C/M/S/ Derks Star Busmann
Advocaten Notarissen Belastingadviseurs

CMS Derks Star Busmann N.V.
Newtonlaan 203
NL-3584 BH Utrecht
Postbus 85250
NL-3508 AG Utrecht
www.cms-dsb.com

mr. W. Seinen
Advocaat
T +31 30 2121 191
F +31 30 2121 157
E wouter.seinen@cms-dsb.com

Bankrekening (Stichting Derdengelden)
Iban: NL64 RABO 0394 7771 66
Swift/bic: RABONL2U

Aan de Staatssecretaris van Veiligheid en Justitie
Mr. F. Teeven
Postbus 20301
2500 EH Den Haag

29 februari 2012

Betreft: Reactie op consultatie wijziging Wbp (gebruik camerabeelden en meldplicht datalekken)

Excellentie,

Hierdoor reageert CMS Derks Star Busmann N.V. (CMS DSB) op het onderdeel **datalekken** van de consultatieversie van het wetsvoorstel wijziging van de Wet bescherming persoonsgegevens d.d. 20 december 2011.

1 Introductie en verantwoording

1.1 De voorbereiding van deze reactie is verzorgd door het data privacy team van CMS DSB. Dit team bestaat uit een groep advocaten die (vanuit verschillende praktijkgebieden specialistische) kennis en ervaring hebben opgedaan met het privacyrecht en dr. J.J. Borking, als bijzonder adviseur privacyrecht verbonden aan CMS DSB.

1.2 Ter voorbereiding van deze reactie heeft dit data privacy team niet alleen een eigen analyse van het voorstel gemaakt, maar tevens gesproken met een aantal bedrijven en instellingen uit haar relatiebestand die op grote schaal (persoons-)gegevens verwerken. Aan een over dit onderwerp gehouden discussiebijeenkomst op 23 februari 2012 participeerden juristen en functionarissen gegevensbescherming van organisaties uit de sectoren IT, verzekeringen, vervoer, pensioen, en (semi-)overheid. Genoemde gesprekspartners zijn werkzaam bij Centraal Bureau voor de Statistiek, Connexxion, Digidentity, PGGM en een aantal instellingen en bedrijven dat er voor heeft gekozen op “no name basis” aan deze consultatie bij te dragen.

1.3 Wij zijn deze gesprekspartners zeer erkentelijk voor hun betrokken en analytische vragen en commentaren. Tegelijkertijd benadrukken wij dat onderstaande observaties niet als het standpunt van een of meerdere van de genoemde partijen dient te worden opgevat.

2 Voorkomen van datalekken dient het doel te zijn, melding een van de middelen

2.1 Wij juichen het toe dat de overheid aandacht besteedt aan de problematiek omtrent datalekken. De Nederlandse regering schept hiermee een kans om een bijdrage te leveren aan een verbetering van de informatiebeveiliging die, als een en ander goed wordt aangepakt, als voorbeeld kan dienen in (andere delen van) Europa. Daarvoor is wel nodig dat de regering verder gaat dan het louter centraal registreren van datalekken en een daaraan gekoppelde informatieverplichting jegens betrokkenen. Met een uitsluitend administratieve meldplicht zullen datalekken ons inziens onvoldoende effectief worden bestreden. Wij zijn van mening dat een meldplicht alleen nut heeft, wanneer de focus ligt op het daadwerkelijk voorkomen van datalekken en de melding van een datalek daarbij slechts een hulpmiddel is, dat onderdeel uitmaakt van een breder pakket aan maatregelen.

2.2 Voor het verbeteren van de informatiebeveiliging is het van groot belang dat kennis over digitale inbraken en pogingen daartoe wordt gedeeld. Wanneer alle incidenten op één centrale plaats – en op uniforme wijze – worden gemeld en geanalyseerd, kunnen patronen sneller worden herkend, kwetsbaarheden opgemerkt en kunnen aanbevelingen worden gedaan om herhaling of verdere verspreiding te voorkomen. Daarbij zou gebruik moeten worden gemaakt van de reeds bestaande kennis op dat gebied, zoals bijvoorbeeld aanwezig binnen het NICC.

2.3 Wij wijzen erop dat dit een *best practice* is die bestrijders van computervirussen al jaren gebruiken: alle onregelmatigheden die zich voordoen in de computersystemen worden bijgehouden en direct geanalyseerd, ongeacht of zij op eerste gezicht een gevaar vormen of niet. Juist hierdoor vergaart men informatie over hoe nieuwe virussen zich verspreiden, op welke technologieën en gebruikersgroepen hackers en internetcriminelen zich richten, etc.

2.4 Overigens is het ook in de *offline* wereld algemeen aanvaard dat een effectieve bestrijding van veiligheidsrisico's begint bij het opbouwen van een informatiepositie en het (al dan niet geautomatiseerd) onderzoeken van de vergaarde informatie. Ter illustratie verwijzen wij naar de bestrijding van epidemieën en pandemieën (waar bijvoorbeeld het RIVM, de medische sector en de universiteiten nauw samenwerken) en de centrale registratie en aanpak van incidenten in de transport- en financiële sector.

2.5 Het is daarom van belang dat alle datalekken worden gemeld bij het College Bescherming Persoonsgegevens (Cbp) of een andere autoriteit. De meldingen dienen vervolgens (al dan niet gedeeltelijk geautomatiseerd) te worden geanalyseerd, zodat men daarvan kan leren en waar nodig de gevolgen van een datalek verder kan beperken. Om deze aanpak succesvol te laten zijn, moeten zoveel mogelijk drempels worden weggenomen om kennis over veiligheidsincidenten te delen. Wij ervaren een sterke bereidheid van de sector om een actieve bijdrage te leveren aan het verbeteren van de informatiebeveiliging in Nederland en verwachten op zichzelf dan ook breed draagvlak voor maatregelen ter bestrijding van datalekken. Juist vanuit deze betrokkenheid wordt er groot belang gehecht aan een daadwerkelijke behandeling van de meldingen. Zonder concrete opvolging is een wettelijke meldplicht zinloos.

3 Gebruik en doel van de "meldingendatabase" moeten bij wet geregeld worden

3.1 Hoewel de database van gemelde "datalekken" een potentieel zeer waardevolle informatiebron is, besteedt het wetsontwerp nauwelijks aandacht aan de wijze waarop deze informatie ten algemenen nutte zal worden gebruikt. Ook wordt amper aandacht besteed aan de beveiliging van

de informatie over gemelde datalekken zelf. Een dergelijke database kan immers ook misbruikt worden als basis voor vervolginbraken in systemen. De Memorie van Toelichting biedt weinig informatie op deze punten. Wij menen dat het van wezenlijk belang is om de centrale behandeling van de te melden incidenten in dezelfde wet te regelen als waarmee de meldplicht wordt ingevoerd.

3.2 Het Cbp dient een concrete en voldoende specifieke opdracht te krijgen ten aanzien van het beheer van de meldingendatabase en het (laten) analyseren van de meldingen. Er moet worden gezorgd voor een voldoende wettelijke grondslag. Tevens moet het Cbp worden toegerust voor het vervullen van deze extra taken en dus onder meer beschikking krijgen over de technische kennis en middelen die nodig zijn om de informatie die is vervat in de meldingen adequaat te (laten) analyseren en vertalen naar adviezen en maatregelen. Zodoende kan o.a. worden tegengegaan dat andere verantwoordelijken (en daarmee de burger) onnodig slachtoffer worden van reeds bekende beveiligingsproblemen.

3.3 Vanuit een oogpunt van informatiebeveiliging is het van belang dat geen onderscheid wordt gemaakt tussen persoonsgegevens en andere informatie die door hackers wordt ontvreemd of anderszins wordt gecompromitteerd. Tevens zou het instellen van een "bagatel"-regeling of een drempel afbreuk doen aan de waarde en betekenis van de meldingendatabase als informatiebron voor bestrijding van beveiligingsinbreuken.

4 Onderscheid tussen "melding aan betrokkenen" en "melding aan het Cbp"

4.1 Daarnaast valt of staat de bereidheid om aan dit soort initiatieven mee te werken met het garanderen van een vertrouwelijke behandeling van de gemelde incidenten. Wanneer het melden van een datalek automatisch leidt tot een verplichte melding aan de betrokkenen (*data subjects*) en / of het risico van handhaving met zich brengt (zelfincriminatie), vormt dat een prikkel aan de verantwoordelijken om zich waar mogelijk aan hun meldplicht te onttrekken. Daarbij komt dat onnodige, vroegtijdige of onjuiste informatie aan betrokkenen kan leiden tot onrust en mogelijk extra schade (voor de bescherming van persoonsgegevens) kan veroorzaken.

4.2 De melding aan het college dient daarom vertrouwelijk te geschieden. Het register van meldingen zou niet moeten worden gebruikt om bedrijven en instellingen aan de schandpaal te nagelen of anderszins handhavend op te treden. Waarborgen daartoe moeten vastgelegd worden in de wet.

5 Meldplicht aan betrokkene op basis van zelfstandige belangenafweging

5.1 Het staat buiten twijfel dat de betrokkene onder omstandigheden recht en belang heeft om te weten wanneer de hem of haar betreffende gegevens gecompromitteerd zijn geraakt. Dat is met name het geval indien (i) de gegevens door hun aard of omvang diep ingrijpen in de persoonlijke levenssfeer van de betrokkene of (ii) de betrokkene zijn schade kan beperken indien hij weet dat hem betreffende gegevens zijn ontvreemd. De ernst van de inbreuk kan veelal worden beoordeeld aan de hand van de aard van de gegevens (gevoelige gegevens of niet) maar ook aan de hand van andere factoren zoals bijv. de hoeveelheid gegevens. Wanneer bijvoorbeeld een volledig medisch dossier uitlekt, is de inbreuk op de persoonlijke levenssfeer van de betrokkene veel groter dan wanneer alleen het feit dat iemand ooit zijn been heeft gebroken op straat komt te liggen.

5.2 Anderzijds kan het bekend maken van beveiligingsincidenten ook ernstige negatieve gevolgen hebben. Zo kunnen meldingen van beveiligingsincidenten tot grote onrust leiden en/of het

vertrouwen van de burger schaden in plaats van versterken. Dat zal met name het geval zijn wanneer niet duidelijk is welke gegevens zijn gelekt, wie ze heeft en wat de betrokkene kan doen om zijn schade te beperken.

5.3 Ook hier dringt de parallel met de *offline* wereld zich op. In de luchtvaartsector worden passagiers en omwonenden bijvoorbeeld niet altijd (direct) over incidenten en dreigingen geïnformeerd omdat dergelijke informatie gemakkelijk paniek kan veroorzaken en het vertrouwen in de sector disproportioneel kan schaden, terwijl de betrokkenen weinig baat hebben bij die informatie. Meer in het algemeen worden veelal geen mededelingen gedaan over incidenten zolang het daar naar ingestelde (interne en / of strafrechtelijke) onderzoek nog loopt.

5.4 Ten slotte voorzien wij een ongewenst neveneffect wanneer verantwoordelijken op grote schaal meldingen aan betrokkenen gaan doen (waartoe het huidige voorstel wel uitnodigt; waarover hierna meer). Een ongewenst neveneffect van vele meldingen aan betrokkenen zou immers kunnen zijn dat die meldingen aan betekenis verliezen. Wij vrezen dat dit "erosie" effect vooral zal optreden als het publiek vaak brieven of e-mails krijgt waarin melding wordt gemaakt van een datalek waar de burger niet veel mee kan.

5.5 Een beperking van de meldplicht tot verlies van specifieke categorieën persoonsgegevens (zoals het geval in Duitsland en Oostenrijk) doet niet in alle gevallen recht aan de situatie. Misbruik van niet-gevoelige gegevens kan namelijk grote gevolgen voor de betrokkene hebben (denk aan *phishing* en identiteitsfraude), terwijl openbaarmaking van sommige gevoelige gegevens nauwelijks gevolgen zal hebben (bijvoorbeeld het vakbondslidmaatschap van vakbondsbestuurders).

5.6 Ook de in artikel 34a lid 1 van het wetsvoorstel opgenomen "drempel" biedt geen soelaas. Nog afgezien van de uitvoeringsproblemen die de huidige tekst oproept (waarover hierna meer), gaat het voorstel voorbij aan de nadelige gevolgen die verbonden kunnen zijn aan de mededeling aan betrokkenen.

6 Enkele opmerkingen bij de voorgestelde wetstekst

Koppeling aan beveiliging (art. 34a lid 1 Voorstel Wbp)

6.1 De voorgestelde wetstekst gaat uit van een meldplicht bij een "inbreuk op de maatregelen bedoeld in artikel 13" (artikel 34 a lid 1 Voorstel Wbp). Het lijkt hiermee of er alleen een meldplicht zal bestaan wanneer sprake is van een inbreuk op de door de verantwoordelijke genomen maatregelen en niet wanneer een datalek ontstaat doordat de verantwoordelijke simpelweg niet (volledig) aan zijn beveiligingsverplichtingen van artikel 13 Wbp heeft voldaan of wanneer er anderszins een lacune blijkt te zitten in de beveiligingsmaatregelen.

6.2 Daardoor bestaat het risico dat verantwoordelijken die hun zaakjes op orde hebben en passende beveiligingsmaatregelen treffen eerder blootgesteld worden aan een "inbreuk" op die maatregelen (immers iedere beveiliging, hoe goed ook, is uiteindelijk aan te tasten), dan verantwoordelijken die geen (toereikend) beveiligingsbeleid hebben, maar waarbij zonder dat sprake is van een "inbreuk" wel gegevens op straat kunnen komen te liggen. Dat klemt temeer waar de sancties op verzuim van de meldplicht strenger zijn dan de sancties op niet-naleven van de beveiligingsmaatregelen van artikel 13 Wbp.

6.3 Ook “interne lekken”, waarbij persoonsgegevens worden gebruikt voor een ander doel dan waarvoor zij worden verzameld, moeten o.i. beschouwd worden als een datalek (denk aan situaties waarin *Chinese walls* worden overschreden en binnen een organisatie gegevens die uitsluitend door de ene afdeling gebruikt mogen worden onbevoegdelijk door een andere afdeling gebruikt worden). De voorgestelde wetstekst lijkt dit niet te regelen.

6.4 Wij menen (o.a.) daarom dat het wetvoorstel niet uit zou moeten gaan van een verplichting tot het melden van datalekken in het geval van een inbreuk op de beveiliging, maar dat in plaats daarvan aansluiting zou moeten worden gezocht bij datgene waartegen (o.a.) de beveiligingverplichting tracht te beschermen. De meldplicht zou o.i. gekoppeld moeten zijn aan “verlies of enige vorm van onrechtmatige verwerking van persoonsgegevens” en dus los van de verplichting tot beveiliging moeten worden geformuleerd.

Kennis bij verantwoordelijke(art. 34a lid 1 Voorstel Wbp)

6.5 Voorts wijzen wij erop dat bij het huidige wetsvoorstel onduidelijk is op welk moment de verantwoordelijke wordt geacht op de hoogte te zijn van een inbreuk en dus onverwijld kennisgeving moet doen. Hier geldt wederom dat een verantwoordelijke die zijn zaakjes op orde heeft en dus een inbreuk op de beveiliging eerder op zal merken strenger behandeld wordt dan een verantwoordelijke die dat niet heeft. Bij een verplichting om persoonsgegevens te beveiligen en melding in geval van verlies of onrechtmatige verwerking (dan wel een inbreuk op de beveiligingsmaatregelen), zou o.i. een verplichting passen om beveiliging te monitoren en al dan niet te (laten) auditen en om ervoor te zorgen dat verlies of onrechtmatige verwerking zo spoedig mogelijk wordt geconstateerd, opgelost en voor de toekomst voorkomen.

6.6 Daarbij is in de huidige tekst van het voorstel ook niet duidelijk of de meldplicht zich ook uitstrekt tot datalekken die zich buiten de invloedsfeer van de verantwoordelijke afspelen, maar wel de verantwoordelijke raken. Een voorbeeld daarvan zijn zogenaamde *phishing* aanvallen, waar internetgebruikers naar een nagemaakte website van een dienstverlener worden gelokt en aldaar zelf hun wachtwoorden en andere (persoons)gegevens prijsgeven.

Drempel voor meldingen (art. 34a lid 1 Voorstel Wbp)

6.7 De “drempel” die thans is opgenomen in artikel 34a lid 1 Voorstel Wbp (en die is herhaald in een aantal andere artikelen) om onnodige meldingen te voorkomen, zal voor de praktijk onwerkbaar zijn. Het is o.i. vrijwel onmogelijk voor een verantwoordelijke om in te schatten wanneer “redelijkerwijs kan worden aangenomen” dat een inbreuk zal leiden tot “een aanmerkelijk risico op verlies of onrechtmatige verwerking waaraan nadelige gevolgen voor de persoonsgegevens en de persoonlijke levenssfeer van de betrokkene zijn verbonden”. Deze beperkingen zijn onnodig ingewikkeld (en veel te vaag) geformuleerd en sluiten bovendien niet aan bij de tekst van de Wbp.

6.8 De kans is o.i. groot dat verantwoordelijken die boetes willen voorkomen ondanks de “drempel” toch gewoon iedere inbreuk zullen melden en dat verantwoordelijken die (vanwege imagoschade) melding aan de betrokkene willen voorkomen niet zullen melden (zij kunnen gemakkelijk stellen dat zij hebben ingeschat dat de inbreuk redelijkerwijs niet tot een aanmerkelijk risico zal leiden) en daarbij het risico op een betrekkelijk lage boete voor lief nemen.

6.9 Dit geldt eens te meer nu de verantwoordelijke “onverwijld” moet melden. Hoe kun je “onverwijld” melden na een inschatting of redelijkerwijs sprake is van een aanmerkelijk risico? Een dergelijke inschatting zal veelal de nodige tijd vergen.

6.10 De huidige formulering legt de nadruk op het element kans. Bij een aanmerkelijke kans op nadelige gevolgen moet men melden. Mocht men een daadwerkelijk een drempel voor meldingen aan het CBP en/of aan betrokkenen willen opleggen om onnodige meldingen te voorkomen, dan zou die beperking o.i. directer op de gevolgen betrekking moeten hebben en niet op de kans op gevolgen in het algemeen.

6.11 Daarbij is overigens volstrekt onduidelijk wat wordt bedoeld met “nadelige gevolgen voor de persoonsgegevens” (artikel 34a lid 1, lid 7, artikel 14 lid 1 , lid 3 sub c en lid 5 Voorstel Wbp). Ook is onduidelijk waarom nadelige gevolgen voor de persoonsgegevens en de persoonlijke levenssfeer van de betrokkene zijn vereist. Wij adviseren het element “nadelige gevolgen voor de persoonsgegevens” weg te laten en aansluiting te zoeken bij de inbreuk op de persoonlijke levenssfeer van de betrokkene.

Boete (art. 66 lid 2 Voorstel Wbp)

6.12 De boete van maximaal € 200.000, zoals opgenomen in het wetsvoorstel roept vragen op. De maximale boete zal, zeker voor grote ondernemingen, niet het beoogde afschrikwekkend effect hebben. Een dergelijke boete staat niet in verhouding tot de kosten die de verantwoordelijk zal moeten maken wanneer hij met een datalek naar buiten moet treden.

6.13 In de wet moet vastgelegd worden dat de hoogte van de boete afhankelijk wordt gesteld van de ernst en aard van de inbreuk en het gedrag van de verantwoordelijke. Alleen dan wordt het boeterisico voor de verantwoordelijke inzichtelijk en wordt daarmee een prikkel gecreëerd om daadwerkelijk beveiligingsmaatregelen te treffen en adequaat te handelen indien (desondanks) een datalek plaatsvindt. Het is niet wenselijk dat eerst de boete wordt ingevoerd en pas daarna de richtlijnen worden bepaald en gepubliceerd die komen te gelden voor het opleggen van boetes.

Verplichtingen bewerker (art. 14 Voorstel Wbp)

6.14 Wij juichen het toe dat de verplichtingen tot het melden van een datalek in het Voorstel Wbp tevens worden meegenomen in artikel 14. Echter, de wijze waarop artikel 14 lid 3 sub c Voorstel Wbp thans is geformuleerd, lijkt een zelfstandige verplichting voor de bewerker te creëren. De verantwoordelijke moet er op grond van dat artikel immers voor zorgen dat de bewerker de meldingsverplichtingen nakomt die op de verantwoordelijke rusten. Dat lijkt te betekenen dat de bewerker de melding aan het CBP en de betrokkene moet verrichten in geval van een datalek. Wij vermoeden dat dat niet de bedoeling is. Wij stellen voor om dit te wijzigen in een verplichting voor de bewerker om alle informatie te verschaffen aan de verantwoordelijke die nodig is om te voldoen aan de verplichtingen van artikel 34a, eventueel aangevuld met een verplichting tot melding aan het CBP wanneer de verantwoordelijke volgens de bewerker niet aan zijn verplichtingen voldoet. Voorts menen wij dat het eenvoudiger is om daarbij direct te verwijzen naar de verplichtingen van artikel 34a in plaats van naar de “verplichting tot melding van een inbreuk op de maatregelen, bedoeld in artikel 13” (zoals artikel 14 lid 1, lid 3 sub c en lid 5 lid Voorstel Wbp thans is geformuleerd).

7 Samenvatting en aanbevelingen

I Een wettelijke meldplicht levert alleen wezenlijke toegevoegde waarde op indien zij een onderdeel is van een meeromvattend systeem ter bevordering van de informatiebeveiliging waarbij de meldingen worden geanalyseerd en op basis daarvan de benodigde actie wordt ondernomen.

II Het is noodzakelijk dat gelijktijdig met de invoering van de meldplicht bij wet wordt bepaald dat de gegevens uit de meldingendatabase effectief zullen worden gebruikt voor de verbetering van de informatiebeveiliging.

III Het Cbp (of een andere autoriteit) dient een bij wet omschreven taak te krijgen om de meldingen te (laten) analyseren en gepaste maatregelen te treffen, alsmede de daarvoor benodigde middelen ter beschikking te krijgen.

IV De wetgever moet een duidelijk onderscheid maken tussen de verplichting tot melden aan de autoriteiten en aan betrokkenen.

V De melding aan de autoriteiten zou ruimer moeten zijn dan alleen persoonsgegevens en moet geen uitzondering maken voor geringe of niet-ernstige inbreuken.

VI De meldingen aan de autoriteiten zouden vertrouwelijk moeten worden behandeld.

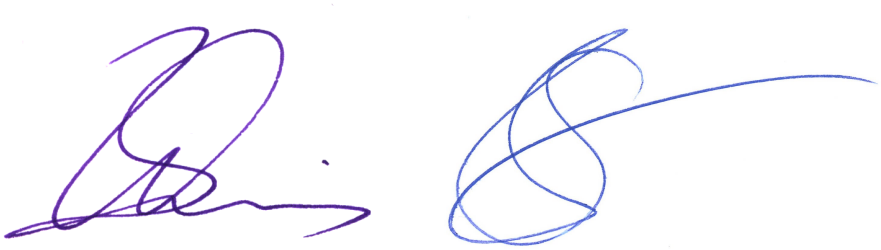
VII De melding aan betrokkenen zou in een zelfstandige wettelijke verplichting vervat moeten worden, met een eigen toetsingskader.

VIII De vraag of de verantwoordelijke een melding aan betrokkenen moet verrichten zou moeten plaatsvinden op grond van een afweging tussen de belangen van de betrokkene(n) bij deze informatie en de nadelige gevolgen die een dergelijke mededeling kan hebben voor de betrokkene, de verantwoordelijke en de samenleving als geheel.

IX De verplichting om te melden moet worden gekoppeld aan verlies of enige vorm van onrechtmatige verwerking van persoonsgegevens in plaats van aan een inbreuk op beveiligingsmaatregelen.

Deze reactie mag openbaar gemaakt worden.

Hoogachtend,
CMS Derks Star Busmann N.V.



Wouter Seinen / Silvia van Schaik