VNO NCW

MKB Nederland

Reactie VNO-NCW en MKB-Nederland op de consultatie van de wijziging Wet bescherming persoonsgegevens inzake gebruik camerabeelden en meldplicht datalekken

Inleiding

Hierbij reageren VNO-NCW en MKB-Nederland op de consultatie van de wijziging van de Wbp inzake meldplicht datalekken. Doel van de meldplicht is om vertrouwen te bevestigen of herstellen dat door markt, publiek, overheid en of toezichthouder in de besbetreffende instelling gesteld wordt, aldus de Memorie van Toelichting. VNO-NCW en MKB-Nederland begrijpen dat wanneer betrokkenen risico lopen op privacyschending doordat risicovolle persoonsgegevens in het publieke domein terecht zijn gekomen, de betreffende persoon dat moet weten.

VNO-NCW en MKB-Nederland zijn evenwel van mening dat deze meldplicht forse impact zal hebben op bedrijven, consumenten en de toezichthouder. Het baart ons grote zorgen dat in de uitwerking de achterliggende problematiek en de reikwijdte niet goed zijn gedefinieerd. Zonder duidelijke context en gerichte focus leidt dit voorstel tot disproportionele lasten voor bedrijven.

Ook is jammer dat gekozen is voor een negatieve benadering (een meldplicht met mogelijk een boete of andere schade voor bedrijven), die paradoxaal genoeg lasten voornamelijk zal neerleggen bij welwillende bedrijven. Überhaupt worden verantwoordelijkheid en lasten die door de gehele keten heen horen te lopen (ook bij consumenten ligt een deel van de oplossing) eenzijdig neergelegd bij bedrijven.

VNO-NCW en MKB-Nederland dringen er bij het Ministerie daarom ook op aan dat alvorens het voorstel naar de Tweede Kamer wordt gezonden, ACTAL de lasten die voortvloeien uit de wetswijziging onderzoekt en dat het voorstel vergezeld gaat van een financiële paragraaf.

De samenloop van deze nationale meldplicht en de meldplicht die zal voortvloeien uit de Europese Privacy Verordening mag van bedrijven niet twee separate trajecten eisen. Bedrijven verplichten om eerst de organisatie in te richten op het Nederlands kader om vervolgens opnieuw te moeten omschakelen naar een Europees kader, is kapitaalvernietiging.

Hierna gaan we in op een aantal algemene opmerkingen, waarna wij per individueel punt ons commentaar geven.

Algemeen commentaar

Honderd procent veilig bestaat niet

Bedrijven hebben een businesscase om zorgvuldig met persoonlijke gegevens om te gaan en zullen – aangespoord door integriteit en de tucht van de markt – gegevens over het algemeen correct verwerken. 100% veiligheid is echter nooit te garanderen.

Criminele hackers voeren – zoals we ook de afgelopen weken weer hebben kunnen zien – constant aanvallen uit op bedrijven en overheden. Veel van die aanvallen worden afgeslagen. Toch kunnen ook bedrijven die hun gegevens uiterst zorgvuldig beveiligen slachtoffer worden van een kwaadwillende hacker met een datalek tot gevolg. Daarom dient maatschappijbreed meer aandacht te worden besteed aan de gehele keten. Flankerend beleid zoals voorlichting (consumenten en bedrijven) is van belang, zo ook een krachtige uitvoering van de cyber security strategie.

100% veilig bestaat niet. Bedrijven die gegevens uiterst zorgvuldig beveiligen, kunnen alsnog slachtoffer worden van een kwaadwillende hacker. Voorlichting en repressie van hacking gaan hand in hand met een maatregel als de meldplicht.

Definieer het probleem, zodat het middel op effectiviteit & proportionaliteit kan worden getoetst
De onderliggende problematiek waarvoor de meldplicht in het leven wordt geroepen moet duidelijker omschreven. Dat kunnen bijvoorbeeld (kwantitatieve gegevens over de impact van) fraude, verlies van vertrouwen of identiteitsdiefstal zijn, waaruit operationele doelstellingen kunnen worden afgeleid. De Memorie van Toelichting dient dit zorgvuldig te beschrijven, zo kunnen ondernemers afwegen wanneer te melden en kunnen effectiviteit en proportionaliteit beoordeeld worden.

Definieer het probleem. Dit geeft ondernemingen referentiekader bij het melden en maakt de meldplicht toetsbaar op effectiviteit en proportionaliteit.

Vertrouwen in de markt is soms gebaat bij vertrouwelijke meldingen
Openbaarmaking van bepaalde lekken kan onbedoelde consequenties hebben voor bedrijven, overheden of voor een gehele sector: faillissement, verdere exploitatie van een lek door criminelen, verlies van vertrouwen in een sector of zelfs verlies in de informatiemaatschappij. Het wetsvoorstel ontbeert de mogelijkheid om – wanneer dat vanwege een groter belang noodzakelijk is – een melding vertrouwelijk te kunnen doen.

Een goed voorbeeld is te vinden in de financiële sector: In de Wet financieel toezicht bestaan geheimhoudingsplichten die verlies van vertrouwen van het publiek of de relevante markt kunnen voorkomen. Ook de AFM behartigt met haar beleid de belangen van de klant, maar moet ook voor rust op de markt zorgen.

Bied expliciet de mogelijkheid in specifieke situaties een balans te kunnen zoeken tussen individuele gevallen en het belang van vertrouwen in bredere zin. Net als in de financiële sector moet onder zwaarwegende omstandigheden de melding aan betrokkene kunnen worden opgeschort.

Nalevingkosten en administratieve lasten in MvT onvoldoende doorgerekend
Meldingen moeten plaatsvinden met een minimum aan lasten voor ondernemers. De Memorie van Toelichting gaat uit van nalevingkosten van de melding van minder dan een half miljoen euro per jaar. De MvT laat achterwege dat het inrichten van een meldingsstructuur, de nazorg, het instrueren van medewerkers etc ook onderdeel zijn van de plicht. Daarnaast gaat de MvT uit van één melding per bedrijf per jaar, terwijl bij een serieus datalek doorgaans gegevens van meerdere personen zullen lekken. Verlies van gegevens van tien personen (conservatief[1]) leidt al tot vertienvoudiging van

[1] De grotere lekken bij Nederlandse websites in het afgelopen jaar varieerden van 824 tot 750.000 personen per onderneming.

nalevingkosten. De proportionaliteit van de maatregel is met deze cijfers niet voldoende aan te tonen, VNO-NCW en MKB-Nederland dringen erop aan dat de Minister ACTAL opdracht geeft onderzoek te doen naar de lasten, alvorens hij het voorstel naar de Tweede Kamer vragen stuurt

Ex ante dient ACTAL te toetsen hoeveel extra lasten deze meldplicht verschillende soorten bedrijven zal opleveren.

Positieve prikkels om te melden ontbreken

Welwillende bedrijven ondervinden geen positieve prikkels. Met de keuze voor een meldplicht is voor een negatieve benadering gekozen, die paradoxaal genoeg vooral goedwillende bedrijven zal raken. Hoe verregaander bedrijven hun beveiliging en monitoring hebben geregeld, des te eerder zij incidenten opmerken. Bedrijven die compliant zijn zullen dus vaker melden en daar mogelijk navenant voor boeten (geldelijk of in de media). Ook zal bij de toezichthouder een 'dossier' worden opgebouwd (zelfs al waren meldingen niet nodig), waardoor bedrijven kans lopen slachtoffer van de WOB te worden.

De Memorie van Toelichting geeft aan dat bedrijven de melding aan toezichthouder desgewenst als bedrijfsvertrouwelijk kunnen aanmerken. VNO-NCW en MKB-Nederland zijn echter van mening dat een hogere mate van bescherming tegen openbaarheid geïntroduceerd dient te worden. Bijvoorbeeld door de toezichthouder de mogelijkheid te geven een informele eerste toets uit te voeren, die bepaalt of wel of niet gemeld hoeft te worden (vergelijk een zienswijze bij de Nma).

Creëer positieve prikkels om te melden door een eerste informele check en door extra vertrouwelijkheid in het meldingsproces.

Reikwijdte

De definities zijn nog niet afgebakend en vereisen hardere criteria wanneer gemeld moet worden.

Door datalekken te koppelen aan artikel 13 van de Wbp wordt de problematiek breder getrokken dan alleen lekken. Data die verloren gaat door brand of waterschade of het niet beschikbaar zijn van gegevens door externe DDOS aanvallen kunnen ook worden aangemerkt als datalek. Dit soort verlies is niet het soort verlies (inzage, kopiëren, gebruik) van gegevens waardoor misbruik kan ontstaan en zou niet moeten leiden tot een melding. Hier wreekt zich dat het achterliggende probleem niet gedefinieerd is en dat er geen leidraad is voor het afwegen van een melding.

Brand, waterschade of een vergeten software-patch kunnen nu reden tot melden zijn. De toezichthouder heeft geen intensieve kennis van specifieke software-patches, virusdefinities, brandvertragende maatregelen, externe DDOS aanvallen of *hacks*. Toch wordt deze door de formulering van de wet gedwongen zich hierover uit te laten. Dit is niet wenselijk en leidt mogelijk tot onkundige oordelen.

Aanmerkelijk risico is een te breed criterium. De meeste breaches leiden tot vergroting van het risico, maar als er waarschijnlijk geen gevolgen zijn, moet dit niet leiden tot een melding. Onrechtmatige verwerking kan door de open norm van de wet al snel het geval zijn. Dit behoeft specificering.

Om misverstanden te voorkomen dient een minimale definitie van 'naar het oordeel van het College gepaste technische beschermingsmaatregelen' ter referentie openbaar te worden gemaakt.

De wetgever moet meer voorbeelden moeten geven over wat wel en wat niet te melden. Nu is niet niet duidelijk waar de verantwoordelijkheid van het bedrijf begint en eindigt. Dient een lek dat ontstaan is in het domein van de klant door malware op zijn pc of door *phishing* vanuit een ander domein gemeld worden, als de onderneming dit opmerkt? Dienen bedrijven actief *hacker-dropzones* te monitoren voor gegevens?

Definieer 'verlies' beter, vanuit de scope van risico. 'Aanmerkelijk risico' en 'onrechtmatige verwerking' dienen beter afgebakend. De toezichthouder moet niet gevraagd worden te oordelen over specifieke technische en organisatorische zaken die buiten haar expertisegebied vallen. De wetgever moet voorbeelden geven die de reikwijdte illustreren.

Aansprakelijkheid toezichthouder
Hoe is de aansprakelijkheid van gevolgen van aanwijzingen van de toezichthouder geregeld, wanneer bijvoorbeeld aanwijzingen van de toezichthouder tot gevolg hebben dat kosten voor organisatie stijgen, zonder dat aantoonbaar is dat deze wijze van handelen beter is voor de consument?

Individuele artikelen:

Wet bescherming persoonsgegevens

Artikel 14
Niet helemaal duidelijk is wat bedoeld wordt met 'nadelige gevolgen voor persoonsgegevens'. Persoonsgegevens zelf lijken ons geen nadelen te kunnen ondervinden. Gesuggereerd wordt 'voor persoonsgegevens' te schrappen, ook in lid 3, lid 4 en in lid 1 en 7 van artikel 34a.

Artikel 14, lid 3
In de MvT zou kunnen worden opgenomen dat – in geval van een voorval bij een door de verantwoordelijke ingeschakelde bewerker – de bewerker in opdracht van, en namens verantwoordelijke melding kan doen bij de toezichthouder.

Artikel 34a, lid 1
Gesuggereerd wordt '*onverwijld*' te veranderen tot 'zo snel als redelijkerwijs mogelijk'. Onverwijld laat geen ruimte voor andere bezigheden die voorrang behoeven, zoals het dichten van het lek zelf. Ook hier geldt weer de paradoxale situatie dat het artikel eerder in werking treedt, wanneer de maatregelen heel uitgebreid zijn.

Artikel 34a, lid 3
Niet helder is tot in hoeverre 'aanbevolen maatregelen' reikt. Welk soort maatregelen dient de verantwoordelijke aan de betrokkene te communiceren? Hoever moet deze daarin gaan?
Ook is niet duidelijk op welke 'instanties' wordt gedoeld waar meer informatie over de inbreuk kan worden verkregen.

Artikel 34a, lid 5
Om extreme kosten voor meldingen te voorkomen wordt gesuggereerd de persoonlijke individuele melding te kunnen laten vervangen door melding op de website of in de krant. Hiertoe bevat de huidige formulering geen aanknopingspunten.

Artikel 34a, lid 6
De toezichthouder dient door de betrokkene onverwijld te worden ingelicht, terwijl naar aanleiding van het oordeel van de toezichthouder bepaald moet worden of maatregelen voldoende waren (lid 6). Wordt de toezichthouder hier ook gehouden aan een tijdsbepaling?

Artikel 34a, lid 6 en 1
Artikel 34a, lid 6 en 1 lijken met elkaar in conflict. Door versleuteling of andere maatregelen die de data onbegrijpelijk maken voor derden (lid 6) is er geen aanmerkelijk risico voor de persoonlijke levenssfeer van de betrokkene en hoeft dus überhaupt niet gemeld te worden (lid 1).

Dit impliceert dat er geen tussencategorie kan zijn waar wél gemeld dient te worden aan de toezichthouder maar niet aan de betrokkene: wanneer een aanmerkelijk risico voor de persoonlijke levenssfeer bestaat dan moet namelijk gemeld bij beiden. Als er geen aanmerkelijk risico bestaat door bijvoorbeeld versleuteling dan is het geen breach onder lid 1 en hoeft ook niet gemeld aan de toezichthouder.

Artikel 34a, lid 11
Gesuggereerd wordt het laatste lid (11) te wijzigen in 'Bij algemene [...] met betrekking tot *dit artikel*.' Dit geeft de wetgever ruimte eventuele nadere regels rondom het gehele artikel te stellen.

Telecommunicatiewet

Artikel 66, lid 2
De verantwoordelijke kan een boete van *ten hoogste* € 200.000,- krijgen. In de Telecommunicatiewet die nu ter goedkeuring in de Eerste Kamer ligt, wordt gesproken over een boete van € 200.000,-. Zuiver technisch geïnterpreteerd betekent dit dat OPTA slechts een boete van precies € 200.000,- kan opleggen. Verzoeke bij artikel 15 lid 4 *ten hoogste* toe te voegen.

Het zou te verkiezen zijn een staffel aan te brengen in boetes. Bijvoorbeeld eerst een waarschuwing, een last onder dwangsom en daarna pas een boete. Ook dient in een eventueel boetekader onderscheid gemaakt te kunnen worden tussen moedwillige en niet moedwillige actie.

Verhouding Wet bescherming persoonsgegevens (Wbp) en de Telecommunicatiewet (Tw)

Melden dienst zo min mogelijk lasten voor bedrijven met zich mee te brengen. Ook moeten bedrijven niet aan twee verschillende (mogelijk conflicterende) regimes te voldoen. Verder onderzocht dient te worden of melden van datalekken door de Telecommunicatiesector bij het Cbp ook daadwerkelijk de minste lasten oplevert voor deze sector. In zowel de Tw als in de Wbp dient ter voorkoming van jurisdictieproblemen een samenloopbepaling te komen.

--