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.