VNO NCW

MKB Nederland

Mevrouw drs. M. Sonnema
Directeur Telecommarkt
Directoraat-Generaal Energie, Telecom en Markten
Ministerie van Economische Zaken
Bezuidenhoutseweg 30 (ALP C/372)
2594 AV DEN HAAG

Onderwerp
Implementatie New Regulatory Framework; artt. 11.3a en 11.3b Tw

Briefnummer
10/10.940/07/HOS/Man

Den Haag
28 mei 2010

Telefoonnummer
349 03 54
E-mail
hos@vno-ncw.nl

Geachte mevrouw Sonnema,

Namens de aangesloten ondernemingen en brancheorganisaties reageren VNO-NCW en MKB-Nederland graag op het concept wetsvoorstel tot wijziging van de Telecommunicatiewet teneinde aan de implementatie van het New Regulatory Framework te voldoen.
Wij danken u en uw collega's voor de inspanningen tot nu toe en voor de gelegenheid om in deze fase met onze opmerkingen en suggesties te kunnen komen. In hoofdlijnen komen deze op de volgende neer.

- Terwijl strikte implementatie voorgenomen is, ontstaan onnodige en voor het bedrijfsleven schadelijke nationale koppen. Wij dringen er op aan zodanig, en desnoods later te implementeren, dat geharmoniseerde regels ontstaan en Nederlandse bedrijven in Europa geen concurrentienadeel ondervinden.
- Ten aanzien van de zogenaamde cookie-bepaling pleiten wij voor het gebruik van een zwaar respectievelijk licht regime, waarbij de cookies in het lichte regime komen te vallen. Acceptatie van cookies kan dan geschieden via de browserinstellingen. Aanvullende publieksvoorlichting over de mogelijkheden lijkt ons zeer wenselijk.
- Ten aanzien van de meldplicht voor inbreuken op persoonsgegevens is het verwonderlijk dat de meldplicht rust op de Internet Service Provider (ISP). Wij pleiten ervoor dat eerst een discussie wordt gevoerd over wenselijkheid en uitvoerbaarheid van een brede meldplicht. De Telecomwet lijkt daarbij niet de geschikte plaats voor implementatie te zijn. Wij vrezen dat grote administratieve lasten voor het bedrijfsleven gepaard zullen gaan met deze maatregel.

Ter uitwerking van deze standpunten gaat deze brief hieronder eerst in op het voorgenomen artikel 11.3a Telecomwet (Tw), de zogenaamde cookie-bepaling. De laatste paragraaf gaat over het concept artikel 11.3b Tw, de meldplicht voor inbreuken op persoonsgegevens.

Schadelijke vs. geaccepteerde toegang tot eindapparatuur

- *Onderscheid een zwaar en licht regime.* Terwijl schadelijke en onschadelijke toegang tot de eind/randapparatuur van de gebruiker over één kam wordt geschoren, zou het wetsvoorstel ons inziens 1) een zwaar regime en 2) een licht regime moeten onderscheiden.
  Het eerste regime voor schadelijke toegang tot apparatuur en het tweede, lichte regime voor gewone toegang. In de eerste categorie valt *malware* (als spyware, etc.) die overduidelijk schadelijk is voor de persoonlijke levenssfeer van de gebruiker en ook voor het vertrouwen in het internet. In de tweede categorie moeten de cookies gaan vallen die op zich onschadelijk zijn, meer geaccepteerd zijn en een erkende bijdrage leveren aan de werking van het internet en surfen. Over het regime voor cookies gaat deze notitie hieronder verder.
- *Gebruiksvriendelijkheid neemt af met schade voor het bedrijfsleven.* Internet en internettoepassingen, informatieverschaffing en cookies zijn onlosmakelijk met elkaar verbonden. Het internet is van grote toegevoegde waarde voor de BV Nederland. Daarbij bestaat het web bij de gratie en cultuur van 'gratis' beschikbare informatie. Consumenten gaan daar ook van uit. Gratis is natuurlijk een betrekkelijk begrip, vanwege de bijdrage van adverteerders. Door de wijze waarop dit voorstel is ingericht wil ik u wijzen op een aantal negatieve effecten voor gebruikers en bedrijven.
  Ten eerste zullen websites niet alleen trager en gebruikersonvriendelijk worden, maar bezoekers worden ook met meer irrelevante advertenties (dus niet met minder advertenties) geconfronteerd. Deze maatregel, die bedoeld is om de consument te beschermen, levert hem dan meer nadelen op dan voordelen.
  Ten tweede vrezen wij een ernstige verschraling van het informatieaanbod doordat adverteerders mogelijk afhaken of uitwijken.
  Tot slot levert het bovenstaande (dus) schade op voor het betrokken bedrijfsleven en de economie. Dit terwijl het bedrijfsleven haar verantwoordelijkheid ten aanzien van gebruik van genoemde technieken (en informatieverstrekking) neemt[1].
- *Het Burgerlijk Wetboek als logischer plaats voor implementatie.* Voorts is het de vraag of een algemeen verbindende regeling als deze überhaupt in een sectorale wet dient te staan. Wij geven u derhalve in overweging om dit artikel in het Burgerlijk Wetboek op te nemen. Dit geldt overigens ook voor het al bestaande spamverbod van artikel 11.7 Tw. Naar verluidt heeft bijvoorbeeld Duitsland er voor gekozen om de spamregels onder de regeling voor oneerlijke handelspraktijken te brengen, wat ons een interessante optie lijkt.

[1] Ik verwijs naar de brief die u van BVA, DDMA, IAB, Thuiswinkel.org, PAN, PIBN, PMA en NUV ontvangt.

Ten aanzien van het art. 11.3a

- *Gewone toestemming verlenen.* Wij pleten ervoor bij het lichte regime de 'gewone' toestemming te implementeren. Dat lijkt ons goed mogelijk en is strikt genomen waar de Richtlijn om vraagt. Praktische realisatie kan via de browserinstellingen, maar ook door het feitelijke gedrag van de internetgebruiker, zoals het aanklikken van opties als "onthoudt mijn login gegevens" of het configureren van een website aan persoonlijke voorkeuren (zie bijvoorbeeld www.kpnvandaag.nl of www.igoogle.nl).

- *Strikte implementatie verlaten; nationale koppen tot gevolg.* Wij vragen ons af waarom de strikte implementatie van art. 5.3 van de Richtlijn hier verlaten is. In dat artikel wordt gesproken over normale 'toestemming' met verwijzing naar de algemene privacyrichtlijn (95/46/EG). Het wetsvoorstel spreekt in art. 11.3a lid 1 sub b over "ondubbelzinnige[2] toestemming". Hierbij hebben wij de volgende opmerkingen. Ten eerste leidt dit leidt nodeloos tot een onwerkbaar opt-in regime. Ten tweede is het ons inziens algemeen aanvaard dat bij verwijzing naar de algemene privacyrichtlijn de gewone toestemming uit art. 1 Wbp aan de orde is. Daar komt bij dat de relevante richtlijnoverweging (66) voorschrijft dat "de wijze waarop het recht van weigering wordt aangeboden zo gebruikersvriendelijk moet zijn". Daarvan is met een opt-in regime hoe dan ook geen sprake. Tot slot leidt de opt-in tot het verzamelen van persoonsgegevens, omdat de toestemming door de aanbieder moet worden geregistreerd. Dit staat haaks op de intenties van de Richtlijn.

- *Regeling niet techniek-neutraal.* Toestemming geven is technisch niet altijd mogelijk. Deze regeling is niet techniek-neutraal doordat geen rekening wordt gehouden met de ontwikkeling dat randapparatuur voortdurend kleiner wordt en daarmee een kleiner of soms helemaal geen user interface meer heeft. Het vragen van toestemming of het informeren van gebruikers via de user interface wordt dan bijzonder lastig of onmogelijk.

- *Informatie verstrekken.* In het licht van ons voorstel kan informatie worden verstrekt in de browserinstellingen of bij het installeren van de browser zelf.
  Wij erkennen het belang dat er groepen gebruikers zijn die de consequenties van hun toestemming niet goed of volledig kunnen overzien. Ouderen en kinderen zijn daar voorbeelden van. Aandacht voor deze steeds groter wordende groep gebruikers is belangrijk. Aan de roep om meer transparantie voor consumenten kan echter op een effectievere en voor het bedrijfsleven minder schadelijke manier tegemoet worden gekomen, dan via dit voorstel. Twee suggesties: Ten eerste kan de overheid via aanvullende publieksvoorlichting inspelen op de informatiebehoefte.

[2] Daarbij is 'ondubbelzinnig' een term die kennelijk in geen andere Nederlandse wet of regeling wordt gebruikt (zie TK 25892, nr.13, vraag 7).

Wij verwijzen daarom naar de bewustwordings- en vaardighedencampagnes die daar de mogelijkheid toe bieden. Ten tweede zijn er alternatieve wijzen van informatie verstrekken door bijvoorbeeld een cookie-zegel[3].

- *Wie plaatst de cookie?* Het wetsvoorstel spreekt van een verplichting dat "een ieder" die cookies plaatst daar eerst toestemming voor vraagt. Wij merken met nadruk op dat degene die de cookie plaatst, vaak niet de eigenaar is van de website. Eigenaars van websites hebben doorgaans zowel geen (enkele) controle over de cookies die via hun website worden geplaatst als over de oorsprong van de cookie.

- *ISP geen poortwachter.* Tijdens de consultatiebijeenkomst op uw departement werd namens uw ministerie aangegeven dat met artikel 11.3a Tw niet wordt beoogd 'poortwachter'-verplichtingen in het leven te roepen ten aanzien van Internet Service Providers (ISP's). Dat lijkt ons terecht, aangezien ISP's onmogelijk kunnen controleren of cookies door middel van verkregen toestemming zijn geplaatst. Wij verzoeken u dit in de memorie van toelichting op te nemen, zodat daarover geen misverstand kan ontstaan.

- *Wie moet toestemming verlenen*? De richtlijn spreekt over abonnee of gebruiker. De keuze in het wetsvoorstel voor de gebruiker zorgt voor lastige situaties, want hoe om te gaan met situaties als:
    - Bedrijfsomgeving; relatie werkgever-werknemer;
    - Handelingsonbevoegde minderjarigen die ook gebruik maken van het internet en websites als hyves en facebook bezoeken;
    - Computers die door meerdere gebruikers worden gedeeld, bijvoorbeeld in bibliotheken, hotels, congrescentra of op de werkvloer.

- *Level playing field in Europa, toepasselijk recht.* Om een level playing field in Europa te borgen en om het internet optimaal te laten functioneren zal de Nederlandse implementatie niet verder dienen te gaan dan de andere EU-landen. Nationale koppen, zo leert de ervaring, lijden tot grote nadelige economische gevolgen.
  Voor wat betreft het toepasselijk recht zal het "*country of origin*" principe moeten gelden. Daarmee wordt voorkomen dat websites aan het recht van meerdere lidstaten tegelijk moeten voldoen.

- *Cookies zijn geen persoonsgegevens.* Dat cookies geen persoonsgegevens zijn in de zin van de Wet bescherming persoonsgegevens (Wbp) dient te worden verhelderd in de memorie van toelichting. Cookies koppelen een namelijk uniek nummer aan een IP adres dat in veel gevallen dynamisch is en voortdurend wijzigt. Vaste IP adressen worden veelal door bedrijven gebruikt met meerdere terminals. Ook een cookie die wordt geplaatst op een vast IP adres kan dus niet leiden naar een specifieke terminal.

[3] Zie daarvoor de brief van BVA, DDMA cs.

Meldplicht voor inbreuk op persoonsgegevens

- *ISP's hebben geen inzicht in gegevens.* In het voorgenomen art. 11.3 b Tw wordt gekozen voor een beperkte meldplicht. Wij vinden het vreemd dat de ISP's verantwoordelijk gemaakt worden om inbreuken op persoonsgegevens te melden. De aanbieders van telecommunicatiediensten hebben (veelal) geen zicht op de inhoud van de data die over hun netwerk wordt getransporteerd. Voor de wijze waarop dit wetsvoorstel onuitvoerbaar wordt, verwijzen wij naar de brief van ICT-Office.

- *Brede meldplicht eerst onderzoeken.* De Tweede Kamer en het Europees Parlement zinnen op de introductie van een brede meldplicht. Het Ministerie van Justitie werkt dit initiatief momenteel uit. Bij een brede meldplicht, zullen andere sectoren betrokken raken dan alleen de telecomsector. Hierdoor rijst de vraag of implementatie in de Telecomwet dan logisch is, gezien het beperkte bereik van deze lex specialis. Ons voorstel is de implementatie van de meldplicht daarom aan te houden. Omdat tegelijkertijd elke onderneming zelf verantwoordelijk is voor het zorgvuldig beheer van data, vinden wij het belangrijk dat eerst een discussie gevoerd wordt over de noodzakelijkheid, wenselijkheid en uitvoerbaarheid van een brede meldplicht. Hierover bieden wij ons graag als gesprekspartner aan.

- *Rol ISP t.o.v. verschillende overheden.* De verhouding tot andere wet- en regelgeving is onvoldoende duidelijk. Kan dit voorstel een ISP verplichten om bijvoorbeeld een door de politie of inlichtingendienst geplaatste tap bij (een ander deel van) de overheid te melden?

- *De administratieve lasten baren ons grote zorgen.* Het probleem zit met name in melden aan betrokkene zelf. Die zal, zeker voor de ISP, lang niet eenvoudig traceerbaar zijn vanwege de herkomst of de vorm van de informatie. De Quickscan van EIM raamt de lasten op een wel heel zuinige 277 duizend euro. Dit is helemaal laag ingeschat indien persoonlijk per e-mail of - duurder nog - per brief moet worden geïnformeerd, waarbij valt te verwachten dat veel tijd, geld en energie moet worden gestoken in het achterhalen van de contactgegevens van de betrokkenen. Te zijner tijd zullen wij zeker de suggestie doen een doorberekening te laten plegen door ACTAL. Tot die tijd zijn wij voorstander van bijvoorbeeld een beperkte publicatieplicht op de eigen website van het bedrijf.

- *Toezichtrol onduidelijk belegd.* Maak een heldere keuze voor wat betreft het toezicht. OPTA wordt aangewezen als loket voor de melding, terwijl in de memorie van toelichting het College Berscherming Persoonsgegevens inzage krijgt in registers die ondernemingen moeten bijhouden. Deze diffuse toezichttaken dienen de rechtszekerheid niet en zal de inspectiedruk op ondernemingen verder doen toenemen.

– *Self-incrimination een probleem?* In hoeverre de meldplicht in feite door het bedrijf zelf aangeleverde bewijslast (*self-incrimination*) is, is een vraagstuk dat wij in overweging geven. Het is onwenselijk als zelf aangedragen bewijs later door een toezichthouder gebruikt kan worden tegen de meldende onderneming, bijvoorbeeld inzake een handhavingsinspanning wegens het niet naleven van de beveiligingseisen voor persoonsgegevens. Naar verluidt heeft Duitsland het gebruik van de informatie uit de meldplicht om die reden uitdrukkelijk uitgesloten van verder toezicht.

Vanzelfsprekend zijn wij bereid om deze punten nader toe te lichten.

Hoogachtend,

drs. C. Oudshoorn
Directeur Beleid