Nederlandse Vereniging van Banken

Betaalvereniging Nederland

Ministerie van Veiligheid en Justitie
T.a.v. Mw. A. G. van Dijk
Directeur Wetgeving en Juridische Zaken
Postbus 20301
2500 EH Den Haag
e: dwjz12@minvenj.nl

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

Datum
5 maart 2015

Telefoon

Kenmerk
PM/MS/006-2015

E-mail

Betreft
Reactie op concept wetsvoorstel gegevensverwerking en meldplicht cybersecurity

Geachte mevrouw Van Dijk,

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:

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

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.