CONSIDERATI

Staatssecretaris van Veiligheid & Justitie
Ministerie van Veiligheid & Justitie
Postbus 20301
2500 EH Den Haag

Amsterdam, 14 juli 2017

Geachte heer Dijkhoff,

Graag dank ik u voor de mogelijkheid om te reageren op het voorstel voor de cybersecuritywet. Als adviesbureau voor de digitale wereld heeft Considerati goed zicht op de beleidsontwikkelingen in het digitale domein en merken wij waar de markt mee worstelt. Dit delen wij graag me u. De reactie van Considerati is op eigen titel.

Graag geef ik u voor het afronden van het wetsvoorstel de volgende punten in overweging:

- **Definitie van Digital Service Providers**: artikel 1 van het wetsvoorstel definieert de digitale dienstverlener (DSP) als een "rechtspersoon die een digitale dienst aanbiedt". De NIB-richtlijn die in deze wet wordt geïmplementeerd, verbijzondert dit tot de categorieën online marktplaats, online zoekmachine en aanbieder van cloud computingdiensten. De richtlijn laat echter nog veel ruimte voor interpretatie welke bedrijven nu precies als een DSP gezien moeten worden. Is het de bedoeling dat iedere softwareleverancier die zijn software *as a service* aanbiedt aan klanten, wordt aangemerkt als aanbieder van een cloud computingdienst? En wat maakt een internetdienst een online marktplaats en wat niet? Het is zeer wenselijk om in de memorie van toelichting verduidelijking aan te brengen wat de wetgever beschouwt als een DSP. Zonder deze verduidelijking zal het voor veel bedrijven onvoldoende kenbaar zijn of zij onder de wet vallen.

- **(Drie)dubbele meldplicht**: het wetsvoorstel bepaalt dat een security incident gemeld dient te worden bij zowel de de hulpverlenende instantie (CSIRT) als de toezichthouder (bevoegde autoriteit). Daar waar dit security incident ook een mogelijk datalek is, zal er ook melding gemaakt moeten worden bij de Autoriteit Persoonsgegevens. Dit creëert een situatie waarin een bedrijf dat bijvoorbeeld door een ernstige hack getroffen is, veel tijd zal moeten besteden aan het doen van meldingen. Tijd die op dat moment ook hard nodig is om het incident zelf af te handelen. Het kabinet stelt voor om via eenzelfde digitaal formulier melding te kunnen maken voor de dubbele security meldplicht. Het is wenselijk om de mogelijkheid te onderzoeken om via datzelfde formulier gelijktijdig ook andere meldingen te kunnen doen.

De Boelelaan 7, 1083 HJ Amsterdam Postbus 76949, 1070 KE Amsterdam
T +31 20 737 0069 **E** info@considerati.com **W** www.considerati.com
KVK 34285744 **BTW** NL8186.06.009.B01 **IBAN** NL64ABNA0535377231

- **Verstrekking van vertrouwelijke gegevens van digitale dienstverleners**: artikel 19 van het wetsvoorstel stelt dat de minister geen vertrouwelijke gegevens met betrekking tot een (vitale) aanbieder verstrekt als geheimhouding onvoldoende geborgd is. Ratio hierachter is dat vitale aanbieders in vertrouwen hun melding moeten kunnen doen. Dit is daarom een noodzakelijke bepaling om te voorkomen dat de bereidheid tot (vrijwillige) melding wordt verlaagd en drempels worden opgeworpen voor het delen van zoveel mogelijk relevante maar bedrijfsgevoelige informatie met het CSIRT. Het waarborgen van vertrouwelijkheid verhoogt daarmee de cybersecurity van Nederland.

  Een belangrijke omissie van het wetsvoorstel is echter dat deze bepaling niet geldt voor DSPs die volgens artikel 13 meldingsplichtig zijn en dienstverleners die volgens artikel 15 vrijwillig melding maken van incidenten. Het is van cruciaal belang voor het vertrouwen van bedrijven in het CSIRT dat gegevens die zij in het kader van een incident delen met het CSIRT voor hulp bij het oplossen van het incident vertrouwelijk blijven.

  Daarnaast is het voor het overzicht en inzicht in de hoeveelheid cyberincidenten voor de respectievelijke CSIRT's ook voor henzelf van groot belang dat incidenten – meldingsplichtig of niet – met hen gedeeld worden. Het waarborgen van de vertrouwelijkheid van de verstrekte gegevens is daarom van cruciaal belang.

  Tevens is het van belang dat ook informatie die met de toezichthouder wordt gedeeld, onder dezelfde vertrouwelijkheidsclausule valt.

- **Verduidelijking *ex post* toezicht voor digitaledienstverleners**: artikel 17 van de NIB-richtlijn regelt de handhaving voor de beveiligings- en meldingsplicht voor DSPs. Hierin wordt expliciet gemaakt dat dit gaat om *ex post* toezichtsmaatregelen. Daarmee wordt in de NIB-richtlijn toezicht voor essentiële aanbieders en DSPs anders geregeld. Overweging 60 spreekt voor DSPs van "licht en reactief toezicht achteraf", geëxpliciteerd in artikel 17 door te spreken over "toezichtsmaatregelen achteraf". Dit onderscheid ontbreekt in de voorgestelde cybersecuritywet. Voor de duidelijkheid is het wenselijk om dit ex post toezicht voor DSPs ook expliciet te maken in het wetsvoorstel.

Ik hoop dat u het voorstel voor de cybersecuritywet op bovenstaande punten kunt aanscherpen. Indien u aanvullende informatie wenst, ben ik graag bereid om mijn punten nader toe te lichten.

Met vriendelijke groet,

Bart Pegge
Director Public Affairs Practice