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.