TEKST & COMMENTAAR TELECOMMUNICATIEWET E.A.
Zwenne 2009 *(T&C Telecomrecht e.a.)* inl. opm. aant. 1 t/m 5; art. 11.1 aant. 1 t/m 4, 6 t/m 8, 10; aant. bij art. 11.2; art. 11.3 aant. 1 t/m 4; art. 11.5, aant. 1 t/m 7; art. 11.7 aant. 1 t/m 5; aant. bij art. 11.8

Hoofdstuk 11 Telecommunicatiewet
Bescherming van persoonsgegevens en de persoonlijke levenssfeer

1 Algemeen. De kwaliteit van elektronische communicatienetwerken en -diensten wordt in sterke mate bepaald door de wijze waarop de vertrouwelijkheid van de communicatie is gewaarborgd. Allerlei technologische ontwikkelingen en marktontwikkelingen maken het mogelijk dat steeds meer verschillende soorten persoonsgegevens worden verwerkt. Daarmee brengen deze ontwikkelingen ook nieuwe bedreigingen met zich mee voor de persoonlijke levenssfeer van eindgebruikers en abonnees. Om een juiste omgang met persoonsgegevens alsmede een adequate bescherming van de persoonlijke levenssfeer te garanderen, moet de verwerking van deze gegevens op een adequate wijze worden genormeerd (MvT, Kamerstukken II 2002/03, 28 851, nr. 3, p. 46). Dit is gebeurd in hoofdstuk 11. De verschillende bepalingen zien op de technische faciliteiten die met name in digitale netwerken (zoals die waarbij gebruikt wordt gemaakt van ISDN, GSM, GPRS of UMTS-technologie) standaard kunnen worden aangeboden. Het betreft het specificeren van de nota, nummeridentificatie en de doorschakeling van oproepen, alsmede ongevraagde oproepen door middel van al dan niet geautomatiseerde oproepsystemen. Verder stelt het hoofdstuk regels in verband met het gebruik van locatiegegevens en verkeersgegevens ("call detail records", afgekort: cdr), het opnemen van persoonsgegevens in telefoongidsen en bestanden voor abonnee-informatiediensten, en het voorkomen van zogenoemde. telefoonterreur. *Richtlijn privacy en elektronische communicatie.* Het hoofdstuk implementeert de Richtlijn privacy en elektronische communicatie (bijlage A5), die de opvolger is van de Telecommunicatie Privacyrichtlijn (97/66/EG) welke richtlijn in de ontwerpfase ervan ook wel werd aangeduid als de ISDN-richtlijn. De bijzondere regeling die art. 5, derde lid, Richtlijn privacy en elektronische communicatie geeft voor het verkrijgen van toegang tot gegevens op randapparatuur van de eindgebruiker (o.a. door middel van "cookies", "spyware" en inbelprogramma's e.d.) is niet in hoofdstuk 11 van de wet geregeld, maar in art. 4.1 BUDE (bijlage B14).

2 Grondrechten. Op nationaal en internationaal niveau zijn regelingen vastgesteld die de wetgever verplichten om inbreuken op de persoonlijke levenssfeer bij wet te regelen. Het betreft met name de art. 10 en 13 Grondwet, alsmede art. 8 EVRM en 17 IVBPR, welke bepalingen respectievelijk betrekking hebben op bescherming van de persoonlijke levenssfeer en op het brief- en telecommunicatiegeheim (MvT, Kamerstukken II 1996/97, 25 533, nr. 3, p. 38-43). *Vertrouwelijke communicatie.* De parlementaire behandeling van de wet vond plaats tegen de achtergrond van de discussie over de grondwettelijke bescherming van vertrouwelijke communicatie (zie m.n. Kamerstukken II 1997/98, 25 531, nr. 16; Handelingen II 1997/98, p. 66-4929, 66-4941 en 67-5008). Vanuit het Ministerie van Binnenlandse Zaken werd het voorstel gedaan art. 13 Gw technologieonafhankelijk te herformuleren, zodat daaronder ook e-mailberichten en andere elektronische uitingsvormen zouden vallen. Uiteindelijk is dit wetsvoorstel (Kamerstukken II 1996/97-1998/99, 25 443, nrs. 1-40d) ingetrokken, omdat er onduidelijkheid bestond over het begrip vertrouwelijkheid. Om duidelijk te maken dat elektronische uitingsvormen onder dezelfde bescherming vallen als het grondwettelijke brief en telefoongeheim,

werd vervolgens bij amendement een nieuw artikel toegevoegd dat de wetgever de opdracht geeft om bij het vaststellen van uitvoeringsregelingen rekening te houden met de bescherming van het brief-, telefoon- en telegraafgeheim en het geheim van daarmee vergelijkbare communicatietechnieken. Dit heeft geresulteerd in art. 18.13 (Kamerstukken II 1997/98, 25 533, nr. 75; zie aant. bij art. 18.13).

3 Wet bescherming persoonsgegevens (Wbp). De specifieke regels in dit hoofdstuk gelden in aanvulling op en ter uitwerking van de Wbp. Deze privacywet is gebaseerd op de algemene Privacyrichtlijn (bijlage A10) en stelt regels voor de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens. Daarmee vormt de Wbp het algemeen kader waarbinnen de verwerking van persoonsgegevens (ook) binnen de sector elektronische communicatie moet plaats vinden. De bepalingen van hoofdstuk 11 hebben ten opzichte van de algemene Privacyrichtlijn en de uitwerking daarvan in de Wbp een aanvullende werking, waarbij op onderdelen sprake is van een nadere uitwerking van de meer algemene normen uit de Wbp. Voor de specifieke, in de sfeer van elektronische communicatie, voorkomende verwerkingen van persoonsgegevens worden daarop toegesneden (en in voorkomend geval uitputtende) normen gesteld. Verder strekt de reikwijdte van dit hoofdstuk zich in beginsel ook uit tot rechtspersonen, terwijl de Wbp alleen betrekking heeft op gegevens over natuurlijke personen. (MvT, Kamerstukken II 2003/04, 28 851, nr. 3, p. 45). De Wbp is in deze uitgave afzonderlijk opgenomen en van commentaar voorzien.

4 Handhaving en toezicht. *OPTA en College bescherming persoonsgegevens (Cbp).* Op grond van art. 15.1, derde lid, is OPTA belast met het toezicht op de naleving van hoofdstuk 11. Daarnaast is het Cbp op grond van de Wbp belast met het toezicht op de naleving van de Wbp in het algemeen, en waar het de verwerking van persoonsgegevens op grond van hoofdstuk 11 van de wet betreft, ook op die bepalingen. Waar de onderscheiden bevoegdheden van het Cbp en OPTA elkaar overlappen, is samenwerking tussen beide instanties geboden. De beide instanties hebben daaraan invulling gegeven in het Samenwerkingsprotocol CBP-OPTA (Stcrt. 2005, 133). Het daarin vastgelegde uitgangspunt is dat OPTA zich bij de uitoefening van zijn bevoegdheden richt op de gevallen waar het vooral gaat om de toepassing van bepalingen van de Tw, BUDE en RUDE, en het Cbp op gevallen waar het vooral gaat om toepassing van de Wbp. Deze samenwerking betekent in de praktijk ook dat de informatie die men in het kader van de toezichthoudende taak verkrijgt, waar dat noodzakelijk is met elkaar wordt gedeeld (MvT, Kamerstukken II 2002/03, 28 851, nr. 3, p. 61; NV, Kamerstukken II 2002/03, 28 851, nr. 7, p. 43 en 52-54). Zie art. 15.1, aant. 3. *Wetsvoorstel bewaarplicht telecommunicatiegegevens (31 145).* Bij dit wetsvoorstel wordt in art. 15.1, eerste lid, een nieuw onderdeel g toegevoegd op grond waarvan het gebruik van verkeersgegevens en locatiegegevens als geregeld in artikel 11.5, artikel 11.5a onderscheidenlijk artikel 11.13 onder het toezicht van de Minister van EZ komt te vallen (zie artt. 15.1, aant. 8). *Strafbaarstelling.* De overtreding van art. 11.7, derde lid, is strafbaar gesteld in de Wet op de economische delicten. Strafbaarstellingen ter bescherming van het belang van de vertrouwelijkheid van telecommunicatienetwerken en -diensten staan verder onder andere in de art. 139a-139e Sr. De bevoegdheden op grond waarvan politie en justitie inbreuk mogen maken op de vertrouwelijkheid van netwerken en diensten zijn geregeld in art. 126l-126na en 126s-126ua Sv. Voor veiligheids- en inlichtingendiensten zijn deze bevoegdheden geregeld in art. 28 Wiv 2002.

5 Herziening Europees Regelgevend Kader: meldingsplicht bij inbreuk op beveiliging. In het kader van de herziening van het Europees Regelgevend Kader (13 november 2007, COM(2007) 698 definitief) worden voorstellen gedaan tot wijziging van onderdelen van onder andere de verplichting voor aanbieders van elektronische communicatiediensten om hun abonnees en OPTA onverwijld in kennis te stellen van beveiligingsinbreuken, als daardoor persoonsgegevens zijn kwijtgeraakt of ten onrechte zijn vrijgegeven.

§ 11.1 Algemene bepalingen

[Definities]

Art. 11.1

In dit hoofdstuk en de daarop berustende bepalingen wordt verstaan onder:

a gebruiker: een natuurlijke persoon die gebruik maakt van een openbare elektronische communicatiedienst voor particuliere of zakelijke doeleinden zonder noodzakelijkerwijze op die dienst te zijn geabonneerd;

b verkeersgegevens: gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronisch communicatienetwerk of voor de facturering ervan;

c verwerking van verkeersgegevens: verwerking als bedoeld in artikel 1, onderdeel b, van de Wet bescherming persoonsgegevens, met dien verstande dat de desbetreffende handelingen mede betrekking hebben op verkeersgegevens van abonnees die geen natuurlijke personen zijn;

[..]

e communicatie: informatie die wordt uitgewisseld of overgebracht tussen een eindig aantal partijen door middel van een openbare elektronische communicatiedienst; dit omvat niet de informatie die via een omroepdienst over een elektronisch communicatienetwerk wordt overgebracht, behalve wanneer de informatie kan worden gerelateerd aan de identificeerbare abonnee of gebruiker die de informatie ontvangt;

f oproep: een door middel van een openbare telefoondienst tot stand gebrachte verbinding die zonder noemenswaardige vertraging communicatie tussen gebruikers of abonnees over en weer mogelijk maakt;

g toestemming van een gebruiker of abonnee: toestemming van een betrokkene als bedoeld in artikel 1, onder i, van de Wet bescherming persoonsgegevens, met dien verstande dat de toestemming mede betrekking kan hebben op gegevens van abonnees die geen natuurlijke personen zijn;

[..]

i elektronisch bericht: tekst-, spraak-, geluids- of beeldbericht dat over een openbaar elektronisch communicatienetwerk wordt verzonden en in het netwerk of in de randapparatuur van de ontvanger kan worden opgeslagen tot het door de ontvanger wordt opgehaald.

1 Algemeen. Dit artikel geeft in aanvulling op artikel 1.1 begripsomschrijvingen. Deze begripsomschrijvingen worden alleen van toepassing verklaard op dit hoofdstuk en daarop berustende bepalingen.

2 Gebruiker (onder a). Onder het begrip "gebruiker" wordt verstaan een natuurlijke persoon die gebruik maakt van een openbare elektronische communicatiedienst voor particuliere of zakelijke doeleinden zonder noodzakelijkerwijze op die dienst te zijn geabonneerd. Anders dan de abonnee staat de gebruiker dus niet noodzakelijk in een contractuele verhouding tot de aanbieder van de dienst. De definitie is een rechtstreekse omzetting van art. 2, onder a, Richtlijn privacy en elektronische communicatie (bijlage A5). *Gebruikersbegrip in andere hoofdstukken*. Het begrip heeft in dit hoofdstuk van de wet een afzonderlijke, op dit hoofdstuk toegesneden betekenis doordat het uitsluitend betrekking heeft op natuurlijke personen. Het wijkt daarmee af van het gebruikersbegrip van art. 1.1, onder n, dat ziet op al dan niet rechtspersoonlijkheid bezittende personen die gebruik maken van of verzoeken om een openbare telecommunicatiedienst (zie art. 1.1, aant. 14).

3 Verkeersgegevens (onder b). Verkeersgegevens zijn de gegevens die worden verwerkt voor het overbrengen van communicatie (in de zin van art. 11.1, onder d) over een elektronisch communicatienetwerk of voor de facturering ervan. Deze definitie is een rechtstreekse omzetting van art. 2, onder b, Richtlijn privacy en elektronische communicatie (bijlage A5). Waar het gaat om spraaktelefonie heeft het begrip onder andere betrekking op het oproepende en opgeroepen nummer, begin en einde van de oproep, duur van de oproep en (waar het mobiele telefonie betreft) ook op de locatiegegevens (zie art. 11.1, aant. 5). Waar het gaat om internetverkeer heeft het begrip betrekking op gegevens als de identiteit van de aansluiting, gebruikersnaam ("user id"), IP-adressen, e-mailadres, het gebruikte protocol, begin- en eindtijd sessie, type dienst, volume (aantal kilobytes of megabytes) etc. Abonneegegevens, zoals naam, adres, woonplaats, gegevens betreffende de wijze van betaling e.d. zijn wel nodig voor de facturering, maar vallen niet onder het begrip verkeersgegevens (MvT, Kamerstukken II 2003/04, 28 851, nr. 3, p. 151). *Relatie tot begrip gegevens in art. 13.2a*. In art. 13.2a wordt de gedefinieerd welke gegevens moeten worden bewaard ten behoeve van politie, justitie en inlichtingendiensten. Deze te bewaren gegevens betreffen de verkeers- en locatiegegevens, bedoeld in artikel 11.1, onder b en onder d, alsmede de daarmee verband houdende gegevens die nodig zijn om de abonnee of gebruiker te identificeren. In de bijlage bij de wet (opgenomen na art. 13.10) is voor mobiele en vaste telefonie, alsmede internetgebruik, gespecificeerd welke verkeers-, locatie en andere gegevens moeten worden bewaard op grond van artikel 13.2a. *Relatie tot begrip persoonsgegevens in Wbp*. Ten behoeve van bijvoorbeeld de facturering moeten verkeersgegevens worden gerelateerd aan abonneegegevens. Voorzover het daarbij gaat om geïdentificeerde of identificeerbare natuurlijke personen vallen deze gegevens onder het begrip persoonsgegevens, zodat de Wbp van toepassing is op de (geautomatiseerde) verwerking daarvan (zie art. 1, onder a en b, Wbp, aant. 2 en 3, alsmede art. 2, eerste lid, Wbp, aant. 1). Als het gaat om prepaid abonnementen zal daarvan in veel gevallen geen sprake zijn omdat er geen identificerende gegevens betreffende de abonnee beschikbaar zijn (MvT, Kamerstukken II 2002/03, 28 851, nr. 3, p. 151).

4 Verwerking verkeersgegevens (onder c). Onder het begrip "verwerking van verkeersgegevens" wordt verstaan de verwerking als bedoeld in art. 1, onder b, Wbp, met

dien verstande dat de desbetreffende handelingen mede betrekking hebben op verkeersgegevens van abonnees die geen natuurlijke personen zijn. De definitie is opgenomen met het oog op de afstemming van de regeling van art. 11.5 voor de verwerking van verkeersgegevens en de regeling van de Wbp voor de verwerking van persoonsgegevens. Onder "verwerking" verstaat art. 1, onder b, Wbp elke handeling of geheel van handelingen met betrekking tot persoonsgegevens, zijnde gegevens over geïdentificeerde of identificeerbare natuurlijke personen (zie art. 1, aant. 2b Wbp). Om de aansluiting met de Wbp zoveel mogelijk te behouden wordt voor de toepassing van de wet de reikwijdte van het begrip "verwerking" zodanig opgerekt dat daaronder ook de verkeersgegevens worden begrepen die niet worden aangemerkt als persoonsgegevens in de zin van art. 1, onder a, Wbp. Dat zijn dus de verkeersgegevens betreffende abonnees die géén natuurlijke personen zijn (MvT, Kamerstukken II 1998/99, 26 410, nr. 3, p. 53-54).

6 Communicatie (onder e). Het begrip "communicatie" wordt omschreven als de informatie die wordt uitgewisseld of overgebracht tussen een eindig aantal partijen door middel van een openbare elektronische communicatiedienst. Het begrip omvat niet de informatie die via een omroepdienst over een elektronisch communicatienetwerk wordt overgebracht, behalve wanneer de informatie kan worden gerelateerd aan de identificeerbare abonnee of gebruiker die de informatie ontvangt. Het begrip ziet derhalve op datgene wat wordt uitgewisseld dan wel wordt overgebracht en niet op de gegevens die worden verwerkt om die uitwisseling of overbrenging mogelijk te maken, de zogeheten verkeersgegevens die zijn gedefinieerd in art. 11.1, onder b (zie aant. 3). De definitie van het begrip is een rechtstreekse omzetting van art. 2, onder d, Richtlijn privacy en elektronische communicatie (bijlage A5) en is opgenomen met het oog op de regeling van verkeersgegevens in art. 11.5 (zie resp. aant. 3 en art. 11.5 aant. 2) en de regeling met betrekking tot ongevraagde communicatie in art. 11.7 (zie art. 11.7 aant. 1)

7 Oproep (onder f). Onder het begrip "oproep" wordt verstaan een door middel van een openbare telefoondienst (in de zin van art. 1.1, onder x) tot stand gebrachte verbinding die zonder noemenswaardige vertraging ("in real time") communicatie tussen gebruikers of abonnees over en weer mogelijk maakt. De definitie van het begrip sluit nauw aan bij de definitie van art. 2, onder e, Richtlijn privacy en elektronische communicatie (bijlage A5) en is opgenomen met het oog op de regeling betreffende ongevraagde communicatie in art. 11.7, nummeridentificatie in art. 11.9 en kwaadwillige oproepen in art. 11.11.

8 Toestemming van een gebruiker of abonnee (onder g). Onder "toestemming van een gebruiker of abonnee" wordt verstaan de toestemming van een betrokkene (als bedoeld in art. 1, onder i, Wbp), met dien verstande dat de toestemming mede betrekking kan hebben op gegevens van abonnees die geen natuurlijke personen zijn. Deze definitie sluit aan bij art. 2, onder f, Richtlijn privacy en elektronische communicatie (bijlage A5), dat weer verwijst naar de algemene privacyrichtlijn (bijlage A10). In art. 2, onder h, van laatstgenoemde richtlijn en art. 1, onder i, Wbp wordt het begrip "toestemming van een betrokkene" omschreven als elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem of haar betreffende persoonsgegevens worden verwerkt. Omdat de "betrokkene" alleen betrekking heeft op natuurlijke personen en de reikwijdte van verschillende bepalingen in hoofdstuk 11 van de wet zich ook uitstrekt tot rechtspersonen, wordt in het artikel bepaald dat de toestemming mede betrek-

king kan hebben op gegevens van abonnees die geen natuurlijke personen zijn (MvT, Kamerstukken II 2002/03, 28 851, nr. 3, p. 152-153; overw. 17 Richtlijn privacy en elektronische communicatie). *Vereisten aan toestemming.* Om van toestemming in de zin van het artikel te kunnen spreken, moet zijn voldaan aan een aantal criteria. In de eerste plaatst moet er sprake zijn van een vrije wilsuiting. Art. 3:33 en 3:35 BW (over de wilsverklaring en het gerechtvaardigd vertrouwen daarop) zijn van overeenkomstige toepassing. In de tweede plaats moet de wilsuiting betrekking hebben op een bepaalde gegevensverwerking of een beperkte categorie van gegevensverwerkingen. Het moet duidelijk zijn welke verwerking, van welke (soort) gegevens voor welke doeleinden zal plaatsvinden (gerichte toestemming). In de derde plaats moet de gebruiker of abonnee zodanig zijn geïnformeerd dat hij begrijpt waarvoor hij toestemming geeft ("informed consent"). Toestemming kan derhalve worden gegeven op elke wijze die de gebruiker of abonnee in staat stelt vrijelijk een specifieke en geïnformeerde indicatie te geven omtrent zijn wensen, bijvoorbeeld door bij een bezoek aan een website een vakje aan te vinken (overw. 17 Richtlijn privacy en elektronische communicatie). Gelet op het voorgaande wordt de enkele verwijzing naar een bepaling in de algemene voorwaarden, waarin toestemming voor de een of andere verwerking wordt geformuleerd, niet zonder meer aangemerkt als toestemming in de zin van het artikel (MvT, Kamerstukken II 2002/03, 28 851, nr. 3, p. 152-153; zie ook MvT, Kamerstukken II 1997/98, 25 892, nr. 3, p. 65-66). Zie art. 1, onder i, Wbp, aant. 10. *Toestemming minderjarigen.* Als de abonnee of gebruiker minderjarig is en de leeftijd van zestien jaren nog niet heeft bereikt, is in plaats van zijn of haar toestemming die van de wettelijk vertegenwoordiger vereist. Hetzelfde geldt ten aanzien van onder curatele gestelden of als er ten behoeve van de abonnee of gebruiker een mentorschap is ingesteld. (zie art. 5 Wbp, aant. 1).

10 Elektronisch bericht (onder i). Het begrip "elektronisch bericht" wordt gedefinieerd als het tekst-, spraak-, geluids- of beeldbericht dat over een openbaar elektronisch communicatienetwerk wordt verzonden en in het netwerk of in de randapparatuur van de ontvanger kan worden opgeslagen tot het door de ontvanger wordt opgehaald. De definitie sluit nauw aan bij art. 2, onder h, Richtlijn privacy en elektronische communicatie (bijlage A5), waarin gebruik wordt gemaakt van de term "e-mail". Omdat de in de richtlijn gegeven begripsomschrijving ruimer is dan dat wat in zijn algemeenheid onder "e-mail" of elektronische post wordt verstaan, is bij de omzetting van dit onderdeel van de richtlijn gekozen voor het bredere begrip "elektronisch bericht". De begripsomschrijving maakt duidelijk dat het begrip ook betrekking heeft op sms- en mms-berichten, alsmede op voice-mailberichten (overw. 40 Richtlijn privacy en elektronische communicatie en MvT, Kamerstukken II 2002/03, 28 851, nr. 3, p. 46, 48 en 153). Het begrip is opgenomen met het oog op de regeling voor ongevraagde communicatie van art. 11.7 (zie art. 11.7, aant. 2).

[Wet bescherming persoonsgegevens]

Art. 11.2

Onverminderd de Wet bescherming persoonsgegevens en het overigens bij of krachtens deze wet bepaalde dragen de aanbieder van een openbaar elektronisch communicatienetwerk en de aanbieder van een openbare elektronische communicatiedienst zorg voor de bescherming van persoonsgegevens en de bescher-

ming van de persoonlijke levenssfeer van abonnees en gebruikers van zijn netwerk, onderscheidenlijk zijn dienst.

Betekenis. Het artikel bevat de algemene zorgplicht van de aanbieders van openbaar telecommunicatienetwerken en -diensten ten behoeve van abonnees en gebruikers. Het geldt als vangnetbepaling (NV II, Kamerstukken II 1997/98, 25 533, nr. 5, p. 120). Wet bescherming persoonsgegevens (Wbp). Het artikel stelt buiten twijfel dat de rechten en verplichtingen van dit hoofdstuk gelden in aanvulling op die van de Wbp. Aanbieders van diensten en -netwerken hebben dan ook niet alleen te maken met OPTA maar ook met het College bescherming persoonsgegevens (Cbp) dat toeziet op de naleving van de Wbp (NV II, Kamerstukken II 1997/98, 25 533, nr. 5, p. 120). *Rechtspersonen.* Onder het begrip "abonnee" worden ook rechtspersonen begrepen (zie art. 11.1, aant. 2 en 8). Dit betekent dat de zorgverplichting van dit artikel ook betrekking kan hebben op gegevens over rechtspersonen.

[Beveiligingsmaatregelen]

Art. 11.3

1 De in artikel 11.2 bedoelde aanbieders treffen in het belang van de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers passende technische en organisatorische maatregelen ten behoeve van de veiligheid en beveiliging van de door hen aangeboden netwerken en diensten. De maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau dat in verhouding staat tot het desbetreffende risico.

2 De in artikel 11.2 bedoelde aanbieders dragen er zorg voor dat de abonnees worden geïnformeerd over:

a bijzondere risico's voor de doorbreking van de veiligheid of de beveiliging van het aangeboden netwerk of de aangeboden dienst;

b de eventuele middelen waarmee de onder a bedoelde risico's kunnen worden tegengegaan, voor zover het andere maatregelen betreft dan die welke de aanbieder op grond van het eerste lid gehouden is te treffen, alsmede een indicatie van de verwachte kosten.

1 Algemeen. Het artikel implementeert art. 4 Richtlijn privacy en elektronische communicatie (bijlage A5). Anders dan de richtlijn adresseert het artikel echter niet alleen de aanbieder van elektronische communicatiediensten, maar ook de aanbieder van elektronische communicatienetwerken. Dit is gedaan omdat de dienstenaanbieder voor de beveiliging afhankelijk is van de netwerkaanbieder (MvT, Kamerstukken II 1996/97, 25 533, nr. 3, p. 119).

2 Verplichtingen met betrekking tot veiligheid en beveiliging (lid 1).

De netwerk- en dienstenaanbieders dienen rekening te houden met de stand van de techniek en de kosten van de tenuitvoerlegging. De aanbieders worden geacht de veiligheidsrisico's af te wegen tegen het beveiligingsniveau en hebben daarmee de nodige ruimte om ook te concurreren op beveiligingsniveau (MvT, Kamerstukken II 1996/97, 25 533, nr. 3, p. 119). Art. 18.8 biedt de minister een grondslag om regels te stellen met

betrekking tot veiligheid bescherming van openbare telecommunicatienetwerken en -diensten (zie aant. bij art. 18.8). *Door de minister te stellen regels (art. 18.8).* De Minister van EZ kan op grond van art. 18.8 regels stellen met betrekking tot de veiligheid en de beveiliging van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten regels stellen. Deze regels bevatten technische en organisatorische eisen die aan deze aanbieders van kunnen worden gesteld (zie aant. bij art. 18.8). *Zelfregulering.* OPTA is bevoegd toe te zien op de naleving van de in het artikel vastgelegde zorgplicht. Om deze bevoegdheid nader in te vullen heeft OPTA op 17 augustus 2007 een consultatiedocument gepubliceerd met voorgenomen beleidsregels, de zogenoemde basismaatregelen zorgplicht internetveiligheid (www.opta.nl). De uitkomst van deze consultatie was dat hij vooralsnog geen beleidsregels vaststelde, maar marktpartijen in de gelegenheid stelde om door middel van zelfregulering te komen met een 'robuust systeem' ter verbetering van veiligheid van consumenten op internet. *Art. 13 Wbp.* Art. 13 Wbp bevat zorgplicht met betrekking tot de beveiliging van persoonsgegevens. Op grond daarvan is degene die verantwoordelijk is voor de verwerking van deze gegevens gehouden passende technische en organisatorische maatregelen ten uitvoer te leggen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen dienen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, te leiden tot een passend beveiligingsniveau (art. 13 Wbp, aant. 2).

3 Informatieplicht (lid 2) De informatieplicht ziet op de bijzondere risico's die er bestaan voor de doorbreking van de veiligheid en de beveiliging van het aangeboden netwerk of de aangeboden dienst en voorts op de eventuele middelen waarmee de bedoelde bijzondere risico's en de kosten die daarmee gemoeid zijn kunnen worden uitgesloten of verkleind. a) Bijzondere risico's (onder a). De netwerk- en dienstenaanbieders zijn niet verplicht de abonnees te informeren over elk beveiligingsrisico maar alleen over bijzondere risico's en dan met name die risico's die een bijzondere band hebben met de aard van het desbetreffende netwerk of de desbetreffende dienst. De zorgverplichting strekt tot het informeren van de abonnees en gaat niet zo ver dat het afdekken van de risico's voor rekening komt van de aanbieders. Het treffen van extra voorzieningen tegen de risico's komt voor rekening van de abonnee (MvT, Kamerstukken II 1996/97, 25 533, nr. 3, p. 119). b) Beveiligingsmaatregelen (onder b). De informatieverplichting betreft verder de maatregelen die met betrekking tot bijzondere beveiligingsrisico's zouden kunnen worden genomen. Daarbij gaat het, omdat het moet gaan om andere maatregelen dan die welke de aanbieder op grond van het eerste lid moet treffen, ook om de eventuele maatregelen die de abonnee zelf zou kunnen treffen en een indicatie van de verwachte kosten. De middelen waarover het hier in het bijzonder gaat, betreffen onder andere middelen om de inhoud van berichten ("communicatie" in de zin van art. 11.1, onder e) te versleutelen en middelen om aanvallen van derden op de eigen computer tijdens het afnemen van een elektronische communicatiedienst af te slaan ("firewalls"). De aanbieder kan hier volstaan met het aangeven van enkele van die middelen en een indicatie van de verwachte kosten daarvan (MvT, Kamerstukken II 2002/03, 28 851, nr. 3. p. 153-154).

4. Herziening Europees Regelgevend Kader: meldingsplicht bij inbreuk op beveiliging. In de het kader van de herziening van het Europees Regelgevend Kader wordt de Richtlijn privacy en elektronische communicatie (bijlage A5) op onderdelen

gewijzigd. Als gevolg daarvan wordt in de richtlijn aan art. 4 een nieuw derde en vierde lid toegevoegd. Daarin wordt verlangd dat in de wet een meldplicht wordt opgenomen voor aanbieders van openbare elektronische communicatiediensten in geval van beveiligingsinbreuken. Als er als gevolg van zo een inbreuk persoonsgegevens verloren zijn gegaan of ten onrechte zijn vrijgegeven moeten deze aanbieders de betrokken abonnees en OPTA daarvan onverwijld in kennis stellen. In de kennisgeving aan de abonnee wordt minimaal de aard van de inbreuk omschreven en worden maatregelen voorgesteld om de eventuele negatieve effecten daarvan te verlichten. De kennisgeving aan OPTA bevat bovendien een omschrijving van de gevolgen van de inbreuk en van de door de aanbieder getroffen maatregelen om de inbreuk aan te pakken.

[Verkeers- en rekeninggegevens]

Art. 11.5

1 De aanbieder van een openbaar elektronisch communicatienetwerk en de aanbieder van een openbare elektronische communicatiedienst verwijderen dan wel anonimiseren de door hen verwerkte en opgeslagen verkeersgegevens met betrekking tot abonnees of gebruikers, zodra deze verkeersgegevens niet langer nodig zijn ten behoeve van de overbrenging van communicatie, onverminderd het tweede, derde en vijfde lid.

2 De aanbieder mag verkeersgegevens verwerken die noodzakelijk zijn voor facturering, waaronder het opstellen van een factuur voor een abonnee of voor degene die zich tegenover de aanbieder rechtens verbonden heeft die factuur te voldoen, dan wel ten behoeve van een betaling van verleende toegang. De verkeersgegevens mogen worden verwerkt tot het einde van de wettelijke termijn waarbinnen de factuur in rechte kan worden betwist of de betaling in rechte kan worden afgedwongen.

3 De aanbieder van elektronische communicatiediensten mag voorts de in het eerste lid bedoelde verkeersgegevens verwerken, voor zover en voor zolang dat noodzakelijk is voor:

a marktonderzoek of verkoopactiviteiten met betrekking tot elektronische communicatiediensten, of

b de levering van diensten met toegevoegde waarde,

mits de abonnee of de gebruiker waarop de verkeersgegevens betrekking hebben daarvoor zijn toestemming heeft gegeven. De abonnee of gebruiker kan de gegeven toestemming voor de verwerking van verkeersgegevens te allen tijde intrekken.

4 De aanbieder stelt de abonnee of gebruiker in kennis van de soorten verkeersgegevens die worden verwerkt voor de in het tweede en derde lid bedoelde doeleinden alsmede omtrent de duur van de verwerking. Voor zover het de verwerking van verkeersgegevens ten behoeve van de doeleinden, bedoeld in het derde lid betreft, wordt de desbetreffende informatie verstrekt voorafgaand aan het verkrijgen van de in dat lid bedoelde toestemming van de abonnee of gebruiker.

5 De verwerking van verkeersgegevens in overeenstemming met het eerste tot en met vierde lid mag alleen geschieden door personen die werkzaam zijn onder het gezag van de aanbieder voor facturering, verkeersbeheer, behandeling van verzoeken om inlichtingen van klanten, opsporing van fraude alsmede

marktonderzoek of verkoopactiviteiten met betrekking tot elektronische communicatiediensten of de levering van diensten met toegevoegde waarde en moet beperkt blijven tot hetgeen noodzakelijk is om die activiteiten te kunnen uitvoeren.
6 De aanbieder mag de verkeersgegevens verstrekken aan personen en instanties die zijn belast met de berechting van enig geschil dan wel de beslissing van een geschil als bedoeld in de artikelen 12.1, 12.2 voor zover van toepassing, of 12.9.

1 Algemeen. Het artikel implementeert art. 6 Richtlijn privacy en elektronische communicatie (bijlage A5) en geeft regels voor de verwerking van verkeersgegevens door aanbieders van openbare elektronische communicatienetwerken of -diensten. Het begrip verkeersgegevens is gedefinieerd in art. 11.1, onder b (zie art. 11.1, aant. 3). Zie voor een analyse van technische en juridische aspecten betreffende verkeersgegevens: Asscher & Ekker (red.) Verkeersgegevens. Een juridische en technische inventarisatie, Otto Cramwinckel 2003. *Relatie tot Wbp.* Het artikel geeft invulling aan enkele in de Wbp gestelde vereisten, zoals met name het vereiste van art. 9 Wbp dat persoonsgegevens die voor een bepaald doel zijn verzameld niet mogen worden verwerkt voor een ander doel dat daarmee onverenigbaar is, alsmede het vereiste van art. 10 Wbp dat persoonsgegevens niet langer mogen worden bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren, dan nodig is voor het doel waarvoor ze zijn verkregen (zie resp. art. 9 Wbp, aant. 1-5 en art. 10 Wbp, aant. 1-3). Zie voor de verhouding tussen verkeersgegevens en persoonsgegevens art. 11.1, aant. 3.

2 Hoofdregel: verkeersgegevens verwijderen of anonimiseren (lid 1). Als hoofdregel geldt dat alle door aanbieders van openbare elektronische communicatienetwerken en -diensten verwerkte en opgeslagen verkeersgegevens met betrekking tot abonnees en gebruikers worden verwijderd dan wel geanonimiseerd, zodra deze gegevens niet langer nodig zijn ten behoeve van (het doel van) de overbrenging van communicatie. Daarbij wordt onder anonimiseren verstaan dat de betreffende gegevens volledig en op onomkeerbare wijze worden ontdaan van hun persoonsidentificerende kenmerken (MvT, Kamerstukken II 2002/03, 28 851, nr. 3, p. 154). Het gaat erom dat de gegevens zodanig worden bewerkt dat deze redelijkerwijs niet meer zijn te herleiden tot individuele natuurlijke personen of, waar het gaat om abonnees, rechtspersonen. Er kan niet altijd worden volstaan met het verwijderen van naamgegevens. Het kan nodig zijn dat er andere maatregelen worden getroffen om daadwerkelijke herleiding van de gegevens tot individuele (rechts)personen te voorkomen (MvT, Kamerstukken II 1997/98, 25 892, nr. 3, p. 48). *Moment van verwijdering of anonimisering.* De verkeersgegevens moeten als hoofdregel worden verwijderd op het moment dat ze niet meer nodig zijn voor de overbrenging van de communicatie. Voor spraaktelefoniediensten betekent dit dat de gegevens, behoudens de in het tweede en derde lid opgenomen uitzonderingen, moeten worden verwijderd of geanonimiseerd zodra één van de gebruikers het gesprek heeft beëindigd. Voor internetverkeer is dit afhankelijk van de soort activiteit die wordt verricht. Als het gaat om elektronische post zullen de verkeersgegevens moeten worden verwijderd of geanonimiseerd zodra de gebruiker zijn of haar elektronische post heeft gedownload en deze niet meer wordt bewaard op de server van de dienstverlener (overw. 28 Richtlijn privacy en elek-

tronische communicatie (bijlage A5); MvT, Kamerstukken II 2002/03, 28 851, nr. 3, p. 154-155).

3 Uitzonderingen op hoofdregel (leden 2 en 3). Het gebruiken van niet-geanonimiseerde verkeersgegevens is, behalve voor het gebruik ten behoeve van de levering van de elektronische communicatiediensten, toegestaan voor factureringsdoeleinden in ruime zin. Verder mogen deze gegevens onder nadere voorwaarden worden gebruikt voor marktonderzoek of verkoopactiviteiten met betrekking tot elektronische communicatiediensten of de levering van diensten met toegevoegde waarde zoals gedefinieerd in art. 11.1, onder h (zie art. 11.1, aant. 9). **a) Facturering (lid 2).** Verkeersgegevens mogen (uiteraard) worden verwerkt ten behoeve van de facturering van de geleverde elektronische communicatiedienst. Dit verwerkingsdoel wordt ruim opgevat. Onder de verwerking ten behoeve van de facturering wordt niet alleen het opstellen van een factuur verstaan, maar ook bijvoorbeeld het registreren van het beltegoed van prepaid-klanten (NvW, Kamerstukken II 2002/03, 28 851, nr. 13, p. 20) alsmede de betaling van verleende toegang in de zin van art. 1.1, onder l, zoals interconnectiebetalingen (overw. 26 Richtlijn privacy en elektronische communicatie (bijlage A5); MvT, Kamerstukken II 2002/03, 28 851, nr. 3, p. 154-155). Verder blijkt uit het vijfde lid dat onder dit verwerkingsdoel ook verkeersbeheer, inlichtingenverstrekking aan klanten en fraudebestrijding moet worden begrepen (overw. 28-19 Richtlijn privacy en elektronische communicatie; MvT, Kamerstukken II 2002/03, 28 851, nr.3, p. 156). *Noodzakelijkheid.* De niet-geanonimiseerde verkeersgegevens mogen worden verwerkt zolang de verwerking voor de genoemde doeleinden noodzakelijk is. Dit noodzakelijkheidscriterium wordt nader ingevuld doordat is bepaald dat de verwerking is toegestaan tot het einde van de wettelijke termijn waarbinnen de factuur in rechte kan worden betwist of de betaling in rechte kan worden afgedwongen. In veel gevallen zal dat op grond van art. 3:307 e.v. BW neerkomen op een termijn van ten hoogste 5 jaar. Een en ander betekent echter niet dat in alle gevallen – ongeacht of er sprake is van wel of niet betaling of wel of niet betwisting van de factuur – de verkeersgegevens tot het einde van die termijn mogen worden bewaard. In de gevallen dat de factuur is betaald en er voor het overige daaromtrent geen geschillen ontstaan, is het niet nodig de desbetreffende verkeersgegevens langer voor deze doeleinden te bewaren. In die gevallen moeten de gegevens dan ook worden verwijderd of geanonimiseerd. (MvT, Kamerstukken II 2002/03, 28 851, nr. 3, p. 155). **b) Marktonderzoek en verkoopactiviteiten met betrekking tot elektronische communicatiediensten (lid 3 onder a).** Verwerking van niet-geanonimiseerde verkeersgegevens ten behoeve van marktonderzoek en de verkoop van elektronische communicatiediensten is toegestaan als de abonnee of de gebruiker waarop de gegevens betrekking hebben daarvoor toestemming heeft gegeven. Het begrip toestemming is gedefinieerd in art. 11.1, onder g, en sluit aan bij de definitie van art. 1, onder i, Wbp (zie art. 11.1, aant. 8). Het moet gaan om een vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt (zie art. 11.1, aant. 8, alsmede art. 1, onder i, Wbp, aant. 10). De toestemming kan te allen tijde worden ingetrokken. Dit is, voorzover het persoonsgegevens betreft, ook bepaald in art. 5, tweede lid, Wbp (art. 5 Wbp, aant. 2). *Niet per se eigen diensten.* Er is geen sprake meer van het in eerdere wetgeving opgenomen vereiste dat het marktonderzoek en verkoopactiviteiten betrekken moeten hebben op eigen diensten. Wél geldt het in het vijfde lid neergelegde vereiste dat de gegevens alleen mogen worden verwerkt door personen onder het gezag van aanbieder. Verwerking door derden ten behoeve van de leve-

ring van deze diensten is derhalve niet toegestaan (zie art. 11.5, aant. 5). **c) Levering toegevoegde waarde diensten (lid 3, onder b).** Verkeersgegevens mogen ook worden verwerkt voor de levering van diensten met toegevoegde waarde (in de zin van art. 11.1, onder h) ofwel diensten die de verwerking vereist van verkeersgegevens of locatiegegevens en die verder gaat dan hetgeen noodzakelijk is voor de overbrenging van de communicatie of de facturering daarvan (zie art. 11.1, aant. 9). Evenals bij de verwerking van verkeersgegevens ten behoeve van marktonderzoek en verkoopactiviteiten (lid 3, onder a) moet de abonnee of gebruiker waarop de gegevens betrekking hebben daarvoor toestemming (in de zin van art. 11.1, onder g) hebben gegeven. De verwerking van verkeersgegevens voor dit doel mag plaatsvinden zowel voor de levering van eigen diensten als voor de levering van diensten van derden. Echter evenals bij het marktonderzoek en de verkoopactiviteiten genoemd in het tweede lid, onder a, mogen de gegevens alleen worden verwerkt door personen onder het gezag van aanbieder (zie art. 11.5, aant. 5).

4 Informatieplicht aanbieder (lid 4). Voor de verwerking van verkeersgegevens ten behoeve van het overbrengen van de communicatie en de facturering (resp. lid 1 en lid 2) is geen toestemming van de desbetreffende abonnee of gebruikers vereist. Wel moet de aanbieder de abonnee of gebruikers waar de gegevens betrekking op hebben in kennis stellen van de soorten verkeersgegevens die worden verwerkt voor deze doeleinden alsmede de duur van de verwerking. Voorzover het gaat om verwerkingen ten behoeve van marktonderzoek of verkoopactiviteiten en de levering van toegevoegde waardediensten, waarvoor toestemming van de betrokken abonnee of gebruiker wél is vereist (lid 3, onder a en b) moet deze informatie worden verstrekt voordat de toestemming wordt gevraagd en verkregen (overw. 26 Richtlijn privacy en elektronische communicatie (bijlage A5); MvT, Kamerstukken II 2002/03, 28 851, nr. 3, p. 155). De abonnee of gebruiker moet immers begrijpen waarvoor hij toestemming geeft ("informed consent", zie art.11.1, aant. 8).

5 Verwerking alleen door personen werkzaam onder gezag aanbieder (lid 5). *Werkzaam onder gezag van de aanbieder*. De verwerking van de verkeersgegevens mag uitsluitend geschieden door personen die werkzaam zijn onder het gezag van de aanbieder. Wat precies wordt bedoeld met "werkzaam onder het gezag" blijkt niet uit de wetsgeschiedenis. In overweging 32 Richtlijn privacy en elektronische communicatie (bijlage A5) staat evenwel dat de aanbieder de voor het aanbieden van zijn diensten noodzakelijke verwerkingen aan een derde ("een andere entiteit") mag uitbesteden, onder de voorwaarde dat deze onderaanneming en de daaruit voortvloeiende verwerking plaatsvinden met inachtneming van de regels die de algemene Privacyrichtlijn (bijlage A10) geeft met betrekking tot de personen die verantwoordelijk zijn voor de verwerking en de verwerkers van persoonsgegevens. Daaruit kan worden opgemaakt dat de aanbieder moet worden aangemerkt als verantwoordelijke in de zin art. 1, onder d, Wbp. Dat wil zeggen dat hij, binnen de in het artikel gestelde grenzen, zeggenschap heeft over de doeleinden van en de middelen voor de verwerking van de gegevens. Hij bepaalt hoe de gegevens worden gebruikt, of de gegevens worden verstrekt aan derden, hoelang ze worden opgeslagen enz. (MvT, Kamerstukken II 2002/03, 28 851, nr. 3, p. 156; zie ook art. 1, onder d, Wbp, aant. 5 en 6). *Verwerkingsdoeleinden.* De gegevens mogen worden verwerkt voor facturering, verkeersbeheer, behandeling van verzoeken om inlichtingen van klanten, opsporing van fraude alsmede marktonderzoek en verkoopactiviteiten met betrekking tot elektronische communicatiediensten of de levering van diensten met toegevoegde waar-

de. Volgens de wetgever betreffen verkeersbeheer, inlichtingenverstrekking en opsporing van fraude geen zelfstandige verwerkingsdoeleinden, maar worden deze geacht afgeleid te zijn uit het factureringsdoel en waarschijnlijk ook het doeleinde van het overbrengen van de communicatie, zoals genoemd in de leden 1 en 2 (zie aant. 3). *Noodzakelijkheid.* De verwerking moet beperkt blijven tot hetgeen noodzakelijk is om die activiteiten te kunnen uitvoeren. Hiermee wordt art. 6, vijfde lid, Richtlijn privacy en elektronische communicatie geïmplementeerd.

6 Gegevensverstrekking aan geschilbeslechtende personen en instanties (lid 6). In het zesde lid wordt art. 6, zesde lid, Richtlijn privacy en elektronische communicatie (bijlage A5) geïmplementeerd. Het stelt buiten twijfel dat de aanbieder de verkeersgegevens in voorkomend geval kan verstrekken aan personen en instanties die zijn belast met de berechting van de geschillen bedoeld in de art. 12.1, 12.2, voorzover van toepassing, of 12.9. De gegevens mogen derhalve worden verstrekt aan de geschillencommissie telecommunicatie (art. 12.1), alsmede aan OPTA in zijn rol als beslechter van geschillen tussen marktpartijen onderling (art. 12.2) en van geschillen tussen marktpartijen en consumenten (art. 12.9).

7 Uitzonderingen in verband met nationale veiligheid en opsporing strafbare feiten. In het eerste lid van art. 11.13 staat dat aanbieders de regeling van verkeersgegevens in het artikel buiten toepassing kunnen laten, als dat nodig is in het belang van de nationale veiligheid of de voorkoming, opsporing en vervolging van strafbare feiten,. Daarmee is duidelijk dat aanbieders desgevraagd kunnen voldoen aan de vorderingen van politie en justitie op grond van met name art. 126n of 126u Sv tot verstrekking van locatiegegevens. Om misverstanden te voorkomen staat vervolgens in het tweede lid van art. 11.13 dat de gegevens die op grond van artikel 13.2a moeten worden bewaard (zijnde de verkeers- en andere gegevens van de bijlage bij de wet) alleen voor deze nationale veiligheids-, opsporings- en vervolgingsdoeleinden mogen worden gebruikt, tenzij het gegevens betreft waarvan de verwerking op grond van de artikelen 11.5 (of 11.5a) is toegestaan en de verwerking plaatsvindt met inachtneming van die artikelen (MvT, Kamerstukken II 2006/07, 31 145, nr. 3, p. 12-13, 44-45). In het derde lid van artikel 11.13 is ten slotte bepaald dat aanbieders bevoegd zijn om, in afwijking van het artikel verkeersgegevens te verwerken, als dat nodig is voor een onderzoek naar hinderlijke en kwaadwillige oproepen, zoals bedoeld in art. 11.11, vierde en vijfde lid (MvT, Kamerstukken II 2002/03, 28 851, nr. 3, p. 165). Zie art. 11.13, aant. 2.

[Ongevraagde oproepen voor commerciële, ideële of charitatieve doeleinden]

Artikel 11.7

1. Het gebruik van automatische oproepsystemen zonder menselijke tussenkomst, faxen en elektronische berichten voor het overbrengen van ongevraagde communicatie voor commerciële, ideële of charitatieve doeleinden aan abonnees is uitsluitend toegestaan, mits de verzender kan aantonen dat de desbetreffende abonnee daarvoor voorafgaand toestemming heeft verleend, onverminderd hetgeen is bepaald in het tweede en derde lid.

2. Indien de abonnee, bedoeld in het eerste lid, een rechtspersoon is dan wel een natuurlijke persoon die handelt in de uitoefening van zijn beroep of bedrijf, geldt met betrekking tot het door middel van elektronische berichten overbrengen van

ongevraagde communicatie voor commerciële, ideële of charitatieve doeleinden dat geen voorafgaande toestemming is vereist:
a. indien de verzender bij het overbrengen van de communicatie gebruik maakt van elektronische contactgegevens die door de abonnee daarvoor zijn bestemd en bekendgemaakt, en deze zijn gebruikt in overeenstemming met de door de abonnee aan die contactgegevens verbonden doeleinden, of
b. indien de abonnee is gevestigd buiten de Europese Economische Ruimte en voldaan is aan de in het desbetreffende land geldende voorschriften met betrekking tot het verzenden van ongevraagde communicatie.

3. Een ieder die elektronische contactgegevens voor elektronische berichten heeft verkregen in het kader van de verkoop van zijn product of dienst mag deze gegevens gebruiken voor het overbrengen van communicatie voor commerciële, ideele of charitatieve doeleinden met betrekking tot eigen gelijksoortige producten of diensten, mits bij de verkrijging van de contactgegevens aan de klant duidelijk en uitdrukkelijk de gelegenheid is geboden om kosteloos en op gemakkelijke wijze verzet aan te tekenen tegen het gebruik van die elektronische contactgegevens, en, indien de klant hiervan geen gebruik heeft gemaakt, hem bij elke overgebrachte communicatie de mogelijkheid wordt geboden om onder dezelfde voorwaarden verzet aan te tekenen tegen het verder gebruik van zijn elektronische contactgegevens. Artikel 41, tweede lid, van de Wet bescherming persoonsgegevens is van overeenkomstige toepassing.

4. Bij het gebruik van elektronische berichten voor de in het eerste lid genoemde doeleinden dienen te allen tijde de volgende gegevens te worden vermeld:

a. de werkelijke identiteit van degene namens wie de communicatie wordt overgebracht, en

b. een geldig postadres of nummer waaraan de ontvanger een verzoek tot beëindiging van dergelijke communicatie kan richten.
5. Het gebruik van andere dan de in het eerste lid bedoelde middelen voor het overbrengen van ongevraagde communicatie voor commerciële, ideële of charitatieve doeleinden aan abonnees is toegestaan met inachtneming van het bepaalde in het zesde tot en met twaalfde lid, tenzij de abonnee op de in het zesde lid bedoelde wijze dan wel anderszins te kennen heeft gegeven dat hij de ongevraagde communicatie niet wenst te ontvangen.
[..]

1 Algemeen. Het artikel implementeert art. 13 Richtlijn privacy en elektronische communicatie (bijlage A5) dat regels geeft voor ongewenste (in de Engels versie: "unsollicited" dus eigenlijk ongevraagde) communicatie met het oog op direct marketing. *Commerciële, ideële of charitatieve doeleinden.* Het artikel spreekt over communicatie voor commerciële, ideële of charitatieve doeleinden. Met de terminologie wordt beoogd aan te sluiten bij art. 435e Sv. Deze strafbepaling ziet op de telefonische verkoop van diensten en goederen waarbij de indruk wordt gewekt dat de opbrengst geheel of ten dele voor een liefdadig of ideëel doel is bestemd. Daaronder worden niet begrepen ongevraagde oproepen ten behoeve van markt- en verkiezingsonderzoek, omdat deze oproepen zijn gericht op het verkrijgen van informatie en op vrijwillige basis worden gedaan zonder dat deze informatieverwerving direct is gekoppeld of gecombineerd wordt met de verkoop of wer-

ving (NMvA I, Kamerstukken I 1997/98, 25 533, nr. 309d, p. 6; Handelingen II 2002/03, p. 14-789). *Opt-in en opt-out.* Voor automatische oproepsystemen zonder menselijke tussenkomst, faxen en elektronische berichten, geldt een opt-in regime, waarbij de abonnee van tevoren toestemming moet hebben gegeven voor het overbrengen van de communicatie. Met betrekking tot andere middelen voor het overbrengen van communicatie geldt een opt-out regime, waarbij de abonnee achteraf bezwaar kan maken. *Rechtspersonen, natuurlijke personen en consumenten (art. 11.8).* Art. 13, vijfde lid, Richtlijn privacy en elektronische communicatie (bijlage A5) biedt de mogelijkheid om de werking van het artikel te beperken tot abonnees die natuurlijke personen zijn. De wetgever heeft daarvan gebruik gemaakt in art. 11.8. Daarin wordt de toepassing van het vijfde tot en met twaalfde lid van het artikel (d.w.z. de regeling met betrekking tot telemarketing) beperkt tot abonnees die natuurlijke personen zijn. Zie aant. 6 en aant. bij art. 11.8. Verder wordt in het tweede lid een versoepelde regeling gegeven voor het overbrengen van de ongevraagde elektronische berichten aan abonnees die rechtspersonen zijn of natuurlijke personen die handelen in de uitoefening van beroep of bedrijf (d.w.z. abonnees die geen consumenten zijn). Zie aant. 3. Voor het overige houdt de wetgever vast aan het uitgangspunt om zoveel mogelijk aan te sluiten bij de algemene privacyregelgeving van de Wbp, die alleen natuurlijke personen betreft (zie MvT, Kamerstukken II 2005/06, 30 661, nr. 3, p. 8-10). *Bestuursrechtelijke handhaving.* Op grond van art. 15.1, derde lid, is OPTA bevoegd tot handhaving van het artikel. Voor klachten over ongevraagde communicatie heeft OPTA een website beschikbaar gesteld waar abonnees terecht klachten kunnen indienen: www.spamklacht.nl. Daarnaast is het Cbp bevoegd terzake van de naleving van de Wbp. In het Samenwerkingsprotocol CBP-OPTA (Stcrt. 2005, 133) zijn afspraken vastgelegd over de afstemming van beider bevoegdheden (zie Inl. opm. bij dit hoofdstuk, aant. 4). In zijn beleidsregels Handhaving spam (Stcrt. 2008, 50) geeft OPTA aan hoe hij invulling geeft aan zijn handhavingsbeleid met betrekking tot het spamverbod en formuleert hij zijn boetebeleid ten aanzien daarvan. Bij de bestuursrechtelijke handhaving van het spamverbod is OPTA gehouden aan de eisen die voortvloeien uit art. 6 EVRM (Rb. Rotterdam 23 mei 2007, LJN BA6377; zie ook Rb. Rotterdam 23 mei 2007, LJN BA 6384). *Strafrechtelijke handhaving.* Alleen overtreding van de informatieplicht van het vierde lid is als economisch delict strafbaar gesteld. Bij amendement is geprobeerd om het gehele artikel onder de werking van de WED te brengen. Dit is niet overgenomen, omdat dat zou kunnen leiden tot verstopping van het opsporingsapparaat. Verder meende de regering dat het artikel, met uitzondering van het vierde lid, teveel onbepaalde en onbestemde elementen bevat, waardoor er sprake zou zijn van kennelijk ongewenst geachte symboolwetgeving (Amend., Kamerstukken II 2002/03, 28 851, nr. 16; Handelingen II 2003/004, p. 14-790). *Art. 7:46h BW en Consumentenautoriteit.* In art. 7:46h, tweede tot en met vijfde lid, BW is een vergelijkbare regeling vastgelegd met betrekking tot het overbrengen van ongevraagde communicatie ter bevordering van de totstandkoming van een koop op afstand. Op grond van art. 2.7, eerste lid, jo 8.5, tweede tot en met vierde lid, Wet handhaving consumentenbescherming (Stb. 2006, 592) is (ook) de Consumentenautoriteit bevoegd tot handhaving van deze bepaling. *Reclame Code Commissie.* In de Nederlandse Reclame Code zijn gedragscodes opgenomen voor e-mail reclame en voor telemarketing (resp. Code Verspreiding Reclame via E-mail en Code Telemarketing). Als aangesloten bedrijven niet voldoen aan deze gedragscodes kan op grond daarvan kan worden geklaagd bij de Reclame Code Commissie. De gedragscodes zijn te vinden op de website van de Stichting Reclame Code: www.reclamecode.nl.

2 Opt-in voor automatische oproepsystemen zonder menselijke tussenkomst, faxen en elektronische berichten (lid 1). Er geldt een opt-in regime voor het overbrengen van ongevraagde communicatie voor direct marketing-doeleinden, waarbij gebruik wordt gemaakt van de drie genoemde communicatiemiddelen (automatische oproepsystemen, faxen en elektronische berichten). Voor dergelijke ongevraagde communicatie moet de abonnee voorafgaand toestemming in de zin van art. 11.1, onder g, hebben gegeven. Daarvan is geen sprake als de toestemming slechts is gebaseerd op een bepaling in de algemene voorwaarden (NV II, Kamerstukken II 2002/03, 28 851, nr. 7, p. 41; zie ook art. 11.1, aant. 8). *Ideële en charitatieve doeleinden.* Op grond van art. 13, tweede lid, en overw. 41 Richtlijn privacy en elektronische communicatie (bijlage A5) meende de regering dat het toegestaan gegevensgebruik beperkt kon blijven tot commerciële doeleinden, en dus niet ook op ideële of charitatieve doeleinden betrekking hoefde te hebben. De laatste twee doeleinden zijn bij amendement toegevoegd (zie NV, Kamerstukken II 2002/03, 28 851, nr. 7, p. 42; Amend. Kamerstukken II 2002/03, 28 851, nr. 14; Handelingen II 2003/04, p. 14 788-789). *Communicatiemiddelen.* Deze in het eerste lid van het artikel genoemde communicatiemiddelen kenmerken zich doordat daarmee op grote schaal berichten kunnen worden verspreid zonder dat dit noemenswaardige kosten voor de verzender met zich meebrengt, terwijl de ontvangers daarvan grote overlast hebben (m.n. e-mail spam en junkfax; Brief Min. EZ, Kamerstukken II 2003/04, 26 643, nr. 46). *Automatisch oproepsysteem.* Er moet worden gedacht aan apparaten die met behulp van een databank zonder menselijke tussenkomst op grote schaal oproepen plegen en een bericht afspelen. Dergelijke apparaten worden ook wel belautomaten genoemd. *Elektronisch bericht.* Het begrip "elektronisch bericht" wordt in art. 11.1, onder i, gedefinieerd als tekst-, spraak-, geluids- of beeldbericht dat over een openbaar elektronisch communicatienetwerk wordt verzonden en in het netwerk of in de randapparatuur van de ontvanger kan worden opgeslagen tot het door de ontvanger wordt opgehaald. Het betreft dus met name e-mail en sms (zie art. 11.1, aant. 10). *Bewijslast verleende toestemming.* De verzender moet kunnen aantonen dat de desbetreffende abonnee voor het overbrengen van ongevraagde communicatie voorafgaand toestemming heeft verleend. De bewijslast voor de verleende toestemming ligt dus bij de verzender (Amend. Kamerstukken II 2002/03, 28 851, nr. 15; Handelingen II 2003/04, 28 851, p. 14-788).

3. Versoepeld regime voor rechtspersonen, bedrijven en ondernemingen (lid 2). Het in het eerste lid gestelde opt-in vereiste wordt in het tweede lid versoepeld voorzover het gaat om verzending van ongevraagde elektronische berichten (dus e-mail en sms, maar niet fax en automatische oproepautomaten) aan abonnees die rechtspersonen zijn of natuurlijke personen die handelen in de uitoefening van beroep of bedrijf. Voor de verzending van ongevraagde elektronische berichten aan deze categorieën van abonnees is geen voorafgaande toestemming vereist in de gevallen genoemd onder a en b, te weten a) bij gebruik van daarvoor bedoelde elektronische contactgegevens en b) als het gaat om abonnees gevestigd buiten EER. **a) gebruik van daarvoor bedoelde elektronische contactgegevens (onder a).** Geen voorafgaande toestemming is vereist als er gebruik wordt gemaakt elektronische contactgegevens die abonnees (rechtspersonen, bedrijven, ondernemers) voor dat doel bekend hebben gemaakt. Deze abonnees hebben dus de mogelijkheid om de in het eerste lid bedoelde toestemming niet van geval tot geval maar in zijn algemeenheid te geven. *Elektronische contactgegevens.* Onder elektronische contactgegevens wordt niet alleen verstaan het e-mailadres, maar ook het mobiele telefoonnum-

mer, indien dat wordt gebruikt voor de verzending van sms- of mms-berichten voor direct marketing doeleinden. *Achtergrond.* Met deze versoepeling wordt tegemoetgekomen aan de veronderstelde behoefte van bedrijven om zelf te bepalen of zij elektronische communicatie met marketingdoeleinden willen ontvangen, op welk adres zij dit willen ontvangen en voor welk doel. De in dit lid bedoelde abonnees kunnen dit bijvoorbeeld doen door dit aan te geven op hun website of door daarvoor bedoeld e-mailadres bekend te maken (zeg: marketinginfohierheen@bedrijfsnaam.nl). Zie Kamerstukken II 2006/07, 30 661, nr. 3, p. 10 en 24, nr. 5, p. 12. **b) abonnee gevestigd buiten de EER en voldaan aan aldaar geldende vereisten (onder b).** Voor het overbrengen van ongevraagde elektronische communicatie naar abonnees buiten de EER (d.w.z. EU met IJsland, Noorwegen en Liechtenstein) is geen voorafgaande toestemming vereist, als is voldaan aan de voorschriften die daarvoor in het desbetreffende land gelden. Alleen als in dat land een opt-in vereiste geldt moet voorafgaande toestemming worden verkregen. *Achtergrond.* Deze regeling beoogt ondernemingen in Nederland in staat te stellen om op voet van gelijkheid met buitenlandse concurrenten aan (potentiële) klanten hun producten diensteninformatie te zenden. Kamerstukken *II* 2005/06, 30 661, nr. 3, p. 11-12, 23-24. *Relatie situatie onder a) en onder b).* Ook in de gevallen bedoeld onder b) is de onder a) genoemde specifieke regeling van toepassing. Ook dan mag dus van voorafgaande toestemming worden uitgegaan als reclame wordt verzonden naar het adres van de abonnees die in het algemeen bekend hebben gemaakt marketinginformatie te willen ontvangen op het daarvoor bedoelde contactadres. Kamerstukken II 2005/06, 30 661, nr. 3, p. 12.

4 Elektronische contactgegevens van bestaande klanten (lid 3). Het derde lid betreft een specifieke voorziening voor het gebruik van elektronische contactgegevens die zijn verkregen in het kader van een bestaande klantrelatie, ofwel bij de verkoop van een eigen product of dienst. Voor het gebruik van deze elektronische contactgegevens geldt een opt-out regime als het gaat om het overbrengen van ongevraagde communicatie met betrekking tot eigen en gelijksoortige diensten en producten. *Elektronische contactgegevens.* Onder elektronische contactgegevens wordt niet alleen verstaan het e-mailadres, maar ook het mobiele telefoonnummer, indien dat wordt gebruikt voor de verzending van sms- of mms-berichten voor direct marketing doeleinden. *Gelijksoortige producten of diensten.* Het begrip "gelijksoortig" is een begrip dat zich niet eenduidig laat omschrijven. Van belang is dat de regeling voor elektronische klantgegevens van het derde lid wordt gezien als een beperkte verzachting of versoepeling van de harde opt-in regel uit het eerste lid – er wordt wel gesproken van 'soft opt-in'. Dat brengt met zich mee dat een beperkter toepassingsbereik voor de hand ligt. Verder zijn van belang de redelijke verwachtingen die de ontvanger van de commerciële communicatie op het moment van de aankoop van een product of dienst gekregen heeft omtrent de soort producten of diensten waaromtrent hij dergelijke communicatie zou mogen verwachten. Daarbij komt vooral betekenis toe aan de informatie die is verstrekt bij de aankoop van de producten of diensten (NV II, Kamerstukken II 2002/03, 28 851, nr. 7, p. 42). *Opt-out.* Bij de verzameling en het gebruik van de elektronische contactgegevens moet de klant een opt-out mogelijkheid worden geboden. Er moet duidelijk en uitdrukkelijk de gelegenheid worden geboden om kosteloos en op gemakkelijke wijze verzet aan te tekenen tegen het gebruik van deze contactgegevens. Als de klant daarvan geen gebruik heeft gemaakt, moet hem bij elke overgebrachte communicatie de mogelijkheid worden geboden om onder dezelfde voorwaarden (dus kosteloos en op gemakkelijke wijze) verzet aan te tekenen tegen

het verder gebruik dat van zijn contactgegevens wordt gemaakt voor dit doel. (MvA I, Kamerstukken I 2003/04, 28 851, C, p. 23). *Wet bescherming persoonsgegevens.* Art. 41, tweede lid, Wbp is van overeenkomstige toepassing. Dat wil zeggen dat degene die de contactgegevens voor het hier bedoelde doel heeft aangewend, maatregelen dient te nemen om in het geval van verzet de verwerking van deze gegevens voor dat doel terstond te beëindigen (zie art. 41 Wbp, aant. 1 en 2).

5 Informatieplicht (lid 4). Aan het gebruik van elektronische berichten voor de toezending van ongevraagde communicatie voor de in het eerste en tweede lid bedoelde doeleinden wordt in het derde lid een aanvullende eis gesteld. Bij het gebruik van elektronische berichten voor de commerciële, ideële en charitatieve doeleinden van het eerste en tweede lid moet te allen tijde de werkelijke identiteit worden medegedeeld van degene namens wie de communicatie wordt overgebracht. Het gebruik van een pseudoniem is dus niet toegestaan. Verder moet in het elektronisch bericht een geldig postadres of nummer (in de zin van art. 1.1, onder bb; zie art. 1.1, aant. 24) worden vermeld waar de ontvanger een verzoek tot beëindiging van dergelijke communicatie kan indienen. Het niet voldoen aan deze eis is als economisch delict strafbaar gesteld (art. 1, onder 4, WED). Een amendement om de werking van het hele artikel strafbaar te stellen, is niet overgenomen, omdat dat zou kunnen leiden tot verstopping van het opsporingsapparaat. Verder meende de regering dat het artikel, met uitzondering van het derde lid, teveel onbepaalde en onbestemde elementen bevat, waardoor er sprake zou zijn van symboolwetgeving (Kamerstukken II 2002/03, 28 851, nr. 16; Handelingen II 2003/04, p. 14-790).

[Toepassing art. 11.6 en 11.7, vijfde t/m twaalfde lid, beperkt tot natuurlijke personen]

Art. 11.8

De toepassing van de artikelen 11.6 en 11.7, *vijfde tot en met twaalfde lid,* is beperkt tot abonnees die natuurlijke personen zijn.

Betekenis.

In art. 11.1, onder a, staat dat het begrip "abonnee" betrekking heeft op natuurlijke personen en rechtspersonen. Daarmee wijkt de wet af van de Wbp waarvan de werking is beperkt tot gegevens over natuurlijke personen. Om de aansluiting met deze algemene privacywet zoveel mogelijk te bewaren, beperkt het artikel de toepassing van de art. 11.6 (algemeen beschikbare telefoongidsen en abonnee-informatiediensten) en de laatste negen leden van art. 11.7 (telemarketing) tot abonnees die natuurlijke personen zijn. De Richtlijn privacy en elektronische communicatie (bijlage A5) biedt deze mogelijkheid in art. 12, vierde lid, respectievelijk art. 13, vijfde lid (zie art. 11.1, aant. 4; MvT, Kamerstukken II 1996/97, 25 533, nr. 3, p. 121).