Staatssecretaris van Veiligheid & Justitie
De heer mr. F. Teeven, MPM
Postbus 20301
2500 EH DEN HAAG

Woerden, 29 februari 2012

Betreft : reactie ICT~Office op wetsvoorstel wijziging WBP, meldplicht voor datalekken
Kenmerk : 20120229/BT/BP

Geachte heer Teeven,

In uw brief van 19 december 2011 heeft u ICT~Office gevraagd te reageren op de consultatie van het wetsvoorstel Wet Bescherming Persoonsgegevens (Wbp). Graag maakt ICT~Office, de brancheorganisatie voor ICT- en Telecombedrijven in Nederland, gebruik van deze mogelijkheid. ICT~Office beperkt haar reactie tot het voorstel omtrent de meldplicht voor datalekken.

Recent heeft de Europese Commissie voorstellen gedaan voor een Verordening inzake de gegevensbescherming. In dit voorstel wordt een meldplicht voor datalekken voorzien. Europese harmonisatie is zeer gewenst in dit kader, aangezien niet alleen het internet geen grenzen kent, maar ook veel bedrijven buiten de landsgrenzen actief zijn. ICT~Office verzoekt u om in Nederland geen nieuwe privacyregelgeving te introduceren die binnen afzienbare tijd zal worden vervangen door Europese regelgeving. Dit verdubbelt de implementatielasten van het bedrijfsleven en creëert veel onduidelijkheid.

ICT~Office vraagt u om het Nederlands wetsvoorstel te gebruiken als inzet in het wetgevingsproces in Brussel opdat de Verordening aansluit bij de Nederlandse behoefte. In reactie op het huidige wetsvoorstel wil ICT~Office u vragen om deze meer in lijn te brengen met het beoogde doel: het voorkomen van datalekken en het minimaliseren van de impact op de betrokkene indien er onverhoopt toch een datalek is.

In de bijlage gaat ICT~Office uitgebreid in op het huidige voorstel met opmerkingen of suggesties. Deze opmerkingen kunnen als volgt worden samengevat:

› ICT~Office ziet een meldplicht als signalerende maatregel voor wanneer het onverhoopt fout gaat in de beveiliging van gegevens, die verantwoordelijken bewuster maakt van het belang van transparantie bij een datalek. De meldplicht zal echter leiden tot een forse verzwaring van de lasten van het bedrijfsleven en van de toezichthouder Cbp zonder dat deze meldplicht de beveiliging van gegevens direct verhoogt.

› De verhouding met andere, bestaande en nog uit te werken, meldplichten is ICT~Office nog onduidelijk. Vooral de relatie met de nog uit te werken meldplicht *security breaches* roept vragen op.

Postbus 401
3440 AK Woerden
Pompmolenlaan 7
3447 GK Woerden

T 0348 49 36 36
F 0348 48 22 88
info@ictoffice.nl
www.ictoffice.nl

ING Bank
Rek.nr. 66 25 90 546
KvK 30174840

- Beveiligd zijn is niet hetzelfde als 100 procent veilig zijn. Een verantwoordelijke kan passende maatregelen hebben genomen om persoonsgegevens te beveiligen – en daarmee de Wbp naleven – en toch geconfronteerd worden met een datalek. De samenleving zal de beveiliging echter als te laag ervaren. Dat vergroot de impact van een meldplicht. ICT~Office vraagt het kabinet om in de opzet van en toelichting op de meldplicht sterkere aandacht te geven hieraan.

- Een melding moet worden gedaan als er – kort gezegd – een inbreuk is geconstateerd op de beveiligingsmaatregelen. Organisaties die hun beveiliging niet goed op orde hebben zullen deze inbreuken niet snel opmerken, terwijl het risico bij deze organisaties het grootst is. De meldplicht geeft geen positieve prikkels aan organisaties om die situatie te veranderen. Om deze paradox tegen te gaan, stelt ICT~Office voor om prikkels in te bouwen, bijvoorbeeld door bij aantoonbaar adequate beveiliging een alternatief toezichts- en/of meldingsregime mogelijk te maken.

- In algemene zin pleit ICT~Office voor proportionaliteit bij een verplichting tot melding en vraagt alleen die (zware) gevallen onder de meldplicht te laten vallen waaraan het Cbp ook daadwerkelijk navolging kan geven.

- ICT~Office pleit daarbij voor een heldere afbakening van de reikwijdte van de meldplicht en het opstellen van duidelijke criteria waaraan wordt getoetst, zowel wanneer het een inbreuk betreft als wanneer er sprake is van aanmerkelijk risico en nadelige gevolgen voor de betrokkene.

- De meldplicht vraagt om onverwijlde melding aan toezichthouder en betrokkene. ICT~Office stelt voor om bij een onverwijlde melding aan de toezichthouder een verantwoordelijke de ruimte te laten om eerst de aard en omvang van de inbreuk te onderzoeken. ICT~Office stelt daarnaast voor om de melding aan betrokkene te veranderen in 'zo spoedig als redelijkerwijs mogelijk'. Hierdoor blijft er ruimte om per incident de beste aanpak te bepalen.

- ICT~Office is tevreden met de insteek om meldingen aan de toezichthouder niet te publiceren. Wel ziet ICT~Office te weinig waarborgen om meldingen echt vertrouwelijk te houden. ICT~Office pleit ervoor dat de gehele melding als bedrijfsvertrouwelijk wordt aangemerkt in het kader van de Wet Openbaarheid Bestuur.

- Tot slot vraagt ICT~Office om een hernieuwd onderzoek naar de administratieve lasten, bij voorkeur uitgevoerd door Actal. ICT~Office vindt de huidige inschatting weinig realistisch.

ICT~Office is graag bereid om de opmerkingen en suggesties op het huidige wetsvoorstel nader toe te lichten.

Met vriendelijke groet,
ICT~Office

(w.g.)

mr. Sylvia J.M. Roelofs
algemeen directeur

Postbus 401
3440 AK Woerden
Pompmolenlaan 7
3447 GK Woerden

T 0348 49 36 36
F 0348 48 22 88
info@ictoffice.nl
www.ictoffice.nl

ING Bank
Rek.nr. 66 25 90 546
KvK 30174840

Bijlage: Reactie ICT~Office op wetsvoorstel meldplicht voor datalekken

De reactie van ICT~Office op het wetsvoorstel meldplicht voor datalekken (hierna: de meldplicht) is uitgesplitst in twee onderdelen: algemene opmerkingen over het voorstel voor de meldplicht en enkele specifieke opmerkingen gerelateerd aan artikelen van het wetsvoorstel.

Meldplicht kan leiden tot betere bewustwording

ICT~Office onderschrijft het belang dat verantwoordelijken transparant zijn over de wijze waarop zij met gegevens van klanten omgaan, ook als het onverhoopt een keer mis gaat. Verantwoordelijken die hierover een goede relatie opbouwen met hun klanten kunnen in beginsel rekenen op meer begrip dan verantwoordelijken die dat niet doen. Als een meldplicht op een goede manier wordt opgezet en uitgevoerd kan een meldplicht helpen om verantwoordelijken bewuster te laten zijn van het feit dat transparantie helpt om het vertrouwen te versterken. Tevens zou het ook een bijdrage kunnen leveren aan de maatschappelijke bewustwording van het feit dat aan de verwerking van gegevens ook risico's zijn verbonden die nooit voor 100 procent zijn af te dekken.

Vooral een signalerende maatregel

ICT~Office ziet in een meldplicht kansen voor een betere beveiliging (voorkomen van datalekken) en het minimaliseren van de impact op de betrokkene als er toch onverhoopt een datalek is. ICT~Office staat echter nog niet onverdeeld achter het huidige wetsvoorstel. Een meldplicht zal leiden tot een forse verzwaring van de lasten van het bedrijfsleven en het Cbp zonder dat dit de effectiviteit van de gegevensbescherming vergroot. ICT~Office vindt een meldplicht voornamelijk een signalerende maatregel die erop is gericht om te repareren wanneer het onverhoopt fout gaat, terwijl de aandacht vooral uit zou moeten gaan naar een sterkere preventie op het terrein van de beveiliging.

Verhouding met andere meldplichten: Europese Verordening leidend

ICT~Office ziet een wildgroei aan meldplichten ontstaan. Naast de reeds bestaande beperkte meldplicht voor bijzondere situaties, volgt op afzienbare termijn een meldplicht voor de aanbieders van elektronische communicatiediensten, volgt dit wetsvoorstel voor een algemene meldplicht en volgt er nog een uitwerking van de door de Tweede Kamer gevraagde meldplicht bij *security breaches* (inbreuken op de beveiligingsmaatregelen). Tevens is door de Europese Commissie in januari 2012 een Verordening inzake de gegevensbescherming gepubliceerd die ook een meldplicht datalekken introduceert. Deze Europese meldplicht zal snel na invoering van een Nederlandse meldplicht van kracht worden en daarmee de Nederlandse werkelijkheid inhalen.

ICT~Office vraagt zich daarom sterk af waarom een eigen Nederlandse algemene meldplicht datalekken op dit moment nodig is. ICT~Office stelt voor het huidige wetsvoorstel te gebruiken om de Europese meldplicht in lijn te krijgen met het voorziene Nederlandse voorstel en stelt tevens voor om de Nederlandse meldplicht samen te laten vallen met de invoering van de Europese privacyregels.

Beveiligd zijn is niet hetzelfde als 100 procent veilig zijn

Een verantwoordelijke kan de volgens de Wbp geëiste passende maatregelen hebben genomen om persoonsgegevens te beschermen – en daarmee de wet volledig naleven – en toch geconfronteerd worden met een datalek. Bij het ontdekken van een datalek zal het algemene oordeel van betrokkenen en in de samenleving echter zijn dat de gegevensbeveiliging te laag was. Beveiligen is echter niet absoluut maar het zoeken naar een balans op basis van een risicoafweging. Het wetsvoorstel lijkt weinig rekening te houden dat met de invoering van de meldplicht deze te ongenuanceerde perceptie over beveiliging onbedoelde neveneffecten kan hebben voor het vertrouwen in de digitale samenleving. Dit wordt mogelijk nog verstrekt als te vaak melden tot een 'meldingsvermoeidheid' gaat leiden waardoor minder adequaat wordt geregeerd op echte problemen.

Tevens ziet ICT~Office het als risico dat bij gevallen die buiten de scope vallen van wat de wetgever beoogt met dit wetsvoorstel, toch door de samenleving wordt verwacht dat dit door de verantwoordelijke wordt gemeld. Een meldplicht kan wel wettechnisch afgebakend worden maar zal in de praktijk weinig afbakening kennen. Dat creëert een nog grotere impact van het concept meldplicht.

ICT~Office constateert daarnaast een in onze ogen zorgelijke tendens waarbij verantwoordelijken die openheid betrachten direct worden geconfronteerd met extra (negatieve) aandacht, nog voordat de verantwoordelijke zelf zijn incidentrespons heeft kunnen afronden. De samenleving moet duidelijk nog wennen aan het idee dat gegevens soms helaas toegankelijk blijken voor onbevoegden. Gecombineerd met de bovenstaande constateringen leidt dit ertoe dat een verantwoordelijke nooit juist zal kunnen handelen.

› ICT~Office verzoekt het kabinet om in de opzet van en toelichting op de wet een sterkere aandacht te geven hieraan, zodat de juiste verwachting ontstaat van een meldplicht en de context waarvoor deze is bedoeld. Daarnaast vraagt ICT~Office het kabinet om een sterkere afkeuring richting diegenen die inbreken in andermans systemen en gegevensbestanden.

Positieve prikkels nodig voor beveiligingsmaatregelen

Een meldplicht kan bijdragen aan een sterkere beveiliging van systemen en gegevens als deze de juiste prikkels geeft voor het steeds beter beveiligen. Het huidige wetsvoorstel regelt dat bij een inbreuk op de beveiligingsmaatregelen er een melding moet plaatsvinden. Dat veronderstelt dat een verantwoordelijke eerst moet constateren dat een inbreuk heeft plaatsgevonden. Een verantwoordelijke die zich goed beveiligt en veel kennis over beveiliging in huis heeft, zal eerder opmerken dat er zich een inbreuk heeft voorgedaan dan een verantwoordelijke die onvoldoende aandacht besteedt aan het beveiligingsvraagstuk.

De paradox van de meldplicht is dat het risico op verlies van persoonsgegevens juist het grootst is bij verantwoordelijken die onvoldoende hebben geïnvesteerd in beveiliging en daardoor inbreuken op de beveiliging ook minder snel zullen opmerken. Wanneer een inbreuk niet wordt opgemerkt, kan deze echter ook niet worden gemeld. Buiten het voorkomen van (abstracte) reputatieschade geeft het huidige wetsvoorstel geen prikkels om deze situatie te veranderen. Het beter zicht hebben op eigen systemen (en daarmee monitoren van inbreuken) moet lonen voor een verantwoordelijke.

Juist verantwoordelijken die veel zicht hebben op eigen systemen, zullen inbreuken sneller opmerken en daarmee beter kunnen melden bij het Cbp. Wanneer deze meldingen echter publiek zouden worden, kan dat een verkeerd beeld geven van het daadwerkelijke beveiligingsniveau van verantwoordelijken. Met andere woorden: de verantwoordelijke doet beter zijn best met als mogelijk gevolg dat daardoor een slechtere indruk ontstaat. In lijn met de hierboven geschetste paradox stelt ICT~Office voor dat verantwoordelijken die hun beveiliging aantoonbaar adequaat hebben georganiseerd op een andere wijze worden benaderd en beoordeeld door het Cbp dan verantwoordelijken die dat niet adequaat hebben georganiseerd. ICT~Office stelt voor om te onderzoeken of verantwoordelijken die hun beveiliging volgens de eisen van de Wbp hebben ingericht in een alternatief toezichts- en/of meldingsregime terecht kunnen komen. Dit zou bijvoorbeeld kunnen door een functionaris gegevensbescherming een plek te geven in dat lichtere regime, of door alleen een register van incidenten bij te hoeven houden.

› ICT~Office stelt voor de inrichting van de meldplicht datalekken de verantwoordelijke aanmoedigt met positieve prikkels om beveiligingsmaatregelen te treffen, bijvoorbeeld door een alternatief toezichts- en/of meldingsregime mogelijk te maken.

Scope van de meldplicht

ICT~Office steunt de intentie om alleen de zwaardere gevallen onder een meldplicht te laten vallen, maar vindt de afbakening met de niet-zware gevallen nog te abstract. Daardoor is het aan verantwoordelijken zelf ter beoordeling wanneer men denkt binnen de afbakening te vallen. Dat leidt tot onzekerheid. ICT~Office pleit voor concrete criteria die duidelijk stellen in welke gevallen een verantwoordelijke onderhevig is aan de meldplicht en in welke gevallen niet. Dit is in het kader van de handhaving ook noodzakelijk voor de vraag wanneer een boete wordt opgelegd bij het niet-nakomen van de meldplicht.

In het voorstel is ervoor gekozen om een meldplicht te laten gelden wanneer er een inbreuk is op de maatregelen, bedoeld in artikel 13 Wbp, waarvan redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijke risico op verlies of onrechtmatige verwerking waaraan nadelige gevolgen voor de persoonsgegevens en de persoonlijke levenssfeer zijn verbonden. ICT~Office heeft vragen bij verschillende onderdelen van deze bepaling.

Inbreuk op de maatregelen, bedoeld in artikel 13 Wbp

Het gaat hierbij om een inbreuk op "passende technische en organisatorische maatregelen" bedoeld om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Dat is een dusdanige brede omschrijving dat onduidelijk is welke digitale of fysieke inbreuken hieronder vallen. Moeten bijvoorbeeld een brand in een serverruimte, of een schoonmaker die niet geautoriseerd was voor toegang tot bepaalde ruimtes, als 'inbreuken op de maatregelen' worden beschouwd? Ook in dit geval leiden meer beveiligingsmaatregelen er overigens toe dat er eerder sprake zal zijn van een inbreuk op die maatregelen. Een brede interpretatie van deze bepaling brengt grote lasten mee. Weliswaar kan uit onderzoek van de verantwoordelijke blijken dat geen risico bestaat voor de persoonsgegevens, maar door het op te nemen binnen de definitie leidt het er wel toe dat ieder van dit soort incidenten onderzocht moet worden door de verantwoordelijke.

Aanmerkelijk risico op verlies of onrechtmatige verwerking en nadelige gevolgen
Het is ICT~Office niet duidelijk wanneer de afweging moet worden gemaakt dat er sprake is van een aanmerkelijk risico op verlies. De wijze waarop dit is verwoord leidt ertoe dat het niet gaat om een daadwerkelijk risico of een daadwerkelijk verlies aan data maar al dat een inbreuk leidt tot een vergroting van het risico. De meeste inbreuken zullen tot een vergroting van het risico leiden. Ook de term 'onrechtmatige verwerking' zou verder uitgewerkt kunnen worden. Met de abstracte kaders van de Wbp kan al snel sprake zijn van een onrechtmatige verwerking.

De passage 'nadelige gevolgen voor de persoonsgegevens en de persoonlijke levenssfeer' is een dusdanige open norm dat deze moeilijk in te vullen zal zijn. ICT~Office is overigens benieuwd wat moet worden verstaan onder nadelige gevolgen voor de persoonsgegevens. ICT~Office stelt voor de nadelige gevolgen te beperken tot alleen de persoonlijke levenssfeer.

› ICT~Office pleit voor een heldere afbakening van de reikwijdte van wanneer een melding moet worden gedaan en het opstellen van duidelijke criteria waaraan wordt getoetst, zowel wanneer het een inbreuk betreft als wanneer er sprake is van aanmerkelijk risico en van nadelige gevolgen.

'Onverwijld' melden van een datalek aan het Cbp
De meldplicht datalekken stelt dat bij een inbreuk op de maatregelen het Cbp onverwijld in kennis wordt gesteld en dat de betrokkene ook onverwijld in kennis moet worden gesteld. ICT~Office vraagt zich af hoe deze tijdsindicatie moet worden geïnterpreteerd. Er zit een afruil tussen de tijdigheid van informatievoorziening en de zorgvuldigheid daarvan. Bij constatering van de inbreuk zal namelijk eerst goed moeten worden onderzocht wat de inbreuk precies was en vervolgens moet worden afgewogen of sprake is van een 'aanmerkelijk risico op verlies of onrechtmatige verwerking van persoonsgegevens' en vervolgens of aan deze onrechtmatige verwerking ook 'nadelige gevolgen zijn verbonden aan de persoonlijke levenssfeer van de betrokkene'.

Bij een melding aan het Cbp moet voorkomen worden dat ook ieder vermoeden van een datalek moet worden gemeld. Dat levert niet alleen verhoogde administratieve lasten op maar zonder goede duiding en informatie van een incident kan dat ook leiden tot een onjuiste inschatting bij het Cbp en daarmee leiden tot een onnodige of onjuiste aanwijzing.

› ICT~Office stelt voor om onverwijld dusdanig in te interpreteren in de memorie van toelichting dat deze ruimte laat om eerst te beoordelen wat de inbreuk is, en daarna te melden.

'Zo spoedig als redelijkerwijs mogelijk' melden van een datalek aan de betrokkene
Een onverwijlde melding aan de betrokkene wil ICT~Office graag veranderd zien in "zo spoedig als redelijkerwijs mogelijk". Naast de bovengenoemde redenen van een zorgvuldig onderzoek naar de impact van een datalek op de persoonlijke levenssfeer van de betrokkene, geldt ook dat bij kwaadwillende bedoelingen van criminelen het in het belang van de bestrijding van die criminelen kan zijn om betrokkenen pas later te informeren. Ieder incident moet op een eigen manier worden opgelost. Verantwoordelijken hebben de ruimte nodig om (verergering van de) gevolgen van een

datalek te voorkomen. De wet zal hen die ruimte moeten geven. Of de verantwoordelijke de ruimte goed heeft gebruikt, is achteraf ter beoordeling van het Cbp. Deze aanpassing geeft het Cbp in tijd ook de gelegenheid om te beoordelen of er sprake is van gepaste technische beschermings-maatregelen die persoonsgegevens onbegrijpelijk heeft gemaakt. Pas na deze beoordeling van het Cbp kan de betrokkene worden geïnformeerd (artikel 34a lid 6 versus artikel 34a lid 2).

Hetgeen bepaald in artikel 34a lid 2 veronderstelt overigens dat de verantwoordelijke precies weet welke personen in zijn gegevensverwerking zijn opgenomen en dat de desbetreffende database reconstrueerbaar is. Dat is niet altijd het geval, met name niet wanneer de inbreuk gepaard gaat met gegevensverminking. ICT~Office stelt voor om artikel 34a lid 2 in die zin te nuanceren.

› ICT~Office stelt voor om flexibiliteit te houden in het wetsvoorstel over het moment van melden en 'onverwijld' in artikel 34a lid 2 aan te passen naar 'zo spoedig als redelijkerwijs mogelijk'.

Relatie tussen verantwoordelijke en bewerker

ICT~Office onderschrijft het in het voorstel opgenomen uitgangspunt om ook in het geval van uitbesteding de meldplicht bij de verantwoordelijke te laten rusten. Dat sluit aan bij de praktijk waarbij vaak nu al tussen verantwoordelijke en bewerker contractueel is geregeld dat incidenten door de bewerker aan de verantwoordelijke worden gemeld. Dit hoeft in de ogen van ICT~Office niet extra te worden geregeld in een aanpassing van artikel 14.

ICT~Office heeft enige zorg dat de bewerker via zijn relatie met de verantwoordelijke wel de verantwoordelijkheid (en eventuele financiële aansprakelijkheid) van de gevolgen van datalekken wordt toegeschoven, vooral in die gevallen waar een verantwoordelijke heeft verzuimd om contractueel voldoende maatregelen aan de bewerker toe te wijzen voor de bescherming van persoonsgegevens.

Respons van het Cbp

Er worden op jaarbasis ongeveer 66.000 meldingen verwacht in het kader van de meldplicht. In de memorie van toelichting staat dat het Cbp slechts een beperkt deel daarvan kan onderzoeken. Gegeven het doel van de meldplicht moet worden afgevraagd waarom het Cbp niet alle zaken die binnenkomen in onderzoek neemt. Dat betekent dat voor al die gevallen die het Cbp niet onderzoekt, de melding slechts een papieren exercitie en administratieve handeling is geweest. Daar heeft het Cbp, noch de betrokkene, noch de verantwoordelijke baat bij. In de Memorie van Toelichting moet duidelijk worden welke navolging wordt gegeven aan die meldingen waar het Cbp geen concrete actie op kan ondernemen.

› ICT~Office pleit ervoor om de criteria voor het doen van een melding dusdanig worden aangepast dat het Cbp alleen die meldingen ontvangt waaraan zij ook navolging kan geven.

Aanwijzingen door het Cbp en aansprakelijkheid

In de aanhef van de Memorie van Toelichting wordt aangegeven dat het Cbp door de verantwoordelijke moet worden geïnformeerd opdat het Cbp kan beoordelen of een onderzoek of het

geven van aanwijzingen noodzakelijk is. Het is ICT~Office niet duidelijk op basis waarvan dit onderzoek zou moeten plaatsvinden en wat de aard is van de aanwijzingen of het interveniëren is. ICT~Office vindt het ongewenst als het Cbp aan een melder concrete aanwijzingen kan geven hoe te reageren op een incident. Het Cbp moet vooral ondersteuning bieden en (vrijblijvend) adviseren. Het is aan de verantwoordelijke zelf om te bepalen welke acties nodig zijn in reactie op een inbreuk op de maatregelen.

Als het Cbp toch directe aanwijzingen kan geven over de acties die nodig zijn, dan vraagt ICT~Office zich af of het Cbp aansprakelijk kan worden gesteld voor schade die ontstaat door een aanwijzing van het Cbp die tot grotere schade heeft geleid dan wanneer de verantwoordelijke eigen keuzes had kunnen maken of waardoor acties uitblijven die de schade vergroten.

Geen naming & shaming, wel goede algemene adviezen

ICT~Office leidt uit het wetsvoorstel af dat meldingen niet openbaar zullen worden gemaakt door het Cbp. ICT~Office steunt dit standpunt. Naming & shaming door het Cbp is uiterst onwenselijk, en zelfs contraproductief. Om het leren van andere incidenten te bevorderen, zou het Cbp in samenwerking met het Nationaal Cyber Security Centrum periodiek adviezen kunnen publiceren over het beschermen tegen veel voorkomende incidenten. Dit kan het Cbp doen op basis van alle meldingen die zij ontvangt.

› ICT~Office stelt voor dat het Cbp voor adviezen over het voorkomen van incidenten samenwerkt met het Nationaal Cyber Security Centrum.

Sanctionering

ICT~Office ziet weinig in het idee van een bestuurlijke boete wanneer niet aan de meldplicht wordt voldaan. Een boete is niet de manier om verantwoordelijken te dwingen om te melden. Het zorgt alleen voor een vergroting van de discussie of een melding wel of niet binnen de afbakening valt en voor de discussie of een verantwoordelijke een inbreuk heeft opgemerkt. Energie wordt daarmee gestoken in het instrument van de meldplicht en niet in de verhoging van beveiligingsmaatregelen. In lijn met eerdere opmerkingen zullen veel verantwoordelijken pas in een later stadium, of helemaal niet, opmerken dat een inbreuk heeft plaatsgevonden. ICT~Office vraagt zich af hoe het Cbp bij het uitblijven van een melding zal handhaven, bijvoorbeeld wanneer een datalek niet is opgemerkt.

Sanctionering leidt er bovendien toe dat verkeerde overwegingen een rol kunnen gaan spelen bij het al dan niet melden van een datalek. Juist voor die verantwoordelijken die hun beveiliging wel op orde hebben, leidt sanctionering tot een afweging om sneller te melden om zeker te zijn dat hen achteraf geen boete wordt toebedeeld. Dit vergroot de lastendruk bij bedrijven maar ook bij het Cbp.

Vertrouwelijkheid

Het wetsvoorstel maakt niet duidelijk welke waarborg de verantwoordelijke heeft dat de door de verantwoordelijke aan het Cbp verstrekte gegevens vertrouwelijk worden behandeld. In het kader van laagdrempeligheid van melden zal vertrouwelijkheid gegarandeerd moeten worden. Voorkomen moet worden dat verantwoordelijken die in vertrouwen een melding doen bij het Cbp via een omweg alsnog in de media komen met hun melding, zeker voor die gevallen waarin er geen noodzaak is tot melden aan de betrokkenen.

Om het doel van de meldplicht te bereiken moet vertrouwelijkheid worden gegarandeerd. Het moet niet mogelijk zijn om via een WOB-verzoek meldingen van bedrijven en overheidsinstanties te achterhalen. Dit geeft een zeer negatieve prikkel aan het doen van meldingen. ICT~Office verzoekt met nadruk dat de melding als geheel als bedrijfsvertrouwelijk in de zin van artikel 10, eerste lid, onder c, van de Wet openbaarheid bestuur kan worden aangemerkt en niet alleen dat dit kan met gegevens binnen een melding.

In de memorie van toelichting wordt in paragraaf 4.4 de verhouding met het strafrecht besproken. Daarin wordt niet duidelijk dat de verantwoordelijke zelf de aangifte moet doen en niet dat het Cbp verstrekte gegevens zonder afstemming met de verantwoordelijke aan het Openbaar Ministerie doorgeeft. Welke waarborgen geeft het kabinet dat het Cbp de verkregen gegevens niet ongevraagd doorgeeft naar het Openbaar Ministerie?

› ICT~Office pleit ervoor dat de gehele melding als bedrijfsvertrouwelijk in het kader van de Wet Openbaarheid Bestuur kan worden aangemerkt, of dat andere voorzorgsmaatregelen worden getroffen die de vertrouwelijkheid van meldingen garanderen.

Internationale vraagstukken

De meldplicht op het gebied van de Wbp sluit niet uit dat ingeval van een datalek de verantwoordelijke op grond van buitenlandse wetgeving ook een meldplicht heeft jegens buitenlandse instanties en/of in het buitenland woonachtige betrokkenen. Een cumulatie van meldplichten kan aanzienlijke lasten met zich meebrengen, zeker wanneer die niet op elkaar zijn afgestemd. Om die reden verzoekt ICT~Office de wetgever om zich te buigen over de problematiek van de samenloop van Nederlandse en buitenlandse meldplichten. In de memorie van toelichting wordt geen inzicht gegeven hoe de Nederlandse wetgever hiermee om wenst te gaan. ICT~Office zou graag verhelderd zien hoe gehandeld moet worden in geval van een datalek met een grensoverschrijdend karakter.

Aansprakelijkheid / financiële effecten

In de memorie van toelichting wordt toegelicht dat het doen van een kennisgeving aan de betrokkene de verantwoordelijke op zichzelf genomen niet ontheft van eventuele burgerrechtelijke aansprakelijkheid voor schade die voortvloeit uit het toerekenbaar niet of niet voldoende naleven van de verplichting neergelegd in artikel 13 van de Wbp. In de praktijk zal echter blijken dat betrokkenen schade die zij (denken te) hebben geleden als gevolg van het datalek alsnog zullen proberen te verhalen op de verantwoordelijke, ook al zijn de verplichtingen neergelegd in artikel 13 van de Wbp nageleefd. Dat leidt tot een verzwaring van de last bij verantwoordelijken.

ICT~Office pleit ervoor dat in de memorie van toelichting steviger wordt uitgesproken dat wanneer een verantwoordelijke de verplichtingen in artikel 13 naleeft het voor betrokkenen niet mogelijk is om op basis van de Wbp schade te verhalen van een eventueel datalek. Dit ter voorkoming van een claimcultuur. Daarnaast bepleit ICT~Office een niet-aansprakelijkheid voor schade die ontstaat als een betrokkene de in een melding aan hem aangeraden maatregelen niet opvolgt. Dit stimuleert verantwoordelijken om te zorgen dat de juiste maatregelen worden getroffen voor beveiliging van gegevens en stimuleert een snellere melding aan betrokkenen (positieve prikkels).

Nalevingskosten en administratieve lasten
ICT~Office vindt de berekening van de administratieve lasten weinig realistisch. Het al dan niet hebben van een meldplicht bepaalt niet de mate waarin verantwoordelijken transparant zouden moeten zijn naar hun klanten. Maar wel zorgt een meldplicht dat verantwoordelijken extra lasten ervaren doordat:

- Verantwoordelijke en bewerker extra onderzoeksinspanning moeten plegen om te bepalen of er een meldingsplicht geldt,
- Alle potentiële (grote, maar ook zeer kleine) inbreuken in beginsel beoordeeld moeten worden om te zien of melding noodzakelijk is (die lasten verzwaren nu de reikwijdte nog onduidelijk is)
- Zowel verantwoordelijke als bewerker een organisatorische systematiek moeten inrichten gericht op melden.
- de aanwijzingen van het Cbp kunnen leiden tot extra kosten zonder dat dit leidt tot een betere bescherming van gegevens of betere opvolging van een incident
- in navolging van het hierboven vermelde verantwoordelijken extra kosten gaan maken doordat een meldplicht impliceert dat schade verhaald kan worden op de verantwoordelijke.

De toets op de administratieve lasten is gebaseerd op een onderzoek gedaan ter voorbereiding van het wetsvoorstel tot wijziging van de Telecommunicatiewet. ICT~Office heeft in de consultatie toentertijd reeds gewezen op de onrealistische berekening van de administratieve lasten van de meldplicht.

› ICT~Office vraagt om een hernieuwd onderzoek naar de administratieve lasten, bij voorkeur uitgevoerd door Actal.

Specifieke artikelgerichte opmerkingen
Hierin worden niet de opmerkingen meegenomen die reeds hierboven zijn vermeld.

Artikel I

Artikel 34a lid 5
Het is niet duidelijk wat een 'behoorlijke en zorgvuldige informatievoorziening' is. ICT~Office vindt dat de kosten voor de kennisgeving zo laag mogelijk moeten zijn om personen wiens gegevens het betreft te informeren en proportioneel moeten zijn aan de impact. Het is ICT~Office niet duidelijk of de huidige omschrijving toelaat dat een algemene melding wordt gemaakt aan het publiek.

Artikel 34a lid 6 versus artikel 34a lid 1
In artikel 34a lid 6 wordt een uitzondering gemaakt voor het melden aan de betrokkene indien er (naar oordeel van de het Cbp) gepaste technische beschermingsmaatregelen zijn genomen. Indien er echter sprake is van beschermingsmaatregelen zal ook geen sprake zijn een aanmerkelijk risico op verwerking van gegevens waaraan nadelige gevolgen zijn verbonden voor de persoonlijke levenssfeer van de betrokkene (lid 1). Dat impliceert dat er geen gevallen mogelijk zijn waaraan wel aan het Cbp gemeld moet worden, maar de betrokkene niet geïnformeerd hoeft te worden.

Artikel 34a, lid 6
De betrokkene dient door de verantwoordelijke onverwijld te worden ingelicht, terwijl naar aanleiding van het oordeel van de toezichthouder bepaald moet worden of maatregelen voldoende waren (lid 6). Daar de verantwoordelijke volgens het wetsvoorstel een melding onverwijld moet gebeuren, mag daaruit worden afgeleid dat de toezichthouder onverwijld laat weten of maatregelen voldoende waren? ICT~Office herhaalt het voorstel om in lid 2 'onverwijld' te vervangen in 'zo spoedig als redelijkerwijs mogelijk'.

Lid 6 spreekt van 'gepaste technische beschermingsmaatregelen' naar oordeel van het Cbp. ICT~Office stelt voor om een minimale definitie van deze maatregelen te publiceren, zodat het alle verantwoordelijken duidelijk is wat de referentie is voor toetsing.

Artikel II
De Telecommunicatiewet wordt zodanig gewijzigd dat het Cbp de toezichthouder wordt op de meldplicht datalekken voor elektronische communicatieaanbieders. ICT~Office twijfelt sterk over de effectiviteit van deze aanpassing. In de afgelopen periode is veel contact geweest tussen telecommunicatiesector en OPTA, de huidige toezichthouder, om te komen tot pragmatische aanpak in de handhaving van de toekomstige meldplicht datalekken voor aanbieders van elektronische communicatiediensten.

ICT~Office vraagt zich af waarom voor de telecommunicatiesector de markttoezichthouder voor een algemene toezichthouder wordt ingeruild. Gezien de complexiteit binnen de telecommunicatiesector is een specialistische, op deze gevoelige en complexe markt gerichte toezichthouder noodzakelijk, zoals dat ook het geval is bij de banken. Dit kan eventueel in samenwerking met het Cbp, maar niet zonder de specialistische kennis binnen OPTA.

ICT~Office stelt voor om artikel II in zijn geheel uit het wetsvoorstel te schrappen en eerst te oordelen hoe de in de Telecommunicatiewet beoogde situatie in de praktijk zal uitwerken. ICT~Office verwacht dat het beoogde meldpunt voor diverse meldplichten voor deze aanbieders minder lasten oplevert dan het uiteen trekken van de meldingen, met specifieke meldingen voor het CBP en specifieke meldingen voor de markttoezichthouder. Mochten de getroffen voorzieningen geen pragmatische aanpak blijken, dan stelt ICT~Office voor om via een latere wetswijziging de toezichthouder naar het Cbp te veranderen.

Artikel 15 lid 4
In dit artikellid wordt gesproken over een bestuurlijke boete van € 200.000. Dit staat in contrast met artikel 66 lid 2 waarin wordt gesproken over een boete van *ten hoogste* € 200.000. ICT~Office pleit ervoor dat, indien sprake is van sanctionering, boetes in staffels kunnen worden opgelegd. Derhalve verzoekt ICT~Office om 'ten hoogste' ook toe te voegen aan artikel 15 lid 4.