere samenwerking op dit onderwerp.

Naast deze inbreng stuur ik hierbij tevens een link naar het Microsoft whitepaper *"A framework for Cybersecurity Information Sharing and Risk Reduction"*, waarin in meer detail wordt ingegaan op enkele elementen van deze reactie: http://www.microsoft.com/en-us/download/details.aspx?id=45516

Hoogachtend,

Jochem de Groot

Government Affairs Manager
Microsoft Nederland