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 E-MAIL info@cbpweb.nl INTERNET www.cbpweb.nl

Wetgevingsadvies CBP inzake wijziging van de Telecommunicatiewet
4 juni 2010, z2010-00475

De minister van Economische Zaken heeft het College bescherming persoonsgegevens (CBP) gevraagd te adviseren, als bedoeld in artikel 51, tweede lid, van de Wet bescherming persoonsgegevens (Wbp).

Inhoud van het wetsvoorstel
De wijziging van de Telecommunicatiewet strekt tot implementatie van richtlijn nr. 2009/140/EG (PbEG L337), richtlijn nr. 2009/136/EG (PbEG L337) en Verordening nr. 1211/2009. Richtlijn nr. 2009/140 wijzigt de Kaderrichtlijn (2002/21/EG), de Toegangsrichtlijn (2002/19/EG) en de Machtigingsrichtlijn (2002/20/EG) en richtlijn nr. 2006/136/EG wijzigt de Universeledienstrichtlijn (2002/22/EG) en de Bijzondere privacyrichtlijn (2002/58/EG).
Volgens de Memorie van Toelichting beoogt de herziening van bovengenoemd Europees regelgevend kader de volgende wijzigingen:

- Minder maar meer effectieve *ex ante* regulering
- Meer harmonisatie
- Flexibilisering spectrumbeheer
- Betere consumentenbescherming
- Privacy en beveiliging

Beoordeling

1) Algemeen
De Bijzondere Privacyrichtlijn vormt één van de grondslagen voor deze wijziging van de Telecommunicatiewet. Privacybescherming is derhalve één van de fundamentele belangen van het Europees regelgevend kader. Op pagina 3 en 4 van de Memorie van Toelichting worden de hoofdkenmerken genoemd die moeten bijdragen aan verbetering van dit kader. Eén van die kenmerken betreft 'Privacy en beveiliging'. De Memorie van Toelichting stelt: "*Met name door de invoering van een meldplicht voor privacy- en veiligheidsinbreuken zal de kwaliteit en beveiliging van netwerken en diensten beter inzichtelijk worden, waardoor de consument beter kan kiezen en het vertrouwen in en daarmee het gebruik van ICT-diensten zal toenemen*". Deze passage lijkt privacybescherming slechts als een nevendoel van de wijziging van het regelgevend kader te karakteriseren. In overweging 51 van de considerans van richtlijn 2009/136/EG wordt echter uiteengezet dat het doel van de Bijzondere Privacyrichtlijn het harmoniseren van de regelgeving is, die nodig is om een gelijk niveau te waarborgen van de bescherming van de fundamentele rechten en vrijheden, met name het recht op vertrouwelijkheid bij de verwerking van persoonsgegevens in de sector elektronische communicatie. Daarnaast, aldus de considerans, beoogt de Bijzondere Privacyrichtlijn te zorgen voor vrij verkeer van dergelijke gegevens en van elektronische communicatieapparatuur en –diensten in de Gemeenschap. Voorts stelt de considerans in overweging 69 dat de noodzaak zich doet gevoelen van effectieve tenuitvoerleggings- en handhavingsbevoegdheden teneinde adequate nalevingsstimulansen te leveren, aangezien een toereikend niveau van bescherming van de persoonlijke levenssfeer en de persoonsgegevens, verzonden en verwerkt in het kader van het gebruik van elektronische communicatienetwerken in de Gemeenschap, moet worden gewaarborgd.

2) Meldplicht voor inbreuken in verband met persoonsgegevens en meldplicht voor veiligheidsinbreuken en het verlies van integriteit

In het wetsvoorstel worden twee meldplichten geïntroduceerd. Ten eerste de meldplicht voor aanbieders van openbare elektronische communicatiediensten, indien sprake is van inbreuken in verband met persoonsgegevens (artikel 11.3b, eerste lid). Het moet gaan om inbreuken op de beveiliging die tot gevolg hebben onbedoelde of onwettige vernietiging, wijziging of niet geautoriseerde toegang tot persoonsgegevens. Deze meldplicht vloeit voort uit artikel 4, derde lid, van de Bijzondere Privacyrichtlijn en het toezicht zal worden belegd bij de Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA).

Daarnaast wordt in artikel 11a.2, eerste lid, neergelegd dat aanbieders van openbare elektronische communicatienetwerken en –diensten melding maken van een inbreuk op de veiligheid en een verlies van integriteit, waardoor de continuïteit van openbare elektronische communicatienetwerken en –diensten in belangrijke mate werd onderbroken. Deze eis volgt uit artikel 13bis van de Kaderrichtlijn en het toezicht zal worden belegd bij de minister van Economische Zaken. Dit betekent dat er twee meldplichten voor vrijwel dezelfde groep normadressaten zal ontstaan en het toezicht op die meldplichten bij twee toezichthouders wordt belegd, namelijk bij de OPTA en de minister van Economische Zaken.

De Memorie van Toelichting stelt voorts: "*Om administratieve lasten zo veel mogelijk te beperken zal ervoor worden gezorgd dat beide meldingen praktisch gezien bij eenzelfde punt kunnen worden gedaan. De inrichting van het meldpunt moet nog gestalte krijgen. Uitgangspunt is dat het meldpunt zal fungeren als een brievenbus en op geen enkele manier zich met de inhoud van klachten zal bemoeien. Vanuit dat meldpunt wordt er voor gezorgd dat de melding bij de juiste instantie, dat wil zeggen bij de minister, het college, of in geval van genoemde overlap, bij beiden terecht komt.*"

Bij de meldplichten, het centraal belegde meldpunt en de belegging van het toezicht worden de volgende opmerkingen gemaakt.

Allereerst geeft de Memorie van Toelichting aan dat het centrale meldpunt als een brievenbus zal fungeren en zich op geen enkele manier met de inhoud van klachten zal bemoeien. Met het doorgeleiden van de meldingen is het waarschijnlijk dat het meldpunt echter een bredere functie hebben dan slechts die van brievenbus. Het meldpunt zal immers de inhoudelijke afweging moeten maken of de binnengekomen melding betrekking heeft op inbreuken in verband met persoonsgegevens, op inbreuken op de veiligheid en verlies van integriteit of beide. De suggestie dat het meldpunt een brievenbusfunctie heeft, lijkt daarmee een onjuiste kwalificatie van de taak die het centrale meldpunt zal moeten gaan uitvoeren.

Daarnaast besteedt de Memorie van Toelichting ten onrechte onvoldoende aandacht aan de samenloop tussen beide meldplichten. De Memorie van Toelichting stelt slechts: *"Een veiligheidsinbreuk kan immers tegelijkertijd leiden tot een belangrijk effect op de continuïteit en het ongewild vrijkomen van persoonsgegevens*". Bovenstaande passage gaat echter uit van de fictie dat er veiligheidsinbreuken plaatsvinden die niet leiden tot verlies van persoonsgegevens, terwijl in de praktijk inbreuken op de veiligheid en verlies van integriteit nagenoeg altijd gepaard zullen gaan met het vrijkomen van persoonsgegevens. Dit leidt ertoe dat het centrale meldpunt, in het geval een melding binnenkomt met betrekking tot een inbreuk op de veiligheid en verlies van integriteit, deze vrijwel altijd ook als een inbreuk in verband met persoonsgegevens zal moeten duiden. Als gevolg hiervan zal het meldpunt die melding dan naar de minister van Economische Zaken én de OPTA moeten doorzenden. In de Memorie van Toelichting wordt echter niet uiteengezet wat de consequenties van een dubbele doorzending zijn. Het risico is aanwezig dat in een dergelijk geval de

melding aan een dubbel toezicht zal worden onderworpen. Dit kan niet alleen leiden tot een verhoging van bestuurlijke lasten, maar zeker ook van administratieve lasten. De betrokken communicatiedienst wordt bij samenloop immers geconfronteerd met twee toezichthouders waaraan verantwoording moet worden afgelegd, die ieder vanuit hun eigen rol en toetsingskader opereren. Bovendien zijn in totaal vier instanties betrokken bij het toezicht: het centrale meldpunt, de OPTA voor de meldplicht inbreuken in verband met persoonsgegevens, de minister van Economische Zaken wat betreft de meldplicht inbreuken op de veiligheid en verlies van integriteit en tot slot het CBP als toezichthouder op de algemene beveiligingseisen die uit de Wbp voortvloeien, alsmede de toezichthouder op de aangekondigde brede meldplicht (zie onderstaand, onder 3). Hierdoor neemt de toezichtsdruk toe, hetgeen niet in lijn is met de beperking van lasten van overheidstoezicht die het kabinet nastreeft.[1]

Tot slot heeft het Europees Hof van Justitie in een uitspraak van 9 maart 2010 bepaald dat de autoriteiten die belast zijn met het toezicht op de verwerking van persoonsgegevens door niet-publieke organen en publiekrechtelijke ondernemingen die op de markt concurreren hun taken in *volledige onafhankelijkheid* moeten kunnen vervullen en derhalve niet aan overheidstoezicht moeten zijn onderworpen.[2] Aan deze eis van volledige onafhankelijkheid wordt niet voldaan, nu wordt voorgesteld om de meldingen via een centraal meldpunt te laten plaatsvinden en vervolgens het toezicht op de inbreuken op de veiligheid en verliezen van integriteit bij de minister van Economische Zaken te beleggen. Inbreuken op de veiligheid en verliezen van integriteit zullen, zoals hiervoor reeds aangegeven, nagenoeg altijd gepaard gaan met het vrijkomen van persoonsgegevens. Toezicht op inbreuken op de veiligheid en verliezen van integriteit houdt daardoor ook toezicht op verwerkingen van persoonsgegevens in. Om te waarborgen dat het toezicht in volledige onafhankelijkheid plaats zal vinden, dienen het centrale meldpunt en het toezicht op de inbreuken op de veiligheid en verliezen van integriteit daarom bij een onafhankelijk toezichthouder te worden belegd.

3) Algemene meldplicht

Het wetsvoorstel beperkt zich tot de invoering van een smalle meldplicht. De Memorie van Toelichting blikt vooruit op de toekomstige 'brede meldplicht', die zal gelden voor het bedrijfsleven en overheidsorganen: *"Een brede meldplicht voor inbreuken op persoonsgegevens past beter binnen de algemene privacyregels, dat wil zeggen binnen het kader van de algemene privacyrichtlijn en, op nationaal niveau, binnen de Wet bescherming persoonsgegevens. (…) Het College bescherming persoonsgegevens zal belast zijn met het toezicht op de naleving van die verplichtingen. De meldplicht voor aanbieders van elektronische communicatiediensten kent specifieke eisen met betrekking tot de uitvoering er van. Aangezien de in de Wet bescherming persoonsgegevens[3] neer te leggen verplichting tot openbaarmaking van veiligheidsinbreuken een meer algemeen karakter zal krijgen, kan het in stand houden van een meer specifieke regeling in de vorm van een meldplicht voor aanbieders van telecommunicatiediensten noodzakelijk zijn om te voldoen aan de vereisten van de richtlijn."*

Het Europees Parlement en de Tweede Kamer zijn voorstander van een brede meldplicht. De invoering van een brede meldplicht is ook bevestigd door uw ambtgenoot van Justitie tijdens een

---

[1] Zie visiedocument "Minder last, meer effect", 2005

[2] C-518/07, Europese Commissie vs Duitsland

[3] De Memorie van Toelichting spreekt abusievelijk van de Wet bescherming persoonlijke levenssfeer

algemeen overleg met de vaste Kamercommissies voor Justitie en Binnenlandse Zaken en Koninkrijksrelaties op 3 februari 2010.[4]

De Memorie van Toelichting stelt dat, indien de brede meldplicht wordt ingevoerd, het toezicht bij het CBP zal worden belegd. Een specifieke regeling voor de meldplicht voor aanbieders van openbare elektronische communicatiediensten zal overeind blijven.
Hieruit volgt dat na invoering van de brede meldplicht het toezicht op inbreuken in verband met persoonsgegevens verdeeld zal worden; openbare elektronische communicatiediensten bij de OPTA en de overheid en alle overige bedrijven bij het CBP.

Bij deze verdeelde belegging van toezicht worden de volgende opmerkingen gemaakt.
Ten eerste bestaat het risico dat onduidelijkheid ontstaat voor de normadressaat bij welke toezichthouder de melding moet worden gedaan. Ook is de mogelijkheid aanwezig dat bedrijven binnen de reikwijdte van beide meldplichten zullen vallen, gezien de ontwikkeling dat bedrijven steeds meer een verscheidenheid aan diensten leveren, zowel communicatiediensten als andere diensten. Dit zal leiden tot dubbele meldingen bij beide toezichthouders en toepassing van een inhoudelijk gedifferentieerd normenkader voor het betrokken bedrijf, hetgeen een verhoging van administratieve lasten met zich meebrengt. Maatregelen ter vermijding van deze inefficiëntie brengen uiteraard een verhoging van toezichtskosten met zich mee.

4) Bevoegdheid tot stellen van nadere regels voor inbreuken in verband met persoonsgegevens
In de Memorie van Toelichting wordt ten onrechte geen aandacht besteed aan het feit dat in artikel 13 Wbp reeds de plicht voor verantwoordelijken is neergelegd om passende technische en organisatorische maatregelen te treffen om persoonsgegevens te beveiligen. Het stellen van nadere regels ter invulling van de meldplicht voor inbreuken in verband met persoonsgegevens zal daarom direct raken aan het bepaalde in artikel 13 Wbp. Het moet voorkomen worden dat de nadere regelgeving op basis van artikel 11.3b op gespannen voet komt te staan met de invulling en het bestaande toezicht op artikel 13 Wbp, dat is opgedragen aan het CBP. Teneinde negatieve interferenties in met de reeds geldende privacywetgeving te voorkomen adviseert het CBP om in artikel 11.3b de verplichting op te nemen om de nadere regelgeving op basis van artikel 11.3b in overeenstemming met de minister van Justitie vast te stellen en ter advisering aan het CBP voor te leggen. Overigens zal een algemene maatregel van bestuur reeds op grond van artikel 51, tweede lid, Wbp aan het CBP ter advisering moeten worden voorgelegd. Aangezien deze adviseringsverplichting echter niet geldt voor ministeriële regelingen, adviseert het CBP om die verplichting aan artikel 11.3b toe te voegen.

5) Voorafgaande toestemming en informatieplicht bij opslag in randapparatuur
In artikel 11.3a, eerste lid, wordt de toegang tot gegevens die zijn opgeslagen in de randapparatuur (cookies, spyware) van de gebruiker dan wel de opslag van gegevens in die randapparatuur onderworpen aan een voorafgaande toestemming en informatieplicht. Het CBP maakt de volgende opmerkingen bij dit voorstel.

==========

[4] Uit het verslag van het AO: Mevrouw Azough (Groen Links): *Zal de meldplicht gaan gelden voor alle sectoren, dus overheid, ngo's en bedrijfsleven?* Minister Hirsch Ballin: *Voor de overheid kunnen wij het in eigen beheer regelen. Voor de private sector moeten wij nagaan of er aanvullende wetgeving nodig is of convenanten of een combinatie daarvan. Het is de bedoeling dat het ook voor de private sector geldt. Het antwoord op de vraag is dus "ja".*

De eis van voorafgaande toestemming van de internetgebruiker en een informatieplicht van de internet- en telecomtoegangsaanbieders aan de internetgebruiker met betrekking tot het gebruik van de betreffende randapparatuur zoals cookies, spyware et cetera, zoals voorgesteld in artikel 11.3a, vormt een specialis van hetgeen in de artikelen 8 en 33 van de Wbp is bepaald. Dat betekent dat de toestemming en informatieplicht van artikel 11.3a Telecommunicatiewet mede moet worden uitgelegd en ingevuld met het oog op de algemene toestemmingseis van artikel 8 Wbp en de algemene informatieplicht van artikel 33 Wbp. Hoewel de Memorie van Toelichting op pagina 41 refereert aan deze generalis-specialis relatie[5], wordt geen gewag gemaakt van het feit dat de eis van artikel 11.3a Telecommunicatiewet een aanvulling vormt op hetgeen in de artikelen 8 en 33 Wbp ten aanzien van het algemene vereiste van toestemming voor het verwerken van persoonsgegevens en de informatieplicht dienaangaande is bepaald. Naast de eis van artikel 11.3a Telecommunicatiewet blijven de artikelen 8 en 33 Wbp, alsmede de daarop gebaseerde toezichts- en handhavingspraktijk immers onverkort van kracht.

Het voornemen is om het toezicht op artikel 11.3a Telecommunicatiewet bij de OPTA te beleggen. Dit betekent dat de gegevensverwerking middels randapparatuur, zoals beschreven in artikel 11.3a, binnen het toezichtsveld van zowel de OPTA als het CBP zal vallen. Het CBP behoudt immers zijn reeds bestaande bevoegdheid tot toezicht op grond van de artikelen 8 en 33 Wbp. Dubbel toezicht kan leiden tot verhoging van administratieve lasten. Dit noopt tot voorzieningen ter vermijding van inefficiency in toezicht en handhaving, en ter vermijding van inconsistenties in de interpretatie van de regelgeving c.q. negatieve interferentie met de bestaande privacywetgeving.

Dit geldt eens te meer omdat de essentie van de Telecommunicatiewet van een geheel andere aard is dan de essentie van privacywetgeving. Waar de Telecommunicatiewet vooral het transport van communicatiesignalen regelt, .is de essentie van de Bijzondere Privacyrichtlijn het Europees (8 EVRM) en grondrechtelijk(artikelen 10 en 13 Grondwet) vastgelegde recht op eerbiediging van de persoonlijke levenssfeer en correspondentie. Terwijl de Telecommunicatiewet zich richt op de beperkte groep van aanbieders van internet en telefoontoegang, geldt privacywetgeving voor eenieder.

6) Instellen van rechtsvorderingen tegen ongewenste communicatie

In artikel 13, zesde lid, van de Bijzondere Privacyrichtlijn is de plicht voor lidstaten neergelegd om er voor te zorgen dat natuurlijke of rechtspersonen die een rechtmatig belang hebben bij de bestrijding van inbreuken op nationale bepalingen rechtsvorderingen tegen dergelijke inbreuken kunnen instellen. Deze zorgplicht strekt mede uit naar aanbieders van elektronische communicatiediensten die hun rechtmatige ondernemingsbelangen of de belangen van hun klanten moeten kunnen beschermen. Volgens de transponeringstabel behoeft deze bepaling geen implementatie in de Telecommunicatie, aangezien een actie uit onrechtmatige daad, zoals neergelegd in artikel 6:162 Burgerlijk Wetboek (BW), voldoende uitvoering geeft aan deze zorgplicht. In de Memorie van Toelichting wordt echter geen aandacht besteed aan de vraag of artikel 6:162 BW inderdaad

==========

[5] *"Het verstrekken van de informatie als hiervoor bedoeld betreft een specifieke invulling van de informatieplicht die men op grond van richtlijn 95/46/EG (de algemene privacyrichtlijn), welke is geïmplementeerd in de Wet bescherming persoonsgegevens (Wbp), al heeft. Op basis van de Wbp dient de gebruiker onder meer geïnformeerd te worden over de identiteit van de verantwoordelijke (voor de gegevensverwerking) alsmede over alle nadere informatie voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover betrokkenen een behoorlijke en zorgvuldige verwerking te waarborgen (artikel 33 Wbp)."*

voldoende mogelijkheden biedt voor aanbieders van elektronische communicatiediensten en andere belanghebbenden om de belangen van gebruikers middels rechtsvorderingen tegen dergelijke inbreuken te beschermen. Het CBP adviseert derhalve om in het voorgestelde artikel 11.7 Telecommunicatiewet uitdrukkelijk de mogelijkheid te scheppen voor aanbieders van elektronische communicatiediensten en andere belanghebbenden om middels een zogenoemde 'class action' de belangen van hun klanten te behartigen. Door de mogelijkheid van een dergelijke 'class action' te creëren wordt zeker gesteld dat wordt voldaan aan de zorgplicht die in artikel 13, zesde lid, van de Bijzondere Privacyrichtlijn expliciet aan lidstaten is opgelegd.

7) Wetstechnische opmerkingen

- In het voorgestelde artikel 11.1 Telecommunicatiewet wordt in onderdeel j 'inbreuk in verband met persoonsgegevens' gedefinieerd. Aan deze definitie dient het begrip 'verlies' te worden toegevoegd, aangezien het begrip 'loss' deel uitmaakt van de definitie van 'personal data breach' (artikel 2 van de gewijzigde Bijzondere Privacyrichtlijn).

- In het voorgestelde artikel 11.3, tweede lid, onderdeel c, Telecommunicatiewet dient 'veiligheidsbeleid' te worden vervangen door 'het vaststellen en implementeren van een informatiebeveiligingsbeleid' conform artikel 4, eerst lid bis, van de gewijzigde Bijzondere Privacyrichtlijn.

- Het voorgestelde artikel 11.3b, zesde lid, Telecommunicatiewet stelt dat de aanbieder van een elektronische communicatiedienst een overzicht bijhoudt van alle inbreuken in verband met persoonsgegevens en dat dit overzicht in elk geval de feiten en de in het derde lid bedoelde gegevens bevat. Artikel 4, vierde lid, van de gewijzigde Bijzondere Privacyrichtlijn is echter breder geformuleerd en eist dat ook de gevolgen en de genomen herstelmaatregelen in het overzicht worden opgenomen.

- Artikel 11.3b, zevende lid, geeft aan dat bij of krachtens algemene maatregel van bestuur nadere regels kunnen worden gegeven met betrekking tot de in dit artikel bedoelde eisen met betrekking tot het verstrekken van informatie en de kennisgeving. Volgens de Memorie van Toelichting is deze delegatiebepaling opgenomen om de door de Europese Commissie te nemen uitvoeringsmaatregelen bij lagere wetgeving te kunnen implementeren. De wijze waarop artikel 11.3b nu is geformuleerd geeft echter ruimte om meer nadere regels te stellen dan die ter implementatie van de uitvoeringsmaatregelen van de Europese Commissie. Geadviseerd wordt om de delegatiebepaling stringenter te formuleren.

- In artikel 13bis van de Kaderrichtlijn wordt de term 'breach of security or loss of integrity' gehanteerd. In het voorgestelde artikel 11.a2 Telecommunicatiewet en in de Memorie van Toelichting wordt deze term vertaald als 'inbreuk op de veiligheid en verlies van integriteit'. Door deze terminologie wordt onvoldoende uiting gegeven aan het feit dat 'security' niet alleen 'veiligheid', maar ook de aspecten 'beschikbaarheid, integriteit en vertrouwelijkheid' in zich draagt. Geadviseerd wordt om in de Memorie van Toelichting het begrippenkader zoals gehanteerd in de Kaderrichtlijn en de Bijzondere Privacyrichtlijn nader uit te werken en toe te lichten.