*Mr. ir. J.M. van Essen**

Nieuwe meldplichten in privacyland

176

Trefwoorden:
meldplicht, beveiligingsinbreuk, datalek, cybersecurity

In deze technologie gedreven samenleving is de beveiliging van gegevens steeds belangrijker geworden. Dataverlies en hacking vormen een grote bedreiging en zijn aan de orde van de dag. Het is dan ook niet verwonderlijk dat zowel op Europees als nationaal niveau initiatieven door de wetgever worden ontplooid om meer grip te krijgen op beveiligingsincidenten. Met het Wetsvoorstel meldplicht datalekken[1] wordt een nieuwe meldplicht geïntroduceerd voor bedrijven, de overheid en anderen mits zij als 'verantwoordelijke'[2] in de zin van de Wet bescherming persoonsgegevens (Wbp) zijn aan te merken. In dit artikel wordt ingegaan op de huidige meldingsverplichtingen, de nieuwe verplichtingen ingevolge het Wetsvoorstel meldplicht datalekken en te verwachten ontwikkelingen.

1 Bestaande wettelijke meldplichten aan toezichthouder

1.1 *Incidenten melden aan toezichthouder*

Voor bepaalde sectoren bestaan al wat langer wettelijke meldplichten.[3] Zo geldt voor financiële instellingen, zoals banken, de verplichting incidenten die een ernstig gevaar vormen voor de integere bedrijfsvoering te melden aan de toezichthouder.[4] Voorvallen met betrekking tot gastransport waardoor nadelige gevolgen voor de mens of het milieu zijn ontstaan of dreigen te ontstaan, dient de netbeheerder zo spoedig mogelijk te melden aan de Minister van Economische Zaken.[5] Een zorgaanbieder moet iedere calamiteit binnen de instelling die betrekking heeft op de kwaliteit van de zorg en die tot een ernstig schadelijk gevolg voor een patiënt of cliënt van de instelling heeft geleid onverwijld aan de IGZ melden.[6] In de telecomsector bestaat een meldplicht voor aanbieders van openbare elektronische communicatienetwerken en -diensten om inbreuken op de veiligheid of verlies van integriteit waardoor de continuïteit van het netwerk of de dienst in belangrijke mate is onderbroken, onverwijld te melden.[7]

1.2 *Telecommunicatiewet*

Een van de reeds bestaande meldplichten verdient in het kader van dit artikel een uitgebreidere uiteenzetting. De meldplicht die nu wordt geïntroduceerd in het Wetsvoorstel meldplicht datalekken voor *alle* 'verantwoordelijken' in de zin van de Wbp die persoonsgegevens verwerken, is al vastgelegd in artikel 11.3a Telecommunicatiewet (TCOMW) voor aanbieders van openbare elektronische communicatiediensten. Deze meldplicht geldt dus wel voor internetserviceproviders (partijen die elektronisch transport verzorgen), maar niet voor andere partijen die betrokken zijn bij het internet zoals banken, webwinkels en aanbieders van websites.

Aanbieders van openbare elektronische communicatiediensten dienen de ACM[8] *onverwijld* in kennis te stellen van een inbreuk op beveiliging die *nadelige gevolgen* heeft voor de bescherming van persoonsgegevens die zijn verwerkt in verband met de levering van een openbare elektronische communicatiedienst.[9] Degene wiens persoonsgegevens het betreft dient *onverwijld* in kennis te worden gesteld van een inbreuk in verband met persoonsgegevens indien de inbreuk waarschijnlijk *ongunstige gevolgen* zal hebben voor diens persoonlijke levenssfeer.[10] Individuen hoeven echter niet op de hoogte te worden gesteld indien de aanbieder gepaste technische beschermingsmaatregelen heeft genomen waardoor de persoonsgegevens die het betreft, versleuteld of anderszins onbe-

---

* **Jacqueline van Essen is Associate Partner bij NautaDutilh NV. Dit artikel is voor het laatst bijgewerkt op 10 september 2013.**

1 Wijziging van de Wet bescherming persoonsgegevens en de Telecommunicatiewet in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens (meldplicht datalekken).
2 De verantwoordelijke is de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt (artikel 1d Wbp), bijvoorbeeld de werkgever voor werknemersgegevens en de leverancier ten aanzien van zijn klantgegevens.
3 Vgl. ook Cyber Security Juridisch Kader d.d. 8 december 2011; een onderzoek uitgevoerd in opdracht van het Ministerie van Veiligheid en Justitie. En *Kamerstukken II* 2011/12, 26 643, nr. 247.
4 Vgl. artikel 3:10 lid 3 en artikel 4:11 lid 4 Wet op het financieel toezicht (Wft); respectievelijk artikel 12 lid 3 Besluit prudentiële regels Wft en artikel 19 lid 3 Besluit gedragstoezicht financiële ondernemingen in welke gevallen melding aan de DNB respectievelijk de AFM moet plaatsvinden.
5 Artikel 8a Gaswet.
6 Zie artikel 4a Kwaliteitswet zorginstellingen. Ingevolge NEN 7510 moeten patiënten door de zorginstelling in kennis worden gesteld wanneer patiëntgegevens onbedoeld openbaar zijn geraakt.
7 Artikel 11a.2 TCOMW.
8 Autoriteit Consument & Markt.
9 Artikel 11.3a lid 1 TCOMW.
10 Artikel 11.3a lid 2 TCOMW.

grijpelijk zijn voor eenieder die geen recht heeft op de toegang tot die gegevens.[11]

1.3 *Uitvoeringsverordening*

De open normen van artikel 11.3a TCOMW (zoals de vraag wat als 'onverwijld' geldt) zijn recent nader ingevuld door een verordening[12] die op 25 augustus 2013 in werking is getreden. Deze 'Uitvoeringsverordening' bepaalt dat *alle* inbreuken in verband met persoonsgegevens moeten worden gemeld aan de nationale autoriteit (in dit geval de ACM).[13] Dit moet uiterlijk 24 uur na opsporing van de inbreuk gebeuren. Opsporing van een inbreuk wordt geacht te hebben plaatsgevonden zodra de aanbieder zich voldoende bewust is van een veiligheidsincident om een zinvolle kennisgeving te kunnen doen.[14] Indien niet alle informatie beschikbaar is die moet worden gemeld, en de inbreuk verder onderzoek vergt, kan de aanbieder uiterlijk 24 uur na opsporing daarvan voorlopige kennisgeving doen. Zo spoedig mogelijk, maar uiterlijk binnen drie dagen na deze voorlopige kennisgeving dient dan een tweede kennisgeving te gebeuren die wel alle verplichte informatie omvat. Mocht dit niet lukken dan dient alle informatie te worden verstrekt die beschikbaar is en moet worden toegelicht waarom de overige informatie nog niet beschikbaar is. Zodra die resterende informatie beschikbaar is, moet deze alsnog worden verstrekt.[15] Een getrapt systeem dus.

Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk ook *negatieve gevolgen* zal hebben voor de persoonsgegevens of privacy van een betrokkene, dient deze daarvan in kennis te worden gesteld. Of een inbreuk waarschijnlijk negatieve gevolgen heeft, wordt beoordeeld op grond van met name de aard en inhoud van de persoonsgegevens (zo zijn financiële gegevens, bijzondere gegevens als bedoeld in de Privacyrichtlijn 95/46/EG[16] (zoals gezondheid) en locatiegegevens, internetlogbestanden, webbrowsergeschiedenis, e-mailgegevens en gespecificeerde lijsten van oproepen extra gevoelig), de vermoedelijke gevolgen (met name wanneer een inbreuk kan leiden tot bijvoorbeeld identiteitsdiefstal of -fraude, lichamelijke schade, ernstige vernedering of reputatieschade), en de overige omstandigheden (met name wanneer deze zijn gestolen of als bekend is dat gegevens in het bezit zijn van een onbevoegde derde).[17] Betrokkenen moeten zonder onnodige vertraging worden geïnformeerd na opsporing van de inbreuk.[18] Dit moet in heldere en begrijpelijke taal gebeuren. Ook mag de kennisgeving niet worden gebruikt om nieuwe of aanvullende diensten te bevorderen of als reclame.[19]

De Uitvoeringsverordening bevat een lijst met informatie die moet worden gemeld. Met toestemming van de nationale autoriteit kan de kennisgeving worden uitgesteld als een correct onderzoek in gevaar kan komen.[20] De informatie moet beschikbaar worden gesteld via een communicatiemiddel dat een snelle ontvangst van de informatie waarborgt en volgens de laatste technische ontwikkelingen is beveiligd.[21] Mochten niet alle personen binnen de genoemde termijnen geïdentificeerd zijn, dan kan de aanbieder hen daarvan op de hoogte brengen via advertenties in grote nationale of regionale media. De aanbieder dient al het nodige te doen de betrokkenen alsnog te identificeren en de kennisgeving te doen.[22] Kennisgeving is niet vereist als passende maatregelen zijn genomen zodat de gegevens onbegrijpelijk zijn voor personen zonder geautoriseerde toegang. Gegevens worden onbegrijpelijk als ze op veilige wijze zijn versleuteld of vervangen, de sleutel voor decryptie respectievelijk datahashing geen gevaar heeft gelopen en niet toegankelijk is voor onbevoegden.[23]

2 Wetsvoorstel meldplicht datalekken

2.1 *Wat houdt dit wetsvoorstel in?*

Het liet geruime tijd op zich wachten, maar op 17 juni 2013 is het Wetsvoorstel meldplicht datalekken naar de Tweede Kamer gestuurd. De voorgestelde Wbp-bepalingen vertonen grote gelijkenis met de bepalingen in de TCOMW, maar ook enkele verschillen.[24] De wetgever

11 Artikel 11.3a lid 5 TCOMW.
12 Verordening (EU) nr. 611/2013 van de Commissie van 24 juni 2013 betreffende maatregelen voor het melden van inbreuken in verband met persoonsgegevens op grond van Richtlijn 2002/58/EG van het Europees Parlement en de Raad betreffende privacy en elektronische communicatie. Deze verordening vloeit voort uit artikel 4 lid 5 van de herziene Richtlijn 2002/58/EG. Hierin is vermeld dat de Europese Commissie technische uitvoeringsmaatregelen kan nemen in verband met, onder meer, de omstandigheden, het formaat en de procedures die gelden. Bij het opstellen van de definitieve tekst van deze Uitvoeringsverordening is ook rekening gehouden met het advies van de Groep Gegevensbescherming Artikel 29 over het ontwerpbesluit van de Commissie betreffende maatregelen voor het melden van inbreuken in verband met persoonsgegevens op grond van Richtlijn 2002/58/EG betreffende privacy en elektronische communicatie d.d. 12 juli 2012 (WP 197).
13 Artikel 1 Uitvoeringsverordening.
14 Artikel 2 lid 2 Uitvoeringsverordening.
15 Artikel 2 lid 3 Uitvoeringsverordening.
16 Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.
17 Artikel 3 lid 2 Uitvoeringsverordening.
18 Artikel 3 lid 3 Uitvoeringsverordening.
19 Artikel 3 lid 4 Uitvoeringsverordening.
20 Artikel 3 lid 5 Uitvoeringsverordening.
21 Artikel 3 lid 6 Uitvoeringsverordening.
22 Artikel 3 lid 7 Uitvoeringsverordening.
23 Artikel 4 Uitvoeringsverordening.
24 Vgl. ook M. Bolhuis, 'Toenemende aandacht voor meldplicht datalekken ter bescherming van persoonsgegevens, Quo Vadis?', *Mediaforum* 2013, p. 174-186, voor een uitgebreide analyse.

heeft bewust willen aansluiten bij artikel 11.3a TCOMW en voor de verschillen gekozen, gelet op bijvoorbeeld de gevoeligheid van beschikbare gegevens in de telecomsector en in verband met de uitvoerbaarheid van de bepaling.

In dit wetsvoorstel[25] wordt een meldplicht geïntroduceerd om een inbreuk op beveiligingsmaatregelen te melden bij het College bescherming persoonsgegevens (CBP) en aan betrokkene(n). De meldplicht zal gelden voor bedrijven, de overheid en anderen mits zij als 'verantwoordelijke' in de zin van de Wbp zijn aan te merken. De meldplicht wordt opgenomen in (een artikel 34a van) de Wbp.

Het niet voldoen aan de meldplicht kan leiden tot een boete van maximaal € 450 000. Dit sluit aan bij de hoogte van de boete ingevolge de TCOMW. Het is de vraag of een dergelijke boete, gelet op de onbepaaldheid van de verplichtingen, niet in strijd is met het rechtszekerheidsbeginsel.[26] Ook het niet naleven van de medewerkingsplicht in het kader van een onderzoek door het CBP ingevolge artikel 5:20 Algemene wet bestuursrecht kan leiden tot een dergelijke boete. Dit betreft dan ook het niet naleven van de medewerkingsplicht in gevallen van onderzoek naar andere overtredingen dan artikel 34a Wbp.

2.2 *Bij wie moet worden gemeld?*

Het CBP moet *onverwijld* in kennis worden gesteld van een inbreuk op de beveiligingsmaatregelen, waarvan redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijke kans op *nadelige gevolgen* voor de bescherming van persoonsgegevens die worden verwerkt.[27]

De betrokkene dient *onverwijld* in kennis te worden gesteld van een dergelijke inbreuk, indien deze inbreuk waarschijnlijk *ongunstige gevolgen* zal hebben voor diens persoonlijke levenssfeer.[28]

De memorie van toelichting (MvT) vermeldt dat de beoordeling van een inbreuk zo geobjectiveerd mogelijk moet zijn. Er moet worden gekeken naar de feitelijke omstandigheden van het geval. Of het verlies van bijvoorbeeld een mobiele telefoon, de diefstal van een laptop of het zoekraken van een USB-stick moet worden gemeld, is ook afhankelijk van de aard van de data en het vermoedelijke risico dat de betrokkene en de onderneming lopen.[29]

De MvT vermeldt als voorbeeld dat het zoekraken of hacken van de ledenadministratie van een sportvereniging doorgaans zal leiden tot het nodige ongemak voor de vereniging en leden, maar niet snel aanleiding zal hoeven te geven tot een melding bij het CBP. De gevolgen van een dergelijk datalek blijven doorgaans beperkt en ook van betrokkenen kan worden gevergd dat zij een zekere mate van risico aanvaarden. Maar een datalek bij de Belastingdienst, of een bank of verzekeraar is doorgaans van een andere orde. Een dergelijk datalek kan leiden tot financieel nadeel bij de betrokkene(n) of tot 'compromittering' van gegevens die worden beschermd door een geheimhoudingsplicht. Het CBP zal waarschijnlijk richtlijnen opstellen om de praktijk enig houvast te geven.[30] Wellicht wordt hier ook (deels) aangesloten bij de omstandigheden als genoemd in de Uitvoeringsverordening.

Een aantal punten valt op. Zo wordt er evenals in artikel 11.3a TCOMW gesproken over 'onverwijld'. De MvT vermeldt dat bewust niet is gekozen voor een gefixeerde tijdslimiet. Dit geeft de verantwoordelijke enige gelegenheid om onderzoek te doen naar de inbreuk, te overwegen welke maatregelen hij aanbeveelt en de manier waarop hij communiceert met het CBP en betrokkenen.[31] Er wordt bewust aangesloten bij de tekst van artikel 11.3a TCOMW, maar daarin is nu bijvoorbeeld invulling gegeven door de Uitvoeringsverordening die een 24-uurstermijn noemt. Toch ligt het niet per se voor de hand dat voor deze Wbp-meldplicht nu ook een initiële meldplicht geldt van 24 uur[32] (er is immers bewust niet gekozen voor een gefixeerde tijdslimiet en deze meldplicht geldt voor *alle* verantwoordelijken in plaats van voor aanbieders van (gevoelige) openbare elektronische communicatiediensten), hoewel ook de MvT vermeldt dat voor de praktische uitvoering van de Wbp *zo veel mogelijk* zal worden aangesloten bij deze Uitvoeringsverordening (die toen nog niet was gepubliceerd).[33] Wat 'zo veel mogelijk' betekent zal zich ook in de praktijk moeten gaan uitkristalliseren. De MvT vermeldt dat van het CBP wordt verwacht dat het richtsnoeren zal vaststellen waarmee het CBP direct of indirect enig houvast kan geven aan de praktijk. Vermoedelijk zal het CBP ook nog aanvullende voorlichting aan de praktijk geven. Verder zullen bij algemene maatregel van bestuur nadere regels kunnen worden gesteld met betrekking tot de kennisgeving. Wellicht gaat dit net zoals bij de cookieregels waar de ACM aankondigde dat direct zou worden gehandhaafd, maar de wet achteraf moet worden aangepast omdat deze in de praktijk grotendeels onwerkbaar blijkt, althans zijn doel voorbijschiet.[34] Velen waarschuwden hier voor tijdens het wetgevingsproces, maar toch werden deze geluiden pas gehoord na de invoering in de

25 *Kamerstukken II* 2012/13, 33 662, nr. 2.
26 Hierover later meer. Vgl. *Kamerstukken II* 2012/13, 33 662, nr. 3, p. 13; *Kamerstukken II* 2012/13, 33 662, nr. 4, p. 2 en 8; en artikel 7 Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden.
27 Artikel 34a lid 1 van het wetsvoorstel. *Kamerstukken II* 2012/13, 33 662, nr. 2.
28 Artikel 34a lid 2 van het wetsvoorstel.
29 *Kamerstukken II* 2012/13, 33 662, nr. 3, p. 7.
30 *Kamerstukken II* 2012/13, 33 662, nr. 3, p. 7 en 8.
31 *Kamerstukken II* 2012/13, 33 662, nr. 3, p. 22.
32 Anders M. Bolhuis, 'Toenemende aandacht voor meldplicht datalekken ter bescherming van persoonsgegevens, Quo Vadis?', *Mediaforum* 2013, p. 174-186, p. 182 en 185.
33 *Kamerstukken II* 2012/13, 33 662, nr. 3, p. 10.
34 Vgl. conceptwetsvoorstel ten behoeve van internetconsultatie, wijziging van de telecommunicatiewet (wijziging artikel 11.7a).

praktijk. De implementatie van deze regels heeft het bedrijfsleven echter al veel geld gekost.

Om te voorkomen dat het CBP wordt overstelpt met meldingen, hoeven niet alle inbreuken te worden gemeld. Anders dan in artikel 11.3a TCOMW gaat het niet om een inbreuk op beveiligingsmaatregelen die nadelige gevolgen heeft (of kan hebben), maar om inbreuken op beveiligingsmaatregelen waarvan *redelijkerwijs* kan worden aangenomen dat die leiden tot een *aanmerkelijke kans* op nadelige gevolgen. Uit de MvT bij de TCOMW blijkt dat er moet worden gemeld als er sprake is van inbreuken op de beveiliging die nadelige gevolgen *kunnen* hebben voor de veiligheid van persoonsgegevens.[35] De afwijking in de Wbp dat er een *aanmerkelijke kans* moet zijn op dergelijke gevolgen is volgens de staatssecretaris gerechtvaardigd omdat de aanbieders van openbare elektronische communicatiediensten een dergelijke gevoelige dienst bieden die strengere regels rechtvaardigt dan de regels voor willekeurig alle verantwoordelijken van persoonsgegevens.[36] De staatssecretaris wil een werkbare bepaling. Volgens de MvT zou de effectiviteit van de meldplicht snel aan betekenis verliezen indien elk denkbaar datalek zou moeten worden gemeld en een meldplicht zonder enige beperking zou ook tot een nodeloze belasting leiden voor het bedrijfsleven en de overheid.[37] Dit is toe te juichen, maar het is de vraag of het risico van een boete van € 450 000 niet toch zal leiden tot veel onnodige meldingen gelet op de onbepaaldheid van de normen.

Ook de Raad van State wees erop dat begrippen als 'redelijkerwijs', 'aanmerkelijk' en 'nadelig' onbepaalde normen zijn en dat het niet de taak zou zijn van de toezichthouder (het CBP) om een door straf te handhaven bepaling nader te preciseren. Dit is aan de wetgever. De hele Wbp is echter doorspekt met dergelijke onbepaalde en open normen en in die zin past de bepaling hier dus prima bij. Toegegeven, het zal ook lastig zijn deze begrippen nader te specificeren, tenzij bijvoorbeeld een systeem zou worden gekozen zoals in Duitsland (waarbij een melding moet worden gedaan indien bepaalde categorieën gegevens zijn gecompromitteerd), maar hiervoor is bewust niet gekozen.[38]

Een boetebepaling van € 450 000 waar de maximale bestuurlijke boete nu € 4500 bedraagt[39] voor het overtreden van de andere meldplicht (een specifieke bepaling in de Wbp op basis waarvan gegevensverwerkingen moeten worden gemeld bij het CBP,[40] een schending die ook strafbaar is gesteld[41]) past echter niet bij deze onbepaalde normen.[42] Het *lex certa*-beginsel vereist dat de delictsomschrijving van een strafbepaling zo precies en zo beperkt mogelijk is. Voor de burger moet voorzienbaar zijn welke concrete handelingen (of het nalaten ervan) tot straffen kunnen leiden. Bovendien zal de vaagheid van de norm en de forse boete die op het niet naleven van de meldplicht staat er volgens de Raad van State toe kunnen leiden dat vaker onnodig zal worden gemeld met alle gevolgen van dien voor de effectiviteit van de meldingen en de hoogte van bestuurlijke en administratieve lasten.[43]

2.3 *Wat moet worden gemeld?*

Zowel aan het CBP als aan de betrokkene(n) omvat de kennisgeving in ieder geval: (i) de aard van de inbreuk, (ii) de instanties waar meer informatie over de inbreuk kan worden verkregen, en (iii) de aanbevolen maatregelen om de *negatieve gevolgen* van de inbreuk te beperken.[44]

De begrippen '*nadelige gevolgen*', '*ongunstige gevolgen*' en nu weer '*negatieve gevolgen*' worden (evenals in artikel 11.3a TCOMW) naast elkaar gebruikt. Dit komt natuurlijk door de richtlijn[45] ten gevolge waarvan artikel 11.3a TCOMW begrippen als 'ongunstige gevolgen' en 'negatieve gevolgen' introduceerde, maar het is de vraag of het daarom ook moet worden herhaald in artikel 34a Wbp. Aan de andere kant zal er waarschijnlijk ook niet zo'n groot verschil zijn tussen al deze begrippen omdat alles altijd af zal hangen van de bekende omstandigheden van het geval en is het misschien handig zo veel mogelijk aan te sluiten bij artikel 11.3a TCOMW.[46]

De MvT vermeldt dat bij de aard van de inbreuk doorgaans met een algemene omschrijving zal kunnen worden volstaan. Als de betrokkene wil weten waar hij persoonlijk aan toe is, kan hij contact opnemen met het bedrijf. Daarom moeten contactgegevens worden vermeld in de kennisgeving. Wat betreft de aanbevolen maatregelen kan worden gedacht aan het veranderen van ge-

35 Wijziging van de Telecommunicatiewet ter implementatie van de herziene telecommunicatierichtlijnen, *Kamerstukken II* 2010/11, 32 549, nr. 3, paragraaf 1.8.
36 Vgl. ook brief van de Staatssecretaris van Veiligheid en Justitie, 23 oktober 2012, *Kamerstukken II* 2012/13, 32 761, nr. 44.
37 Vgl. *Kamerstukken II* 2012/13, 33 662, nr. 3, p. 6.
38 Vgl. *Kamerstukken II* 2012/13, 33 662, nr. 3, p. 6.
39 Artikel 66 Wbp.
40 Artikel 27 en 28 Wbp.
41 Artikel 75 Wbp.
42 Vgl. *Kamerstukken II* 2012/13, 33 662, nr. 4, p. 7.
43 Uit *Kamerstukken II* 2012/13, 33 662, nr. 4, p. 2 en 8.
44 Artikel 34a lid 3 Wbp.
45 Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische communicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming. Vgl. ook M. Bolhuis, 'Toenemende aandacht voor meldplicht datalekken ter bescherming van persoonsgegevens, Quo Vadis?', *Mediaforum* 2013, p. 174-186 voor een uitgebreide analyse.
46 Hoewel er toch ook belangrijke verschillen zijn.

bruikersnamen en wachtwoorden, of het melden bij de creditcardmaatschappij.[47] Dit is ook van belang voor aansprakelijkheidsclaims in verband met een beroep op 'eigen schuld van de betrokkene'.[48]

Overigens dient deze in de kennisgeving opgenomen informatie, alsmede (anders dan vermeld in artikel 11.3a lid 6 TCOMW[49]) de tekst van de kennisgeving aan betrokkene(n) ook te worden bewaard door de verantwoordelijke zelf. De verantwoordelijke dient een overzicht bij te houden van *alle* inbreuken. Dit betreft dus ook inbreuken die wel zijn geconstateerd, maar niet zijn gemeld. Aan de hand van het protocol zou overigens moeten kunnen worden aangetoond welke inbreuk is geconstateerd en welke maatregelen zijn genomen.[50]

De MvT vermeldt dat wordt verwacht dat het overgrote deel van meldingen bij het CBP geen aanleiding zal geven tot een onderzoek of handhavingsmaatregelen. Het CBP zal de meldingen beoordelen en een inschatting moeten maken of er aanleiding is een onderzoek in te stellen. Een dergelijk onderzoek kan vervolgens leiden tot handhavingsmaatregelen. Factoren als de omvang van het datalek, de potentiële gevolgen ervan en de aard van de gegevens zullen een rol spelen bij deze afweging door het CBP. Het valt nog niet te voorzien in hoeveel gevallen de meldingen aanleiding zullen geven tot verdere actie.[51] Wellicht wordt het CBP dusdanig overspoeld met meldingen dat deze verplichting uiteindelijk feitelijk een wassen neus wordt.

De kennisgeving aan het CBP omvat daarnaast een beschrijving van (i) de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens, en (ii) de maatregelen die de verantwoordelijke heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen.[52] Deze informatie zal veelal technisch van aard zijn. Het kan zijn dat melding moet worden gemaakt van technische details die van vertrouwelijke aard zijn. Bedrijven kunnen dergelijke gegevens volgens de MvT desgewenst expliciet als bedrijfsvertrouwelijk aanmerken in de zin van artikel 10 lid 1 onder c Wet openbaarheid van bestuur.[53]

Waarom er zo veel tekstuele verschillen zijn met artikel 11.3a TCOMW is onduidelijk. Zo staat er in 11.3a lid 3 TCOMW dat de kennisgeving aan de toezichthouder tevens de '*gevolgen van de inbreuk*' moet omvatten en de maatregelen die de aanbieder voorstelt of heeft getroffen '*om de inbreuk aan te pakken*' terwijl artikel 34a Wbp spreekt over een beschrijving van de '*geconstateerde en vermoedelijke gevolgen*' van de inbreuk en de maatregelen die de verantwoordelijke heeft getroffen of voorstelt te treffen '*om deze gevolgen te verhelpen*'. De Uitvoeringsverordening vermeldt overigens dat de potentiële gevolgen en potentiële negatieve gevolgen moeten worden vermeld dus uiteindelijk zullen de meldplichten voor een groot deel op hetzelfde neerkomen door de feitelijke invulling daarvan in nadere richtlijnen, maar het is onduidelijk waarom dit in steeds andere woorden moet. Zo ook de omschrijving van de uitzondering dat geen kennisgeving aan de betrokkene hoeft te worden gedaan indien de gegevens zijn versleuteld, of onbegrijpelijk zijn voor (i) eenieder die '*geen recht heeft op toegang tot die gegevens*' (artikel 11.3a lid 5 TCOMW), respectievelijk (ii) eenieder die '*geen recht heeft op kennisname van de gegevens*' (artikel 34a lid 6 Wbp). In de Uitvoeringsverordening is expliciet bepaald dat de kennisgeving niet mag worden gebruikt om nieuwe of aanvullende diensten te bevorderen of als reclame. Dit is (nog) niet in artikel 34a Wbp opgenomen, maar het is de vraag of dit in de praktijk snel zal gebeuren. Bovendien zijn er nog de algemene (marketing)vereisten waaraan moet worden voldaan.[54]

Ten slotte hoeven slechts inbreuken op beveiligingsmaatregelen te worden gemeld. Dit betekent strikt genomen dat als er geen beveiligingsmaatregelen worden getroffen, er ook niet hoeft te worden gemeld. Ook de Raad van State heeft hierop gewezen, maar de staatssecretaris vond dit een dusdanig hypothetische situatie dat hij heeft besloten de bepaling zo te laten. Een onderneming zonder beveiligingsmaatregelen loopt een te groot risico op bijvoorbeeld aansprakelijkheidsclaims en reputatieschade.[55] Ik voeg daar nog aan toe dat een onderneming altijd wel een beveiligingsmaatregel zal hebben getroffen al is het maar een toegangspassensysteem, een inbraakalarm of de sleutel op de voordeur. Toch meen ik dat een zuivere wettekst waarbij hypothetische situaties zo veel mogelijk worden uitgesloten de voorkeur verdient en niet te snel de gemakkelijke weg moet worden gekozen. Aan de andere kant sluit de bepaling nu wel weer aan bij artikel 11.3a TCOMW.

2.4 *Hoe melden aan betrokkene(n)?*

De kennisgeving aan de betrokkene(n) moet op zodanige wijze worden gedaan dat, rekening houdend met de aard van de inbreuk, de geconstateerde en de feitelijke gevolgen daarvan voor de verwerking van persoonsgegevens, de kring van betrokkenen en de kosten van tenuitvoerlegging, een behoorlijke en zorgvuldige informatievoorziening is gewaarborgd.[56]

47 *Kamerstukken II* 2012/13, 33 662, nr. 3, p. 19 en 22.
48 Vgl. ook *Kamerstukken II* 2012/13, 33 662, nr. 3, p. 9.
49 In zowel artikel 11.3a lid 6 TCOMW als artikel 34a lid 8 Wbp wordt verwezen naar 'het derde lid' van de wet, maar deze bevat in de TCOMW meer informatie. In artikel 34a Wbp wordt ook genoemd 'de tekst van de kennisgeving aan de betrokkene'.
50 Artikel 34a lid 8 Wbp. *Kamerstukken II* 2012/13, 33 662, nr. 3, p. 23.
51 *Kamerstukken II* 2012/13, 33 662, nr. 3, p. 17.
52 Artikel 34a lid 4 Wbp.
53 *Kamerstukken II* 2012/13, 33 662, nr. 3, p. 22.
54 Zoals artikel 8, 9 en 41 Wbp en artikel 11.7 TCOMW en bijvoorbeeld de Reclame Code.
55 Vgl. *Kamerstukken II* 2012/13, 33 662, nr. 4, p. 12.
56 Artikel 34a lid 5 Wbp.

De MvT vermeldt dat wanneer de inbreuk zich beperkt tot een verhoudingsgewijs klein aantal betrokkenen, deze persoonlijk en gericht kunnen worden benaderd. Als de inbreuk een groot aantal betrokkenen betreft zou naast een bekendmaking op een website een advertentie in de dagbladen meer in de rede liggen.[57] Dit is dus anders dan in de Uitvoeringsverordening.

2.5 *Uitzonderingen*

De kennisgeving aan de betrokkene(n) is niet vereist indien gepaste technische beschermingsmaatregelen zijn genomen waardoor de persoonsgegevens die het betreft versleuteld zijn of anderszins onbegrijpelijk zijn gemaakt voor eenieder die geen recht heeft op kennisname van de gegevens.[58] Indien de gegevens versleuteld zijn of onbegrijpelijk zijn, zou overigens beargumenteerd kunnen worden dat de Wbp niet langer op die gegevens van toepassing is (mits het gebruikte algoritme voldoende sterk is en de sleutel niet ook is (mee)gelekt, zodat ten minste geen sprake is van persoonsgegevens voor de ontvanger), maar de toepasselijkheid van de Wbp wordt – ten onrechte – steeds ruimer.[59] Bovendien zou de inbreuk na een dergelijke versleuteling niet meer voldoen aan de criteria van '*waarschijnlijk ongunstige gevolgen*' voor de persoonlijke levenssfeer en zou een uitzondering voor dit geval dus niet nodig zijn.[60] Van zo'n inbreuk zou ook niet *redelijkerwijs* kunnen worden aangenomen dat die leidt tot een *aanmerkelijke kans op nadelige gevolgen voor de bescherming van persoonsgegevens* die door de verantwoordelijke worden verwerkt.[61]

Indien geen kennisgeving is gedaan aan de betrokkene(n), kan het CBP, indien het van oordeel is dat de inbreuk waarschijnlijk *nadelige gevolgen* zal hebben voor de persoonlijke levenssfeer van de betrokkene(n), verlangen dat alsnog een kennisgeving wordt gedaan.[62] De spiegelbeeldige bepaling in artikel 11.3a lid 4 TCOMW vermeldt overigens '*ongunstige gevolgen*' in plaats van '*nadelige gevolgen*'. Dit is ook beter, omdat een betrokkene ingevolge het Wetsvoorstel meldplicht datalekken onverwijld in kennis moet worden gesteld van een inbreuk indien deze inbreuk waarschijnlijk *ongunstige gevolgen* zal hebben voor diens persoonlijke levenssfeer. Waarom dan vervolgens wordt gerefereerd aan nadelige gevolgen is onduidelijk. Een bepaling zoals in de Uitvoeringsverordening inzake mogelijk uitstel als een kennisgeving een correct onderzoek in gevaar kan brengen, is ook wenselijk. Dit zou kunnen worden opgelost door in artikel 43 Wbp te verwijzen naar 34a (lid 2) Wbp. Hoewel het wellicht beter is dit aan toestemming van de toezichthouder onderhevig te laten zijn en dus een aparte uitzondering op te nemen in artikel 34a Wbp.

Er hoeft geen melding te worden gedaan ingevolge artikel 34a Wbp indien de verantwoordelijke in zijn hoedanigheid als aanbieder van een openbare elektronische communicatiedienst (in verband met de levering van openbare elektronische communicatiediensten) al een kennisgeving heeft gedaan ingevolge artikel 11.3a TCOMW.[63] Dergelijke aanbieders moeten nu melden bij de ACM, maar ingevolge het wetsvoorstel zullen zij in plaats daarvan moeten gaan melden bij het CBP. Deze uitzondering geldt overigens niet in situaties waarin de verantwoordelijke een ander is dan de aanbieder van de openbare elektronische communicatiedienst (bijvoorbeeld in het geval de aanbieder een bewerker is in de zin van de Wbp). In dat geval zouden beide partijen een melding moeten doen (op grond van artikel 34a Wbp, respectievelijk 11.3a TCOMW). Indien de verantwoordelijke dezelfde is als de aanbieder van de openbare elektronische communicatiedienst doet deze de melding op grond van artikel 11.3a TCOMW.[64]

Financiële ondernemingen als bedoeld in de Wft hoeven betrokkene(n) niet op de hoogte te stellen, maar moeten wel melden bij het CBP.[65] Financiële ondernemingen hebben een meldplicht ingevolge de Wft (en het Besluit prudentiële regels Wft en het Besluit gedragstoezicht financiële ondernemingen). Openbare kennisgevingen aan betrokkenen worden in de financiële sector – mede tegen de achtergrond van de financiële crisis – als te risicovol ervaren om dwingend te worden voorgeschreven. De zorgplicht van de financiële onderneming waarborgt dat zo'n onderneming verantwoordelijkheid jegens de cliënten zal nemen in rechtstreeks contact met die cliënten.[66] Een dubbele meldplicht bij het CBP respectievelijk de DNB of AFM bestaat alleen als een datalek eveneens een *incident* is in de zin van de Wft (en bovengenoemde Besluiten). Een dergelijk *incident* is een gedraging of gebeurtenis die een ernstig gevaar vormt voor de integere uitoefening van het bedrijf van de financiële onderneming.[67]

---

57 *Kamerstukken II* 2012/13, 33 662, nr. 3, p. 22.
58 Artikel 34 lid 6 Wbp.
59 Vgl. bijvoorbeeld ook de discussie wanneer sprake is van persoonsgegevens zoals IP-adressen, in G.-J. Zwenne, 'Over IP-adressen en persoonsgegevens, en het verschil tussen individualiseren en identificeren', *Tijdschrift voor internetrecht* 2011, p. 4-9; G.-J. Zwenne, 'Regulering van IP-adressen (en andere mogelijke identifiers)', *Tijdschrift voor internetrecht* 2011, p. 40-43; en G.-J. Zwenne, *De verwaterde privacywet* (oratie Leiden), d.d. 12 april 2013.
60 Er zijn onder meer over artikel 34a lid 6 Wbp Kamervragen gesteld. Vergelijk *Kamerstukken II* 2012/13, 33 662, nr. 5.
61 Artikel 34a lid 1 Wbp.
62 Artikel 34a lid 7 Wbp.
63 Artikel 34a lid 9 Wbp.
64 Vgl. ook *Kamerstukken II* 2012/13, 33 662, nr. 3, p. 23 en 24.
65 Artikel 34a lid 10 Wbp.
66 Vgl. *Kamerstukken II* 2012/13, 33 662, nr. 3, p. 11 en 12.
67 Vgl. *Kamerstukken II* 2012/13, 33 662, nr. 3, p. 11 en 12. Definitie van incident in artikel 1 van het Besluit prudentiële regels Wft en artikel 1 van het Besluit gedragstoezicht financiële ondernemingen Wft.

2.6 *Bewerkers*

Voor zover een onderneming (als verantwoordelijke voor persoonsgegevens) bewerkers inschakelt die deze persoonsgegevens in opdracht van en ten behoeve van de verantwoordelijke verwerken, is het belangrijk in de (bewerkers)overeenkomst rekening te houden met deze meldplicht. De bewerker zou minimaal verplicht moeten zijn tot melding aan de verantwoordelijke van een inbreuk op de beveiliging, waarvan redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijke kans op nadelige gevolgen voor de persoonsgegevens die door hem worden verwerkt.[68]

Gelet op deze open norm verdient het aanbeveling de meldplicht in de overeenkomst ruimer te formuleren en aanvullende waarborgen op te nemen. Het CBP heeft hiervoor een checklist opgenomen in de richtsnoeren beveiliging van persoonsgegevens.[69]

2.7 *Meer bevoegdheden voor het CBP*

Bij algemene maatregel van bestuur kunnen nadere regels worden gesteld met betrekking tot de (inhoud en wijze van) kennisgeving. Daarnaast is aangekondigd dat nog een nota van wijziging op het onderhavige wetsvoorstel zal worden ingediend die voorziet in een regeling die strekt tot uitbreiding van de bestuurlijke (boete)bevoegdheden van het CBP met het oog op de versterking van de handhaving van de Wbp. De MvT vermeldt dat de handhaving van algemeen-abstract geformuleerde normen afzonderlijke aandacht vraagt uit hoofde van artikel 7 van het Europees Verdrag ter bescherming van de rechten van de mens en de fundamentele vrijheden, vooral op het punt van het *lex certa*-beginsel en de kwestie van de voorzienbaarheid van overtredingen.[70]

3 Wat staat ons verder nog te wachten

3.1 *Verordening*

Wat staat ons verder nog te wachten aan geïntroduceerde wettelijke meldplichten. Allereerst is daar de Verordening[71] die de Privacyrichtlijn 95/46/EG[72] in de toekomst zou moeten vervangen. Het is de vraag of deze Verordening nog voor de Europese parlementsverkiezingen zal kunnen worden goedgekeurd gelet op het grote aantal amendementen en controversiële onderwerpen.[73]

De in januari 2012 voorgestelde Verordening introduceert een meldplicht waarbij een inbreuk in verband met persoonsgegevens aan de toezichthouder moet worden gemeld *zonder onnodige vertraging en zo mogelijk niet later dan 24 uur* nadat daarvan kennis is gekregen. Indien de melding niet binnen 24 uur plaatsvindt, dient er een motivering mee te worden gestuurd.[74] Indien een onderneming als bewerker optreedt dient deze de verantwoordelijke onmiddellijk na de vaststelling van een inbreuk te waarschuwen.[75]

De melding bevat ten minste:[76]

a. een omschrijving van de aard van de inbreuk, waaronder de betrokken categorieën en aantallen betrokkenen en categorieën en aantallen gegevensrecords;
b. de vermelding van de identiteit en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
c. aanbevelingen voor maatregelen om de mogelijk nadelige gevolgen van de inbreuk te verminderen;
d. een omschrijving van de gevolgen van de inbreuk;
e. een omschrijving van de maatregelen die de verantwoordelijke heeft voorgesteld of genomen om de inbreuk aan te pakken.

Het valt op dat deze bepaling in de Verordening niet is overgenomen in het Wetsvoorstel meldplicht datalekken, maar dat is aangesloten bij artikel 11.3a TCOMW. Blijkbaar heeft de wetgever zelf ook weinig vertrouwen in een goede (althans spoedige) afloop.[77] De Europese Toezichthouder voor gegevensbescherming adviseert overigens een termijn van 72 uur in plaats van 24 uur.[78] Ook in de Raad van de Europese Unie[79] is een voorstel besproken met een termijn van 72 uur. Ook zijn er wijzigingen voorgesteld dat er slechts een meldplicht zou zijn als de 'personal data breach is likely to *severely* affect the rights and freedoms of data subjects'. Voorts zijn wat andere

68 Vgl. ook de voorgestelde aanpassingen in artikel 14 Wbp.
69 CBP-Richtsnoeren beveiliging van persoonsgegevens d.d. februari 2013 die op 1 maart 2013 in werking zijn getreden.
70 *Kamerstukken II* 2012/13, 33 662, nr. 3, p. 13.
71 Voorstel voor een Verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (algemene verordening gegevensbescherming), d.d. 25 januari 2012, COM(2012)11 final.
72 Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.
73 Zie bijvoorbeeld ook H. Kranenborg, 'Nieuwe Europese regels voor de bescherming van persoonsgegevens van belang voor iedereen', *SEW* 2013, p. 309-321; alsmede D. de Bot & E. Kindt, 'Het advies van de Belgische Privacycommissie over het Europese Voorstel Algemene Verordening Gegevensbescherming', *P&I* 2013, p. 168-173.
74 Artikel 31 lid 1 Verordening.
75 Artikel 31 lid 2 Verordening.
76 Artikel 31 lid 3 Verordening.
77 Zie ook *Kamerstukken II* 2012/13, 33 662, nr. 3, p. 3: 'Het is nog te prematuur om ervan uit te gaan dat de Europese wetgever met een redelijke mate van zekerheid regeling overeenkomstig het voorstel zal vaststellen. Naar verwachting zal het bovendien nog geruime tijd duren voor de ontwerpverordening wordt vastgesteld.'
78 Vgl. De Europese Toezichthouder voor gegevensbescherming, 'Samenvatting van het EDPS-advies van 7 maart 2012 over het hervormingspakket gegevensbescherming', (2012/C 192/05). De volledige tekst van dit advies is te vinden op de website van de EDPS, www.edps.europa.eu.
79 De Raad van ministers.

wijzigingen voorgesteld om de verplichting af te zwakken, zoals hetgeen moet worden gemeld.[80]

De verantwoordelijke dient alle inbreuken in verband met persoonsgegevens te documenteren, waaronder de feiten omtrent de inbreuk, de gevolgen van de inbreuk en de corrigerende maatregelen die zijn genomen. Deze documenten moeten de toezichthouder in staat stellen om de naleving van dit artikel te controleren. De documenten omvatten uitsluitend de voor dat doel noodzakelijke informatie.[81]

De Europese Commissie is bevoegd gedelegeerde handelingen vast te stellen met het oog op de nadere invulling van de criteria en de vereisten voor de vaststelling van de inbreuken en voor de bijzondere omstandigheden waarin een verantwoordelijke en een bewerker verplicht zijn de inbreuk te melden.[82]

De Europese Commissie kan het model vaststellen voor deze melding aan de toezichthouder alsmede de toepasselijke procedures en de vorm en de modaliteiten, waaronder de termijnen voor het wissen van de daarin opgenomen informatie.[83]

Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk *negatieve gevolgen* voor de bescherming van de persoonsgegevens of de privacy van de betrokkene heeft, deelt de verantwoordelijke na de melding aan de toezichthouder, de betrokkene de inbreuk *zonder onnodige vertraging* mee.[84] Deze mededeling bevat een omschrijving van de aard van de inbreuk in verband met persoonsgegevens en ten minste:

– de vermelding van de identiteit en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen; en
– aanbevelingen voor maatregelen om de mogelijk nadelige gevolgen van de inbreuk te verminderen.[85]

In de overwegingen van de Verordening wordt vermeld dat een inbreuk moet worden geacht negatieve gevolgen te hebben voor de persoonsgegevens of de persoonlijke levenssfeer van een betrokkene indien de inbreuk kan leiden tot bijvoorbeeld identiteitsdiefstal- of fraude, lichamelijke schade, ernstige vernedering of aantasting van de reputatie.[86] Deze formulering sluit aan bij de formulering van de Uitvoeringsverordening. Ook dienen (net als in de Uitvoeringsverordening) alle inbreuken te worden gemeld bij de toezichthouder, in plaats van – zoals in het Wetsvoorstel meldplicht datalekken – die inbreuken waarbij geldt dat er *redelijkerwijs* kan worden aangenomen dat er een *aanmerkelijke* kans bestaat op nadelige gevolgen.[87]

De melding van een inbreuk aan de betrokkene is niet vereist wanneer de verantwoordelijke tot voldoening van de toezichthouder aantoont dat hij passende technische beschermingsmaatregelen heeft genomen en dat deze maatregelen werden toegepast op de gegevens waarop de inbreuk betrekking heeft. De gegevens moeten onbegrijpelijk zijn voor eenieder die geen recht op toegang heeft.[88] Dit laatste is vergelijkbaar met de bepalingen als opgenomen in artikel 34a Wbp en artikel 11.3a TCOMW. Onverminderd de verplichting van de verantwoordelijke om de inbreuk aan de betrokkene te melden, kan de toezichthouder, na de waarschijnlijkheid van negatieve gevolgen van de inbreuk te hebben overwogen, de verantwoordelijke gelasten de inbreuk aan de betrokkene te melden wanneer dit nog niet is gedaan.[89]

De Europese Commissie is bevoegd gedelegeerde handelingen vast te stellen met het oog op de nadere invulling van de criteria en de vereisten met betrekking tot de omstandigheden waarin een inbreuk in verband met persoonsgegevens waarschijnlijk negatieve gevolgen heeft.[90] De Europese Commissie kan het model van de melding aan de betrokkene en de op die melding toepasselijke procedure vaststellen.[91]

3.2 *Meldplicht ICT-inbreuken vitale sectoren*

Ten slotte is op 22 juli 2013 het wetsvoorstel (Wet melding inbreuken elektronische informatiesystemen) ter consultatie aangeboden. Dit wetsvoorstel introduceert een meldplicht voor ICT-inbreuken; ongeacht of sprake is van persoonsgegevens. De einddatum van de consultatie was 17 september 2013. Het wetsvoorstel voorziet niet in de mogelijkheid van sanctionering.

De meldplicht geldt alleen voor aanbieders van producten of diensten waarvan de beschikbaarheid of betrouwbaarheid van vitaal belang is voor de Nederlandse samenleving, en alleen als de inbreuk tot gevolg heeft of kan hebben dat die beschikbaarheid of betrouwbaarheid in belangrijke mate wordt onderbroken. Deze aanbieders van vitale producten of diensten bevinden zich binnen de sectoren elektriciteit, gas, drinkwater, telecom, keren en beheren oppervlaktewater, financiën, overheid en transport, zoals energienetwerkbeheerders, drinkwater-

80 Interinstitutional file 2012/0011(COD); 10227/13 ADD1; Council of the European Union d.d. 31 mei 2013.
81 Artikel 31 lid 4 Verordening.
82 Artikel 31 lid 5 Verordening.
83 Artikel 31 lid 6 Verordening.
84 Artikel 32 lid 1 Verordening.
85 Artikel 32 lid 2 Verordening.
86 Overweging 67, p. 33 van de Verordening.
87 Zo ook M. Bolhuis, 'Toenemende aandacht voor meldplicht datalekken ter bescherming van persoonsgegevens, Quo Vadis?', *Mediaforum* 2013, p. 174-186, p. 183.
88 Artikel 32 lid 3 Verordening.
89 Artikel 32 lid 4 Verordening.
90 Artikel 32 lid 5 Verordening.
91 Artikel 32 lid 6 Verordening.

bedrijven, telecombedrijven, beheerders van hoofdwaterkeringen, banken, het Havenbedrijf Rotterdam, de NV Luchthaven Schiphol en Luchtverkeersleiding Nederland. Het gaat om onderdelen van de vitale infrastructuur waarbij een ICT-inbreuk direct of indirect tot maatschappelijke ontwrichting kan leiden. De aanbieders worden bij algemene maatregel van bestuur aangewezen.[92] Voor certificaatdienstverleners zal de melding van ICT-inbreuken langs andere weg worden vormgegeven.

De melding moet (onverwijld) worden gedaan aan de Minister van Veiligheid en Justitie. De melding wordt behandeld door het Nationaal Cyber Security Centrum (NCSC), een onderdeel van het ministerie. De meldplicht heeft primair tot doel om het NCSC in staat te stellen om de risico's van de ICT-inbreuk te kunnen inschatten en de door de inbreuk getroffen aanbieder bij te staan met als uiteindelijk doel het voorkomen of beperken van maatschappelijke ontwrichting. De verstrekte gegevens mogen vervolgens ook worden gebruikt als basis voor advies en informatie aan andere vitale aanbieders en het publiek. Dit laatste kan bijvoorbeeld inhouden dat wordt gewaarschuwd voor de risico's van een door internetcriminelen gehanteerde werkwijze of dat ervoor wordt gewaarschuwd dat een bepaald product of een bepaalde dienst tot nader order beter niet kan worden gebruikt.[93]

De melding die moet worden gedaan omvat in ieder geval:[94]

a. de aard en omvang van de inbreuk (op de veiligheid) of het verlies (van integriteit van een informatiesysteem) waardoor de beschikbaarheid of betrouwbaarheid van een product of dienst in belangrijke mate wordt of kan worden onderbroken;
b. het tijdstip van de aanvang van de inbreuk of het verlies;
c. de mogelijke gevolgen van de inbreuk of het verlies;
d. een prognose van de hersteltijd;
e. zo mogelijk de door de aanbieder genomen of te nemen maatregelen om de gevolgen van de inbreuk of het verlies te beperken of herhaling hiervan te voorkomen;
f. de contactgegevens van de in Nederland gevestigde functionaris die verantwoordelijk is voor het doen van de kennisgeving.

Desgevraagd verstrekt de aanbieder die een melding heeft gedaan, de minister onverwijld alle overige gegevens die nodig zijn om:

a. de risico's voor de beschikbaarheid of betrouwbaarheid van het product of de dienst in te schatten;
b. de aanbieder bij te staan bij het treffen van maatregelen om de beschikbaarheid en betrouwbaarheid van het product of de dienst te waarborgen of te herstellen.[95]

Het NCSC gaat geen toezicht houden op de naleving van de meldplicht en krijgt ook geen handhavingsbevoegdheden. Het NCSC is primair gericht op het bieden van hulp. Wel kan het NCSC de instanties die belast zijn met het toezicht op de naleving door de betrokken aanbieder van de op hem van toepassing zijnde wetgeving informeren als blijkt dat de meldplicht opzettelijk niet is nageleefd. Aan de hand daarvan kan de sectorale toezichthouder besluiten of niet-naleving van de meldplicht voor hem aanleiding vormt om het sectorale toezicht aan te scherpen. Mocht blijken dat de meldplicht onvoldoende wordt nageleefd, dan kan alsnog worden besloten tot het inrichten van een stelsel van toezicht en handhaving.[96] Deze meldplicht laat de reeds bestaande, of te introduceren meldplichten dus intact.

Deze meldplicht sluit ten dele aan bij het idee van een voorgestelde Richtlijn inzake netwerk- en informatiebeveiliging.[97] De sectoren waarop de richtlijn van toepassing zou moeten zijn en dit wetsvoorstel verschillen echter.

Ten slotte zullen nog andere wettelijke meldplichten volgen voor bijvoorbeeld certificatiedienstverleners ten aanzien van gekwalificeerde certificaten.[98]

4 Een draaiboek en een slot

4.1 *Een draaiboek*

Alle cybersecurity-incidenten ten spijt lijken veel ondernemingen nog niet doordrongen van de risico's die deze incidenten kunnen hebben. Toch doen bedrijven er goed aan een draaiboek te hebben indien zich onverhoopt een incident voordoet. Zelfs wanneer de onderneming als een onneembare vesting is beveiligd, hoeft er maar één medewerker te zijn die een menselijke fout maakt om al die beveiligingsmaatregelen teniet te doen. Standaardvoorbeelden zijn het in een computer stoppen van een in de parkeergarage gevonden USB-stick, het afgeven van een wachtwoord aan een 'social engineer' die zich voordoet als een helpdeskmedewerker, het openhouden van de deur voor een onbevoegde zonder toegangspas, of het verliezen van USB-sticks en laptops.

In een incidentendraaiboek zouden onderwerpen aan de orde moeten komen als:

– Wie maken er deel uit van het responseteam en hoe werkt de interne rapportage?

92 Artikel 2 van het wetsvoorstel (Wet houdende regels over het melden van een inbreuk op de veiligheid of een verlies van integriteit van elektronische informatiesystemen die van vitaal belang zijn voor de Nederlandse samenleving (Wet melding inbreuken elektronische informatiesystemen)) en p. 1, 3 en 7 van de MvT.
93 MvT, p. 8
94 Artikel 3 van het wetsvoorstel.
95 Artikel 4 van het wetsvoorstel.
96 MvT, p. 5.
97 Voorstel voor een Richtlijn van het Europees Parlement en de Raad houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen, d.d. 7 februari 2013 COM(2013)48 final; 2013/0027(COD). Zie ook M.A.M. Verveld-Suijkerbuijk & A.J.P. Tillema, 'Netwerk- en informatiebeveiliging: ontwikkelingen in het regelgevende kader', *Ondernemingsrecht* 2013, p. 390-395.
98 Zie ook *Kamerstukken II* 2012/13, 33 662, nr. 3, p. 3 en 4.

– Gaan wij het lek onmiddellijk dichten, of in eerste instantie slechts de toegang tot informatie beperken zodat wij eerst informatie kunnen vergaren over de indringer?
– Het inventariseren van de informatie die op straat ligt, alsmede de risico's.
– Het al dan niet doen van aangifte en vaststellen of sprake is van strafrechtelijke verwijtbaarheid. Dit kan bijvoorbeeld spelen wanneer er sprake is van betrokkenheid vanuit de organisatie zelf of wanneer er onvoldoende maatregelen zijn getroffen om ongeregeldheden te voorkomen.[99]
– Moeten autoriteiten worden geïnformeerd? Dit kan een vrijwillige keuze zijn, maar voor bepaalde bedrijven geldt een meldplicht.
– Moeten individuen of bedrijven worden geïnformeerd? Soms bepalen contracten hier iets over. Ook kan het nuttig zijn te informeren in het kader van het beperken van de schade en een mogelijk beroep op eigen schuld.[100] Ook de Wbp en het Burgerlijk Wetboek bevatten open normen zoals de informatieplicht aan individuen waaruit een dergelijke plicht mogelijk kan worden afgeleid.[101] Verder kan er een openbaarmakingsverplichting zijn omdat koersgevoelige informatie is gelekt.[102]
– Hoe zit het met de aansprakelijkheid zoals uit hoofde van wanprestatie[103] (omdat een geheimhoudingsverplichting is geschonden, of in strijd met een contractuele verplichting onvoldoende beveiliging is gerealiseerd) of onrechtmatige daad.[104]
– Welke schade is gedekt door de verzekeringspolis? Het inventariseren van verzekerde risico's verdient aanbeveling voordat zich een beveiligingsincident heeft voorgedaan.

Bij bovengenoemde inventarisatie moet ook rekening worden gehouden met internationale aspecten. Zo kan er een meldplicht zijn in het buitenland. Bij het schrijven van het draaiboek kan alvast worden geanticipeerd op nieuwe meldplichten zodat dit op orde is zodra de meldplicht een feit wordt.

4.2 *Ten slotte*

Voorkomen is beter dan genezen. Het CBP publiceerde recent nieuwe richtlijnen op het gebied van beveiliging.[105] Elke kans op een beveiligingsincident uitsluiten is onmogelijk. De beveiliging is zo sterk als de zwakste schakel. Zo moeten ook medewerkers op de hoogte zijn van de te nemen beveiligingsmaatregelen en risico's. Een draaiboek en training voor de medewerkers zijn dan ook essentiële onderdelen in deze strijd tegen het kwaad. 'May the force be with you.'[106]

Als het allemaal niet geholpen heeft, is er de wirwar van (toekomstige) meldplichten. De open normen zullen zich de komende jaren ongetwijfeld uitkristalliseren in de weerbarstige praktijk van cybersecurity.

---

99 Het doen van aangifte is verplicht indien er sprake is van strafbare feiten met levensgevaar of waarbij staatsgeheimen zijn of kunnen worden geschonden (artikel 160 Wetboek van Strafvordering).
100 Artikel 6:101 BW.
101 Vgl. bijvoorbeeld artikel 6, 33 en 34 Wbp, maar ook artikel 6:162 BW (onrechtmatige daad), artikel 6:248 BW (redelijkheid en billijkheid), artikel 7:401 BW (zorgplicht goed opdrachtnemer), artikel 7:403 BW (informatieplicht opdrachtnemer) of artikel 7:611 BW (goed werkgeverschap). Vgl. J.A.N. Baas & M.H.J. van Rest, 'Informatie- en meldplichten bij datalekken en beveiligingsinbreuken', *P&I* 2012, p. 260-268; J.M.A. Berkvens, 'Datalekken in de financiële sector', *FR* 2011, p. 381-383; F. van der Jagt, 'Iets te melden? De diverse meldplichten in kaart gebracht', *NJB* 2012, p. 1713-1719. Vgl. ook Cyber Security Juridisch Kader d.d. 8 december 2011; een onderzoek uitgevoerd in opdracht van het Ministerie van Veiligheid en Justitie.
102 Vgl. artikel 5:25i lid 2 Wet op het financieel toezicht. Zie ook R. van Staden ten Brink, 'Cybercrime, wie stellen we op de hoogte?', *Tijdschrift voor Sanctierecht en Compliance* 2011, p. 5-10.
103 Artikel 6:74 BW.
104 Artikel 6:162 BW.
105 CBP-Richtsnoeren beveiliging van persoonsgegevens d.d. februari 2013 die op 1 maart 2013 in werking zijn getreden.
106 Aldus Yoda uit de bekende science fiction Star Wars-films; een citaat dat niet misstaat in de wereld van cybersecurity.