BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

Stichting Bits of Freedom
Postbus 10746
1001 ES Amsterdam

Ministerie van Veiligheid en Justitie

Bank account 55 47 06 512
Bits of Freedom, Amsterdam
KVK-nr. 34 12 12 86

Betreft
Inbreng consultatie meldplicht datalekken

Datum
Amsterdam, 29 februari 2012

Geachte heer, mevrouw,

1. Graag reageert stichting Bits of Freedom op het wetsvoorstel voor een meldplicht datalekken.

   Bits of Freedom is zeer verheugd dat het ministerie dit wetsvoorstel heeft gepubliceerd. De vele datalekken in de laatste twee jaar onderstrepen de noodzaak van zo'n meldplicht.[1] We zijn blij dat het ministerie deze noodzaak onderstreept door in het voorstel een maximumboete van 200.000 euro op te nemen. We zien ook dat het ministerie moeite heeft gedaan om de belangen van de betrokkene te behartigen.

2. In deze brief benadrukt Bits of Freedom dat het belangrijkste doel van zo'n meldplicht is: het beschermen van de betrokkene tot wiens gegevens onbevoegde toegang is verkregen en het verkrijgen van inzicht in de aard en omvang van de problematiek. Bits of Freedom komt tot de conclusie dat onder het huidige voorstel i) niet alle meldenswaardige datalekken gemeld hoeven te worden, ii) de betrokkene onvoldoende wordt geïnformeerd en iii) het register bij het College anderen niet in staat stelt om onderzoek te doen naar de aard en de omvang van de problematiek. Bits of Freedom zal dat in deze brief nader toelichten.

3. Bits of Freedom zal eerst het doel van zo'n meldplicht bespreken. Vervolgens wordt ingegaan op het uitgangspunt dat voor het wetsartikel moet gelden. Daarna worden alle belangrijke elementen van een effectieve meldplicht besproken. Tenslotte geeft Bits of Freedom aan hoe de adviezen het beste in het voorgestelde artikel kunnen worden verwerkt.

1 https://www.bof.nl/category/zwartboek-datalekken/

Doel meldplicht is bescherming betrokkene en verkrijgen inzicht

4. Er is sprake van een datalek op het moment dat onbevoegde toegang tot persoonsgegevens, die aan een verantwoordelijke zijn toevertrouwd, is verkregen. Dat is de kern van het probleem. Dit wordt verderop nader toegelicht. De gevolgen van een datalek voor een betrokkene kunnen verstrekkend zijn, waaronder de onthulling van de identiteit van iemand en identiteitsfraude.

   Voorbeeld: Samarium is een platform gericht op jongeren met sadomasochistische gevoelens. Via een forum op de website kunnen zij hun gevoelens met leeftijdsgenoten delen, zonder daarbij hun eigen identiteit kenbaar te maken. In deze anonieme wereld voelen de leden zich vrij om te praten. Toen de beheerders van de website bij de verzending van een e-mail een fout maakten, werden elkaars contact - gegevens bekend. Hierdoor is de identiteit van de betrokkenen bekend geworden bij de andere ontvangers. Als gevolg hiervan kunnen leden niet langer in alle vrijheid met elkaar praten. [2]

   Voorbeeld: Toen T-Mobile een klant probeerde te helpen met het inloggen op zijn persoonlijke pagina, worden de gebruikersnaam en het wachtwoord per ongeluk in een publiek bericht op Twitter gepubliceerd.[3] Snel daarna bleken derden direct zijn facturen te hebben ingezien en zijn abonnement te hebben aangepast.[4]

5. Het doel van een meldplicht is betrokkenen in staat te stellen om bij een datalek zo snel als mogelijk maatregelen te nemen om verdere schade te voorkomen. Ook dit wordt verderop nader toegelicht.

6. Een meldplicht zorgt ook voor bewustwording onder zowel betrokkenen en verantwoordelijken over de risico's die met de grootschalige verwerking van persoonsgegevens samenhangen. Dat zal er aan bijdragen dat een verantwoordelijke niet meer persoonsgegevens verwerkt dan strikt noodzakelijk is. Dat betekent ook dat een verantwoordelijke er voor zal zorgen gegevens te verwijderen indien deze niet meer nodig zijn. Een meldplicht is daar bovenop een stimulans om de verwerkte gegevens afdoende te beschermen. Tenslotte zal een publiek centraal register inzicht geven in de aard en omvang van het probleem. Dat stelt het bedrijfsleven en de overheid in staat beleid op het gebied van de bescherming van persoonsgegevens te maken dat gebaseerd is op feiten.

   Voorbeeld: Via de Nationale Theaterkassa worden toegangskaarten voor concerten en theater verkocht. Sinds 2010 is de website overgestapt op een nieuw systeem voor het verwerken van de aankopen. De oude databank bleef alleen nog maar in gebruik voor de verzending van de nieuwsbrief. Na een datalek bleek deze databank niet alleen nog maar e-mailadressen te bevatten, maar ook de gegevens van 2.100 creditcards, waarvan er nog 226 actief zijn. Deze gegevens waren, tegen de regels van de verstrekkers van de creditcards in, niet versleuteld opgeslagen en konden door onverlaten worden misbruikt. Zodra de eigenaren van deze creditcards op de hoogte worden gesteld, kunnen zij

2 https://www.bof.nl/2011/08/01/mailen-is-moeilijk-juli-2011/
3 https://www.bof.nl/2010/09/18/datalek-t-mobile-tweet-inloggegevens-klant/
4 http://twitter.com/#!/MarkSedney/status/24753362472

maatregelen nemen om misbruik te voorkomen.[5]

Voorbeeld: Nadat de omroep Llink werd opgeheven, werd de website vergeten. Deze blijkt lek te zijn en de databank met de gegevens van 153.000 leden kwamen op straat te liggen. Hoewel Llink inmiddels is opgeheven, zijn dit soort omvangrijke lekken een belangrijk gegeven voor beleidsmakers. Het is dus goed als dit soort lekken in een centraal register worden bijgehouden.[6]

Elk lek moet worden gemeld, ook bij afwezigheid van beveiligingsmaatregelen

7. Onder onbevoegde toegang wordt verstaan elke onbevoegde kennisneming van persoonsgegevens. Hieronder valt élke onbevoegde kennisneming van persoonsgegevens, zowel binnen als buiten de organisatie van de verantwoordelijke. Deze term dient ruim te worden uitgelegd. Naast het onbevoegde kennisnemen valt in ieder geval ook het onbevoegde kopiëren hieronder.

   Voorbeeld: Uit een uitspraak van een rechter blijkt dat een secretaresse van een gezondheidsinstelling haar toegang tot het Elektronisch Patiënten Dossier (EPD) heeft misbruikt voor privé doeleinden. Nadat een dochter van de vrouw was aangerand, werd van aangifte afgezien op voorwaarde dat de man zich zou laten behandelen. De vrouw controleerde de status van de behandeling in het EPD, ook al was zij daartoe niet bevoegd. Dit is een vorm van onbevoegde kennisneming die als datalek zou moeten worden aangemerkt.[7]

   Voorbeeld: Opsporings- en inlichtingendiensten vragen regelmatig de zogenaamde verkeersgegevens van klanten van aanbieders van mobiele telefonie op. Verkeersgegevens zeggen iets over wie met wie en wanneer contact heeft gehad, maar niets over de inhoud van de communicatie. In 2009 werd duidelijk dat Vodafone en T-Mobile ten onrechte ook de inhoud van de sms-berichten met de opsporings- en inlichtingendiensten deelden. De opsporings- en inlichtingendiensten namen de inhoud van de berichten ook over in hun systemen en dossiers. De diensten hadden geen bevoegdheid voor het lezen van de inhoud van de berichten en daarmee is sprake van onbevoegde toegang. Ook dit zou als datalek moeten worden aangemerkt.[8]

   Voorbeeld: In oktober bleek een online winkel voor baby-artikelen onvoldoende beveiligd. Eerder deze maand werden de gegevens van 539 accounts gepubliceerd. Deze publicatie werd ingegeven door een ander datalek en betrof een specifieke selectie van klanten.[9] Het is aannemelijk dat de aanvallers de volledige databank van 134.000 gebruikers hebben gekopieerd en niet slechts de 539 gepubliceerde accounts.[10] Het is niet duidelijk of er, in strikte zin, sprake is van kennisname van álle gegevens. Nu deze gegevens in ieder geval zijn gekopieerd, moet dit ook als datalek worden aangemerkt.

8. Ook als er sprake is van onbevoegde toegang zonder dat beveiligingsmaatregelen worden doorbroken kan dit gevolgen voor de betrokkene hebben.

   Voorbeeld: Met de Rabobank E-Scan kunnen mensen hun geschiktheid als ondernemer onderzoeken.

---

5 https://www.bof.nl/2012/02/23/datalek-nationale-theaterkassa-lekt-creditcardgegevens/
6 https://www.bof.nl/2011/06/16/datalek-gapend-gat-in-databank-opgeheven-omroep-2/
7 https://www.bof.nl/2010/09/24/datalek-secretaresse-raadpleegt-epd-voor-privedoeleinden/
8 http://vorige.nrc.nl/binnenland/article2256668.ece/Smsjes_gaan_ongevraagd_naar_politie
9 https://www.bof.nl/2012/02/17/datalek-gegevens-klanten-baby-dump-op-straat/
10 http://www.nrc.nl/nieuws/2012/02/11/opta-gaat-onderzoeken-of-kpn-klantgegevens-wel-goed-beschermde/

Aan de hand van meer dan honderd vragen, waarin ook iemands psychologische eigenschappen aan bod komen, stelt de bank een persoonlijk profiel op. Het rapport is via de website van de Rabobank te downloaden. Door het aanpassen van een cijfer in het adres van de pagina op de website, waren echter de rapporten van 3.300 anderen te raadplegen. En hoewel de profielen zeer persoonlijke informatie bevatten, leken op het eerste gezicht geen beveiligingsmaatregelen te zijn genomen. [11] Dat betekent dat dit niet als datalek zou worden aangemerkt in het concept-wetsvoorstel van het ministerie: een duidelijk ongewenste uitkomst.

Voorbeeld: Kasboek.nl geeft gebruikers de mogelijkheid om via de website hun persoonlijke financiën inzichtelijk te maken. Gebruikers sturen daarvoor een kopieën van hun digitale rekeningafschriften naar de website. De beheerders plaatsen de afschriften in een publiek toegankelijke en niet-beveiligde directory op de server. Meer dan een miljoen transacties met een totale waarde van ongeveer 200 miljoen euro waren in te zien. Uit de omschrijvingen bleek dat er 3.362 keer salaris werd uitbetaald, in 5.332 gevallen geld van of naar de Belastingdienst werd overgemaakt, 147 mensen alimentatie betaalden en één betrokkene 1.459 euro aan een winkel met erotische artikelen overmaakte. [12] Omdat deze gegevens vrij toegankelijk waren op internet, zou ook dit in het concept-wetsvoorstel van het ministerie niet als datalek worden aangemerkt. Ook dat is een duidelijk ongewenste uitkomst.

9. Zodra onbevoegde toegang is verkregen tot persoonsgegevens moet de betrokkene worden geïnformeerd. Immers: onbevoegde toegang is het probleem (zie paragraaf 2) en de meldplicht is er om de schade voor de betrokkene te beperken (zie paragraaf 3). Het is daarom essentieel dat "onbevoegde toegang" als uitgangspunt voor het wetsartikel wordt gebruikt. In het huidige voorstel is dat niet het geval, want daar wordt uitgegaan van "een inbreuk op de maatregelen als bedoeld in artikel 13".

10. Onbevoegde toegang tot persoonsgegevens als uitgangspunt voor het wetsartikel kent drie belangrijke voordelen:

    - De betrokkene wordt altijd geïnformeerd bij toegang tot zijn persoonsgegevens waaraan (in de meeste gevallen negatieve) consequenties voor de betrokkene zijn verbonden. Onder het huidige voorstel hoeft de verantwoordelijke onbevoegde toegang tot persoonsgegevens niet aan de betrokkene melden als niet ook sprake is van een inbreuk op de maatregelen als bedoeld in artikel 13. Dit wordt bevestigt in de Toelichting, op pagina 8. Dat is zeer problematisch. Uit het Zwartboek Datalekken blijkt dat lang niet altijd passende beveiligingsmaatregelen zijn genomen, zodat bepaalde datalekken dus niet gemeld zouden hoeven te worden.

    - De administratieve lasten voor de verantwoordelijke en het College nemen af omdat incidenten die niet hebben geleid tot onbevoegde toegang tot persoonsgegevens niet hoeven te worden gemeld. In het huidige voorstel geldt dat als is voldaan aan de voorwaarden van het eerste lid, maar de persoonsgegevens niet leesbaar zijn, het incident toch gemeld moet worden bij het College. Door onbevoegde toegang als

11 https://www.bof.nl/2012/01/31/datalek-rabobank-lekt-duizenden-ondernemersrapporten/
12 https://www.bof.nl/2010/10/07/datalek-miljoenen-transacties-van-online-huishoudboek/

uitgangspunt te nemen hoeven lekken van versleutelde informatie niet meer te worden gemeld.

- Het College wordt verder ontlast omdat er geen directe opvolging op de melding door een verantwoordelijke nodig is. In het huidige voorstel moet het College beoordelen of het beroep op lid 6 door de verantwoordelijke terecht is. Deze beoordeling moet direct na de melding gebeuren. Dat is nodig omdat uitstel van de melding aan de betrokkene betekent dat de betrokkene zich minder goed kan beschermen tegen de gevolgen van het lek. Dit wordt nader toegelicht in paragraaf 19.

Elk lek moet gemeld worden, ook indien dat slechts vermoed moet worden

11. Ook bij een vermoeden dat er sprake is van onbevoegde toegang moet de betrokkene hierover worden geïnformeerd.

> Voorbeeld: Twee weken geleden is een rechercheur van de politie Rotterdam-Rijnmond een dossier met informatie over een opsporingsonderzoek verloren. Het dossier bevatte kopieën van verhoren, foto's en persoonlijke informatie van verdachten. De rechercheur had het dossier bij vertrek op het dak van haar auto laten liggen. Een groot aantal medewerkers van de politie heeft het dossier gezocht, maar zonder resultaat.[13] De verantwoordelijke vermoedt in zo'n situatie dat er sprake is van onbevoegde toegang en de betrokkene zou over dit datalek moeten worden geïnformeerd.

Elk lek moet gemeld worden, ongeacht gevolgen voor betrokkene

12. Naar de mening van Bits of Freedom zouden de gevolgen voor de betrokkene van een datalek niet relevant horen te zijn voor de vraag of dit lek gemeld moet worden. In het huidige voorstel hoeft er geen melding aan het College en de betrokkene gedaan worden als niet "redelijkerwijs aangenomen kan worden is dat de inbreuk nadelige gevolgen voor [de betrokkene]" heeft. De verantwoordelijke, noch het College, is echter in staat de gevolgen voor de betrokkene goed in te schatten.

> Voorbeeld: Begin dit jaar lekte een Udense Vuurwerkhandel de gegevens van ruim 9.000 orders. In de orders staan onder meer adressen en telefoonnummers van klanten. De verantwoordelijke zou kunnen betogen dat het niet redelijkerwijs aangenomen kan worden dat dit lek nadelige gevolgen voor de betrokkene heeft. Een betrokkene die, om welke reden dan ook, niet kenbaar heeft willen maken dat hij vuurwerk gekocht heeft, ondervindt van dit lek echter wel nadelige gevolgen. Hetzelfde geldt voor de betrokkene die, om welke reden ook, zijn woon- of e-mailadres geheim wil houden.

Melding aan betrokkene moet altijd geïnformeerd worden, ongeacht andere meldplichten

13. De betrokkene moet altijd geïnformeerd worden, ook als op de verantwoordelijke een meldplicht op grond van bijvoorbeeld de Wet op het financieel toezicht of de Telecommunicatiewet rust. Als

13 http://www.politiepersberichten.nl/rotterdam-rijnmond-zuid-holland-zuid/bericht/29788/

de toets van zo'n meldplicht melding aan de betrokkene niet afdwingt, dan moet dat alsnog gebeuren op grond van deze meldplicht.

Melding aan betrokkene moet volledig zijn

14. De betrokkene kan zich alleen goed beschermen tegen de gevolgen van een datalek als de melding volledig is. In de voorgestelde melding aan de betrokkene ontbreekt i) de aard van de gelekte informatie, ii) de mogelijke consequenties voor de betrokkene en iii) een beschrijving van de door de organisatie genomen stappen voor het inperken van de gevolgen voor de betrokkene. Dat is nodig omdat alleen op die manier de betrokkene goed kan beoordelen welke maatregelen hij zelf kan of moet nemen.

15. Het komt geregeld voor dat de betrokkene geen idee heeft dat zijn gegevens bij de verantwoordelijke bekend zijn en al helemaal niet welke gegevens dat zijn.

> Voorbeeld: Eerder deze maand bleek de website van Nobiles, een bedrijf dat carrièreadvies aan studenten geeft, onvoldoende beveiligd. De achterliggende databank, met gegevens van 338.000 accounts bleek hierdoor publiek toegankelijk. De gegevens van 900 accounts zijn op internet gepubliceerd.[14] In een reactie op een e-mail van Nobiles schrijft een van de betrokkene dat hij niet eens wist dat hij een account had.[15]

16. Alleen als de betrokkene een compleet en gedetailleerd overzicht van het soort gelekte gegevens heeft kan hij goed beoordelen welke maatregelen hij zelf kan of moet nemen. Als in de melding gesproken wordt over gegevens van creditcards, dan is daarmee nog niet duidelijk of dit het volledige creditcardnummer is of slechts de laatste vier cijfers. Evenmin is duidelijk of ook de SecureCode gelekt is. In de melding moet zo nauwkeurig als mogelijk vermeld worden welke gegevens in welke vorm gelekt zijn.

> Voorbeeld: Een website voor de verkoop van concertkaarten bleek bijzonder slecht beveiligd te zijn en lekt behalve vertrouwelijke bedrijfsinformatie ook de administratie van klantgegevens. Een beveiligings - onderzoeker had toegang tot onder meer creditcardnummers, die niet versleuteld zijn opgeslagen. De verantwoordelijke kan in zo een geval niet volstaan met de melding dat een datalek heeft plaats - gevonden. Als hij niet vermeldt dat ook onbevoegde toegang is verkregen tot de gegevens van creditcards, zal de betrokkene zich namelijk mogelijk niet realiseren dat het goed is om de creditcard te blokkeren. [16]

17. De betrokkene moet geïnformeerd worden over de geconstateerde en vermoedelijke gevolgen van het lek. Zo gebruiken veel mensen hetzelfde wachtwoord voor meerdere websites. Dat betekent dat als het wachtwoord via de ene website op straat komt te liggen, de betrokkene ook aangeraden moet worden het wachtwoord op andere websites aan te passen.

---

14 https://www.bof.nl/2012/02/22/datalek-300000-klantgegevens-carrieresite-toegankelijk/
15 https://twitter.com/#!/bvdhaterd/status/170503901437640706
16 https://www.bof.nl/2011/09/06/datalek-ticketsite-lekt-creditcardgegevens/

Voorbeeld: Het eerder genoemde Nobiles stuurde een e-mail aan haar gebruikers om hen te informeren over het gelekte wachtwoord. Nobiles geeft aan dat zij het wachtwoord al aangepast heeft om misbruik te voorkomen. Het bedrijf schrijft verder "Als je het wachtwoord voor Nobiles ook gebruikte op andere plekken (bijvoorbeeld Facebook, Hyves, Marktplaats etc.), dan adviseren wij je om dit ook te wijzigen." [17] Dat is een goed advies.

18. Het is noodzakelijk dat de betrokkene op de hoogte wordt gebracht van de maatregelen die de verantwoordelijke reeds heeft genomen om gevolgen voor de betrokkene te beperken. Op die manier is het de betrokkene direct duidelijk of hij stappen dient te ondernemen.

Voorbeeld: In een niet-beveiligde directory op een server van de Nederlandse Energie Maatschappij (NEM) was een Excel bestand met de gebruikersnaam, e-mailadres en wachtwoord van 63.000 klanten toegankelijk. Met deze gegevens was het mogelijk om in te loggen op de persoonlijke pagina van de klanten. Via deze pagina wordt inzage gegeven in de naam- en adresgegevens, gegevens over het energieverbruik en de facturen van de klant. Enkele gegevens konden ook aangepast worden. In de melding aan de klant moet de verantwoordelijke aangegeven of het wachtwoord al is aangepast. [18] Heeft de verantwoordelijke dat nog niet gedaan dan moet de klant dat zo snel als mogelijk alsnog doen.

Melding moet betrokkene direct bereiken

19. Om te voorkomen dat een betrokkene op ongewenste wijze geconfronteerd wordt met de onbevoegde toegang tot zijn persoonsgegevens, is het noodzakelijk dat de betrokkene direct geïnformeerd wordt. Het heeft weinig zin om betrokkenen te informeren als zij eerder op een andere, onverwachte, manier al hebben ervaren dat hun persoonsgegevens zijn gelekt.

Voorbeeld: Op de website van de Amsterdamse taxicentrale kunnen klanten vertrouwelijk een klacht indienen. De bezoekers vullen daarbij persoonlijke gegevens in, zoals naam, e-mailadres en een telefoonnummer. Door een fout in de beveiliging van de website waren deze klachten, inclusief persoonsgegevens, publiek toegankelijk. [19] Als niet direct wordt gemeld kunnen klagers akelig verrast worden als chauffeurs hen met de klacht confronteren. Betrokkenen moeten dan ook direct geïnformeerd worden, zeker omdat de klachten over bedreigingen zeer ernstig zijn. [20]

20. Voor een effectieve melding is het noodzakelijk dat de verantwoordelijke de betrokkenen individueel benadert (zoals bijvoorbeeld met een bericht via e-mail of, in het geval van een kleine groep betrokkenen, per telefoon). Hierop mogen geen uitzonderingen zijn, ook niet als de melding een administratieve last met zich brengt. Als hierin technisch voorzien kan worden, dient de verantwoordelijke de aflevering van de melding te verifiëren. Als de aflevering niet gelukt is, moet opnieuw een poging ondernomen worden om de betrokkene individueel te benaderen. In aanvulling op deze persoonlijke melding dient er op de website van de door de gebruiker afgenomen dienst een duidelijk zichtbare melding opgenomen worden.

17 http://tweakers.net/nieuws/80123/hacker-steelt-wachtwoorden-338000-accounts-camieresite.html
18 https://www.bof.nl/2010/12/20/datalek-nem-hoe-komen-al-je-gegevens-precies-op-straat-te-liggen/
19 https://www.bof.nl/2011/01/06/datalek-klachten-taxicentrale-openbaar/
20 http://www.dumpert.nl/mediabase/1281181/7b91aaf1/foutje._tca_maakt_taxiklachten_openbaar.html

Voorbeeld: Knus.nl is een website waarop 280.000 singles op zoek gaan naar een partner. Na een overhaaste aanpassing door de beheerders kregen ook leden onbedoeld toegang tot de interface voor beheerders. Zij konden op die manier door de profielen van alle leden bladeren. [21] Het is aannemelijk dat leden de website niet meer bezoeken als zij een partner gevonden hebben. Een melding van het lek op de website is dan ook niet afdoende om betrokkene te informeren dat hun hoogst persoonlijke profiel volledig toegankelijk is geweest voor derden. De betrokkene moet persoonlijk benaderd worden.

21. Enkel en alleen dan wanneer de organisatie niet in staat is om de betrokkenen te selecteren of indien contactgegevens ontbreken (bijvoorbeeld bij verlies van de databank met de persoonsgegevens) volstaat een niet-persoonlijke melding. In die situatie is de keuze van het medium afhankelijk van de betrokkenen die de verantwoordelijke probeert te bereiken. De inhoud van het en het medium voor de melding moet worden afgestemd op de groep van betrokkenen. Een inbreuk met gevolgen voor jongeren kan niet worden afgedaan met een advertentie in het Financieele Dagblad.

Uitzondering voor versleutelde informatie alleen indien niet omkeerbaar

22. Versleuteld zijn gegevens die, door gebruik te maken van een algoritmisch proces, omgezet zijn in een vorm waarin de gegevens onleesbaar of onbruikbaar zijn zonder gebruik van een vertrouwelijk proces of sleutel. De melding aan de betrokkene kan achterwege blijven indien deze versleuteling zodanig is dat deze nu en in de voorzienbare toekomst op geen enkele wijze ongedaan gemaakt kan worden zonder kennis van de geheime sleutel of proces en deze geheime sleutel of proces niet ook voor onbevoegden toegankelijk is of is geweest. Als het wachtwoord makkelijk te raden is, dan is hier geen sprake van. In de afgelopen twee jaar zijn tal van voorbeelden bekend waarbij de versleuteling onvoldoende bleek te zijn

Voorbeeld: Pepper is een betaalde website voor het vinden van een partner. Afgelopen zomer bleek de datingsite lek en lagen 53.000 gebruikersnamen, e-mailadressen en wachtwoorden op straat. Met deze gegevens is toegang te krijgen tot veel en gedetailleerde profielen. [22] De versleuteling van de wachtwoorden kon gemakkelijk ongedaan gemaakt worden. [23] Er zijn ook aanwijzingen dat dat inderdaad gebeurde.[24]

Voorbeeld: Ook de gegevens in databank van de Nederlandse Politiebond waren niet veilig. De gelekte gegevens omvatten onder meer de gebruikersnamen, versleutelde wachtwoorden en een aantal volledige namen. Omdat de versleuteling onvoldoende was waren de wachtwoorden betrekkelijk eenvoudig te herleiden. Daarmee waren ook de profielen van gebruikers op de website toegankelijk. [25]

23. Als onbevoegde toegang tot persoonsgegevens als uitgangspunt wordt gehanteerd, komen lid 6 en 7 overigens te vervallen.

---

21 https://www.bof.nl/2011/07/07/datalek-280-000-profielen-van-datingsite-toegankelijk/
22 https://www.bof.nl/2011/07/05/datalek-gedeelde-zoektocht-nieuwe-liefde/
23 http://webwereld.nl/nieuws/107200/hackers-misbruikten-configuratiefout-in-database-pepper-nl.html
24 http://webwereld.nl/nieuws/107188/wachtwoorden-pepper-nl-worden-actief-gekraakt.html
25 https://www.bof.nl/2011/07/11/datalek-ook-bij-politiebond-gegevens-niet-veilig/

Publiek register moet betrokkenen, verantwoordelijken en beleidsmakers informeren

24. Een publiek register van datalekken bevordert transparantie. Dat stelt anderen dan alleen de toezichthouder in staat onderzoek te doen naar de aard en de omvang van het probleem van datalekken. Dat leidt tot bewustzijn bij zowel betrokkenen als verantwoordelijken over de risico's die grootschalige opslag van persoonsgegevens met zich brengt. Media kunnen onderzoek doen naar bedrijfstakken met een onevenredig groot aantal of omvangrijke lekken. Betrokkenen kunnen een geïnformeerde keuze voor bepaalde bedrijven maken. Beleidsmakers in zowel de private als publieke sector kunnen leren van de ernst en de oorzaken van datalekken. Een publiek register stelt hen in staat beleid op feiten te baseren.

25. Een register bij het College is alleen zinvol als dat door iedereen geraadpleegd kan worden. Hieraan wordt niet voldaan als het College jaarlijks slechts enkele statistieken publiceert. Een register kan opgezet worden op dezelfde wijze als het meldingenregister, zoals bedoeld in artikel 30. Voor een optimale toegankelijkheid moet het register via een gebruiksvriendelijke website geraadpleegd kunnen worden. Goed onderzoek door derden kan worden gestimuleerd door het register toegankelijk te maken via een online interface (een API[26]). In de AMvB, zoals bedoeld in lid 11 van het voorgestelde artikel, kunnen regels gesteld worden met betrekking tot de publieke en vertrouwelijke onderdelen van de melding. Transparantie moet hierbij het uitgangspunt zijn.

26. Om zo'n publiek register te faciliteren moet het College worden geïnformeerd over i) het aantal betrokkenen van wie persoonsgegevens zijn gelekt, ii) de soort gelekte informatie en iii) de manier waarop de betrokkenen zijn geïnformeerd. Deze gegevens hoeven nu echter niet aan het College verstrekt te worden. Deze volledige informatie is noodzakelijk om de ernst van de inbreuk te kunnen beoordelen en om te kunnen controleren of aan de voorwaarden van lid 5, dat een behoorlijke en zorgvuldige informatievoorziening aan de betrokkenen moet waarborgen, is voldaan.

27. De relevante artikelen bevatten overigens ook enkele inconsistenties van meer cosmetische aard. Zo wordt in lid 3 gesproken over de maatregelen om "de gevolgen te beperken" terwijl in artikel 4 wordt gesproken over maatregelen om "de gevolgen te verhelpen".

Voorstel aanpassingen artikel met onbevoegde toegang als grondbeginsel

28. Bits of Freedom is van mening dat onbevoegde toegang tot persoonsgegevens het criterium dient te zijn voor een melding aan de betrokkene en het College. Daarvoor is een andere formulering van het artikel noodzakelijk.

    Aan artikel 1 zou een lid toegevoegd moeten worden:

26 http://nl.wikipedia.org/wiki/Application_programming_interface

onbevoegde toegang: elke onbevoegde kennisneming van persoons gegevens

Artikel 34a komt te luiden:

1. De verantwoordelijke stelt de betrokkene en het College onverwijld in kennis als hij weet of vermoedt dat onbevoegde toegang is verkregen tot de door hem verwerkte persoonsgegevens.
2. De kennisgeving aan de betrokkene en het College omvat in ieder geval:
   a) de wijze waarop onbevoegde toegang is of vermoedelijk is verkregen,
   b) de aard van de persoonsgegevens waartoe onbevoegde toegang is of vermoedelijk is verkregen,
   c) de geconstateerde en vermoedelijke gevolgen voor de persoonlijke levenssfeer van de betrokkene,
   d) de door de verantwoordelijke genomen of nog te nemen stappen om deze gevolgen te beperken,
   e) de aan de betrokkene aanbevolen maatregelen om deze gevolgen te beperken en
   f) de contactgegevens waaraan een verzoek om meer informatie kan worden gericht.
3. De kennisgeving aan het College omvat tevens een opgave van het aantal betrokkenen tot wiens persoonsgegevens onbevoegde toegang is of vermoedelijke is verkregen en een beschrijving van de wijze waarop de betrokkenen in kennis zijn gesteld.
4. De kennisgeving aan de betrokkene wordt op zodanige wijze gedaan dat, rekening houdend met de aard van de persoonsgegevens waartoe onbevoegde toegang is of vermoedelijk is verkregen, de geconstateerde en vermoedelijke gevolgen voor de persoonlijke levenssfeer van de betrokkene, de kring van betrokkenen en de kosten van tenuitvoerlegging, een behoorlijke en zorgvuldige informatievoorziening is gewaarborgd.
5. Het College houdt een register bij van de kennisgevingen als bedoeld in het eerste lid. Het register kan door een ieder kosteloos worden geraadpleegd.
6. Dit artikel is niet van toepassing voor zover
   a) de verantwoordelijke in zijn hoedanigheid als aanbieder van een elektronische communicatiedienst al een kennisgeving heeft gedaan als bedoeld in artikel 11.3a, eerste en tweede lid, of
   b) op de verantwoordelijke een verplichting rust tot het verstrekken van informatie op grond van de artikelen 3:10, derde lid, of 4:11, vierde lid, van de Wet op het financieel toezicht.
7. Bij algemene maatregel van bestuur kunnen nadere regels worden gesteld met betrekking tot de kennisgeving en het register.

Voorstel aanpassingen artikel met zoveel als mogelijk aansluiting op huidige tekst

29. Mocht een herschrijving van het artikel niet mogelijk zijn, dan stelt Bits of Freedom de volgende wijzigingen voor. We hebben daarbij geprobeerd zoveel als mogelijk aan te sluiten bij de tekst van het ministerie.

Aan artikel 1 wordt een lid toegevoegd:

onbevoegde toegang: elke onbevoegde kennisneming van persoons gegevens

Artikel 34a komt te luiden:

1. De verantwoordelijke stelt het College onverwijld in kennis als hij weet of vermoedt dat onbevoegde toegang is verkregen tot de door hem verwerkte persoonsgegevens, danwel door een inbreuk op de maatregelen als bedoeld in artikel 13, danwel anderszins ~~van een inbreuk op de maatregelen, bedoeld in artikel 13, waarvan redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijk risico op verlies of onrechtmatige verwerking waaraan nadelige gevolgen voor de persoonsgegevens en de persoonlijke levenssfeer van de betrokkene zijn verbonden~~.
2. De verantwoordelijke, bedoeld in het eerste lid, stelt de betrokkene onverwijld in kennis van de inbreuk, bedoeld in het eerste lid.
3. De kennisgeving aan het College en de betrokkene omvat in ieder geval de aard van de inbreuk, de aard van de persoonsgegevens waartoe onbevoegde toegang is of vermoedelijk is verkregen, de geconstateerde en vermoedelijke gevolgen voor de betrokkene, de maatregelen die door de verantwoordelijke zijn genomen om de gevolgen te beperken, de contactgegevens waaraan een verzoek om meer informatie kan worden gericht ~~de instanties waar meer informatie over de inbreuk kan worden verkregen~~ en de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken.
4. De kennisgeving aan het College omvat tevens het vermoedelijke aantal betrokkenen tot wiens gegevens onbevoegde toegang is of vermoedelijk is verkregen en de tekst en de vorm van de kennisgeving aan de betrokkene. ~~een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens en de maatregelen die de verantwoordelijke heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen~~.
5. De kennisgeving aan de betrokkene wordt op zodanige wijze 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.
~~6. De kennisgeving aan de betrokkene is niet vereist indien de verantwoordelijke naar het oordeel van het College gepaste technische beschermingsmaatregelen heeft 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.~~
~~7. Indien de verantwoordelijke geen kennisgeving aan de betrokkene doet, kan het College, indien het van oordeel is dat inbreuk waarschijnlijk nadelige gevolgen zal hebben voor de persoonsgegevens en de persoonlijke levenssfeer van de betrokkene, van de verantwoordelijke verlangen dat hij alsnog een kennisgeving doet.~~
8. Het College houdt een register bij van de kennisgevingen als bedoeld in het eerste lid. Het register kan door een ieder kosteloos worden geraadpleegd.
9. De verantwoordelijke houdt een overzicht bij van alle inbreuken. Dit overzicht bevat in elk geval de feiten en de gegevens, bedoeld in het derde lid, alsmede de tekst van de kennisgeving aan de betrokkene.
10. Dit artikel is niet van toepassing voor zover de verantwoordelijke in zijn hoedanigheid als aanbieder van een elektronische communicatiedienst al een kennisgeving heeft gedaan als bedoeld in artikel 11.3a, eerste en tweede lid, van de Telecommunicatiewet.
11. Dit artikel is niet van toepassing indien op de verantwoordelijke een verplichting rust tot het verstrekken van informatie op grond van de artikelen 3:10, derde lid, of 4:11, vierde lid, van de Wet op het financieel toezicht.
12. Bij algemene maatregel van bestuur kunnen nadere regels worden gesteld met betrekking tot de kennisgeving en het register als bedoeld in lid 8.

Europese regelgeving onzeker en langdurig proces; nationale wetgeving doorzetten

30. Bits of Freedom verzoekt u het huidige voorstel door te zetten, ook nu in Europa onderhandelt wordt over de nieuwe verordening voor gegevensbescherming. Deze onderhandelingen zullen zonder twijfel een proces van lange duur zijn en het is onzeker wat het uiteindelijke resultaat zal zijn. Daarom moet Nederland niet wachten met de introductie van een meldplicht. Het Zwartboek Datalekken[27] en de voorbeelden hierboven tonen de urgentie van zo'n meldplicht aan. Bovendien heeft de regering in haar regeerakkoord toegezegd een meldplicht te introduceren.

31. Bits of Freedom ziet daarnaast graag dat u zich ook in Europa sterk maakt voor een effectieve meldplicht. De in deze brief genoemde elementen zorgen ervoor dat de betrokkene, tot wiens gegevens onbevoegde toegang is verkregen, zoveel als mogelijk de gevolgen van een datalek kunnen beperken. Op Europa niveau gelden dezelfde overwegingen.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd. Uiteraard ben ik graag bereid om het bovenstaande nader toe te lichten, mocht daaraan behoefte bestaan.

Hoogachtend,

Rejo Zenger

27 https://www.bof.nl/category/zwartboek-datalekken/

Actal

Aan de staatssecretaris van Veiligheid en Justitie
Mr. F. Teeven
Postbus 20301
2500 EH DEN HAAG

Datum
09-02-2012

Onderwerp
Advies wetsvoorstel gebruik camerabeelden en meldplicht datalekken

Uw kenmerk
5720002/11/6

Ons kenmerk
JtH/FvK/2012/05

Bijlage(n)

Geachte heer Teeven,

Eind 2011 heeft u het wetsvoorstel gebruik camerabeelden en meldplicht datalekken in consultatie gegeven. Het wetsvoorstel verruimt de mogelijkheid om door particulieren vervaardigde camerabeelden van strafbare feiten te benutten voor de ondersteuning van de rechtshandhaving. Cameratoezicht wordt, wanneer met behulp van een camera individuele personen herkenbaar in beeld worden gebracht, aangemerkt als een vorm van verwerking van persoonsgegevens. Voorts introduceert het wetsvoorstel een meldplicht voor verantwoordelijken voor de verwerking van persoonsgegevens in geval van gebleken doorbrekingen van de getroffen maatregelen ter beveiliging van persoonsgegevens. Het nalaten aan deze verplichting te voldoen wordt gesanctioneerd met een bestuurlijke boete.

Wij hebben de consequenties van het wetsvoorstel voor de regeldruk getoetst. Wij toetsen op drie hoofdpunten:

1. Nuloptie: is er een taak voor de overheid en is regelgeving het meest aangewezen instrument?
2. Is de regeldruk proportioneel ten opzichte van het beleidsdoel? Zijn er minder belastende alternatieven mogelijk?
3. Is gekozen voor een passende uitvoeringswijze met het oog op de dienstverlening?

Langs de lijnen van het toetsingskader hebben wij het advies opgebouwd.

1. Nuloptie

In de memorie van toelichting gaat u in op de verhouding tot het geldend Europees recht. De bescherming van persoonsgegevens is een fundamenteel recht dat in internationale verdragen is verankerd en een taak van de overheid betreft. Het wetsvoorstel beoogt een herijking van de privacybescherming zodat een ruimer gebruik kan worden gemaakt van door particulieren vervaardigde camerabeelden, zonder daarbij de belangen van de bescherming van persoonsgegevens te verminderen. Dat vereist wijziging van de regelgeving.

Contact
Lange Voorhout 58
2514 EG Den Haag
Postbus 16228
2500 BE Den Haag
T (070) 310 86 66
F (070) 310 86 79
www.actal.nl
info@actal.nl

2. Proportionaliteit en minder-belastende alternatieven

Kwantificering gevolgen regeldruk
De memorie van toelichting vermeldt dat het voorstel leidt tot een toename van de nalevingskosten voor bedrijven met € 430.355,- per jaar en een toename van de administratieve lasten voor bedrijven met € 430.355,- per jaar. Deze toename draagt niet bij aan de doelstelling van het kabinet om de regeldruk in Nederland te verminderen.

Wij adviseren u in de memorie van toelichting bij het wetsvoorstel Gebruik camerabeelden en meldplicht datalekken te vermelden op welke wijze deze toename van de regeldruk voor bedrijven gecompenseerd wordt.

Daarnaast roept de kwantificering van de gevolgen voor de regeldruk twee vragen op.

In de eerste plaats staat in de toelichting dat de verruiming van de mogelijkheden tot gegevensverwerking door middel van het beschikbaar stellen van camerabeelden van strafbare feiten aan politie en OM geen administratieve lasten en nalevingskosten oplevert. Er is volgens V&J geen sprake van informatieverplichtingen van burgers of bedrijven aan overheid. Een belanghebbende heeft het geheel in eigen hand of hij die beelden wel of niet beschikbaar stelt.

In de toelichting is echter ook vermeld dat cameratoezicht, wanneer met behulp van een camera individuele personen herkenbaar in beeld worden gebracht, wordt aangemerkt als een vorm van verwerking van persoonsgegevens. Deze stellingname suggereert dat dit onderdeel van het wetsvoorstel wel gevolgen heeft voor de regeldruk.

Wij adviseren u in de memorie van toelichting te verduidelijken of het gebruik van camerabeelden kwalificeert als regeldruk en zo ja wat de gevolgen daarvan zijn.

In de tweede plaats is bepaald dat verantwoordelijken zowel de gegevens die aan het College bescherming persoonsgegevens (Cbp) zijn verstrekt, als de tekst van de kennisgeving die zij aan betrokkenen moeten doen toekomen, moeten registreren. Deze protocolplicht ondersteunt het interne en externe toezicht op de gegevensverwerking. Achteraf kan aan de hand van het protocol worden beoordeeld of de inbreuk niet toch had moeten worden gemeld. Uit de memorie van toelichting valt niet op te maken of de administratieve lasten van de protocolplicht in beeld zijn gebracht.

Wij adviseren u in de memorie van toelichting te verduidelijken wat de gevolgen van de protocolplicht zijn voor de administratieve lasten en regeldruk.

2. Minder belastende alternatieven
In de memorie van toelichting is vermeld dat de effectiviteit van de meldplicht voor datalekken snel aan betekenis zal verliezen wanneer elk denkbaar datalek in aanmerking komt om te worden gemeld. Een meldplicht zonder enige beperking leidt bovendien tot een nodeloze belasting

van bedrijfsleven en overheid. U kiest voor een algemene formulering om de meldplicht voor het datalekken te beperken. Hierbij ziet u ook een rol voor het Cbp.

U voorziet in de memorie van toelichting bij het wetsvoorstel nieuwe bestuurlijke lasten voor het Cbp. U verwacht dat de meldplicht bij doorbrekingen van beveiligingsverplichtingen tot 66.000 meldingen per jaar leidt. Volgens de toelichting mag verwacht worden dat het overgrote deel van deze meldingen het Cbp *geen enkele aanleiding* geeft tot een onderzoek of tot handhavingsmaatregelen. Dat betekent dat het Cbp niet meer zal doen dan van de melding kennisnemen en deze gedurende een bepaalde periode zal bewaren. In de memorie van toelichting staat dat het nog niet valt te voorzien in hoeveel gevallen de meldingen aanleiding zullen geven tot verdere actie.

De verwachting dat het overgrote deel van de meldingen uitsluitend wordt gearchiveerd en geen enkele aanleiding geeft tot een onderzoek of handhavingsmaatregelen roept de vraag op welk doel met de meldingen wordt bereikt en of het wetsvoorstel proportioneel is. Indien de meldplicht vooral is bedoeld ter vergroting van de bewustwording bij bedrijven met betrekking tot de risico's van datalekken, achten wij dit instrument met name voor kleinere bedrijven niet proportioneel.

Wij adviseren u zodanige maatregelen te treffen dat nodeloze meldingen worden voorkomen en de gevolgen voor regeldruk voor het bedrijfsleven en het Cbp in verhouding staan tot het doel dat u beoogt te bereiken.

3. Uitvoering

Het wetsvoorstel treedt in werking op een bij Koninklijk Besluit te bepalen tijdstip. In de toelichting is nog geen beoogde datum inwerkingtreding vermeld. Ten einde de kennisnemingskosten voor burgers en bedrijven te beperken hanteert het kabinet zgn. vaste verandermomenten. Wij gaan er van uit dat ook dit wetsvoorstel op een vast verandermoment in werking zal treden.

Conclusie

Alles overwegende adviseren wij u het wetsvoorstel gebruik camerabeelden en meldplicht datalekken niet in te dienen, tenzij met het vorenstaande rekening is gehouden.

Hoogachtend,

J. ten Hoopen
Collegevoorzitter

R.W. van Zijp
Secretaris

Aan de Staatssecretaris van Veiligheid & Justitie
mr. F. Teeven
Postbus 20301
2500 EH DEN HAAG

Den Haag, 9 maart 2012

Excellentie,

Bij brief van 19 december 2011 (kenmerk 5720002/11/6) heeft u het Nederlands Genootschap van Functionarissen voor de Gegevensbescherming (NGFG) uitgenodigd om haar reactie te geven op het conceptwetsvoorstel Wbp (camerabeelden en datalekken). Wij danken u voor deze uitnodiging en zenden u bij dezen onze reactie, waarbij wij ons beperken tot het onderdeel meldplicht datalekken.

1. Algemeen

Het NGFG ondersteunt het idee dat datalekken gemeld moeten worden, zowel aan de toezichthouder als aan de betrokkene. In deze tijd van verregaande informatisering is het belangrijk dat incidenten waarbij persoonsgegevens betrokken zijn, zoveel mogelijk worden voorkomen, en indien deze zich toch voordoen, deze adequaat en snel worden geadresseerd. Daarbij past een zekere mate van transparantie om de betrokkene in staat te stellen zijn/haar belangen te beschermen.

2. Samenvatting opmerkingen en aanbevelingen NGFG

Een gedetailleerd overzicht van de opmerkingen en aanbevelingen van het NGFG treft u aan in de bijlage bij deze brief. Deze opmerkingen en aanbevelingen kunnen als volgt worden samengevat:

1. De verantwoordelijkheid voor het nemen van maatregelen en de communicatie met de betrokkene en/of het Cbp dient te liggen bij de verantwoordelijke. Het NGFG verzoekt u daarom om de passage in de Memorie van Toelichting over de rol van de FG bij datalekken te schrappen en te overwegen om de FG een rol te geven bij de meldplicht die past bij zijn/haar rol als toezichthouder. Voor concrete voorstellen verwijzen wij u naar punt 1 in de bijlage.

2. Het NGFG zou de "zorgplicht" voor de verantwoordelijke graag nader uitgewerkt zien door concrete verplichtingen, maatregelen of instrumenten in de tekst of toelichting waardoor de bewerker waarborgen zal bieden ten aanzien van de meldplicht datalekken en de verplichtingen zal nakomen die op de verantwoordelijke rusten ten aanzien van datalekken.

3. De meldplicht is gekoppeld aan de maatregelen bedoeld in artikel 13 Wbp. Dit kan leiden tot onduidelijkheid over het toepassingsbereik en het melden van incidenten die eigenlijk geen datalek zijn. Het NGFG adviseert u om deze bezwaren in de wet te ondervangen, bijvoorbeeld door de verwijzing naar artikel 13 Wbp te schrappen, en een meer precieze definitie van een datalek op te nemen in artikel 1 Wbp, waarbij de meldplichtige beveiligingsincidenten nader worden omschreven.

4. Het NGFG adviseert u om het voorwerp van de meldplicht te beperken tot die gevallen waarin een aanmerkelijke kans bestaat op nadelige gevolgen voor de persoonlijke levenssfeer van de betrokkene en de woorden "de persoonsgegevens en" te schrappen.

5. Met het oog op de hoge boete en het voorkomen van onnodige meldingen, adviseert het NGFG u om het begrip "verantwoordelijke" in de Memorie van Toelichting nader toe te lichten onder verwijzing naar van de criteria van Opinie WP 169 van de Artikel 29 Werkgroep.

6. Het NGFG adviseert u om een regeling te treffen voor de nakoming van de verplichtingen ex artikel 34a door gezamenlijke verantwoordelijken. Daarnaast adviseert het NGFG u om in de toelichting een opmerking op te nemen over eventuele meervoudige boetes voor hetzelfde datalek in geval van gezamenlijke verantwoordelijkheid.

7. Het NGFG adviseert u om in te gaan op de vraag of de mogelijkheid om gebruik te maken van de uitzondering op de meldplicht niet te beperkt is in verband met criterium van onverwijldheid, en om de interpretatie van de meldplicht in geval van versleuteling van de gegevens, alsmede de gevolgen daarvan, te verduidelijken.

8. Het NGFG adviseert u om het eerste lid van artikel 34a zodanig te verduidelijken dat een melding van een datalek pas moet worden gedaan nadat de verantwoordelijke daarvan daadwerkelijk kennis heeft gekregen.

9. Het NGFG adviseert u om in het eerste lid van artikel 34a de term "onverwijld" te vervangen door een term die meer ruimte biedt voor het noodzakelijke onderzoek naar het datalek en de gevolgen daarvan, en de benodigde corrigerende maatregelen alvorens de melding te doen.
10. Het NGFG adviseert u om in het eerste lid van artikel 34a de uitdrukking "een risico op" te vervangen door "een kans op".
11. Het derde lid van artikel 34a is op een aantal onderdelen onduidelijk. Het NGFG adviseert u om het derde lid op een aantal onderdelen te herformuleren en/of deze in de Memorie van Toelichting te verduidelijken.
12. Het NGFG geeft u in overweging om het zevende lid van artikel 34a te schrappen, dan wel in overeenstemming te brengen met het eerste en tweede lid.

Het NGFG is gaarne bereid om haar standpunt mondeling nader toe te lichten.

Hoogachtend,

mr. J. de Zeeuw
Voorzitter

BIJLAGE

I. INHOUDELIJKE OPMERKINGEN

1. Algemeen

Het wetsvoorstel introduceert in artikel 34a een meldplicht bij datalekken. Deze meldplicht kent niet een heel concrete omschrijving. Er is bovendien sprake van een aantal criteria met open normen die gezamenlijk leiden tot een beslisschema waardoor kan worden bepaald of er in concreto sprake is van een meldplicht. Het wetsvoorstel geeft geen definitie van wat precies wordt verstaan onder een inbreuk op de beveiligingsmaatregelen ("datalek"). De omschrijving van de meldplicht is door deze omstandigheden voor meerdere interpretaties vatbaar. Vanwege het terechte uitgangspunt dat bagatelzaken moeten worden voorkomen, is dat een onvermijdelijk gevolg. Dit kan in de praktijk echter leiden tot situaties waarin het artikel ofwel te eng wordt toegepast, hetgeen zal leiden tot een overmaat aan meldingen, alsook tot situaties waarin het artikel juist te ruim wordt geïnterpreteerd, hetgeen zal leiden tot – al dan niet te goeder trouw – schending van deze regel, hetgeen bedreigd is met een hoge bestuurlijke boete. Het NGFG onderstreept daarom het belang van een goede uitleg van de wettelijke regels, en een juiste toepassing ervan in de praktijk.

2. Rol van de FG bij de meldplicht datalekken

a. Met instemming heeft het NGFG vastgesteld dat het wetsvoorstel voor een deel goed aansluit bij de rol van de Functionaris voor de Gegevensbescherming (FG) als interne toezichthouder. Naar het oordeel van het NGFG is de toezichthoudende rol van de FG in dit voorstel echter nog onvoldoende uitgewerkt. Hoewel de FG wel betrokken dient te zijn bij het adresseren van een datalek, passen niet alle voorgestelde taken bij de functie van FG. Degene die verantwoordelijk is voor de keuze om al dan niet passende beveiligingsmaatregelen te treffen, dient ook verantwoordelijk te zijn voor de gevolgen wanneer zich een incident voordoet dat door die maatregelen juist had kunnen worden voorkomen. Het gaat dan om de verantwoordelijke. Onder die gevolgen moet ook worden begrepen de uitvoerende handelingen die nodig zijn om de bepalingen van de Wbp op het gebied van datalekken na te leven, zoals het doen van de melding, en het onderhouden van contact met betrokkenen over waar zij persoonlijk aan toe zijn. Het kan bij dat laatste om grote aantallen betrokkenen gaan. Het is niet zuiver en niet effectief om de FG in zijn rol van toezichthouder zelf verantwoordelijk te maken voor naleving van verplichtingen die voor de verantwoordelijke bedoeld zijn. Dat geldt ook voor de uitvoering van noodzakelijke acties die het gevolg zijn van beveiligingskeuzes van de verantwoordelijke. Aan de effectiviteit van de (waarschuwende) functie van de FG wordt afbreuk gedaan wanneer de verantwoordelijke dat soort gevolgen op de FG kan afwentelen. Bovendien gaat de capaciteit die de FG moet besteden aan datalekken ten koste van het preventieve toezicht. Voorkomen is beter dan genezen, en al helemaal omdat dat beter bij de rol van FG past.

Voor de volledigheid zij opgemerkt dat het NGFG het onwenselijk vindt dat betrokkenen zich na een datalek onvoorwaardelijk in verbinding kunnen stellen met de FG, zoals voorgesteld door de Europese Commissie in artikel 32, tweede lid, en artikel 35, eerste lid onder (10), van de ontwerp-

Verordening. Het botst met de rol en functiescheiding van de FG ten opzichte van de verantwoordelijke, en de FG mist daarvoor de nodige capaciteit, hetgeen ten koste gaat van het preventieve toezicht.

Naar het oordeel van het NGFG dient de verantwoordelijkheid voor het adresseren van een datalek en de daarbij behorende acties, inclusief de meldplicht, te liggen bij de verantwoordelijke. De opmerking in paragraaf 4.1.5 van de Memorie van Toelichting dat het voor de hand ligt dat bij organisaties die een FG hebben aangesteld, het de FG is die belast is met de feitelijke uitvoering van de melding namens de verantwoordelijke, is naar ons oordeel dan ook ongelukkig. Het beleggen van de genoemde taken bij de FG doet afbreuk aan de onafhankelijke en toezichthoudende rol van de FG binnen de organisatie van de verantwoordelijke, omdat hij dan op de stoel van de verantwoordelijke wordt geplaatst.

De FG moet wel in ieder geval op de hoogte zijn. Daarom zou het NGFG graag zien dat de verantwoordelijke verplicht is om de FG, als deze is aangesteld, **op de hoogte te stellen van** een **datalek en een melding** bij het Cbp en de betrokkene, voor zover daarin nog niet voorzien is door de protocolplicht. Dit omdat het toezicht door de FG zich daar mede toe dient uit te strekken. Bovendien is de meldplicht bedoeld om het toezicht te ondersteunen, dus naar men kan aannemen ook voor het ondersteunen van het interne toezicht. Uiteraard zal de FG de uitvoering van een verplichte melding aan het Cbp bevorderen met alle mogelijkheden die hem ter beschikking staan.

b. De vermelding in paragraaf 4.1.5 van de Memorie van Toelichting dat het Cbp zich, in de gevallen waarin nader contact met de verantwoordelijke nodig is, met de FG in verbinding stelt, is meer voor de hand liggend. De FG heeft immers een intermediaire rol tussen verantwoordelijke en Cbp. Het NGFG merkt echter wel op dat dat niet betekent dat de FG het enige loket is voor alle vragen of opmerkingen van het Cbp, net zo min als de FG het loket is voor alle vragen aan het Cbp. Gelet op zijn specifieke onafhankelijke rol kan de FG als intermediair immers niet puur de boodschapper of de spreekbuis zijn van de verantwoordelijke. Bij contact tussen Cbp en FG is er namelijk in beginsel geen sprake van een dialoog tussen de toezichthouder en de verantwoordelijke, maar van een dialoog tussen de externe toezichthouder enerzijds en de interne toezichthouder anderzijds. Gevolg hiervan is dat in de toelichting aan de betreffende zin onder 4.1.5. de woorden: **in ieder geval** toegevoegd zouden moeten worden, zodat de zin luidt: "Het ligt voor de hand dat het Cbp in de gevallen waarin nader contact met de verantwoordelijke nodig is, zich in ieder geval met de functionaris in verbinding stelt."

Juist omdat de FG een toezichthoudende rol heeft *naast* het Cbp, zou het Cbp, alvorens eventuele corrigerende maatregelen op te leggen als gevolg van het datalek, de FG in de gelegenheid moeten stellen om (aanvullende) informatie te verschaffen die van belang is voor een juiste beoordeling van het incident. De zienswijze van de FG is vanwege zijn onafhankelijke rol van belang voor de beoordeling door het Cbp of een nader onderzoek of het geven van aanwijzingen nodig is. De FG zal vaak ook als geen ander op de hoogte zijn van het feit of de aanwezige compliance-organisatie er voldoende "staat"om op korte termijn intern zaken te onderzoeken of orde op zaken te stellen. Het NGFG is van mening dat indien er bij de verantwoordelijke een FG is aangesteld, het Cbp verplicht zou moeten zijn om **de FG te consulteren** alvorens een eventuele reactie kenbaar te maken aan de verantwoordelijke. Daarmee wordt recht gedaan aan de toezichthoudende rol van de FG.

c. Los van het voorgaande is het NGFG van mening dat reeds het feit dat bij de verantwoordelijke een aantoonbaar geloofwaardig en **effectief intern toezicht** is ingesteld, van belang kan zijn voor de beoordeling van het Cbp of er wel of **geen vervolgstappen door het Cbp** nodig zijn na een melding van een datalek. Vervolgstappen tegen, of bij de verantwoordelijke. Het NGFG adviseert om dit in de toelichting te vermelden. Het Cbp zou dan conform de bedoeling van de Wbp een belangrijk deel van zijn taak aan het interne toezicht kunnen overlaten, en wordt er voor bedrijven en overheden een extra *incentive* geboden voor het instellen van effectief intern toezicht.

d. Daarnaast zou het wenselijk zijn dat de FG een **adviserende rol** krijgt bij de beoordeling of sprake is van een inbreuk waarvan redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijk risico op verlies of onrechtmatige verwerking waaraan nadelige gevolgen zijn verbonden voor de persoonlijke levenssfeer van de betrokkene. De FG is bedoeld als onafhankelijke deskundige, en het ligt daarom voor de hand dat de FG daar een rol in zal hebben. Naar het oordeel van het NGFG vermeldt ten onrechte tekst noch toelichting van het wetsvoorstel daar iets over.

3. Relatie tussen verantwoordelijke en bewerker

Het NGFG is minder gelukkig met de wijze waarop in het voorgestelde artikel 14 Wbp de relatie tussen verantwoordelijke en bewerker met betrekking tot het melden van datalekken wordt vormgegeven. De gekozen formulering betekent impliciet dat het toezicht van de FG wat betreft de gegevensverwerking door de bewerker moet worden geïntensiveerd. Intensivering van het toezicht kan een aanzienlijke impact hebben op de beschikbare capaciteit van de FG. Toezicht op een bewerker is echter sowieso al gecompliceerd, omdat de bewerker niet rechtstreeks aan het gezag van de verantwoordelijke is onderworpen. Hierdoor is de FG in de praktijk onder meer beperkt in zijn/haar mogelijkheden om informatie over de aard van het datalek te verkrijgen en om interventies te doen teneinde de verwerking door de bewerker (weer) in overeenstemming te brengen met de Wbp. Het wetsvoorstel biedt hiervoor geen concrete handvatten die de FG ondersteunen bij deze rol. Het wetsvoorstel regelt op dit gebied slechts een "zorgplicht" voor de verantwoordelijke. Het NGFG zou dit punt graag nader uitgewerkt zien door concrete verplichtingen, maatregelen of instrumenten in de tekst of toelichting waardoor de bewerker waarborgen zal bieden ten aanzien van de meldplicht datalekken en de verplichtingen zal nakomen die op de verantwoordelijke rusten ten aanzien van datalekken. Een mogelijkheid is dat de bewerker, net als in de ontwerp-Verordening, een datalek zou moeten melden bij de verantwoordelijke. De naleving van de meldplicht zal hierdoor beter en efficiënter worden geborgd.

4. Relatie met artikel 13 Wbp

Een van de grootste problemen in artikel 34a lid 1 is de relatie die wordt gelegd met artikel 13 Wbp. Het feit dat het moet gaan om een "inbreuk op de maatregelen, bedoeld in artikel 13" leidt naar het oordeel van het NGFG tot een veel te breed toepassingsbereik.

a. Artikel 13 Wbp ziet op "verlies of *enige vorm van onrechtmatige verwerking*". Dat laatste begrip is breder dan alleen onrechtmatige vernietiging, wijziging, of ongeautoriseerde toegang tot of verstrekking van persoonsgegevens. Gelet op de definitie van het begrip "verwerking" in artikel 1 sub b Wbp omvat het bijvoorbeeld ook het onrechtmatig *gebruik* van persoonsgegevens door personen die wel bevoegd zijn tot kennisneming van de gegevens. Onrechtmatig gebruik moet echter niet als

"datalek" kunnen worden gekwalificeerd, omdat het hier eigenlijk gaat om een gewone overtreding van de Wbp.

Bovendien wordt de (on)rechtmatigheid van een verwerking niet alleen bepaald door het voorschrift de gegevens te beveiligen en toegang te autoriseren, maar ook door alle andere bepalingen van hoofdstuk 2, en de artikelen 33 en 34, van de Wbp. Dit zijn echter geen beveiligingsvoorschriften, zodat inbreuken niet kunnen leiden tot 'datalekken' in de normale zin van het woord. De referentie in artikel 34a lid 1 naar artikel 13 Wbp zou dan ook leiden tot een forse toename van het aantal (oneigenlijke) "datalekken".

Ten overvloede merkt het NGFG op dat de woorden "enige vorm van onrechtmatige verwerking" in artikel 13 Wbp niet alleen een te brede implementatie vormen van artikel 17 lid 1 Richtlijn 95/46/EG, dat een veel genuanceerdere tekst heeft, maar ook ten onrechte bescherming van persoonsgegevens reduceren tot een beveiligingskwestie. Dit laatste is niet bevorderlijk voor een juiste insteek en positionering van de Wbp-compliance binnen bedrijven en overheidsorganisaties. Privacy en gegevensbescherming vallen immers niet uitsluitend onder de noemer van beveiliging. De privacybelangen die in het spel zijn, moeten onafhankelijk van de beveiligingsbelangen van de verantwoordelijke kunnen worden afgewogen. Het NGFG adviseert u derhalve om bij de totstandkoming van de nieuwe EU Verordening voor de bescherming van persoonsgegevens er op aan te dringen dat de passage: *"any unlawful forms of processing, in particular"* in artikel 30, tweede lid, van de Verordening wordt geschrapt dan wel wordt vervangen door: *"any unauthorised forms of processing"* (enige vorm van ongeautoriseerde verwerking).

b. Voorts eist artikel 13 Wbp dat "passende maatregelen" worden genomen, "rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging". Artikel 13 Wbp gaat dus uit van een redelijke inschatting van de risico's en vereist dat de beveiligingsmaatregelen passen bij die risico's. Dit betekent dat een verantwoordelijke geen beveiligingsmaatregelen hoeft te nemen om ten koste van alles datalekken te voorkomen. Het kan zich dus voordoen dat de genomen beveiligingsmaatregelen passend zijn in de zin van artikel 13 Wbp, of die zelfs overstijgen, maar dat er in een dergelijk geval toch een datalek optreedt. In dat geval kan er, vanwege een aanmerkelijk risico op nadelige gevolgen voor de persoonlijke levenssfeer van de betrokkene, wel degelijk sprake zijn van een situatie waarin de betrokkene zou moeten worden geïnformeerd over het datalek. Maar op basis van de tekst van het onderhavige voorstel, is twijfel mogelijk of er in dat geval sprake is van een inbreuk op de maatregelen in de zin van artikel 13. De tekst van artikel 34a, eerste lid, verwijst immers naar de maatregelen van artikel 13 Wbp, en dat moeten volgens het systeem van de Wbp "passende maatregelen" zijn. Het zou in dat geval gaan om het verwerkelijken van een klein risico dat slechts tegen hoge kosten kan worden beperkt en in welk geval artikel 13 dus niet voorschrijft dat daar maatregelen tegen worden genomen. In dit geval zou de huidige tekst van artikel 34a lid 1 Wbp naar de letter dus mogelijk niet leiden tot een meldplicht. Men zou ook kunnen stellen dat in het geval de maatregelen *strenger* zijn dan volgens artikel 13 noodzakelijk is, er bij een datalek geen meldingsplicht zou bestaan omdat de maatregelen niet "passend" zijn, maar strenger.

Daarnaast is er in de gebruikelijke zin van het woord ook sprake van een datalek als de persoonsgegevens in onbevoegde handen komen wegens het *ontbreken* van passende maatregelen als bedoeld in artikel 13 Wbp. Er is dan in strikte zin geen sprake van een inbreuk op de maatregelen, maar van een schending van artikel 13 Wbp zelf. De voorgestelde tekst van artikel 34a lid 1 Wbp zou

naar de letter in zo'n geval dus (ook) niet leiden tot een melding. Daardoor lijkt het niet-naleven van de beveiligingsplicht tot gevolg te hebben dat de verantwoordelijke niet meer de in dit wetsvoorstel opgenomen hoge boete opgelegd kan krijgen wegens niet-melden van zo'n datalek. Daarmee zou een bonus worden geïntroduceerd voor het niet op orde hebben van de beveiliging.

c. Het voorgaande leidt tot de conclusie dat zonder nadere toelichting of aanpassing de verwijzing in artikel 34a, eerste lid, naar de ten uitvoer te brengen passende beveiligingsmaatregelen van artikel 13 Wbp, te veel problemen lijkt op te werpen.

In het licht van het bovenstaande geeft het NGFG u in overweging om de genoemde bezwaren in de wet te ondervangen, bijvoorbeeld door conform de concept-Verordening Bescherming Persoonsgegevens zoals recentelijk gepubliceerd door de Europese Commissie, een definitie van een datalek op te nemen in artikel 1 Wbp, waarbij de meldplichtige beveiligingsincidenten specifiek worden omschreven, en de verwijzing naar artikel 13 Wbp te schrappen.

5. Omvang van de meldplicht: "nadelige gevolgen"

Ondanks de hierboven gemaakte opmerkingen over de omschrijving van meldplichtige datalekken, acht het NGFG het wel noodzakelijk om de meldplicht zinvol te beperken. Het NGFG is het met u eens dat melding van bagatelzaken moet worden voorkomen teneinde de belasting op de organisatie te beperken.

Voor een beperking van de meldplicht tot "nadelige gevolgen voor persoonsgegevens", zoals thans voorgesteld, ziet het NGFG echter geen reden. In de eerste plaats is dit criterium zeer moeilijk te hanteren. Direct rijst de vraag of gegevens überhaupt wel nadeel kunnen ondervinden. Gaat het dan ook om brand of overstroming? In de tweede plaats duidt het gebruik van het woordje "en" op een dubbele eis. Kennelijk moet de inbreuk *zowel* nadelige gevolgen hebben voor de persoonsgegevens *als* nadelige gevolgen hebben voor de persoonlijke levenssfeer van de betrokkene(n). Er zou echter kunnen worden betoogd dat het slecht denkbaar is dat een datalek in de sfeer van de vertrouwelijkheid of de integriteit van de gegevens wel nadelige gevolgen heeft voor persoonsgegevens, maar niet voor de persoonlijke levenssfeer voor de betrokkenen. Ook in de Memorie van Toelichting wordt overigens uitsluitend gesproken over "nadelige gevolgen voor de persoonlijke levenssfeer" (zie blz. 2 en blz. 5). Het criterium "nadelige gevolgen voor persoonsgegevens" is naar het oordeel van het NGFG dus niet alleen moeilijk toe te passen, maar kennelijk ook overbodig.

6. Normadressaat: de verantwoordelijke

De verplichtingen van artikel 34a richten zich tot "de verantwoordelijke".

a. Het NGFG wil u er op wijzen dat er sprake kan zijn van situaties waarin er wel sprake is van een datalek, maar waarvoor de verantwoordelijke partij strikt genomen geen verantwoordelijke in de zin van artikel 1 sub d Wbp is. In de Memorie van Toelichting wordt verwezen naar een concreet voorbeeld waarbij er duidelijk *geen* sprake was van een verantwoordelijke in de zin van de Wbp (DigiNotar). Maar er zijn ook situaties denkbaar waar deze juridische scheiding, zeker in de ogen van het publiek, minder duidelijk is. Denk bijvoorbeeld aan de uitgevers van *apps* voor mobiele apparaten die op de randapparatuur van de gebruiker draaien en waarmee gebruikers communiceren met de infrastructuur van de verantwoordelijke. Als een *app* serieuze security risico's herbergt, is het nog

maar de vraag of het voor iedereen duidelijk is waar precies de grens van de definitie van verantwoordelijke ligt. In zijn opinie WP 169 heeft de Artikel 29 Werkgroep het begrip "verantwoordelijke" nader uitgelegd. Het zou naar het oordeel van het NGFG met het oog op de hoge boete voor niet-melden wenselijk zijn dat in de Memorie van Toelichting de reikwijdte van het begrip "verantwoordelijke" nog eens helder wordt omschreven, mede in het licht van de criteria gegeven in WP 169, zodat er geen twijfel over bestaat op wie de meldplicht rust en op wie niet. Dit geldt ook in zijn algemeenheid voor de reikwijdte van de beveiligingsplicht bij het versturen en ontvangen van gegevens: wanneer bevinden deze zich nog in de beveiligingssfeer van de verzender en wanneer in die van de ontvanger? Duidelijkheid hierover zal helpen om in voorkomende gevallen een goede afweging te maken en onnodige geschillen te voorkomen.

b. Voorts wijst het NGFG erop dat het kan voorkomen dat er meerdere verantwoordelijken zijn voor een verwerking (gezamenlijke verantwoordelijken), zodat de verplichtingen ex artikel 34a in dergelijke gevallen in beginsel ook rusten op elk van die verantwoordelijken. Voor wat betreft de melding ex artikel 27 Wbp is de uitvoering in geval van gezamenlijke verantwoordelijkheid geregeld in artikel 2 Meldingsbesluit Wbp. Het NGFG adviseert u, mede met het oog op de hoge boete voor niet-melden, ook een dergelijke regeling in het leven te roepen voor de meldplicht datalekken. U zou dit kunnen doen door ofwel gelijktijdig met de inwerkingtreding van artikel 34a de Algemene Maatregel van Bestuur ex artikel 34a lid 11 in werking te laten treden, waarin een soortgelijke regeling als artikel 2 Meldingsbesluit Wbp is opgenomen, ofwel om een regeling voor gezamenlijke verantwoordelijken als nieuw lid toe te voegen aan artikel 34a. Een dergelijke regeling zal overigens niet alleen de meldplicht ex artikel 34a lid 1 en lid 2 moeten omvatten, maar ook de verplichtingen omschreven in lid 5, lid 6, lid 7 (zie voor dit lid echter onze opmerkingen hieronder), en lid 8.

Het NGFG gaat er overigens van uit dat in een situatie van gezamenlijke verantwoordelijkheid de boetebevoegdheid van het Cbp ex artikel 66 lid 2 (nieuw) niet is beperkt, zodat het Cbp meervoudige boetes kan opleggen voor hetzelfde datalek ingeval er sprake is van "medeplegen". Het NGFG adviseert u om een opmerking hierover op te nemen in de toelichting bij het wetsvoorstel.

7. Versleuteling (artikel 34a lid 6)

Artikel 34a lid 6 Wbp bepaalt dat de kennisgeving aan de betrokkene niet vereist is, als de verantwoordelijke naar het oordeel van het Cbp gepaste technische beschermingsmaatregelen heeft 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.

Dit voorstel geeft aanleiding tot de volgende opmerkingen.

Het NGFG gaat er van uit dat lid 6 alleen van toepassing is op de gevallen waarin er een meldplicht bij het Cbp in de zin van het eerste lid van toepassing is. Immers alleen dan is het Cbp in staat om in concreto te oordelen over de gepastheid van de technische beschermingsmaatregelen.

In de eerste plaats merkt het NGFG op dat dit niet valt te rijmen met de eis van het tweede lid, dat de betrokkene onverwijld in kennis moet worden gesteld, net zoals het Cbp. Het Cbp zal enige tijd nodig hebben voor de beoordeling van de gepastheid van de maatregelen, zodat de verantwoordelijke naar de letter van de wet nooit van de uitzondering van het zesde lid gebruik zal kunnen maken. In de tweede plaats: persoonsgegevens die op passende wijze zijn versleuteld, of op een andere wijze

onbegrijpelijk zijn gemaakt voor eenieder die geen recht heeft op kennisname van die gegevens, vallen, naar het NGFG aanneemt, niet onder de meldplicht, bedoeld in het eerste lid. Bij dergelijke beveiligingsmaatregelen zal immers geen sprake zijn van een aanmerkelijk risico op onrechtmatige verwerking. Als de verantwoordelijke daarbij nog beschikt over een back up-bestand met de gegevens, zal er ook geen sprake zijn van een aanmerkelijk risico op verlies. In verband daarmee zal er in het geheel geen sprake zijn van een datalek, laat staan van een datalek dat bij het Cbp of de betrokkene moet worden gemeld. De tekst van het zesde lid lijkt echter in geval van versleuteling van de gegevens een ruimere meldplicht in het leven te roepen, omdat de beoordeling van de passendheid van de beveiligingsmaatregel in dat geval niet aan de verantwoordelijke, maar aan het Cbp is.

Het NGFG adviseert u om in de toelichting in te gaan op de vraag welke interpretatie met betrekking tot bovenstaande punten de juiste is, en om aan te geven of die interpretatie geen ongewenste gevolgen zal hebben voor het voorkomen van onnodige meldplichten, of voor het toezicht op de versleutelingstechniek en de positie van verantwoordelijke en de FG die hierbij een (advies)taak heeft.

II.OPMERKINGEN VAN TECHNISCHE AARD

Voorts maakt het NGFG graag van de gelegenheid gebruik om nog enkele opmerkingen te maken van wetstechnische aard.

8. "Onverwijld"

Het eerste lid van artikel 34a schrijft voor dat de melding "onverwijld" moet worden gedaan. Het NGFG heeft hierover een tweetal opmerkingen.

a. Ten eerste geeft de formulering aanleiding tot onduidelijkheid over het moment vanaf wanneer sprake is van een "datalek", en dus wanneer de termijn begint die wordt aangeduid met "onverwijld". De huidige formulering kan zo worden gelezen dat een onverwijlde melding vereist is nadat een inbreuk heeft plaatsgevonden. Echter, het kan zijn dat de verantwoordelijke nog niet op de hoogte is van het feit dat het gaat om een datalek. Hij kan door eigen waarneming, maar ook door een melding door een bewerker of een derde (bijvoorbeeld een journalist) op de hoogte raken van een incident. Maar daarbij zal in veel gevallen in eerste instantie sprake zijn van een beveiligingsincident waarbij nog niet duidelijk is of daar ook persoonsgegevens bij betrokken zijn (denk bijvoorbeeld aan een gestolen laptop, waarbij eerst moet worden vastgesteld of daarop ook persoonsgegevens bewaard zijn). Dat vergt nader onderzoek naar het beveiligingsincident en dat kost enige tijd. Het zou daarom logischer zijn om te bepalen dat de verantwoordelijke de melding onverwijld doet nadat hij *kennis heeft gekregen* van een datalek.

b. In de tweede plaats is niet duidelijk wat precies moet worden verstaan onder "onverwijld". Hier zou enige rek in moeten zitten, omdat het datalek onderzocht moet worden en de noodzakelijke maatregelen moeten worden genomen om het lek onder controle te krijgen, voor zover dat feitelijk mogelijk is. De verantwoordelijke moet bovendien in staat zijn om te kunnen voldoen aan de voorgeschreven inhoud van de melding, als bedoeld in artikel 34a, derde en vierde lid. Een melding aan het Cbp en de betrokkene moet op grond van die bepalingen omvatten: de aard van het datalek, de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken, een beschrijving

van de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens, en de maatregelen die de verantwoordelijke heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen. Het NGFG merkt hierbij op dat de termijn van 24 uur die de Europese Commissie voorstelt naar het oordeel van het NGFG aan de korte kant is. Het is niet ondenkbaar dat ook externe adviseurs moeten worden ingeschakeld om de precieze omvang van het datalek vast te stellen (denk bijvoorbeeld aan advocaten of forensische specialisten). De FG wordt voor grote dilemma's geplaatst als hij op basis van een te onduidelijk of te star criterium zijn toezicht op de meldplicht moet uitoefenen. Het NGFG zou er dan ook de voorkeur aan geven dat de melding *zo snel als redelijkerwijs mogelijk is* moet plaatsvinden. Daarbij moet worden aangegeven dat dit betekent dat binnen de bedoelde termijn het noodzakelijke onderzoek kan worden gedaan om de aard van de inbreuk en de negatieve gevolgen vast te stellen, en de maatregelen te bepalen die in dat verband worden aanbevolen, en dat de noodzakelijke corrigerende of schadebeperkende maatregelen kunnen worden genomen.

9. "Risico"

In artikel 34a, eerste lid, en andere bepalingen, wordt de uitdrukking "een risico op" gebruikt. Onder "risico" wordt in het algemeen verstaan: het product van kans en schade. De schade wordt in dezelfde zin echter al aangeduid, namelijk: verlies of onrechtmatige verwerking waaraan nadelige gevolgen voor de persoonsgegevens of de persoonlijke levenssfeer van de betrokkenen zijn verbonden. Taalkundig lijkt er daardoor sprake te zijn van een contaminatie, en zou het beter zijn de uitdrukking: "een risico op" te vervangen door "een kans op".

10. Artikel 34a lid 3

Dit lid bevat een aantal onderdelen die wellicht nog kunnen worden verduidelijkt. Zo is het niet voldoende duidelijk wat moet worden verstaan onder "instanties waar meer informatie over de inbreuk kan worden verkregen". Het zou naar het oordeel van het NGFG duidelijker zijn om voor te schrijven dat in de kennisgeving *contactgegevens* van de verantwoordelijke moeten worden vermeld *via* welke de betrokkene meer informatie kan krijgen.

Verder moeten de "aanbevolen maatregelen" om de negatieve gevolgen van de inbreuk te beperken onderdeel zijn van de kennisgeving. Het is niet voldoende duidelijk tot wie die aanbeveling zich richt. Het gaat kennelijk niet om de maatregelen die door de FG op grond van artikel 64 lid 4 Wbp worden aanbevolen aan de verantwoordelijke, maar als dat wel bedoeld zou zijn, dan acht het NGFG dat onwenselijk. Als echter bedoeld is dat het de maatregelen zijn die de *betrokkene* zou moeten nemen om de inbreuk te beperken, dan zou het duidelijker zijn om dit met zoveel woorden te vermelden.

11. Artikel 34a lid 7

Het zevende lid lijkt tegenstrijdig met het eerste en het tweede lid. Immers, uit het eerste en tweede lid volgt dat indien er onverwijld aan het Cbp gemeld moet worden, er ook onverwijld gemeld moet worden aan de betrokkene. Wel melden aan het Cbp, maar tegelijkertijd niet aan de betrokkene is op grond van het tweede lid dus niet mogelijk. Daarmee is het de vraag of er wel situaties bestaan waarin het zevende lid praktische toepassing kan krijgen.

NEDERLANDSE VERENIGING VOOR RECHTSPRAAK

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

Datum
29 februari 2012

Kenmerk
B 2.1.11/002833/20//JT

Uw kenmerk
5720002/11/6

Onderwerp
Advies NVvR op het consultatie wetsvoorstel Wbp (camerabeelden en datalekken)

Geachte heer Teeven,

Bij brief van 19 december 2011 met kenmerk 5720002/11/6 heeft u de Nederlandse Vereniging voor Rechtspraak (NVvR) verzocht advies uit te brengen over het daarbij gevoegde wetsvoorstel.

Aard en strekking wetsvoorstel

Volgens de memorie van toelichting strekt dit wetsvoorstel tot het verruimen van de mogelijkheid om door particulieren vervaardigde camerabeelden van strafbare feiten te benutten voor de ondersteuning van de rechtshandhaving. Ook wordt in het wetsvoorstel een meldplicht geïntroduceerd voor verantwoordelijken voor de verwerking van persoonsgegevens in geval van gebleken doorbrekingen van de getroffen maatregelen ter beveiliging van persoonsgegevens.

Commentaar op het wetsvoorstel en de memorie van toelichting

Met de voorgestelde meldplicht en de voorgenomen regeling kan de NVvR instemmen Hoewel het belang van preventieve beveiliging van opslagsystemen van persoonsgegevens veel groter is, kan een goede regeling van de melding van gevallen waarin die beveiliging heeft gefaald, zowel helpen de gevolgen van dat falen te ondervangen als bijdragen aan de preventie van nieuwe inbreuken op die bescherming.
Dat ligt anders bij het, van die meldplicht geheel los staande, voorstel tot verruiming van het mogelijk maken van het gebruik van camerabeelden die zijn vervaardigd door particulieren, waaronder particuliere beveiligingsbedrijven, door die particulieren of beveiligingsbetrijven zelf. Voorop zij gesteld, dat de NVvR in feite geen bezwaar heeft tegen het gebruik van door particulieren vervaardigde beelden bij de opsporingsactiviteiten van politie en justitie, en evenmin tegen publicatie van die beelden door deze diensten aan een algemeen publiek, indien en voor zover die diensten dat na afweging van alle betrokken belangen voor de opsporing van strafbare feiten noodzakelijk achten, ondanks de risico's voor de bescherming van de privacy van degenen die op de beelden voorkomen. De NVvR zet vraagtekens bij de in het vooruitzicht gestelde mogelijkheid dat particulieren min of meer op eigen initiatief persoonsgegevens van derde op internet mogen zetten in geval van vermeende strafbare feiten. Deze vraagtekens worden vooral veroorzaakt doordat het wetsvoorstel op dit punt

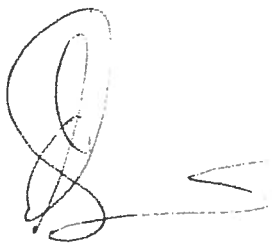
Lange Voorhout 7 • Postbus 30315, 2500 GH Den Haag
Telefoon: 070-3611420 • info@nvvr.org • www.nvvr.org

geen materiële inhoud heeft, maar de beoogde mogelijkheid geheel overlaat aan regeling op amvb-niveau. De NVvR is van mening dat, waar het hier gaat om een inbreuk op het grondrecht van de bescherming van de persoonlijke levenssfeer, in elk geval het materiële deel van de regeling (de criteria) in de wet zelf moeten worden opgenomen, zodat de formele wetgever zelf de afweging maakt tussen de in het geding zijnde grondrechten. Dit klemt temeer om de volgende reden. Blijkens pagina 5 van de memorie van toelichting is het de bedoeling dat, wanneer men blijft binnen de voorwaarden die op grond van het wetsvoorstel worden gesteld, de camerabeelden door particulieren via het internet kunnen worden verspreid. Als de beelden echter op internet zijn geplaatst, zijn deze feitelijk buiten de macht van degene die de beelden heeft geplaatst, daardoor niet meer te verwijderen en vatbaar voor alle mogelijke vormen van manipulatie. De NVvR vraagt zich af hoe het voorgaande zich verhoudt tot de onschuldpresumptie. Een en ander brengt de NVvR tot het advies dit gedeelte van het wetsvoorstel te heroverwegen en in elk geval van een materiële invulling te voorzien.

Uit de memorie van toelichting komt naar voren dat het de bedoeling is dat de betrokken particulier, als hij voornemens is met toepassing van de te stellen algemene regels persoonsgegevens te publiceren (bijvoorbeeld door plaatsing op een elektronisch billboard of door plaatsing op internet), telkens tevoren toestemming moet vragen aan de opsporingsdiensten. Dat leidt ertoe dat in alle gevallen een individuele toetsing vooraf noodzakelijk blijft. In feite lijkt het de bedoeling te zijn de individuele toetsing over te brengen van het Cbp naar het openbaar ministerie. Onduidelijk is of het openbaar ministerie tot de daarvoor benodigde afweging beter is geëquipeerd dan het Cbp en wat de betrokken particulier met de regeling opschiet, als hij toch aan een toestemmingsprocedure gebonden blijft. De NVvR adviseert hierover in de memorie van toelichting duidelijkheid te verschaffen.

De NVvR adviseert de staatssecretaris voorts helderheid te verschaffen over de gevolgen voor de verdere opsporing en vervolging bij handelen in strijd met de onderhavige, in de Wet bescherming persoonsgegevens op te nemen regeling. Wordt hierop gecontroleerd door het College bescherming persoonsgegevens (en op welke wijze), of vindt deze controle alleen plaats in het kader van het strafproces? Dan wel wordt het bekendmaking van persoonsgegevens zonder of in afwijking van een verleende toestemming strafbaar gesteld? De meldplicht die in het leven wordt geroepen bij het niet hebben voldaan aan de voorwaarden voor verwerking van de camerabeelden door particulieren, lijkt de NVvR niet afdoende. De NVvR adviseert de staatssecretaris ook hieraan aandacht te besteden in het wetsvoorstel en de memorie van toelichting.

Namens het bestuur van de NVvR,
de Wetenschappelijke Commissie



J. Silvis
voorzitter

V N O N C W

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.

--

OPTA

2509 LK Den Haag
Telefoon (070) 315 35 00
Fax (070) 315 35 01
E-mail mail@opta.nl
www.opta.nl

Bezoekadres
Zurichtoren
Muzenstraat 41
2511 WB Den Haag

SG/DW

Ministerie van Justitie
DBOB DIV OPERAL-OD
Dossier
Datum 22 FEB. 2012
Nummer 12/572512
Aant

De Minister van Veiligheid en Justitie
De heer mr. F. Teeven
Postbus 20301
2500 EH 'S-GRAVENHAGE

Contactpersoon	Ons kenmerk	Uw kenmerk	Doorkiesnummer
	OPTA/ACNB/2012/200509	5720002116	
Datum	**Onderwerp**		**Bijlage(n)**
21 FEB. 2012	Reactie op consultatie wetsvoorstel Wbp (datalekken)		

Geachte heer Teeven,

Het college van de Onafhankelijke Post en Telecommunicatie Autoriteit (hierna: het college, respectievelijk OPTA) heeft de brief van uw ministerie gedateerd 19 december 2011, waarin het college verzocht wordt te beantwoorden aan de door u uitgevaardigde consultatie, in goede orde ontvangen. Met deze brief geeft het college invulling aan dit verzoek.

Het college verwelkomt de mogelijkheid tot het geven van zijn visie op de door u voorgenomen wijziging van de Wet bescherming persoonsgegevens en enige andere wetten in verband met de verruiming van de mogelijkheid van het gebruik van camerabeelden van strafbare feiten ten behoeve van de ondersteuning van de rechtshandhaving en de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens (gebruik camerabeelden en meldplicht datalekken) (hierna: het wetsvoorstel). Het college zal zich daarbij beperken tot de veranderingen die relevant zijn voor de door de wetgever voorgenomen bevoegdheden van het college, die voortvloeien uit het gewijzigd voorstel van wet[1] dat momenteel voorligt in de Eerste Kamer. De nadruk bij zijn beantwoording aan de consultatie ligt op de uitvoeringsaspecten in relatie tot handhaving van de verplichtingen.

1 Parallelle verplichtingen

1. Het college constateert dat de verplichtingen uit de Telecommunicatiewet en de Wet bescherming persoonsgegevens parallel aan elkaar zullen blijven bestaan, en dat de handhaving van het nog tot stand te brengen artikel 11.3a, Telecommunicatiewet komt te liggen bij het College Bescherming Persoonsgegevens.

2. De nog tot stand te komen bevoegdheden van het college en de verplichtingen voor onder toezicht gestelden in het kader van het voorgenomen artikel 11.3a, Telecommunicatiewet, kennen

[1] Kamerstukken I 2011/12, 32 549, nr. A.

hun eigen oorsprong in het Europees regelgevend kader[2], en de implementatie daarvan in de Telecommunicatiewet (momenteel ter behandeling in de Eerste Kamer)[3]— zo als ook beschreven in paragraaf 4.1.1 van de Memorie van Toelichting bij uw wetsvoorstel. Het college onderschrijft deze notie. Daaraan verbindt hij de conclusie dat, voor zover de Memorie van Toelichting bij uw wetsvoorstel nadere uitleg geeft aan gelijke of gelijksoortige begrippen en overwegingen, het expliciet niet uw bedoeling is dat deze uitleg gevolgen heeft voor de duiding van de begrippen in het voorgenomen artikel 11.3a, Telecommunicatiewet.

2 Normadressaat artikel 11.3a, Telecommunicatiewet

3. In het wetsvoorstel en de Memorie van Toelichting wordt gerefereerd aan de normadressaat van het te vormen artikel 11.3a, Telecommunicatiewet, als '*aanbieder van een elektronische communicatiedienst*'. De normadressaat van artikel 11.3a, Telecommunicatiewet, is echter beperkt tot "*aanbieder van een openbare elektronische communicatiedienst*". Het element openbaar is een kenmerkend verschil voor de kwalificatie van een dienstaanbieder, waarbij de kwalificatie openbaar slechts toekomt aan die dienstaanbieder die zijn diensten beschikbaar stelt aan het publiek.[4] Strikt genomen valt de aanbieder van elektronische communicatiediensten, in tegenstelling tot de aanbieder van *openbare* elektronische communicatiediensten, niet onder artikel 11.3a, Telecommunicatiewet, maar wel onder het door u voorgestelde artikel 34a, Wet bescherming persoonsgegevens.

4. Het college hecht er (wellicht ten overvloede) aan op te merken dat eenzelfde systematiek zich voordoet ten aanzien van het object van de wetgeving van het voorgenomen artikel 11.3a, Telecommunicatiewet. De persoonsgegevens die vallen onder de reikwijdte van de wet strekken tot gegevens die zijn verwerkt in verband met de levering van een openbare elektronische communicatiedienst in de Europese Unie. Zo kan er bij een aanbieder van een openbare elektronische communicatiedienst een beveiligingsincident plaatsvinden bij een database met persoonsgegevens die verzameld zijn in het kader van de loonadministratie van de werknemers. In dat geval is er sprake van een inbreuk op de beveiliging overeenkomstig het voorgenomen artikel 34a, Wet bescherming persoonsgegevens. Deze aanbieder kan van de inbreuk geen melding doen op grond van het voorgestelde artikel 11.3a, Telecommunicatiewet, die haar verschoont van een melding als gevolg van het voorgenomen artikel 34a, Wet bescherming persoonsgegevens. Immers, het betreft hier geen persoonsgegevens die zijn verwerkt in verband met de levering van een openbare elektronische communicatiedienst. Het verschil is van belang, omdat op bepaalde punten een ander regime geldt voor de twee parallelle meldplichten. Pas als

---

[2] 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. (PB L337/11)

[3] Id 2.

[4] Vergelijk artikel 1.1 aanhef en sub f, Telecommunicatiewet, en artikel 1.1 aanhef en sub g, Telecommunicatiewet.

OPTA

terecht een kennisgeving is gedaan op grond het voorgenomen artikel 11.3a, Telecommunicatiewet, dan kan er sprake zijn van verschoning van de plicht die volgt uit het voorgestelde artikel 34a, Wet bescherming persoonsgegevens.[5]

Afgezien van bovengenoemde zaken ziet het college geen aandachtspunten voor de wetgever die verband houden met de uitvoeringstaak van OPTA.

Hoogachtend,

prof.dr. M.W. de Jong
Plv. voorzitter

[5] Vergelijk paragraaf 4.1.8 van de Memorie van Toelichting van het wetsvoorstel.

COLLEGE **BESCHERMING** PERSOONSGEGEVENS

POSTADRES Postbus 93374, 2509 AJ Den Haag BEZOEKADRES Juliana van Stolberglaan 4-10
TEL 070 - 88 88 500 FAX 070 - 88 88 501 INTERNET www.cbpweb.nl www.mijnprivacy.nl

AAN Ministerie van Veiligheid en Justitie
T.a.v. de Staatssecretaris
De heer mr. F. Teeven
Postbus 20301
2500 EH DEN HAAG

DATUM 15 maart 2012
ONS KENMERK z2011-00970
CONTACTPERSOON

ONDERWERP Advies wetsvoorstel gebruik camerabeelden en meldplicht datalekken

UW BRIEF VAN 19 december 2011
UW KENMERK 5720002/11/6

Geachte heer Teeven,

Bij brief van 19 december 2011 heeft u het College bescherming persoonsgegevens (CBP) gevraagd, op grond van het bepaalde in artikel 51, tweede lid van de Wet bescherming persoonsgegevens (Wbp) te adviseren over het wetsvoorstel wijziging van de Wbp en enige andere wetten in verband met de verruiming van de mogelijkheid van het gebruik van camerabeelden van strafbare feiten ten behoeve van de ondersteuning van de rechtshandhaving en de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens (hierna: *het wetsvoorstel*).

Het CBP voldoet hiermee aan uw verzoek.

De invoering van de meldplicht datalekken hebben de staatssecretaris en de minister reeds aangekondigd in de brief van 29 april 2011 aan de voorzitters van de Eerste en Tweede Kamer der Staten-Generaal en de daarbij behorende Notitie Privacybeleid. In deze brief en notitie werd een aantal wetgevingsvoornemens bekendgemaakt, waaronder het kwalitatief versterken van de bestuursrechtelijke handhaving van de Wbp, waarbij de materiële gedragsnormen van de Wbp zouden worden gesanctioneerd met een bestuurlijke boete . Ondanks het feit dat de door Eurocommissaris Reding op 25 januari 2012 gepresenteerde *REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012)11*, (hierna: *ontwerpverordening gegevensbescherming*) onder andere een voorstel bevat voor de zogenaamde meldplicht datalekken, vormt dit geen belemmering om de meldplicht met voorrang uit te werken in wetgeving, aldus de staatssecretaris in zijn brief van 20 februari 2012 aan de voorzitter van de Eerste Kamer. Het CBP heeft met instemming van dat deel van het standpunt van de staatssecretaris kennis genomen. Niet valt echter in te zien waarom met betrekking tot de invoering van de boetebevoegdheid een geheel ander standpunt kan of moet worden ingenomen, te weten dat publicatie van de ontwerpverordening wel een belemmering zou vormen voor indiening van het wetsvoorstel inclusief invoering van de bevoegdheid van het CBP om een bestuurlijke boete op te leggen. Dat klemt temeer daar de argumenten voor invoering zoals die zijn verwoord in de brief van 29 april 2011 nog onverminderd van toepassing zijn en de reikwijdte van de ontwerpverordening bekend is. Het CBP dringt er daarom met grote klem op aan thans

BIJLAGEN 1
BLAD 1

ook over te gaan tot kwalitatieve versterking van de bestuursrechtelijke handhaving van de WBP, waarbij de materiële gedragsnormen van de Wbp zullen worden gesanctioneerd met een bestuurlijke boete.

Inhoud van het wetsvoorstel

De adviesaanvraag betreft de volgende wijzigingsvoorstellen:

1. Een verruiming van de mogelijkheid om door particulieren vervaardigde camerabeelden van strafbare feiten te benutten voor de ondersteuning van de rechtshandhaving. Dit zal worden gerealiseerd door wijziging van de artikelen 22 en 31 Wbp.
2. Het invoeren van een algemene meldplicht voor verantwoordelijken voor de verwerking van persoonsgegevens in geval van gebleken doorbrekingen van de getroffen maatregelen ter beveiliging van persoonsgegevens. Daarvoor zal een nieuw artikel 34a in de Wbp worden opgenomen.
3. De zorgplichten van de verantwoordelijke op grond van artikel 14 Wbp strekken zich expliciet uit over de datalekken waarvan een bewerker kennis krijgt. Dit zal worden gerealiseerd door het wijzigen van artikel 14 Wbp.
4. De melding door aanbieders van elektronische communicatiediensten in geval van doorbrekingen van de maatregelen die zijn getroffen om persoonsgegevens te beveiligen, wordt belegd bij het CBP. Dit zal worden gerealiseerd door het wijzigen van enkele artikelen in de Telecommunicatiewet.
5. Het nalaten te voldoen aan de algemene meldplicht en de meldplicht in het kader van de Telecommunicatiewet wordt gesanctioneerd met een bestuurlijke boete. Hiervoor zullen artikel 66 Wbp en artikel 15.4 j° artikel 15.1 Telecommunicatiewet worden aangevuld.

Samenvatting van het advies

Gebruik van door particulieren vervaardigde camerabeelden in de opsporing

In zijn algemeenheid kan worden opgemerkt dat het CBP zich in grote lijnen kan vinden in de voorstellen die leiden tot een verruiming van de mogelijkheid om door particulieren vervaardigde camerabeelden van strafbare feiten te benutten voor de ondersteuning van de rechtshandhaving. Het CBP heeft slechts enkele opmerkingen:

1. In het wetsvoorstel en de Memorie van Toelichting dient duidelijk en kenbaar te zijn welke instantie bevoegd is om actie te ondernemen wanneer beelden op een beeldscherm of internet worden geplaatst *zonder voorafgaande toestemming* van de Officier van Justitie.

2. In de Memorie van Toelichting dient te worden verduidelijkt welke actie een instantie, die in eerste instantie persoonsgegevens openbaar heeft gemaakt via zijn eigen website, maar inmiddels heeft verwijderd, neemt tegen het beschikbaar blijven van deze persoonsgegevens via andere websites of andere media.

3. Het CBP verzoekt om de in de Memorie van Toelichting voorgestelde algemene maatregelen van bestuur (AMvB) aan het CBP voor te leggen op grond van artikel 51, tweede lid, Wbp.

4. In de Memorie van Toelichting dient duidelijk te zijn onder welke voorwaarden geen voorafgaand onderzoek is vereist en volstaan enkel de "passende en specifieke waarborgen".

Conclusie
Het CBP adviseert u aan het vorenstaande op passende wijze aandacht te schenken.

Meldplicht datalekken
Het CBP is van oordeel dat de invoering van een meldplicht datalekken de bescherming van persoonsgegevens in het algemeen, en de versterking van de positie van de burger in het bijzonder in hoge mate zal dienen. De meldplicht zal stimulerend werken op de op verantwoordelijken rustende verplichting om zorg te dragen voor adequate beveiliging van verzamelde en opgeslagen persoonsgegevens (krachtens artikel 13 Wbp). De wijze waarop de meldplicht datalekken in het onderhavige wetsvoorstel is vormgegeven, biedt daarvoor een eerste aanzet, maar dient op bepaalde onderdelen te worden gewijzigd. Dit leidt tot de volgende opmerkingen:

1. De invoering meldplicht datalekken loopt vooruit op de regelgeving die op dit moment in Brussel wordt voorbereid. Zodra de ontwerpverordening gegevensbescherming wordt aangenomen, zal deze bindend zijn in Nederland. In de ontwerpverordening gegevensbescherming is een meldplicht datalekken opgenomen, die op hoofdlijnen overeenkomt met het huidige Nederlandse voorstel. Er zijn echter een aantal relevante verschillen. Het CBP geeft u in overweging bij de uitwerking van de meldplicht datalekken zo nauw mogelijk aan te sluiten bij de ontwerpverordening gegevensbescherming.

2. Het wetsvoorstel voorziet in artikel 34a, eerste lid, Wbp in een beperking van het aantal meldingen van datalekken bij de toezichthouder. Hoewel het CBP uw zorgen deelt over betekenisverlies van de meldplicht als elke bagatelzaak bij de toezichthouder moet worden gemeld, acht het CBP het Europeesrechtelijk onwenselijk en praktisch onmogelijk om dergelijke beperkingen aan de meldplicht aan de competente toezichthouder nu al te definiëren. Het CBP adviseert u daarom om pas na enige praktijkervaring via een AMvB of ministeriële regeling te voorzien in uitzonderingen op de algemene meldplicht.

3. In het wetsvoorstel dient de termijn waarbinnen moet worden gemeld nader te worden gespecificeerd. Het CBP adviseert u een termijn van maximaal 24 uur na eerste kennisname van de inbreuk te hanteren.

4. In tegenstelling tot de wijze van melden aan betrokkenen, is het CBP van oordeel dat de wijze van melden aan de toezichthouder niet vorm-vrij dient te zijn.

5. Naar het oordeel van het CBP past het niet in zijn toezichthoudende taak om een voorafgaande beoordeling te maken van de mate waarin onbevoegden de mogelijkheid hebben tot kennisname van de gegevens (in de zin van artikel 34a, zesde lid, Wbp). In de

verdeling van verantwoordelijkheden is het de verantwoordelijke zelf die de wet moet toepassen en deze afweging dient te maken.

6. Het CBP verzoekt om helderheid te verschaffen over de vraag wat de verwachting is dat het CBP doet met de ontvangen meldingen. In dit kader verzoekt het CBP tevens om aandacht te besteden aan de doeleinden die met de invoering van de meldplicht datalekken worden beoogd.

7. Het CBP is van oordeel dat inbreuken op de medewerkingsplicht (artikel 5:20 Algemene wet bestuursrecht) dan wel op beveiligingsverplichting (artikel 13 Wbp) bestuurlijk moeten kunnen worden beboet.

8. Het CBP adviseert de hoogte van het boete in het wetsvoorstel in overeenstemming te brengen met de ontwerpverordening gegevensbescherming.

9. Wanneer een verantwoordelijke is gevestigd buiten Nederland, maar binnen de EU dient aandacht te worden besteed aan welk recht van toepassing is.

10. Bij de berekening van de hoogte van de administratieve lasten en nalevingskosten moeten de kosten die voortvloeien uit de protocolplicht voor de verantwoordelijke (op grond van artikel 34a, achtste lid, Wbp) worden meegerekend.

11. Het CBP is daarom van oordeel dat op korte termijn de beheersmatige gevolgen van de invoering van de meldplicht datalekken voor het CBP in kaart dienen te worden gebracht. Het CBP verzoekt de staatssecretaris en de minister een dergelijk onderzoek uit te (laten) voeren en de resultaten te incorporeren in het budget van het CBP.

12. Op grond van artikel 24 Wet Onafhankelijke post- en telecommunicatie autoriteit is de OPTA bevoegd om zijn toezichtsgegevens te delen met andere instanties. Het CBP ziet graag dat het de beschikking krijgt over een dergelijke bevoegdheid.

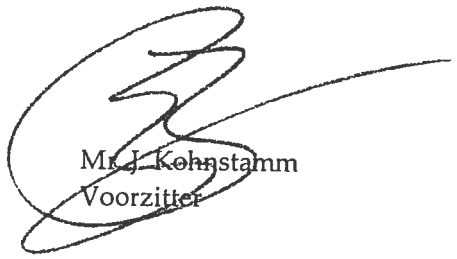
<u>Conclusie</u>
Het CBP adviseert u niet tot indiening van het voorstel inzake meldplicht datalekken over te gaan, dan nadat daarin met het vorenstaande rekening zal zijn gehouden.

Het volledige advies treft u in de bijlage aan. Het CBP verneemt graag op welke wijze u gevolg geeft aan het advies. Het CBP is beschikbaar indien nadere toelichting is vereist.

DATUM 15 maart 2012
ONS KENMERK z2011-00970

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,
Het College bescherming persoonsgegevens,



Mr. J. Kohnstamm
Voorzitter

Bijlage bij de brief van het College bescherming persoonsgegevens van 15 maart 2012 (z2011-00970)

Advies van het College bescherming persoonsgegevens (CBP) over het wetsvoorstel tot wijziging van de Wet bescherming persoonsgegevens en enige andere wetten in verband met de verruiming van de mogelijkheid van het gebruik van camerabeelden van strafbare feiten ten behoeve van de ondersteuning van de rechtshandhaving en de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens.

1. *Algemeen*

De adviesaanvraag van de Staatssecretaris van Veiligheid en Justitie (V&J) (hierna: *de staatssecretaris*), mede namens de Minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) (hierna: *de minister*), heeft betrekking op wijzigingen van de Wet bescherming persoonsgegevens (Wbp), de Telecommunicatiewet en de Wet bestuursrechtspraak bedrijfsorganisatie.

Het onderhavige wetsvoorstel beoogt een verruiming van de mogelijkheid om door particulieren vervaardigde camerabeelden van strafbare feiten te benutten voor de ondersteuning van de rechtshandhaving. Verder wordt in het wetsvoorstel een meldplicht geïntroduceerd voor verantwoordelijken in geval van gebleken doorbrekingen van de getroffen maatregelen ter beveiliging van persoonsgegevens. Voorts zal de meldplicht voor aanbieders van elektronische communicatiediensten in geval van inbreuken op de beveiliging in het kader van de Telecommunicatiewet bij het CBP worden belegd en niet langer bij de Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA). Tot slot wordt het nalaten aan deze meldplichten te voldoen gesanctioneerd met een bestuurlijke boete.

De invoering van de meldplicht datalekken hebben de staatssecretaris en de minister reeds aangekondigd in de brief van 29 april 2011 aan de voorzitters van de Eerste en Tweede Kamer der Staten-Generaal en de daarbij behorende Notitie Privacybeleid. In deze brief en notitie werd een aantal wetgevingsvoornemens bekendgemaakt, waaronder het kwalitatief versterken van de bestuursrechtelijke handhaving van de Wbp, waarbij de materiële gedragsnormen van de Wbp zouden worden gesanctioneerd met een bestuurlijke boete . Ondanks het feit dat de door Eurocommissaris Reding op 25 januari 2012 gepresenteerde *REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012)11,* (hierna: *ontwerpverordening gegevensbescherming*) onder andere een voorstel bevat voor de zogenaamde meldplicht datalekken, vormt dit geen belemmering om de meldplicht met voorrang uit te werken in wetgeving, aldus de staatssecretaris in zijn brief van 20 februari 2012 aan de voorzitter van de Eerste Kamer. Het CBP heeft met instemming van dat deel van het standpunt van de staatssecretaris kennis genomen. Niet valt echter in te zien waarom met betrekking tot de invoering van de boetebevoegdheid een geheel ander standpunt kan of moet worden ingenomen, te weten dat publicatie van de ontwerpverordening wel een belemmering zou vormen voor indiening van het wetsvoorstel inclusief invoering van de bevoegdheid van het CBP om een bestuurlijke boete op te leggen. Dat klemt temeer daar de argumenten voor invoering zoals die zijn verwoord in de brief van 29 april 2011 nog onverminderd van toepassing zijn en de reikwijdte van de ontwerpverordening bekend is. Het CBP dringt er daarom met grote klem op aan thans ook over te gaan tot kwalitatieve versterking van de bestuursrechtelijke handhaving van de WBP, waarbij de materiële gedragsnormen van de Wbp zullen worden gesanctioneerd met een bestuurlijke boete.

Het wetsvoorstel en de bijbehorende Memorie van Toelichting geven aanleiding tot de volgende opmerkingen.

2. *Beoordeling*

2.1 Gebruik van door particulieren vervaardigde camerabeelden in de opsporing

Camerabeelden van strafbare feiten blijken een nuttig hulpmiddel bij de opsporing van strafbare feiten. Het doel van de wetswijziging is om een meer efficiëntere benutting van het beeldmateriaal van particulieren te bewerkstellingen. Voorkomen dient te worden dat burgers overgaan tot het zelfstandig plaatsen van camerabeelden op internet zonder betrokkenheid van politie en justitie. Door cameratoezicht vervaardigde beelden kunnen de opsporing en vervolging van strafbare feiten in belangrijke mate ondersteunen, aldus de staatssecretaris en de minister. Zij stellen daarom voor om:

- beelden die worden verwerkt door particuliere beveiligingsorganisaties ook buiten de relatie tussen beveiligingsbedrijf en opdrachtgever te kunnen verwerken.
- particulieren zelf in staat te stellen om beelden te verspreiden.

Beide voorstellen dienen te gebeuren onder voorwaarden die in het belang van de opsporing en vervolging van strafbare feiten en het belang van de bescherming van persoonsgegevens moeten worden gesteld.

In zijn algemeenheid kan het CBP zich in grote lijnen vinden in het wetsvoorstel. Het CBP heeft slechts enkele opmerkingen. Overigens geeft het CBP in zijn A&V-studie 'Camera's in het publieke domein. Privacynormen voor het cameratoezicht op de openbare orde' een praktische verheldering van de privacynormen die gelden bij cameratoezicht[1].

2.1.1 Plaatsen beelden zonder toestemming Officier van Justitie

In de Memorie van Toelichting (p.4) wordt een aantal concrete toepassingen genoemd, waaronder het plaatsen van opgenomen beelden van strafbare feiten op de beeldschermen van winkelcentra dan wel het verspreiden van de beelden via private middelen. Deze mogelijkheden mogen volgens de Memorie van Toelichting alleen worden geboden indien de Officier van Justitie toestemming heeft verleend. Wat gebeurt er als de Officier van Justitie een dergelijke plaatsing of verspreiding niet goedkeurt of zelfs niet om toestemming is gevraagd en een particulier plaatst de beelden toch op een beeldscherm of internet? Welke organisatie is dan bevoegd om actie te ondernemen? Het CBP verzoekt de staatssecretaris en de minister dringend om in de wettekst duidelijk op te nemen welke instantie(s) in dergelijke situaties geacht wordt om actie te ondernemen.

2.1.2 Nacontrole verwijderen persoonsgegevens

In de Memorie van Toelichting wordt een aantal keer verwezen naar de Aanwijzing Opsporingsberichtgeving (2009A004), onder andere ten aanzien van het verwijderen van persoonsgegevens wanneer deze onterecht openbaar zijn gemaakt. Het CBP vraagt zich af (en kon dat niet in deze aanwijzing teruglezen) welke actie de instantie – die deze persoonsgegevens openbaar heeft gemaakt – neemt tegen het beschikbaar blijven van deze persoonsgegevens via andere websites of andere media, ondanks dat deze instantie de persoonsgegevens wel van zijn eigen website heeft verwijderd. Zorgt deze instantie voor een nacontrole na de verwijdering van het medium? Zo ja: op welke manier? Het CBP is namelijk van oordeel dat een dergelijke

[1] Achtergrondstudie en Verkenning 'Camera's in het publieke domein. Privacynormen voor het cameratoezicht op de openbare orde', december 2004.

instantie daarvoor verantwoordelijk blijft. Het CBP adviseert de staatssecretaris en de minister dringend om aan dit aspect aandacht te besteden in de Memorie van Toelichting.

2.1.3 Algemene maatregel van bestuur (AMvB)

Op diverse plekken in de Memorie van Toelichting wordt aangegeven dat er bij AMvB nader zal worden geregeld onder welke voorwaarden particulieren een ruimere mogelijkheid kan worden geboden tot verwerking van camerabeelden "(...) zonder dat de omslachtige en langdurige procedure van het voorafgaand onderzoek door het CBP moet worden gevolgd." Het CBP verzoekt de staatssecretaris en de minister om deze AMvB aan het CBP voor te leggen, conform artikel 51, tweede lid, Wbp.

2.1.4 Rechtmatigheidstoets

Het aanpassen van "en" naar "of" in artikel I, b, lid 1 (artikel 22, vierde lid, sub c, Wbp) heeft de consequentie dat er eventueel geen rechtmatigheidstoets meer zal plaatsvinden bij het verwerken van strafrechtelijke gegevens ten behoeve van derden. Onder welke voorwaarde is geen voorafgaand onderzoek vereist en volstaan enkel de "passende en specifieke waarborgen"? Daarnaast blijft het CBP van mening dat ingeval een verantwoordelijke de procedure van een voorafgaand onderzoek volgt, hij ook passende en specifieke waarborgen moet hebben getroffen ten aanzien van de verwerking van strafrechtelijke persoonsgegevens ten behoeve van derden. Het CBP adviseert de staatssecretaris en de minister om aan deze aspecten aandacht te besteden in de Memorie van Toelichting.

2.1.5 Conclusie

Het CBP adviseert aan het vorenstaande op passende wijze aandacht te schenken.

2.2 Meldplicht datalekken

Het CBP is van oordeel dat de invoering van een meldplicht datalekken de bescherming van persoonsgegevens in het algemeen, en de versterking van de positie van de burger in het bijzonder in hoge mate zal dienen. De meldplicht zal stimulerend werken op de op verantwoordelijken rustende verplichting om zorg te dragen voor adequate beveiliging van verzamelde en opgeslagen persoonsgegevens (krachtens artikel 13 Wbp). De wijze waarop de meldplicht datalekken in het onderhavige wetsvoorstel is vormgegeven, biedt daarvoor een eerste aanzet, maar dient op bepaalde onderdelen te worden gewijzigd.

2.2.1 Nieuwe EU ontwerpverordening gegevensbescherming

De invoering van de meldplicht datalekken loopt vooruit op de regelgeving die op dit moment in Brussel wordt voorbereid. Zodra de ontwerpverordening gegevensbescherming wordt aangenomen, zal deze bindend zijn in Nederland. De meldplicht datalekken opgenomen in artikel 31 van de ontwerpverordening gegevensbescherming komt op hoofdlijnen overeen met het huidige Nederlandse voorstel. Er zijn echter een aantal relevante verschillen. Bovendien zal de ontwerpverordening zeer waarschijnlijk nog wijzigingen ondergaan alvorens te worden aangenomen. Het is dus zeer aannemelijk dat de Nederlandse regelgeving omtrent de meldplicht voor datalekken, en de reeds genomen uitvoeringsmaatregelen, zullen moeten worden gewijzigd na adoptie van de ontwerpverordening.

Een belangrijk verschil tussen beide voorstellen is dat het Nederlandse wetsvoorstel een drempel kent voor het melden van zaken. De ontwerpverordening gegevensbescherming verplicht tot het melden van ieder datalek. Een ander opmerkelijk verschil is de inhoud van de kennisgeving aan de toezichthouder. Ten aanzien van de aard van de inbreuk stelt de Memorie van Toelichting bij het wetsvoorstel dat "doorgaans met een algemene omschrijving [zal] kunnen worden volstaan".

De ontwerpverordening is op dit punt specifieker. Artikel 31(3)a stelt dat in de beschrijving van de aard van het datalek inbegrepen moeten zijn " the categories and number of data subjects concerned and the categories and number of data records concerned". Dit is een relevante specificatie want dergelijke informatie maakt het mogelijk een oordeel te vormen van de ernst van de inbreuk. Het CBP adviseert om deze specificatie ook op te nemen.

Wijziging van onder andere omvang en inhoud van de melding nadat de wetgeving een relatief korte tijd in werking is, is onwenselijk. Reeds eerder gedane investeringen worden daarmee deels teniet gedaan. Dit kan eveneens afbreuk doen aan de kenbaarheid van de wetgeving. De urgentie van deze wetgeving is desalniettemin zo groot dat het CBP het besluit van de minister om dit onderwerp met voorrang uit te werken in nationale wetgeving onderschrijft. Het CBP geeft de staatssecretaris en de minister echter wel in overweging om vanwege bovengenoemde bezwaren bij deze uitwerking zo nauw mogelijk aan te sluiten bij de ontwerpverordening gegevensbescherming.

2.2.2 Omvang en definitie meldplicht

Het wetsvoorstel voorziet in artikel 34a, eerste lid, Wbp in een beperking van het aantal meldingen van datalekken bij de toezichthouder. De verantwoordelijke moet aan de toezichthouder melden: *een inbreuk op de maatregelen, bedoeld in artikel 13, waarvan redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijk risico op verlies of onrechtmatige verwerking waaraan nadelige gevolgen voor de persoonsgegevens en de persoonlijke levenssfeer van de betrokkene zijn verbonden*.[2] Voor deze constructie is gekozen, omdat een meldplicht zonder enige beperking zou leiden tot een nodeloze belasting van bedrijfsleven en overheid. Voorts zou de effectiviteit van de meldplicht voor datalekken snel aan betekenis verliezen wanneer elk denkbaar datalek in aanmerking kwam om te worden gemeld. Hoewel het CBP de zorgen van de staatssecretaris en de minister deelt over betekenisverlies van de meldplicht als elke bagatelzaak bij de toezichthouder moet worden gemeld, acht het CBP het Europeesrechtelijk onwenselijk en praktisch onmogelijk om dergelijke beperkingen aan de meldplicht aan de competente toezichthouder nu al te definiëren.

De algemene meldplicht is beperkter dan de meldplicht voorzien in de Richtlijn 2002/58/EG[3] (hierna: *de Bijzondere privacyrichtlijn*), zoals gewijzigd door de Richtlijn 2009/136/EG[4] (de Richtlijn burgerrechten). Deze richtlijnen zullen worden geïmplementeerd in de Telecommunicatiewet. Dit wetsvoorstel, waarover het CBP op 4 juni 2010 heeft geadviseerd (z2010-00475), ligt thans bij de Eerste Kamer (32 549). Op grond van het nieuwe artikel 11.3a Telecommunicatiewet zal een meldplicht bij de toezichthouder ontstaan bij *een inbreuk op de beveiliging die nadelige gevolgen heeft voor de bescherming van persoonsgegevens*. Een meldplicht aan de betrokkene ontstaat alleen *indien een inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer*. Het

---

[2] Deze definitie zal ook worden opgenomen in artikel 14, eerste lid, Wbp.

[3] Richtlijn 2002/58/EG van het Europees Parlement en de Raad van de Europese Unie van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie).

[4] Richtlijn 2009/136/EG van het Europees Parlement en de Raad van de Europese Unie van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische communicatienetwerken en –diensten, de E-Privacyrichtlijn en verordening (EG) nr. 2006/2004 betreffende samenwerking met betrekking tot consumentenbescherming (PbEG L 337).

onderhavige wetsvoorstel maakt geen onderscheid tussen datalekken die aan de toezichthouder moeten worden gemeld, en datalekken die aan de betrokkene[5] moeten worden gemeld.

In de ontwerpverordening gegevensbescherming is evenmin gekozen voor het introduceren van een drempel voor bagatelzaken. De verplichting die voortvloeit uit de ontwerpverordening is identiek aan de verplichtingen die voortvloeien uit de Bijzondere privacyrichtlijn, namelijk het melden van elke inbreuk op de persoonsgegevens aan de toezichthouder. Het voorgestelde artikel 31, eerste lid, luidt: *In the case of a personal data breach, the controller shall (...) notify the personal data breach to the supervisory authority* en artikel 32, eerste lid, beschrijft wanneer aan betrokkenen moet worden gemeld: *When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject.*

Er ontstaan volgens voornoemde wetsvoorstellen twee verschillende meldplichten in Nederland, één uitgebreide voor de telecomsector en een beperktere voor alle overige verantwoordelijken voor de gegevensverwerking in de publieke en in de private sector. Het wetsvoorstel bevat geen motivatie waarom de telecomsector anders dient te worden behandeld dan overige verantwoordelijken. Het toezicht op deze nieuwe meldplicht voor de telecomsector wordt na inwerkingtreding van het onderhavige wetsvoorstel overgedragen aan het CBP, waardoor het CBP merkwaardigerwijze twee toezichtspraktijken moet ontwikkelen.

Ook analytisch kleven er bezwaren aan het op voorhand introduceren van beperkingen aan de meldplicht aan de competente toezichthouder. Feit is dat noch de toezichthouders noch de wetgever noch de verantwoordelijken op dit moment voldoende overzicht hebben van de mogelijke nadelige gevolgen van datalekken voor betrokkenen. Dit terwijl de meldplicht primair bedoeld is om het belang van betrokkenen beter te beschermen, door hen te informeren over maatregelen die zij kunnen treffen om nadelige gevolgen van datalekken te voorkomen. Het is van belang voor de effectiviteit van het toezicht op naleving van de wetgeving dat de toezichthouder aan de hand van gedane meldingen achteraf kan controleren of verantwoordelijken terecht hebben besloten betrokkenen niet in te lichten, zeker in de eerste periode na invoering van de wet. De toezichthouder kan ook prioriteit leggen bij verantwoordelijken die nooit een datalek melden bij de toezichthouder. Dat zou een teken kunnen zijn van het ontbreken van adequate processen om datalekken te detecteren, dan wel van onwil om datalekken te melden.

Tenslotte is van belang dat de toezichthouder op basis van de meldingen geanonimiseerde overzichtsrapportages zal uitbrengen met veel gemaakte beveiligingsfouten die tot datalekken hebben geleid, om verantwoordelijken te stimuleren het beveiligingsniveau van de verwerking van hun persoonsgegevens te verhogen.

Bij de analyse van de ernst van datalekken zal in ieder geval rekening moeten worden gehouden met de combinatie van verschillende gegevens. Bijvoorbeeld in het op pagina 8 en 9 van de Memorie van Toelichting genoemde voorbeeld van de ledenlijst van een vereniging, is ten onrechte geen rekening gehouden met het feit dat een verenigingslidmaatschap ook bijzondere persoonsgegevens kan bevatten, zoals het lidmaatschap van een bepaalde patiëntenvereniging, of gegevens die op andere wijze gevoelig kunnen liggen, zoals lidmaatschap van een schietsportvereniging. Een (zoekgeraakte of gehackte ledenlijst kan ook andere gegevens bevatten, zoals bijvoorbeeld de financiële administratie of (op internet gebruikte) accountnamen.

---

[5] Op grond van artikel 34a, zesde lid, Wbp is de kennisgeving aan de betrokkene niet vereist indien de gegevens adequaat ontoegankelijk zijn gemaakt.

Als die (mogelijk bewust anoniem gekozen) accountnamen zijn gebruikt om publieke bijdragen te posten op bijvoorbeeld het ledenforum op de website van die patiëntenvereniging, ontstaat een groot risico voor betrokkenen, bijvoorbeeld op een andere behandeling door een ziektekostenverzekeraar.

Juist omdat er vaak sprake is van een combinatie van gegevens, kunnen er op voorhand geen soorten datalekken worden uitgesloten van de meldplicht aan de toezichthouder. De enige generieke vrijstelling die het CBP op dit moment mogelijk en wenselijk acht, is een onvoorziene vernietiging van persoonsgegevens, mits die fout makkelijk hersteld kan worden vanuit een up-to-date database, zonder gevolgen voor betrokkenen.

Het CBP is van harte bereid om te assisteren bij het naderhand vrijstellen van bepaalde soorten datalekken van melding aan de toezichthouder, als uit de praktijk is gebleken dat deze geen nadelige gevolgen opleveren voor betrokkenen. Om daarover te kunnen adviseren aan de wetgever dient de toezichthouder in de eerste periode na invoering van de meldplicht een zo compleet mogelijk beeld te krijgen van datalekken en niet alleen een afschrift van datalekken die toch al aan betrokkenen worden gemeld.

Het CBP adviseert de staatssecretaris en de minister daarom om pas na enige praktijkervaring via een AMvB of ministeriële regeling te voorzien in uitzonderingen op de algemene meldplicht.

2.2.3 *Termijn*

Artikel 34a, eerste lid, Wbp stelt dat de verantwoordelijke het College "onverwijld" in kennis stelt van een inbreuk op de beveiligingsmaatregelen. Het CBP adviseert de termijn reeds in de wet te specificeren en adviseert een termijn van maximaal 24 uur na eerste kennisname van de inbreuk te hanteren. Indien het binnen deze termijn nog niet mogelijk is om alle meldingsplichtige informatie te verschaffen, zou in eerste instantie kunnen worden volstaan met een beperkte melding binnen 24 uur, die nader aangevuld kan worden binnen een langere termijn.

2.2.4 *Wijze van melden*

In tegenstelling tot de wijze van melden aan betrokkenen, is het CBP van oordeel dat de wijze van melden aan de toezichthouder niet vorm-vrij dient te zijn.

In deze context constateert het CBP met genoegen dat de Memorie van Toelichting melding maakt van het feit dat in Europees verband gewerkt wordt aan een geharmoniseerd formulier voor het melden van datalekken, en dat een dergelijk formulier goede diensten kan bewijzen bij datalekken met grensoverschrijdende effecten, waarbij samenwerking tussen de toezichthouders van de lidstaten nodig is. In aanvulling hierop kan worden medegedeeld dat de ontwikkeling van dat (web)formulier inmiddels is afgerond en dat het eind 2011 is gepubliceerd. Aan de ontwikkeling van het formulier hebben ook experts vanuit het bedrijfsleven en de toezichthouders van de lidstaten deelgenomen. Het formulier is zodanig opgesteld dat de verantwoordelijke op eenvoudige wijze alleen die vragen krijgt voorgeschoteld, die relevant zijn voor de betreffende zaak, en te allen tijde nadere informatie kan geven, als meer informatie bekend raakt over de oorzaken van het datalek en beveiligingsmaatregelen, die zijn getroffen om dit in de toekomst te voorkomen.

De Memorie van Toelichting stelt ook dat het gebruik van het formulier zonodig bij AMvB op grond van artikel 34a, elfde lid, van de Wbp kan worden voorgeschreven. Het CBP onderschrijft het belang van het werken met een in Europa overeengekomen formulier en benadrukt de

noodzaak tot nauwe afstemming met alle betrokken uitvoerders over de nadere regels voor de meldplicht. Dit is van belang voor een effectieve samenwerking tussen toezichthouders, maar eveneens voor de verantwoordelijken en de aanbieders van openbare elektronische communicatiediensten, aangezien ook zij in toenemende mate grensoverschrijdend opereren en dus mogelijk bij meerdere toezichthouders datalekken moeten melden. Op deze wijze worden voor alle partijen de administratieve lasten zo laag mogelijk gehouden.

2.2.5 Uitzonderingen op de meldplicht

Artikel 34a, tweede lid, Wbp voorziet in een kennisgeving van de inbreuk aan de betrokkene. Artikel 34a, zesde lid, Wbp stelt dat deze kennisgeving niet is vereist indien de verantwoordelijke naar het oordeel van het College gepaste technische beschermingsmaatregelen heeft 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. Ook de Memorie van Toelichting stelt op pagina 10 dat "het CBP beoordeelt of dit feitelijk het geval is". Naar het oordeel van het CBP past het niet in zijn toezichthoudende taak om een voorafgaande beoordeling te maken van de mate waarin onbevoegden de mogelijkheid hebben tot kennisname van de gegevens. In de verdeling van verantwoordelijkheden is het de verantwoordelijke zelf die de wet moet toepassen en deze afweging dient te maken. De verantwoordelijke zelf is ook het beste geëquipeerd om deze beoordeling in de omstandigheid van een datalek te maken. Het CBP dient hierop, conform artikel 34a, zevende lid, Wbp toezicht te houden en achteraf te beoordelen of de verantwoordelijke gelet op de feiten en omstandigheden de juiste afweging heeft gemaakt. Naast dit principiële argument ten aanzien van de rolverdeling tussen partijen zal het invulling geven aan deze plicht ook in de praktijk, gelet op het aantal verwachte meldingen, een te grote last voor het CBP met zich meebrengen. Dit zal ten koste gaan van de toezichthoudende en handhavende taken die het CBP in het kader van de meldplicht zal moeten uitvoeren. Het CBP verzoekt de staatssecretaris en de minister artikel 34a, zesde lid, Wbp op dit punt te wijzigen.

Om overlap van meldingen te voorkomen geldt de meldplicht krachtens het voorgestelde artikel 34a Wbp niet, indien de verantwoordelijke in zijn hoedanigheid van aanbieder van een elektronische communicatiedienst op grond van artikel 11.3a Telecommunicatiewet al een kennisgeving heeft gedaan (artikel 34a, negende lid, Wbp). Deze uitzondering geldt niet in situaties waarin de verantwoordelijke een ander is dan de aanbieder. Beide partijen dienen dan te melden op grond van artikel 34a Wbp, respectievelijk artikel 11.3a Telecommunicatiewet. Het is voor het CBP niet duidelijk aan welke situaties moet worden gedacht. Het CBP adviseert de staatssecretaris en de minister om dit aspect nader toe te lichten met praktijkvoorbeelden.

2.2.6 Doel van de meldplicht en rol van het CBP ten aanzien van de melding

Met de meldplicht aan het CBP wordt volgens de staatssecretaris en de minister beoogd het toezicht op potentieel ernstige datalekken te ondersteunen. Door het ontvangen van informatie kan het CBP beoordelen of een onderzoek of het geven van aanwijzingen noodzakelijk is. Het is zeker geen gegeven dat het CBP iedere melding laat volgen door een onderzoek of andere maatregelen. Een verantwoordelijke die handelt op de manier die van hem mag worden verwacht treft immers zelf zo spoedig mogelijk de nodige maatregelen om het datalek te dichten en herhaling van het voorval tegen te gaan. Een melding bij het CBP zal in die gevallen veelal zonder enige reactie blijven. Het CBP zal deze meldingen wel opslaan en daarover verantwoording afleggen, bijvoorbeeld in het jaarverslag, aldus de staatssecretaris en de minister.

Uit het bovenstaande volgt dat de staatssecretaris en de minister niet de bedoeling hebben dat het CBP bij iedere melding een onderzoek instelt dan wel op iedere melding reageert. In de Memorie van Toelichting ontbreekt vervolgens een nadere uitwerking. Het CBP verzoekt om helderheid te

verschaffen over de vraag wat de verwachting is dat het CBP doet met de ontvangen meldingen. Het CBP adviseert om dit aspect, daarbij rekening houdend met de overige taken en bevoegdheden van het CBP, nader uit te werken in de Memorie van Toelichting. In dit kader verzoekt het CBP om ook aandacht te besteden aan de doeleinden die met de invoering van de meldplicht datalekken worden beoogd. De Memorie van Toelichting schenkt hieraan momenteel te weinig aandacht.

2.2.7 Sanctionering

Medewerkingsplicht

Het nieuwe artikel 15.4 Telecommunicatiewet geeft het CBP het recht een boete op te leggen wegens het niet meewerken in het kader van meldplicht datalekken in de Telecommunicatiewet (artikel 5:20 Algemene wet bestuursrecht (Awb)). Voor overtreding van artikel 5:20 Awb in het kader van de Wbp kan het CBP echter 'slechts' een last onder dwangsom opleggen (artikel 61, vierde lid, Wbp j° artikel 5:32 Awb). Dit leidt tot inconsistentie.

Het CBP heeft reeds in het verleden benadrukt dat het graag over een boetebevoegdheid wenst te beschikken bij niet voldoen aan de medewerkingsplicht krachtens artikel 5:20 Awb.[6] Voor het bereiken van het doel van de medewerkingsplicht – het mogelijk maken dat toezichthouders de hun toekomende bevoegdheden kunnen effectueren – heeft het opleggen van een last onder dwangsom onvoldoende afschrikwekkend effect. Dit geldt temeer als gegevens of bescheiden zijn of worden vernietigd. Ook de Nederlandse Mededingingsautoriteit, de OPTA en de Autoriteit Financiële Markten beschikken over de bevoegdheid een bestuurlijke boete op te leggen bij niet-medewerking.

Op grond van het voorgaande meent het CBP dat het onderhavige wetsvoorstel een goed moment is voor het toekennen van een boetebevoegdheid aan het CBP bij niet medewerken (overtreding artikel 5:20 Awb) en verzoekt het wetsvoorstel op dit punt aan te vullen.

Beveiligingsverplichting

De meldplicht voor datalekken staat in nauw verband met de beveiligingsverplichting van artikel 13 Wbp. Op grond van deze bepaling is de verantwoordelijke verplicht om passende technische en organisatorische maatregelen ten uitvoer te leggen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Gelet op deze samenhang ziet het CBP graag dat inbreuken op deze bepaling (de materiële norm) ook bestuurlijk door het CBP kunnen worden beboet.

Ook de OPTA heeft op grond van het huidige artikel 15.4, vierde lid, Telecommunicatiewet de mogelijkheid om een bestuurlijke boete van ten hoogste € 450.000,- op te leggen bij overtreding van de beveiligingsplicht, die krachtens artikel 11.3 Telecommunicatiewet op de aanbieders van openbare elektronische communicatienetwerken en -diensten rust.

Tot slot bevat ook de ontwerpverordening gegevensbescherming in artikel 79 (6e) een maximale boete van € 1.000.000,- dan wel 2% van de jaarlijkse omzet wereldwijd voor schending van de beveiligingsverplichting.

---

[6] Zie brief van het CBP d.d. 9 juni 2011 aan de leden van de vaste commissies voor Veiligheid en Justitie en Binnenlandse Zaken van de Tweede Kamer over Brief en notitie privacybeleid; TK 2010-2011, 32761, nr. 1 en bijlagen (z2011-00407).

Het CBP verzoekt de staatssecretaris en de minister om het wetsvoorstel op dit punt aan te vullen.

2.2.8 Hoogte van de boete

Het nieuwe tweede lid van artikel 66 Wbp geeft het CBP het recht een boete op te leggen van maximaal € 200.000 voor overtreding van de meldplicht. De ontwerpverordening gegevensbescherming bevat echter een maximale boete van € 1.000.000 voor het schenden van de meldplicht (artikel 79(6h)). Dit is strijdig met elkaar. Het CBP adviseert de boete in het wetsvoorstel in overeenstemming te brengen met het Europese voorstel.

2.2.9 Toepasselijk recht

In de artikelsgewijze toelichting bij de wijzigingen van de Telecommunicatiewet wordt gesteld dat het CBP volgens *de systematiek van de Telecommunicatiewet* wordt belast met het toezicht op de naleving van de bepalingen met betrekking tot de beveiligingsplichten en de meldplicht. De beveiligingsplicht geldt op grond van de Telecommunicatiewet voor een aanbieder van een openbaar elektronisch communicatienetwerk of –dienst en de meldplicht voor een aanbieder van een dergelijke dienst.

Op grond van artikel 4, eerste lid, Wbp is deze wet van toepassing op de verwerking van persoonsgegevens in het kader van activiteiten van een vestiging van een verantwoordelijke in Nederland. Het kan in de praktijk voorkomen dat een verantwoordelijke binnen Nederland persoonsgegevens verwerkt, maar zijn vestiging in een ander EU-land heeft. Dit betekent dan dat het recht van dat betreffende EU-land van toepassing is en het CBP is daardoor niet bevoegd. Wanneer deze verantwoordelijke tevens een openbare elektronische communicatienetwerk of –dienst aanbiedt, is de Telecommunicatiewet van toepassing en is het CBP wel bevoegd. In geval van een datalek is het voor de verantwoordelijke en/of de aanbieder niet duidelijk of en op grond van welke wetgeving zij geacht worden bij welke toezichthouder wat te melden. Het CBP verzoekt de staatssecretaris en de minister aan deze aspecten aandacht te besteden in de Memorie van Toelichting.

2.2.10 Administratieve lasten en nalevingskosten

Bij de berekening van de hoogte van de administratieve lasten en nalevingskosten zijn de kosten die voortvloeien uit de protocolplicht voor de verantwoordelijke op grond van artikel 34a, achtste lid, Wbp niet meegerekend. Het CBP adviseert de staatssecretaris en de minister dat alsnog te doen.

2.2.11 Bestuurlijke lasten

In de Memorie van Toelichting wordt gesteld dat de consequenties van het onderhavige wetsvoorstel voor de organisatie van het CBP nog niet goed in kaart zijn te brengen. De eventuele veranderingen in de werklast van het CBP als gevolg van de introductie van de meldplicht moeten eerst feitelijk worden vastgesteld, voordat een beslissing kan worden genomen over de gevolgen die aan die vaststelling moet worden verbonden. Het CBP heeft grote bezwaren tegen een dergelijke constructie. Het CBP vreest namelijk dat de invoering van de meldplicht datalekken zodanige beheersmatige gevolgen heeft, dat de reële kans aanwezig is dat het CBP zijn reeds bestaande taken en bevoegdheden niet meer naar behoren kan uitoefenen als voor de nieuwe taken geen extra middelen ter beschikking komen.

Het CBP is daarom van oordeel dat op korte termijn de beheersmatige gevolgen van de invoering van de meldplicht datalekken voor het CBP in kaart dienen te worden gebracht. Het CBP

verzoekt de staatssecretaris en de minister een dergelijk onderzoek uit te (laten) voeren en de resultaten te incorporeren in het budget van het CBP.

2.2.12 Het delen van informatie met andere nationale toezichthouders

Op grond van artikel 24 Wet Onafhankelijke post- en telecommunicatie autoriteit is de OPTA bevoegd om zijn toezichtsgegevens te delen met andere instanties. Het CBP ziet graag dat het de beschikking krijgt over een dergelijke bevoegdheid.

2.2.13 Conclusie

Het CBP adviseert niet tot indiening van het voorstel over te gaan, dan nadat daarin met het vorenstaande rekening zal zijn gehouden.

3. Redactioneel

1. College bescherming persoonsgegevens wordt consequent onjuist als "Cbp" afgekort. Dit moet CBP zijn. Het CBP verzoekt dit aan te passen.
2. Op pagina 6 van de Memorie van Toelichting wordt in het kader van de bevoegdheid van het CBP om toezicht te houden op de naleving van verwerkingen van persoonsgegevens verwezen naar artikel 51, tweede lid, van de Wbp. Deze verwijzing is niet juist. Dit moet namelijk artikel 51, eerste lid, zijn. Het CBP adviseert dit aan te passen.
3. In artikel 34a, negende lid, Wbp wordt gesproken over de "aanbieder van een elektronische communicatiedienst". In deze context, waarin wordt verwezen naar artikel 11.3a, eerste en tweede lid, van de Telecommunicatiewet, wordt echter de "aanbieder van een *openbare* elektronische communicatiedienst" bedoeld. Het CBP adviseert derhalve artikel 34a, negende lid, van de Wbp aan te passen.