Bescherming van persoonsgegevens en de persoonlijke levenssfeer

Zwenne, G.J.

HOOFDSTUK 11

Bescherming van persoonsgegevens en de persoonlijke levenssfeer

[Inleidende opmerkingen]

1. Algemeen. De kwaliteit van elektronische communicatienetwerken en -diensten wordt in sterke mate bepaald door de omstandigheid dat de vertrouwelijkheid van de communicatie is gewaarborgd Technologische ontwikkelingen en marktontwikkelingen maken het mogelijk dat steeds meer en steeds meer verschillende soorten persoonsgegevens kunnen 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) en het opnemen van persoonsgegevens in telefoongidsen en bestanden voor abonnee-informatiediensten *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 d m v 'cookies', 'spyware' en inbelprogramma's e d) is met in hoofdstuk 11 van de wet geregeld, maar in art 4 1 BUDE (bijlage C13) *Wetsvoorstel 28 962* Omdat twee artikelen uit de inmiddels ingetrokken Telecommunicatie Privacyrichtlijn (97/66/EG) niet of niet goed in de nationale wetgeving waren geïmplementeerd, heeft de Europese Commissie een inbreukprocedure tegen Nederland geïnitieerd Daardoor was de regering genoodzaakt om met een wetsvoorstel te komen waarin de desbetreffende bepalingen alsnog zouden worden geïmplementeerd Het desbetreffende wetsvoorstel Wijziging van de Telecommunicatiewet in verband met de implementatie van richtlijn 97/66/EG (Wetsvoorstel 28 962) had echter na aanvaarding van het wetsvoorstel voor de Wet implementatie Europees regelgevingskader voor de elektronische communicatiesector 2002 (Kamerstukken 28 851) geen zelfstandige betekenis meer, zodat het is ingetrokken

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, Parl Gesch , p 417) *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 voo gedaan art 13 Gw technologieonafhankelijk te herformuleren, zodat daaronder oo mailberichten en andere elektronische uitingsvormen zouden vallen Uiteindelijk r wetsvoorstel (Kamerstukken II 1996/97-1998/99, 25 443, nrs 1-40d) ingetrokl omdat er onduidelijkheid bestond over het begrip vertrouwelijkheid. Om duidelij maken dat elektronische uitingsvormen onder dezelfde bescherming vallen als grondwettelijke brief en telefoongeheim, werd vervolgens bij amendement een nie artikel toegevoegd dat de wetgever de opdracht geeft om bij het vaststellen van uitv ingsregelingen rekening te houden met de bescherming van het brief-, telefoon- en legraafgeheim en het geheim van daarmee vergelijkbare communicatietechnieken heeft geresulteerd in art 18 13 (Kamerstukken II 1997/98, 25 533, nr 75, Parl. Ges p. 572-573, zie aant bij art 18 13)

3. Wet bescherming persoonsgegevens (Wbp). De specifieke regels in dit hoo stuk gelden in aanvulling op en ter uitwerking van de Wbp Deze privacywet is ge seerd op de algemene Privacyrichtlijn (bijlage A5) en stelt regels voor de geheel of deeltelijk geautomatiseerde verwerking van persoonsgegevens Daarmee vormt de W het algemeen kader waarbinnen de verwerking van persoonsgegevens (ook) binnen sector elektronische communicatie moet plaats vinden De bepalingen van hoofdstuk hebben ten opzichte van de algemene Privacyrichtlijn en de uitwerking daarvan in Wbp een aanvullende werking, waarbij op onderdelen sprake is van een nadere uitw king van de meer algemene normen uit de Wbp Voor de specifieke, in de sfeer v elektronische communicatie, voorkomende verwerkingen van persoonsgegevens w den daarop toegesneden (en in voorkomend geval uitputtende) normen gesteld Ver strekt de reikwijdte van dit hoofdstuk zich in beginsel ook uit tot rechtspersonen, terw de Wbp alleen betrekking heeft op gegevens over natuurlijke personen (MvT, Kam stukken II 2003/04, 28 851, nr 3, p 45) De Wbp is in deze uitgave afzonderlijk g genomen en van commentaar voorzien

4. Handhaving en toezicht. *OPTA en College bescherming persoonsgegevens (Cbp)* C grond van art 15 1, derde lid, is OPTA belast met het toezicht op de naleving v hoofdstuk 11 Daarnaast is het Cbp op grond van de Wbp belast met het toezicht op naleving van de Wbp in het algemeen, en waar het de verwerking van persoonsgegeve op grond van hoofdstuk 11 van de wet betreft, ook op die bepalingen Waar de onde scheiden bevoegdheden van het Cbp en OPTA elkaar overlappen, is samenwerking tu sen beide instanties geboden Beide instanties geven daaraan in toenemende mate mv ling, waarbij gestreefd wordt naar een taakverdeling waarin de meest gerede toezich houder het voortouw neemt. Deze samenwerking betekent in de praktijk ook dat informatie die men in het kader van de toezichthoudende taak verkrijgt, waar dat noo zakelijk is met elkaar wordt gedeeld (MvT, Kamerstukken II 2002/03, 28 851, nr 3, 61, NV, Kamerstukken II 2002/03, 28 851, nr 7, p. 43 en 52-54) Zie art 15 1, aa 3. *Strafbaarstelling* De overtreding van art 11 7, derde lid, is strafbaar gesteld in de W economische delicten Strafbaarstellingen ter bescherming van het belang van de ve trouwelijkheid van telecommunicatienetwerken en -diensten staan verder onder ande in de art 139a-139c Sr De strafvorderingsbevoegdheden op grond waarvan politie justitie inbreuk mogen maken op de vertrouwelijkheid van netwerken en diensten zi geregeld in art 126l-126na en 126s-126ua Sv

§ 11 1 Algemene bepalingen

[Definities]

Artikel 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;**

d. **locatiegegevens: gegevens die worden verwerkt in een elektronisch communicatienetwerk waarmee de geografische positie van de randapparatuur van een gebruiker van een openbare elektronische communicatiedienst wordt aangegeven;**

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;**

h. **dienst met toegevoegde waarde: dienst die de verwerking vereist van verkeersgegevens of locatiegegevens, niet zijnde verkeersgegevens, en die verder gaat dan hetgeen noodzakelijk is voor de overbrenging van een communicatie of de facturering daarvan;**

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 recht-

streekse 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-mailadressen, het gebruikte protocol, begin- en eindtijd sessie, type dienst, volume (aantal kilobytes) 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 persoonsgegevens in de 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)

5. Locatiegegevens (onder d). Onder het begrip 'locatiegegevens' worden de gegevens verstaan die worden verwerkt in een elektronisch communicatienetwerk waarmee de geografische positie van de randapparatuur (mobiel toestel, pda) van een gebruiker van een openbare elektronische communicatiedienst wordt aangegeven Daarbij kan worden gedacht aan gegevens betreffende de breedte-, hoogte- en lengtegraad waarmee

de locatie van het mobiele toestel wordt weergegeven, gegevens betreffende de reisrichting, de nauwkeurigheidsgraad van de locatiegegevens, de identificatie van de netwerkcel waarbinnen de randapparatuur zich op een bepaald tijdstip bevindt, en het tijdstip waarop de locatiegegevens zijn opgeslagen (overw 14 Richtlijn privacy en elektronische communicatie (bijlage A5)) *Locatiegegevens en verkeersgegevens* Locatiegegevens kunnen verkeersgegevens zijn als deze gegevens ook vallen onder de definitie van verkeersgegevens van art 11 1, onder b (zie aant 4) Een voorbeeld van locatiegegevens, die tevens als verkeersgegevens worden aangemerkt, zijn gegevens die in het kader van mobiele telefonie worden verwerkt betreffende de basisstations waar het mobiele toestel van de gebruiker contact mee heeft en welke noodzakelijk zijn voor het overbrengen van communicatie tussen de oproepende en opgeroepen gebruiker (MvT, Kamerstukken II 2003/03, 28 851, nr 3, p 47 en 151, alsmede Aanh Handelingen II 1999/2000, p 2413-2416) Dat geldt ook in die gevallen waarbij dergelijke gegevens ook voor andere, locatiegebonden doeleinden, zoals de levering van daaraan gerelateerde toegevoegde waardediensten, worden gebruikt Daarnaast zijn er locatiegegevens die niet tevens als verkeersgegevens worden aangemerkt en die derhalve niet worden verwerkt voor het overbrengen van communicatie in de zin van art 11 1, onder e Voor de verwerking van dergelijke locatiegegevens, niet zijnde verkeersgegevens, geeft art 11 5a een regeling (zie art 11 5a, aant 2)

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 A15) 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 A12) 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 berus-

tende wilsuiting waarmee de betrokkene aanvaardt dat hem of haar betreffende persoonsgegevens worden verwerkt. Omdat de '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 betrekking 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 plaats 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)

9. Dienst met toegevoegde waarde (onder h). Onder 'dienst met toegevoegde waarde' wordt verstaan de dienst die de verwerking vereist van verkeersgegevens of locatiegegevens, niet zijnde verkeersgegevens, en die verder gaat dan hetgeen noodzakelijk is voor de overbrenging van een communicatie of de facturering daarvan. De definitie sluit nauw aan bij art. 2, onder g. Voorbeelden van toegevoegde waardediensten zijn adviezen over de voordeligste tariefpakketten, routegeleiding, verkeersinformatie, weerberichten, toeristische informatie. In veel gevallen betreffen toegevoegde waardediensten zogeheten locatiegebonden diensten, waarbij van locatiegegevens gebruik wordt gemaakt om een dienst te verlenen die verband houdt met de locatie waar de afnemer van de dienst zich bevindt (MvT, Kamerstukken II 2002/03, 28 851, nr. 3, p. 153 en 157, zie ook overw. 18 Richtlijn privacy en elektronische communicatie). De definitie van het begrip is opgenomen met het oog op de regeling voor het gebruik van verkeersgegevens en locatiegegevens in respectievelijk art. 11.5, derde lid, onder b, en art. 11.5a, tweede lid (resp. art. 11.5, aant. 3c en art. 11.5a, aant. 4).

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 mmsberichten, 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]

Artikel 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 bescherming 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, Parl Gesch , p 429) *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, Parl Gesch , p 424) *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

[Passende technische en organisatorische maatregelen]

Artikel 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 al-

leen 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 (Mv T, Kamerstukken II 1996/97, 25 533, nr 3, p 119, Parl Gesch , p 430)

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, Parl Gesch , p 430) 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) *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, Parl Gesch , p 430) **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 c) 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)

[Niet-gespecificeerde rekening; ongedaan maken doorschakeling]

Artikel 11.4. — 1. De aanbieder van een openbare elektronische communicatiedienst is verplicht de abonnee op diens verzoek:

***a.* geleverde elektronische communicatiediensten door middel van geheel of gedeeltelijk niet-gespecificeerde nota's in rekening te brengen;**

b. de mogelijkheid te bieden kosteloos en op eenvoudige wijze de doorschakeling van oproepen van derden naar het bij hem in gebruik zijnde netwerkaansluitpunt ongedaan te maken.

— 2. Bij algemene maatregel van bestuur kunnen in het belang van de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van oproepende gebruikers en opgeroepen abonnees regels worden gesteld met betrekking tot het specificeren van nota's voor geleverde elektronische communicatiediensten. Deze regels kunnen onder meer betrekking hebben op de toekenning van rechten aan abonnees, de behandeling van klachten, de verstrekking van informatie en de vergoeding van kosten. Bij de algemene maatregel van bestuur kunnen aan het college taken worden opgedragen en bevoegdheden verleend.

— 3. Bij algemene maatregel van bestuur kunnen regels worden gesteld ten aanzien van de keuzemogelijkheden voor de wijze van betaling van geleverde elektronische communicatiediensten.

1. Algemeen. In het artikel worden twee verplichtingen opgelegd aan aanbieders van elektronische communicatiediensten (en dus niet aan aanbieders van elektronische communicatienetwerken) De met deze rechten corresponderende rechten van abonnees (niet noodzakelijk gebruikers) betreffen het recht op een niet-gespecificeerde rekening (lid 1 onder a) en het recht op het ongedaan kunnen maken van geautomatiseerde doorschakelingen (lid 1 onder b) De onderscheiden rechten zijn afkomstig van in art 7 respectievelijk 11 Richtlijn privacy en elektronische communicatie (bijlage A5) Om redenen van systematiek zijn deze bepalingen, die beide rechten voor abonnees bevatten, bij elkaar in hetzelfde art lid geplaatst (MvT, Kamerstukken II 1996/97, 25 533, nr 3 p 119 Parl Gesch , p 432) **a) Niet gespecificeerde nota (lid 1, onder a).** Digitale netwerken (zoals de netwerken waarin gebruik wordt gemaakt van ISDN, GSM, GPRS of UMTS-technologie) stellen de aanbieders daarvan in staat details betreffende de verleende diensten te specificeren in de nota, zoals de opgeroepen nummers, datum, tijdstip en duur van gesprekken De abonnee kan door een gespecificeerde rekening inzicht verkrijgen in de wijze waarop andere gebruikers (bijv huisgenoten) van de diensten gebruik maken Om de persoonlijke levenssfeer van deze gebruikers te kunnen beschermen, heeft de abonnee (niet noodzakelijk de gebruiker) het recht op een niet of niet volledig gespecificeerde rekening Voorafgaand aan de inwerkingtreding van de Wet implementatie Europees regelgevingskader voor de elektronische communicatiesector 2002 hadden abonnees voor de beperktere categorie van telefoondiensten op grond van art 31 BOHT een recht op een wél gespecificeerde rekening Dit recht is in de huidige wetgeving niet meer opgenomen (NvT BUDE, Stb 2004, 203, p 9) **b) Ongedaan maken doorschakeling van derden (lid 1, onder b).** Veel (digitale) elektronische communicatienetwerken bieden de mogelijkheid oproepen door te schakelen naar een andere abonnee zonder dat deze van de doorschakeling tevoren op de hoogte wordt gesteld Het artikel biedt de abonnee de mogelijkheid in bijzondere, door de abonnee aangedragen, gevallen van de overlast van doorschakeling gevrijwaard te blijven Het artikel gaat echter niet zo ver dat de aanbieder op verzoek van de abonnee doorschakeling van alle oproepen naar zijn aansluiting categorisch onmogelijk moet maken De ongedaanmaking moet kosteloos en eenvoudig zijn te realiseren Verder wordt het aan de aanbieders overgelaten op welke manieren zij aan abonnees tegemoet komen (NV II, Kamerstukken II 1997/98, 25 533, nr 5, p 120-121, Parl Gesch p 432) *Ontheffing ex art 11 12* Op grond van art 11 12 komt een aanbieder in aanmerking voor ontheffing van de verplichtingen die voortvloeien uit het artikel als is voldaan aan de

volgende (cumulatieve) voorwaarden (a) het gaat om abonneelijnen die zijn verbonden met analoge centrales, én (b) de nakoming van de verplichting is niet haalbaar of brengt onevenredig veel financiële lasten voor de aanbieder met zich. Deze ontheffingsvoorwaarden zijn afkomstig van art 3, tweede lid, Richtlijn privacy en elektronische communicatie (MvT, Kamerstukken II 2002/03, 28 851, nr. 3, p 162).

2. Algemene maatregelen van bestuur (leden 2 en 3). De AMvB's die op grond van het tweede en het derde lid kunnen worden vastgesteld, maken het mogelijk om uitvoering te geven aan de verplichting van art 7, tweede lid, Richtlijn privacy en elektronische communicatie (bijlage A5) Daarin staat dat lidstaten nationale bepalingen moeten toepassen om de rechten van abonnees die gespecificeerde facturen ontvangen, in overeenstemming te brengen met het recht op bescherming van de persoonlijke levenssfeer van oproepende abonnees en opgeroepen gebruikers Dat kan door ervoor te zorgen dat die gebruikers en abonnees beschikken over voldoende alternatieve communicatie- of betalingswijzen, waarmee waarborgen worden geboden voor de bescherming van de persoonlijke levenssfeer van deze gebruikers en abonnees Voorbeelden van alternatieve mogelijkheden zijn openbare telefooncellen, telefoonkaarten en mogelijkheden tot betaling met kredietkaarten, prepaidkaarten voor mobiele telefonie, collect call en gratis 0800-nummers Verder kan worden gedacht aan de mogelijkheid van een gespecificeerde factuur waarin een aantal cijfers van het opgeroepen nummers is weggelaten (overw 33 Richtlijn privacy en elektronische communicatie, NV II, Kamerstukken II 1997/98, 25 533, nr 5, p 126-127, Parl. Gesch , p. 432) *Discretionaire bevoegdheid* De wetgever is van mening dat de behoefte aan de bij AMvB te stellen regels betreffende gespecificeerde facturen beperkt is tot openbare (vaste en mobiele) telefoondiensten en carrier(pre)selectiediensten Voor andere diensten, zoals internetdiensten, is deze behoefte niet duidelijk, laat staan dat al duidelijk zou zijn welke nadere regels er dan zouden moeten worden gesteld. Om deze reden is niet de verplichting opgenomen om nadere regels te stellen maar een discretionaire bevoegdheid daartoe (Kamerstukken II 2002/03, 28 851, nr 13, p 19) *Inhoud AMvB* Om misverstanden te voorkomen is opgenomen dat deze bij AMvB te stellen regels kunnen worden gesteld in het belang van zowel oproepende gebruikers en opgeroepen abonnees, alsmede dat die regels onder meer betrekking kunnen hebben op de toekenning van rechten aan abonnees, klachtenafhandeling, informatieverstrekking en vergoeding van kosten In dezelfde AMvB kunnen aan OPTA taken worden opgedragen en bevoegdheden worden verleend. *Geen subdelegatie* De Tweede Kamer heeft bij amendement de mogelijkheid tot subdelegatie geschrapt door delegatie alleen 'bij' (en niet ook 'krachtens') AMvB toe te staan (Amend Kamerstukken II 1997/98, 25 533, nr. 53,, Handelingen II 1998/98, p 4926 en p 5205, Parl Gesch , p 188 en 433)

3. Afschermingsrecht van art. 4.2 BUDE. Van de in het tweede lid geregelde discretionaire bevoegdheid is gebruik gemaakt door in het BUDE (bijlage C13) een bepaling op te nemen, waarin is bepaald dat de abonnee het recht heeft om aan te geven dat zijn nummer niet mag worden vermeld op de nota van degene met wie hij heeft gebeld Als de abonnee dit aan zijn eigen aanbieder heeft kenbaar gemaakt, moet deze aanbieder dit vervolgens doorgeven aan de aanbieder die de nota opstelt ten behoeve van degene met wie de abonnee heeft gebeld Deze laatste aanbieder is dan gehouden het nummer af te schermen Dit moet gebeuren door dat nummer weg te laten of door de laatste vier cijfers daarvan onleesbaar te maken Dit 'nota-afschermingsrecht' geldt vanaf 1 maart 2005 Voor de gebruikmaking ervan mogen geen kosten in rekening worden gebracht Zie besluit van 8 september 2004 (Stb 2004, 458) *Relatie met 'geheime nummers' en nummeridentificatie* Het nota-afschermingsrecht vormt een logisch complement op het in art

11.6 opgenomen recht van de abonnee om niet te worden opgenomen in een abonneelijst of het bestand van een abonneeinformatiedienst, alsmede op de in art. 11.9, eerste lid, onder a, geregelde mogelijkheid voor de oproepende abonnee en gebruiker om de weergave van zijn nummer te blokkeren (resp. art. 11.6, aant. 3 en art. 11.9, aant. 2a).

[Anonimisering verkeers- en rekeninggegevens]

Artikel 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 met 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 elektronische 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 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* Het in eerdere wetgeving opgenomen vereiste dat het marktonderzoek en verkoopactiviteiten betrekken moeten hebben op eigen diensten is komen te vervallen 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 levering 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 of 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 A12) 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 van 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 waarde. 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 zonodig in het belang van de nationale veiligheid of de voorkoming, opsporing en vervolging van strafbare feiten, de regeling van verkeersgegevens in het artikel buiten toepassing kunnen laten. 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 In het tweede lid is 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

8. Overgangsrecht. Met de inwerkingtreding van de Wet implementatie Europees regelgevingskader voor de elektronische communicatiesector 2002 zijn de regels voor verkeersgegevens veranderd Om te voorkomen dat verwerkingen van verkeersgegevens in strijd zouden zijn met de nieuwe regels zijn in art 19 9 enige overgangbepalingen opgenomen Deze hebben betrekking op de verwerkingen van verkeersgegevens bedoeld in het tweede lid en het derde lid, onder a, ofwel de verwerkingen ten behoeve van de facturering en ten behoeve van marktonderzoek en verkoopactiviteiten Een overgangsrechtelijke bepaling voor de verwerking van verkeersgegevens bedoeld in het derde lid, onder b, ofwel de verwerkingen ten behoeve van toegevoegde waardediensten werd niet nodig geacht, omdat dit een nieuwe mogelijkheid tot verwerking van verkeersgegevens betreft (MvT, Kamerstukken II 2002/03, 28 851, nr 3, p 186) Zie aant bij art 19 9

[Verwerking locatiegegevens]

Artikel 11.5a. — 1. De verwerking van locatiegegevens, niet zijnde verkeersgegevens, betreffende abonnees of gebruikers van openbare elektronische communicatienetwerken of openbare elektronische communicatiediensten, is slechts geoorloofd, indien:

a. deze gegevens zijn geanonimiseerd, of

***b.* de desbetreffende abonnee of gebruiker voor de verwerking van deze gegevens toestemming heeft gegeven ten behoeve van de levering van een dienst met toegevoegde waarde.**

— 2. Voorafgaand aan het verkrijgen van toestemming als bedoeld in het eerste lid, onderdeel *b*, verstrekt de aanbieder van de toegevoegde waardedienst aan de abonnee of gebruiker de volgende informatie:

***a.* de soort locatiegegevens die zullen worden verwerkt;**

***b.* de doeleinden waarvoor de locatiegegevens worden verwerkt;**

***c.* de duur van de verwerking, en**

***d.* of de gegevens aan een derde zullen worden verstrekt ten behoeve van de levering van de dienst met toegevoegde waarde.**

— 3. De verwerking van de gegevens ten behoeve van de levering van een dienst met toegevoegde waarde als bedoeld in het eerste lid, onderdeel *b*, is slechts toegestaan voor zover en voor zolang dat noodzakelijk is voor de levering van de desbetreffende dienst. In afwijking van de eerste volzin mag de aanbieder van de dienst met toegevoegde waarde die gegevens verwerken die noodzakelijk zijn voor het opstellen van een factuur. Artikel 11.5, tweede lid, laatste volzin, is van overeenkomstige toepassing.

— 4. Een abonnee of gebruiker kan de verleende toestemming voor de verwerking van de hem betreffende gegevens op elk moment intrekken.

— 5. De aanbieder van een dienst met toegevoegde waarde biedt aan de abonnee of gebruiker wiens gegevens worden verwerkt de mogelijkheid om kosteloos en op eenvoudige wijze de verwerking van diens gegevens tijdelijk te beletten voor elke overbrenging van communicatie of elke verbinding met het openbare elektronische communicatienetwerk dat gebruikt wordt voor de levering van de desbetreffende dienst.

— 6. De verwerking van de gegevens mag slechts plaatsvinden door personen die werkzaam zijn onder het gezag van de aanbieder of de derde, bedoeld in het tweede lid, onder *d*, en is beperkt tot die gegevens die noodzakelijk zijn om de dienst met toegevoegde waarde te kunnen aanbieden.

1. Algemeen. Het artikel implementeert art 9 Richtlijn privacy en elektronische communicatie (bijlage A5), dat een specifieke regeling introduceert voor de verwerking van andere locatiegegevens dan verkeersgegevens (in het artikel aangeduid als locatiegegevens, niet zijnde verkeersgegevens) Definities van de begrippen 'verkeersgegevens' en 'locatiegegevens' zijn opgenomen in art 11 1, onder c en d (zie art 11 1, aant 4 en 5) Aan de hand van dergelijke locatiegegevens niet zijnde verkeersgegevens kunnen diverse soorten toegevoegde waardediensten aan de gebruiker worden geleverd Tegelijkertijd kunnen deze gegevens een bedreiging vormen voor de persoonlijke levenssfeer van de gebruiker, aangezien dergelijke gegevens een nauwkeurige indicatie kunnen geven waar een eindgebruiker (althans diens randapparaat) op welk moment was Met het oog op de privacybescherming van abonnees en gebruikers vereist dit dan ook aanvullende normering (MvT, Kamerstukken II 2003/04, 28 851, nr 3, p 46) *Afzonderlijke regeling naast die van verkeersgegevens* Het artikel heeft geen betrekking op de locatiegegevens die tevens verkeersgegevens zijn (ofwel de locatiegegevens die worden verwerkt voor het overbrengen van communicatie over het netwerk) en waarvoor art 11 5 de relevante regels geeft De reden om voor locatiegegevens niet zijnde verkeersgegevens een afzonderlijke regeling op te nemen houdt verband met de omstandigheid dat voor deze gegevens in het netwerk specifieke voorzieningen moeten worden getroffen, waardoor deze veel nauwkeuriger kunnen zijn dan verkeersgegevens Anders dan verkeersgegevens die betrekking hebben op netwerkcellen met een omvang van veelal honderden meters, kunnen dergelijke locatiegegevens de locatie van de gebruiker met een nauwkeurigheid van een tiental meters worden bepaald Deze locatiegegevens zullen vaak uitsluitend worden gebruikt voor de levering van toegevoegde waardediensten En daarbij geldt dat hoe nauwkeuriger de locatiegegevens zijn, hoe specifieker en meer op de situatie van de desbetreffende abonnee of gebruiker toegesneden de desbetreffende toegevoegde waarde dienst kan zijn Een en ander betekent dat deze locatiegegevens veel meer inzicht kunnen geven in de exacte locatie van gebruiker (althans diens het randapparaat) en het mogelijk maken om deze gebruiker 'in real time' te volgen Dit betekent dat aan de verwerking van deze gegevens verdergaande eisen moeten worden gesteld die erop zijn gericht om de persoonlijke levenssfeer van de desbetreffende abonnees en gebruikers zo optimaal mogelijk te beschermen (MvT, Kamerstukken II 2003/04, 28 851, nr 3, p 157)

2. Verwerking van locatiegegevens, niet zijnde verkeersgegevens (lid 1, onder a en b). De locatiegegevens waar het artikel betrekking op heeft mogen alleen onder strikte voorwaarden worden verwerkt Het uitgangspunt is dat de gegevens alleen in niet-geanonimiseerde vorm mogen worden verwerkt voorzover dat nodig is voor de levering van toegevoegde waardediensten, en dan alleen als de gebruiker of abonnee waarop de gegevens betrekking hebben, daarvoor toestemming heeft verleend Verder

moet aan de gebruiker of abonnee de mogelijkheid worden geboden om op een eenvoudige en kosteloze wijze tijdelijk de verwerking van diens locatiegegevens te beletten (MvT, Kamerstukken II 2003/04, 28 851, nr 3, p 46-47) *Toestemming* Het begrip toestemming is gedefinieerd in art 11 1, onder g, en sluit aan bij de definitie van art 1, onder i, Wbp Het moet gaan om een vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt Zoals ook blijkt uit het vierde lid kan de toestemming te allen tijde worden ingetrokken (zie aant 5 en art 11 1, aant 8 en art. 1, onder i, Wbp, aant 10f en en art. 5, tweede lid, Wbp, aant 2) Of de toestemming van de abonnee of van de gebruiker moet worden verkregen, hangt af van de te verweiken gegevens en de aard van de te leveren toegevoegde waardedienst, alsmede van de technische procedurele en contractuele mogelijkheden om onderscheid te maken tussen de persoon die gebruik maakt van de dienst (de gebruiker) en degene die daarvoor een overeenkomst heeft gesloten (de abonnee) (overw 31 Richtlijn privacy en elektronische communicatie, MvT, Kamerstukken II 2003/04, 28 851, nr 3, p 157)

3. Informatieplicht (lid 2). Voorafgaand aan het verkrijgen van de in het eerste lid genoemde toestemming van de abonnee of gebruiker, dient de aanbieder van de dienst met toegevoegde waarde aan de abonnee of gebruiker de volgende informatie te hebben verstrekt: de soort locatiegegevens die zullen worden verwerkt, de doeleinden waarvoor de locatiegegevens worden verwerkt, de duur van de verwerking en, voorzover van toepassing, of de gegevens aan een derde zullen worden verstrekt voor de levering van de dienst met toegevoegde waarde

4. Verwerking ten behoeve van de levering en facturering van de toegevoegde waardedienst (lid 3). Als de abonnee of gebruiker toestemming heeft gegeven voor de verwerking van de gegevens ten behoeve van de levering van een toegevoegde waardedienst, is deze verwerking alleen toegestaan voorzover en voor zolang dat noodzakelijk is voor de levering van de desbetreffende dienst Na de levering van de dienst moet de verwerking worden gestaakt, met de (vanzelfsprekende) uitzondering dat de gegevens nog wel mogen worden gebruikt voorzover dat nodig is voor het opstellen van factuur *Opstellen van factuur* Met betrekking tot de in het artikel bedoelde locatiegegevens wordt verwerking strikt genomen alleen toegestaan voor het opstellen van de factuur, en niet zoals in art 11 5, tweede lid, is bepaald voor het ruimer omschreven verwerkingsdoel van 'de 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' Het is evenwel met aannemelijk dat de wetgever wat dat betreft een onderscheid heeft willen maken, zodat kan worden aangenomen dat de gegevens zonodig ook mogen worden gebruikt voor eventuele andere factureringsdoeleinden dan het opstellen van de factuur (MvT, Kamerstukken II 2003/04, 28 851, nr 3, p 80, NVII, Kamerstukken II 2003/04, 28 851, nr 3, p 80, NvW, Kamerstukken II 2003/04, 28 851, nr 13, p 19) *Duur van de verwerking* Met betrekking tot de duur van de verwerking voor dit doel is art 11 5, derde lid, laatste volzin, van overeenkomstige toepassing Dit betekent 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 Daarbij wordt opgemerkt dat dit niet betekent 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 en 157-158) Zie art 11 5, aant 3a.

5. Intrekking toestemming (lid 4). De abonnee of gebruiker kan de in het eerste lid vereiste toestemming voor de verwerking van de locatiegegevens te allen tijde intrekken (MvT, Kamerstukken II 2003/04, 28 851, nr 3, p 157) Voorzover het persoonsgegevens betreft is dit ook bepaald in art 5, tweede lid, Wbp (zie aant 2 en art. 5 Wbp, aant 2)

6. Mogelijkheid om gegevensverwerking tijdelijk te beletten (lid 5). De aanbieder van een dienst met toegevoegde waarde moet de abonnee of gebruiker wiens gegevens worden verwerkt, de mogelijkheid bieden om kosteloos en op eenvoudige wijze de verwerking van diens gegevens tijdelijk te beletten voor elke overbrenging van communicatie of elke verbinding met het elektronisch communicatienetwerk dat voor de levering van de desbetreffende dienst wordt gebruikt Anders dan bij het in het vierde lid vastgelegde recht van de abonnee of gebruiker om de toestemming tot verwerking te allen tijde in te kunnen trekken, waarmee de verwerking van de locatiegegevens, niet zijnde verkeersgegevens, permanent wordt belet, gaat het hier om een tijdelijke onderbreking, waarbij de abonnee of gebruiker tijdelijk geen dienst met toegevoegde waarde wenst te ontvangen (MvT, Kamerstukken II 2003/04, 28 851, nr 3, p 158) *Wel verstrekking aan beheerder van alarmnummer* De gegevens moeten altijd worden verstrekt aan de aangewezen beheerders van een alarmnummer voor publieke diensten, zoals bedoeld in art 11 10, eerste lid, als er communicatie over een dergelijk alarmnummer wordt afgewikkeld Dit moet ook als de abonnee of gebruiker gebruik heeft gemaakt van de mogelijkheid om tijdelijk de verwerking van de hem betreffende locatiegegevens te beletten Zie art 11 10, aant 3

7. Verwerking alleen door personen werkzaam onder gezag aanbieder (lid 6). De locatiegegevens waar het artikel op ziet mogen alleen worden verwerkt door personen die werkzaam zijn onder het gezag van de aanbieder of de derde aan wie de gegevens worden verstrekt ten behoeve van de levering van de toegevoegde waardedienst, bedoeld in het derde lid, onder d De verwerking is beperkt tot die gegevens die noodzakelijk zijn om de dienst met toegevoegde waarde te kunnen aanbieden (MvT, Kamerstukken II 2003/04, 28 851, nr 3, p 158, zie art. 11 5, aant 4) *Werkzaam onder gezag van de aanbieder* Evenals bij de regeling voor de verwerking van verkeersgegevens in art 11 5 is met precies duidelijk wat wordt bedoeld met 'werkzaam onder het gezag' 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 A12) 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 Wbp, aant 5 en 6). *Noodzakelijkheid* De verwerking moet beperkt blijven tot hetgeen noodzakelijk is om de toegevoegde waardediensten te kunnen leveren en te factureren Zie aant 4

8. Uitzonderingen in verband met nationale veiligheid en opsporing strafbare feiten. In eerste lid van art 11 13 staat dat aanbieders zonodig in het belang van de nationale veiligheid of ter voorkoming, opsporing en vervolging van strafbare feiten, de regeling van locatiegegevens in het artikel buiten toepassing kunnen laten 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 In het tweede lid is bepaald dat aanbieders bevoegd zijn om, in afwijking van het artikel locatiegegevens 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

[Verwerking persoonsgegevens door certificatiedienstverleners elektronische handtekeningen]

Artikel 11.5b. — 1. Certificatiedienstverleners die certificaten aan het publiek afgeven, verwerken alleen persoonsgegevens die van de betrokkene zelf of met diens uitdrukkelijke toestemming zijn verkregen, en voor zover de verwerking van deze persoonsgegevens voor de afgifte en het beheer van het certificaat is vereist.

— 2. De in het eerste lid bedoelde persoonsgegevens worden niet voor andere doeleinden verzameld of verwerkt, tenzij de betrokkene daarvoor zijn uitdrukkelijke toestemming heeft gegeven.

— 3. In afwijking van het tweede lid is de uitdrukkelijke toestemming van de betrokkene niet vereist, indien de verwerking van de in het eerste lid bedoelde persoonsgegevens noodzakelijk is ten behoeve van de opsporing van fraude, of indien de verwerking overigens bij of krachtens de wet wordt gevorderd.

Betekenis. Het artikel implementeert art 8, tweede lid, van de Richtlijn elektronische handtekeningen (bijlage A8) en bepaalt dat certificatiedienstverleners alleen persoonsgegevens mogen verwerken die van de betrokkene (in de zin van art 1, onder f, Wbp) zelf of met diens uitdrukkelijke toestemming zijn verkregen, en dan alleen voorzover de afgifte en het beheer van het certificaat dit vereisen Verdere verwerking van deze gegevens, zoals voor het opmaken en versturen van nota's, is alleen toegestaan als de betrokkene daarvoor uitdrukkelijk toestemming heeft gegeven Het artikel is opgenomen in de wet omdat het verder gaat dan de bepalingen over het verwerken en verkrijgen van persoonsgegevens in de Wbp (met name art 8 en 9 Wbp) De regel dat uitdrukkelijke toestemming is vereist lijdt alleen uitzondering als het verwerken van de bij de certificatiedienstverlener bekende gegevens noodzakelijk is voor het opsporen van fraude alsmede in die gevallen dat de medewerking van de certificatiedienstverlener op grond van een bij of krachtens de wet gegeven bevoegdheid wordt gevorderd (MvT, Kamerstukken II 27 743, nr 3, p 11-12 en 21) *Uitdrukkelijke toestemming* Aan de toestemming worden verdergaande eisen gesteld dan aan de toestemming van de art 11 5, 11 5a, 11 6 en 11 7 Aan het uitdrukkelijkheidsvereiste is voldaan als de betrokken abonnee expliciet zijn wil omtrent de verwerking heeft geuit De abonnee dient in woord, schrift of gedrag uitdrukking te hebben gegeven aan zijn wil toestemming te geven voor de gegevensverwerking (MvT, Kamerstukken II 27 743, nr 3, p 65-66 en 122-123, zie art 23 Wbp, aant 2)

[Algemeen beschikbare abonneelijsten en abonee-informatiediensten]

Artikel 11.6. — 1. Eenieder die een algemeen beschikbare abonneelijst uitgeeft of een algemeen beschikbare abonnee-informatiedienst verzorgt, stelt de abonnee voorafgaand aan opneming van hem betreffende persoonsgegevens in de abonneelijst of in het voor de abonnee-informatiedienst gebruikte abonneebestand kosteloos op de hoogte van:

***a.* de doeleinden van de desbetreffende abonneelijst en de desbetreffende abonnee-informatiedienst en, voor zover het een elektronische versie van de abonneelijst betreft, van de gebruiksmogelijkheden op basis van daarin opgenomen zoekfuncties, en**

***b.* de soorten persoonsgegevens die, gelet op de vastgestelde doeleinden van de desbetreffende abonneelijst en desbetreffende abonnee-informatiedienst, daarin kunnen worden opgenomen.**

— 2. In een algemeen beschikbare abonneelijst en in het voor een abonnee-informatiedienst gebruikte abonneebestand worden uitsluitend persoonsgegevens van een abonnee opgenomen, indien de abonnee daarvoor toestemming heeft verleend en blijft deze beperkt tot de door hem daarbij aangegeven persoonsgegevens. Aan het niet opgenomen zijn in een abonneelijst of het voor een abonnee-informatiedienst gebruikte abonneebestand mogen geen kosten worden verbonden.

— 3. Voor zover de verwerking van persoonsgegevens in een algemeen beschikbare abonneelijst en in het voor een abonnee-informatiedienst gebruikte abonneebestand betrekking heeft op andere doeleinden dan het bieden van de mogelijkheid tot het zoeken van nummers aan de hand van gegevens betreffende de naam in combinatie met gegevens betreffende het adres en huisnummer, postcode en woonplaats van de abonnee, is met betrekking tot elk van die andere doeleinden afzonderlijke toestemming van de abonnee vereist.

— 4. De abonnee heeft het recht om kosteloos hem betreffende persoonsgegevens in een algemeen beschikbare abonneelijst of in het voor een abonnee-informatiedienst gebruikte abonneebestand te verifiëren, te laten verbeteren of te laten verwijderen.

1. Algemeen. Het artikel implementeert art. 12 Richtlijn privacy en elektronische communicatie (bijlage A5), dat regels geeft voor abonneelijsten *Abonneelijst en abonnee-informatiedienst* De begrippen 'abonneelijst' en 'abonnee-informatiedienst' worden niet gedefinieerd De 'abonneelijst' is een synoniem voor de telefoongids (NvT, art. 3.1 BU-DE, p. 11) Het betreft niet alleen de traditionele telefoongids maar ook de gedrukte of elektronische gidsen (op CD-rom of internet) waarin adressen voor elektronische post en andere contactgegevens van abonnees zijn opgenomen. Dit blijkt uit overweging 38 van de richtlijn waarin wordt gesproken van abonneelijsten van elektronische communicatiediensten (MvT, Kamerstukken II 2002/03 28 851, nr. 3, p. 158). De abonnee-informatiedienst betreft in elk geval de dienst waar men het nummer van gebruikers kan opvragen, zoals bijvoorbeeld het informatienummer '118' (MvT, Kamerstukken II 2002/03, 28 851, nr. 3, p. 142) *Algemeen beschikbaar.* Het moet gaan om algemeen beschikbare abonneelijsten en abonnee-informatiediensten. Interne telefoongidsen of informatiediensten op een intranet van bedrijven en instellingen vallen dus niet onder de werking van het artikel *Geadresseerden* Het artikel legt verplichtingen op aan iedereen die een algemeen beschikbare abonneelijst uitgeeft of een algemeen beschikbare abonnee-informatiedienst verzorgt Dat is niet noodzakelijk een aanbieder van een elektro-

nische communicatiedienst of -netwerk Zo zijn de verplichtingen ook van toepassing op aanbieders die via internet een telefoongids met mobiele telefoonnummers aanbieden, waarin men zich op de desbetreffende website kan doen opnemen door het invullen van enkele gegevensvelden (MvT, Kamerstukken II 2002/03, 28 851, nr 3, p 158) *Alleen natuurlijke personen (art 11 8)* In art 11 8 heeft de wetgever gebruik gemaakt van de in art 12, vierde lid, Richtlijn privacy en elektronische communicatie geboden mogelijkheid om de werking van het artikel te beperken tot abonnees die natuurlijke personen zijn, zodat er geen toestemming nodig is voor het opnemen van gegevens van bedrijven Dit is gedaan om de aansluiting met de algemene privacyregelgeving van de Wbp zo veel mogelijk te handhaven (MvT, Kamerstukken II 1996/97, 25 533, nr 3, p 120, Parl Gesch , p 417-418, NV II, Kamerstukken II, 1997/98, 25 533, nr 5, p 128, Parl Gesch , p 427-428) Bij amendement is geprobeerd ook abonnees die geen natuurlijke personen zijn onder de werking van het artikel te brengen Dit amendement evenwel niet overgenomen, omdat bedrijven in het algemeen juist zo goed mogelijk telefonisch vindbaar willen zijn en er volgens de regering geen signalen waren van het bedrijfsleven dat men zit te wachten om onder de werking van het artikel te worden gebracht (Kamerstukken II 2002/03, 28 851, nr 18, Handelingen II 2002/03, p 14-789)

2. Informatieplichten (lid 1). Aanbieders van abonneelijsten en abonnee-informatiediensten zijn verplicht om de desbetreffende abonnees te informeren over de gegevens die over hen worden opgenomen en wat daarmee gebeurt Voorzover het gaat om abonneelijsten of abonnee-informatiedienst(en) van een aanbieder van een elektronische communicatiedienst kan deze informatie worden verstrekt op het moment dat deze abonnee de overeenkomst terzake van de desbetreffende diensten aangaat Zo kan een mobiele aanbieder zijn nieuwe abonnees informeren op het moment dat deze een abonnement aangaat Abonneelijst- of informatiedienstaanbieders die met ook elektronische communicatiediensten aanbieden zouden ofwel zelf de abonnees kunnen informeren ofwel daarover afspraken maken met de aanbieders van elektronische communicatiediensten *Wet bescherming persoonsgegevens (Wbp)* Het artikel geeft invulling aan de in de art 33 en 34 Wbp opgenomen verplichtingen van de verantwoordelijke om degene op wie de gegevens betrekking hebben, informatie te verstrekken over (onder andere) de doeleinden van gegevensverwerkingen (zie art 33 Wbp, aant 3 en 4 en art 34 Wbp, aant 3 en 4) **a) Doeleinden en gebruiksmogelijkheden (onder a).** Voordat persoonsgegevens van de abonnee worden opgenomen, moet de abonneelijst- of abonnee-informatiedienstaanbieder deze abonnee kosteloos op de hoogte te stellen van de doeleinden van de abonneelijst of abonnee-informatiedienst Voorzover het een elektronische versie van de abonneelijst (cd-rom of internetdienst) betreft moet hij de abonnee ook op de hoogte stellen van de gebruiksmogelijkheden op basis van de opgenomen zoekfuncties Dit laatste omdat, anders dan bij de gedrukte versie van een abonneelijst (de traditionele telefoongids) bij een elektronische versie meer zoekmogelijkheden kunnen worden geboden Gedacht moet worden aan omgekeerde zoekmogelijkheden ('reversed search') waarbij bijvoorbeeld naw-gegevens gegevens kunnen worden gevonden aan de hand van een telefoonnummer Ook als de gegevens in de abonneelijst of abonnee-informatiedienst aan derden kunnen worden verstrekt, moet de abonnee daarvan op de hoogte worden gesteld (MvT, Kamerstukken II 2002/03, 28 851, nr 3, p 159, NV II, Kamerstukken II 2002/03, 28 851, nr 7, p 80-81) **b) Soorten persoonsgegevens (b).** Verder moet de abonnee op de hoogte worden gesteld van de soorten persoonsgegevens die, gelet op de doeleinden van de desbetreffende abonneelijst of abonnee-informatiedienst, daarin kunnen worden opgenomen

3. Toestemming voor opneming gegevens (lid 2). Er geldt een 'opt-in' regime, en daarmee een recht op een 'geheim nummer'. De gegevens mogen alleen worden opgenomen in de abonneelijst of abonnee-informatiedienst voorzover de abonnee daarvoor toestemming heeft gegeven En de gegevens die worden opgenomen, zijn beperkt tot die welke de abonnee heeft aangegeven Als de abonnee niet wil worden opgenomen in de abonneelijst of de abonnee-informatiedienst mogen daaraan geen kosten zijn verbonden Echter, desgewenst kan de aanbieder van de abonneelijst of abonnee-informatiedienst een vergoeding vragen voor het wél opnemen van gegevens Overigens hebben de abonnees waaraan telefoonnummers zijn toegekend, op grond van art 2 3 BUDE (bijlage C13) ook het recht op vermelding van hun gegevens in de gedrukte en elektronische universele abonneelijst cq telefoongids (zie art 9.1, aant 2, MvT, Kamerstukken II 2002/03, 28 851, nr 3, p 159-160). *Toestemming* Het begrip 'toestemming' betreft elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem of haar betreffende persoonsgegevens worden verwerkt Zie art 11 1, aant 8 *Voor opneming in standaardgids toestemming gevraagd door telefoonaanbieders (art 3 2 BUDE)* In art 3 2 BUDE is een regeling getroffen met betrekking tot het verkrijgen van toestemming voor het opnemen van gegevens in zogeheten 'standaard abonneelijsten' en 'standaard abonnee-informatiediensten' Uit art. 1 1, onder d en e, BUDE blijkt dat daaronder worden verstaan de abonneelijsten en abonnee-informatiediensten die alleen de mogelijkheid bieden tot het zoeken van telefoonnummers aan de hand van naw-gegevens van de abonnee (dus geen omgekeerde zoekmogelijkheden of mogelijkheden om te zoeken naar andere nummers dan telefoonnummers). Met betrekking tot deze standaardabonneelijsten en informatiediensten wil de wetgever voorkomen dat iedere abonneelijst- en abonnee-informatiedienstaanbieder aan iedere abonnee afzonderlijk toestemming moet vragen voor het opnemen van de gegevens Om deze reden wordt in art. 3 2 BUDE aan aanbieders van openbare telefoondiensten een verplichting opgelegd, die inhoudt dat als zo een aanbieder voor of bij het sluiten van een overeenkomst de naam, het adres en huisnummer, postcode en woonplaats van de abonnees vraagt, hij tevens aan deze abonnee moet vragen of deze gegevens en zijn telefoonnummer(s) in een algemeen beschikbare telefoongids of abonnee-informatiedienst mogen worden opgenomen De desbetreffende aanbieder mag dus niet alleen toestemming vragen voor opname in zijn eigen telefoongids of abonnee-informatiedienst, maar moet in algemene zin toestemming vragen voor opname in alle (standaard)abonneelijsten en abonnee-informatiediensten Een aanbieder van een standaard abonneelijst of abonnee-informatiedienst kan deze toestemming vervolgens 'opvragen' bij de aanbieder van de openbare telefoondienst en behoeft dan zelf geen toestemming meer te vragen van de betrokken abonnees voor opname in zijn abonneelijst of abonnee-informatiedienst Daarbij wordt opgemerkt dat deze regeling niet af doet aan de informatieplicht van het eerste lid (NvT, BUDE, Stb 2004, 203, p 11) (zie aant 2) *Relatie met het 'nota-afschermingsrecht' en nummeridentificatie* De opt-in regeling met betrekking tot de opneming van abonneegegevens in de abonneelijst en abonnee-informatiedienst vormt een logisch complement op het in art 4 2 BUDE geregelde 'nota-afschermingsrecht' en de in art 11 9, tweede lid, onder a, opgenomen mogelijkheid voor de oproepende abonnee en gebruiker om de weergave van het nummer te blokkeren Zie resp art 11.4, aant 3 en art. 11.9, aant 2a

4. Afzonderlijke toestemming voor verdergaande doeleinden (lid 3). Als de abonneegegevens worden gebruikt voor andere doeleinden dan het zoeken van een nummer aan de hand van naw-gegevens, wordt verlangd dat de desbetreffende abonnee daarvoor aanvullend toestemming verleent Dit betekent dat voor het opnemen van de

gegevens in een abonneelijst die 'omgekeerd zoekmogelijkheden' bevatten afzonderlijk toestemming moet worden gevraagd en verkregen Hetzelfde geldt als de gegevens aan derden worden verstrekt (overw 39 Richtlijn privacy en elektronische communicatie (bijlage A5), MvT, Kamerstukken II 2002/03, 28 851, nr 3, p 84 en 159) Deze afzonderlijke toestemming moet worden onderscheiden van de toestemming die openbare telefoonaanbieders op grond van art 3 2 BUDE (bijlage C13) moeten vragen Deze laatste toestemming heeft immers geen betrekking op andere doeleinden dan het opnemen van gegevens in een standaardabonneelijst of abonnee-informatiedienst die alleen de mogelijkheid bieden tot het zoeken van nummers aan de hand van naw-gegevens van de abonnee

5. Verificatie-, verbeterings- en verwijderingsrecht (lid 4). De abonnee heeft het recht om kosteloos de hem betreffende persoonsgegevens in een algemeen beschikbare abonneelijst of in het voor een abonnee-informatiedienst gebruikte abonneebestand te verifiëren, te laten verbeteren of te laten verwijderen Dit recht sluit aan bij de verbeterings- en verwijderings- of afschermingsrechten van art 36 Wbp (zie art 36 Wbp, aant 1)

6. Overgangsrecht. In art 16 Richtlijn privacy en elektronische communicatie (bijlage A5) worden enkele overgangsbepalingen voor abonneelijsten en abonnee-informatiediensten geformuleerd Deze zijn geïmplementeerd in art 19 10 De regeling komt erop neer dat het artikel niet geldt voor reeds gereed zijnde duurzame publicaties van abonneelijsten, zoals gedrukte telefoongidsen en elektronische abonneelijsten die anders dan on-line worden aangeboden (cd-rom) Voor persoonsgegevens die reeds worden verwerkt op het moment van inwerkingtreding van het artikel wordt van aanbieders van algemeen beschikbare abonneelijsten en abonnee-informatiediensten niet verlangd dat zij voldoen de informatieplicht van het eerste lid en de toestemming van het tweede lid verkrijgen Met het oog op verwerking van persoonsgegevens die reeds in de abonneelijsten en abonneebestanden zijn opgenomen op het moment van inwerkingtreding, moet aan de desbetreffende abonnees binnen zes maanden de informatie als bedoeld in het eerste lid worden verstrekt Voor de (verdere) verwerking van deze gegevens is geen toestemming vereist, maar kan de abonnee tegen (verdere) verwerking verzet aantekenen Zie aantekening bij art 19 10

[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 lid.

— 2. 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, ideële 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 ge-

boden 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.

— 3. 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.**

— 4. 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, tenzij de desbetreffende abonnee te kennen heeft gegeven dat hij communicatie waarbij van deze middelen gebruik wordt gemaakt, niet wenst te ontvangen en indien de abonnee bij elke overgebrachte communicatie de mogelijkheid wordt geboden om verzet aan te tekenen tegen het verder gebruik van zijn elektronische contactgegevens. Aan de abonnee worden in dat geval geen kosten in rekening gebracht van voorzieningen waarmee wordt voorkomen dat hem een ongevraagde communicatie wordt overgebracht.

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 *Commerciele, ideele of charitatieve doeleinden* Het artikel spreekt over communicatie voor commerciele, ideële of charitatieve doeleinden Met de terminologie wordt beoogd aan te sluiten bij art 435c 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 ideeel 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 werving (NMvA I, Kamerstukken I 1997/98, 25 533, nr 309d, p 6, Parl Gesch , p 450, 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 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. *Alleen natuurlijke personen (art 11 8)* In art 11 8 heeft de wetgever gebruik gemaakt van de in art 13, vijfde lid, Richtlijn privacy en elektronische communicatie geboden mogelijkheid om de werking van het artikel te beperken tot abonnees die natuurlijke personen zijn. Dit is gedaan om de aansluiting met de algemene privacyregelgeving van de Wbp zo veel mogelijk te handhaven (MvT, Kamerstukken II 1996/97, 25 533, nr 3, p 120, Parl Gesch , p 417-418, NV II, Kamerstukken II, 1997/98, 25 533, nr 5, p 128, Parl Gesch , p 427-428) Bij amendement is geprobeerd de werking van het artikel uit te breiden tot communicatie naar abonnees die geen natuurlijke personen zijn, zodat ook ongevraagde e-mail naar bedrijven onder het opt-in regime zou vallen Daarnaast is voorgesteld om ook ongevraagde communicatie naar gebruikers (natuurlijke personen, niet noodzakelijk abonnees) onder de werking van het artikel te brengen, waarmee het opt-in regime ook zou gelden voor

ongevraagde communicatie aan werknemers De desbetreffende amendementen zijn niet overgenomen omdat de regering geen signalen had ontvangen dat ongevraagde communicatie (m n reclame e-mail of spam) voor het bedrijfsleven een probleem zou zijn (Kamerstukken II 2002/03, 28 851, nrs 18 en 42, Handelingen II 2003/04, p 14-789) *Bestuursrechtelijke handhaving* Op grond van art 15 1, derde lid, is OPTA bevoegd tot handhaving van het artikel Voor klachten over reclame die in grote hoeveelheden per e-mail, sms of mms wordt verstuurd ('spam') heeft OPTA een website beschikbaar gesteld waar particuliere abonnees terecht kunnen voor het indienen van klachten www spamklacht nl Daarnaast is het Cbp bevoegd terzake van de naleving van de Wbp (zie Inl opm bij dit hoofdstuk, aant 4) *Strafrechtelijke handhaving* Alleen overtreding van de informatieplicht van het derde 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 derde lid, teveel onbepaalde en onbestemde elementen bevat, waardoor er sprake zou zijn van symboolwetgeving (Amend , Kamerstukken II 2002/03, 28 851, nr 16, Handelingen II 2003/004, p 14-790) *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 tussenkomt, 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 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) *Communicatiemiddelen* Deze in 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 Zie voor een analyse van verschillende spam-technieken Lodder e a , Spam, spammer , ITeR-reeks deel 68, Den Haag 2004 *Elektronisch bericht* Het begrip 'elektronisch bericht' wordt in art 11 1, onder r, 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 (zie art 11 1, aant 10) *XS4ALL-Abfab-procedures* Voor de inwerkingtreding van de Wet implementatie Europees regelgevingskader voor elektronische communicatiesector 2002 werd het begrip ' elektronische post niet in het artikel genoemd Dit leidde tot de vraag of een programma dat grote hoeveelheden reclame e-mailberichten uitstuurt ('spam') als automatisch oproepsysteem moest worden aangemerkt, zodat het onder het strenge opt-in regime zou vallen Het Hof Amsterdam beantwoordde deze rechtsvraag ontkennend, hetgeen (voorzover het

deze vraag betrof) door de Hoge Raad werd bevestigd Zie resp. Hof Amsterdam 18 juni 2002, LJN AE5514 en HR 12 maart 2004, LJN AN8483 (zie ook art. 8 Wbp, aant. 1f). *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, p 14-788)

3. Elektronische contactgegevens van bestaande klanten (lid 2). Het tweede lid betreft een specifieke voorziening voor het gebruik van zogeheten elektronische contactgegevens voor elektronische berichten die in het kader van een bestaande klantrelatie, namelijk bij de verkoop van een product of dienst, zijn verkregen 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 mmsberichten voor direct marketing doeleinden *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). *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 tweede lid wordt aangemerkt als een (beperkte) verzachting van de harde opt-in regel uit het eerste lid. 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 betekenis toe aan de informatie die is verstrekt bij de aankoop van de producten of diensten (NV, Kamerstukken II 2002/03, 28 851, nr. 7, p 42) *Opt-out* Bij de verzameling 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 Als het gaat om telemarketing moet dit dus in elk gesprek tussen telemarketeer en de abonnee worden aangegeven (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)

4. Informatieplicht (lid 3). 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 pseu-

domein 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 art. strafbaar te stellen, is niet overgenomen, omdat dat zou kunnen leiden tot verstopping van het opsporingsapparaat Verder meende de regering dat het art , 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

5. Opt-out voor andere middelen (lid 4). Er geldt een opt-out regime voor het gebruik van andere dan de in het eerste lid van het artikel genoemde middelen voor het overbrengen van ongevraagde communicatie voor commerciele, ideele of charitatieve doeleinden Van deze andere middelen mag gebruik worden gemaakt, tenzij de desbetreffende abonnee daartegen bezwaar heeft gemaakt Bij deze andere middelen kan in elk geval worden gedacht aan allerlei vormen van telemarketing, zoals de krantenverkoper die meestal tegen etenstijd belt met een aanbieding voor een proefabonnement De abonnee moet bij elke overgebrachte communicatie (dus in voorkomend geval in het gesprek tussen telemarketeer en de abonnee) een opt-out mogelijkheid worden geboden (MvA I, Kamerstukken I 2003/04, 28 851, C, p 23-24)

[Toepassing art. 11.6 en 11.7 beperkt tot natuurlijke personen]

Artikel 11.8. *De toepassing van de artikelen 11.6 en 11.7 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 11 7 (ongevraagde oproepen) 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, Pail Gesch , p 417-418) Bij amendement is geprobeerd het artikel te doen schrappen, teneinde de werkingsfeer van de art 11 6 en 11 7 uit te breiden tot abonnees, met zijnde natuurlijke personen De desbetreffende amendementen zijn evenwel niet overgenomen (Kamerstukken II 2002/03, 28 851, nrs 18 en 42, Handelingen II 2003/04, p 14-789, zie art 11 6, aant 1 en art 11 7, aant 1)

§ 11 2 Nummeridentificatie

[Nummeridentificatie]

Artikel 11.9. — 1. De aanbieder van een openbaar elektronisch communicatienetwerk en de aanbieder van een openbare elektronische communicatiedienst die door middel van dat netwerk of als onderdeel van die dienst nummeridentificatie aanbiedt, biedt:

a. aan iedere oproepende gebruiker onderscheidenlijk abonnee mogelijkheden aan om kosteloos de verstrekking van het nummer van het oproepende netwerkaansluitpunt dan wel een nummer waarmee een individuele gebruiker kan worden geïdentificeerd te blokkeren onderscheidenlijk de verstrekking van nummers van oproepende netwerkaansluitpunten dan wel nummers waarmee individuele gebruikers kunnen worden geïdentificeerd voor elke afzonderlijke abonneelijn te blokkeren;

b. aan iedere opgeroepen abonnee mogelijkheden aan om:

1° de verstrekking van het nummer van het oproepende netwerkaansluitpunt dan wel een nummer waarmee een individuele gebruiker kan worden geïdentificeerd te verhinderen;

2° oproepen waarbij de verstrekking van het nummer van het oproepende netwerkaansluitpunt dan wel een nummer waarmee een individuele gebruiker kan worden geïdentificeerd is geblokkeerd, te weigeren;

3° indien nummeridentificatie als bedoeld in artikel 1.1, onderdeel cc, onder 2°, wordt aangeboden, kosteloos de verstrekking van het nummer van het opgeroepen netwerkaansluitpunt dan wel een nummer waarmee een individuele gebruiker kan worden geïdentificeerd aan het oproepende netwerkaansluitpunt te blokkeren.

— 2. Bij ministeriële regeling worden nadere regels gesteld met betrekking tot:

a. mogelijkheden tot blokkering en weigering;

b. de voorwaarden waaronder de abonnee de identificatie van het nummer van oproepende netwerkaansluitpunten dan wel een nummer waarmee een individuele gebruiker kan worden geïdentificeerd kan doen verhinderen;

c. de wijze waarop uitvoering aan nummeridentificatie in het internationale elektronische communicatieverkeer kan worden gegeven, en

d. de wijze waarop de aanbieders gebruikers en abonnees voorlichten over het gebruik van nummeridentificatie.

1. Algemeen. Het artikel implementeert art 8 Richtlijn privacy en elektronische communicatie (Bijlage A5) en stelt regels voor nummeridentificatie ('calling line identification' afgekort 'CLI'), een faciliteit die standaard wordt aangeboden in digitale netwerken (zoals ISDN, GSM en UMTS) maar ook wel in analoge netwerken en bepaalde randapparatuur Het begrip wordt in art 1 1, onder cc, gedefinieerd Het betreft de faciliteit die erin bestaat dat het nummer van de opgeroepen of het oproepende netwerkaansluitpunt — voordat de verbinding tot stand komt — zichtbaar wordt gemaakt op het beeldscherm of afleesvenster van het desbetreffende telefoontoestel of andere randapparaat waarvan gebruik wordt gemaakt (zie art 1 1, onder cc, aant 25) Voor de bescherming van persoonsgegevens en de persoonlijke levenssfeer is nummeridentificatie met name van belang omdat het de opgeroepene in staat stelt geautomatiseerd het nummer vast te leggen waarvan gebruik wordt gemaakt om hem te bellen (MvT, Kamerstukken II 27 576, nr 3, p 8, MvT, Kamerstukken II 1997/98, 25 533, nr 3, p 121-122, NV II, Kamerstukken II 1997/98, 25 533, nr 5, p 124-125, 129, Pail Gesch , p 456)

2. Rechten met betrekking tot nummerblokkering (lid 1). Het artikel legt in algemene zin verplichtingen op aan alle aanbieders van elektronische communicatienetwerken en -diensten die nummeridentificatie aanbieden Op grond van art 11 12 kan OPTA evenwel in individuele gevallen ontheffing van deze verplichtingen verlenen

Deze ontheffingsbevoegdheid is geclausuleerd. Overeenkomstig art 3, tweede lid, Richtlijn privacy en elektronische communicatie (bijlage A5) is ontheffing uitsluitend mogelijk, als deze betrekking heeft op abonneelijnen verbonden met analoge centrales, en nakoming van de desbetreffende verplichtingen technisch niet haalbaar is of onevenredig veel financiële lasten voor de aanbieder met zich meebrengt. OPTA kan een ontheffing onder beperkingen verlenen en kan daaraan voorschriften verbinden (MvT, kamerstukken II 2002/03, 28 851, nr. 3, p. 162 (zie aant. bij art. 11.12). **a) Rechten van oproepende abonnee en gebruiker (onder a).** De aanbieders moeten ervoor zorgdragen dat oproepende abonnees en gebruikers kosteloos de mogelijkheid wordt geboden de nummeridentificatie te blokkeren. De abonnee of gebruiker die de oproep doet, kan zo voorkomen dat het nummer waarvandaan hij de oproep doet, wordt bekend gemaakt aan degene die wordt opgeroepen. Deze verplichting geldt voor elke afzonderlijke abonneelijn ('per line blocking'; NV II, Kamerstukken II 2002/03, 28 851, nr. 7, p. 81-82). *Relatie met 'het nota-afschermingsrecht' en 'geheime nummers'.* Een logisch complement van deze rechten van oproepende abonnees en gebruikers met betrekking tot nummeridentificatie betreft het 'nota-afschermingsrecht' van art. 4.2 BUDE en het recht op een 'geheim nummer' van art. 11.6, tweede lid (zie resp. art. 11.4, aant. 3 en art. 11.6, aant. 2). **b) Rechten van opgeroepen abonnee (onder b).** De opgeroepen abonnee heeft drie rechten met betrekking tot de nummeridentificatie, namelijk het recht om nummeridentificatie te blokkeren, het recht om geblokkeerde oproepen te weigeren, en het recht om de identificatie van het opgeroepen nummer te voorkomen. *Blokkering nummeridentificatie (1°).* Aan de abonnee moet de mogelijkheid worden geboden om ervoor te zorgen dat het nummer van degenen die hem oproepen, niet aan hem worden doorgegeven. De abonnee kan daarmee bewerkstelligen dat degenen die hem bellen anoniem blijven. Deze mogelijkheid tot blokkering van nummeridentificatie door de opgeroepen abonnee is met name van belang voor artsen, geestelijken en juridische bijstandsverleners. *Weigering oproepen met blokkering nummeridentificatie (2°).* Dit recht van de opgeroepen abonnee is het logische complement van het recht van het in het tweede lid, onder a, neergelegde recht van de oproepende gebruiker of abonnee om de nummeridentificatie te voorkomen. De abonnee moet de mogelijkheid worden geboden om oproepen te blokkeren waarvan de oproepende abonnee of gebruiker de nummeridentificatie heeft geblokkeerd. Dit stelt de opgeroepen abonnee in staat verschoond blijven van oproepen waarvan de herkomst onbekend is. Het belang daarvan ligt bijvoorbeeld bij abonnees die te maken hebben met telefoonterreur. *Blokkering nummeridentificatie opgeroepen nummer (3°).* Tenslotte moet de opgeroepen abonnee de mogelijkheid worden geboden om te voorkomen dat zijn eigen nummer wordt bekend gemaakt aan degene die de oproep maakt. Dit recht heeft betekenis voor het geval het gekozen nummer is doorgeschakeld naar een ander nummer of een elektronische postbus (MvT, Kamerstukken II 1996/97, 25 533, nr. 3, p. 120, Parl. Gesch., p. 127, 418-419).

3. Ministeriële regeling (lid 2). De in het tweede lid bedoelde nadere regels zijn neergelegd in de art. 4.1 tot en met 4.5 van de Regeling universele dienstverlening en eindgebruikersbelangen (RUDE) (bijlage C21). Daar is onder andere bepaald dat de aanbieders ervoor moeten zorgdragen dat onderscheiden faciliteiten eenvoudig te gebruiken zijn en dat daarover op genoegzame wijze informatie beschikbaar is. Ook is bepaald dat het blokkeren van nummeridentificatie (eerste lid, onder b, onderdeel 1°) kosteloos is, tenzij er sprake is van herhaald gebruik zonder redelijk doel, in welk geval de aanbieder een redelijke vergoeding in rekening mag brengen.

[Nummeridentificatie en gegevensverstrekking bij publiek alarmnummer]

Artikel 11.10. — 1. De aanbieder van een openbaar elektronisch communicatienetwerk en de aanbieder van een openbare elektronische communicatiedienst die nummeridentificatie aanbiedt, is verplicht aan de door Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties, in overeenstemming met Onze Minister, aangewezen beheerders van een alarmnummer voor publieke diensten, indien er elektronische communicatie met een alarmnummer wordt afgewikkeld, gelijktijdig:

***a.* het nummer van het oproepende netwerkaansluitpunt te verstrekken, ook indien bij dat netwerkaansluitpunt gebruik wordt gemaakt van een in artikel 11.9, tweede lid, onder *a*, bedoelde blokkeringsmogelijkheid;**

***b.* de naam, en de beschikbare adres-, postcode- en woonplaatsgegevens van de abonnee, dan wel de locatie van de openbare betaaltelefoon, die onder het desbetreffende nummer is aangesloten, te verstrekken.**

— 2. De aanbieder van een openbaar elektronisch communicatienetwerk en de aanbieder van een openbare elektronische communicatiedienst, die locatiegegevens kan verwerken omtrent abonnees of gebruikers, is verplicht aan de aangewezen beheerders van een alarmnummer voor publieke diensten, bedoeld in het eerste lid, indien er communicatie over een dergelijk alarmnummer wordt afgewikkeld, gelijktijdig de daarop betrekking hebbende locatiegegevens te verstrekken, ook indien de abonnee of gebruiker, voor zover het betreft de locatiegegevens als bedoeld in artikel 11.5*a*, op de voet van het vijfde lid van dat artikel, gebruik heeft gemaakt van de mogelijkheid om tijdelijk de verwerking van de hem betreffende locatiegegevens te beletten.

— 3. De verstrekte nummers, alsmede de in het eerste lid, onder *b*, en de in het tweede lid, bedoelde gegevens worden door de beheerders, bedoeld in het eerste lid, vastgelegd met het oog op de hulpverlening in noodsituaties of de bestrijding van het misbruik van een alarmnummer voor publieke diensten. De beheerders zijn verantwoordelijke in de zin van artikel 1, onderdeel *d*, van de Wet bescherming persoonsgegevens voor deze vastlegging.

— 4. Verstrekking van nummers en gegevens door de beheerder vindt slechts plaats met het oog op de hulpverlening in noodsituaties of de bestrijding van het misbruik van een alarmnummer voor publieke diensten. De beheerder is verantwoordelijke in de zin van artikel 1, onderdeel *d*, van de Wet bescherming persoonsgegevens voor deze verstrekkingen.

— 5. Verstrekking van nummers en gegevens met het oog op de hulpverlening in noodsituaties vindt slechts plaats aan de door Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties, in overeenstemming met Onze Minister, aangewezen publieke diensten belast met hulpverleningstaken.

— 6. Verstrekking van nummers en gegevens met het oog op de bestrijding van het misbruik van een alarmnummer voor publieke diensten vindt slechts plaats aan degene die op grond van artikel 141 of 142 van het Wetboek van Strafvordering is belast met de opsporing van strafbare feiten.

— 7. De termijn gedurende welke de nummers en gegevens door de beheerder worden bewaard bedraagt ten hoogste:

***a.* een maand indien de nummers en gegevens betrekking hebben op gevallen waarin kennelijk sprake is van een verzoek om hulpverlening in een noodsituatie;**

b. zes maanden indien de nummers en gegevens betrekking hebben op gevallen waarin kennelijk sprake is van misbruik van een alarmnummer voor publieke diensten;

c. 24 uur in alle overige gevallen.

— 8. De op grond van het eerste lid aangewezen beheerder vergoedt de kosten die zijn gemoeid met het verstrekken van de in het eerste lid, onder *a* en *b*, en de in het tweede lid bedoelde gegevens.

— 9. De bekendmaking van het besluit tot aanwijzing van de beheerders, bedoeld in het eerste lid, en de publieke diensten, bedoeld in het vierde lid, geschiedt door plaatsing in de *Staatscourant* door Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties.

— 10. De beheerders, bedoeld in het eerste lid, zijn bevoegd om ten behoeve van de controle op de effectiviteit van de hulpverlening in noodsituaties de bij het alarmnummer voor publieke diensten ingekomen oproepen vast te leggen en voor ten hoogste een maand te bewaren. Bij de vastlegging worden de datum en het tijdstip van de oproep geregistreerd.

1. Algemeen. Het artikel implementeert art 10, onder b, Richtlijn privacy en elektronische communicatie (bijlage A5) en treft ten behoeve van politie, brandweer en ambulancediensten een regeling voor de ongedaanmaking van de blokkering van nummeridentificatie Een dergelijke regeling stelt deze hulpdiensten in staat oproepen te beantwoorden die om wat voor reden dan ook voortijdig zijn afgebroken In aanvulling daarop voorziet het artikel in een niet in de richtlijn opgenomen regeling voor de vastlegging en het gebruik van abonnee- en andere gegevens (waaronder locatiegegevens) ter voorkoming van misbruik van alarmnummers Verder voorziet het artikel in een eveneens niet in de richtlijn opgenomen regeling die het mogelijk maakt gesprekken vast te leggen teneinde deze te gebruiken om in voorkomende gevallen de effectiviteit van de hulpverlening te reconstrueren en te controleren

2. Verplichtingen (lid 1). Het artikel legt verplichtingen op aan de in art 11 9 genoemde aanbieders die nummeridentificatie aanbieden (zie art 11 9, aant. 2) **a) Verstrekking nummer (lid 1, onder a).** De aanbieders zijn verplicht het nummer te verstrekken waar vandaan naar het alarmnummer wordt gebeld ongeacht de eventuele blokkering daarvan op grond van art 11 9, tweede lid, onder a **b) Verstrekking andere gegevens (lid 1, onder b).** De aanbieders zijn verder verplicht naam- en voorzover beschikbaar adres-, postcode- en woonplaatsgegevens van de desbetreffende abonnee te verstrekken Als de oproep wordt gedaan vanuit een openbare telefooncel, moet worden opgegeven waar deze telefooncel zich bevindt **c) Aangewezen beheerder van alarmnummers voor publieke diensten (lid 1, aanhef).** Het nummer en de andere gegevens moeten worden verstrekt aan de aangewezen beheerders van publieke alarmnummers De aanwijzing heeft plaatsgevonden in het Besluit 1-1-2 alarmcentrales (Stb 1998, 235) Aangewezen zijn de korpsbeheerders, bedoeld in art 23 Politiewet 1993, en de Minister van Justitie als beheerder van het Korps landelijke politiediensten *Alarmnummer voor publieke diensten* Het begrip 'alarmnummer voor publieke diensten' wordt gebruikt om aan te geven dat het gaat om politie, brandweer en ambulancevervoerders, en niet om de particuliere alarmdiensten van de ANWB, verzekeringsmaatschappijen of beveiligingsbedrijven en dergelijke

3. Verstrekking locatieggevens (lid 2). Voor aanbieders die locatiegegevens kunnen verwerken geldt een extra verplichting Als er communicatie naar een alarmnummer wordt verzorgd moeten deze aanbieders gelijktijdig de in verband daarmee ver-

werkte locatiegegevens verstrekken Deze verplichting geldt niet alleen in de gevallen dat daadwerkelijk locatiegegevens worden verwerkt, maar ook als de aanbieder deze zou kunnen verwerken Dit betekent echter niet dat aanbieders op grond van deze verplichting ten behoeve van deze verplichting nieuwe systemen zouden moeten bouwen, waarmee nog nauwkeurigere locatiegegevens kunnen worden gegenereerd Alleen als aanbieders ertoe overgaan een dergelijk systeem te bouwen, moeten de als gevolg daarvan beschikbare gegevens worden verstrekt (MvA I, Kamerstukken I 2003/04, 28 851, C, p 34) De verplichting geldt ook in het geval het gaat om locatiegegevens, met zijnde verkeersgegevens, zoals bedoeld in art 11 5a, ook als de abonnee of gebruiker gebruik heeft gemaakt van de mogelijkheid in het vijfde lid daarvan om tijdelijk de verwerking van de hem betreffende locatiegegevens te beletten *Locatiegegevens* Het begrip 'locatiegegevens' wordt in art 11 1, onder d, gedefinieerd als de gegevens die de geografische positie van de randapparatuur (bijv mobiel telefoontoestel) aangeven (zie art 11 1, aant 5) *Bedoeling* Met de verstrekking van de locatiegegevens wordt beoogd de desbetreffende instanties beter in staat te stellen om de oproepen die met het alarmnummer plaatsvinden op adequate wijze te beantwoorden Afhankelijk van de mate van nauwkeurigheid kunnen de verstrekte locatiegegevens een indicatie geven van de locatie van waaruit de oproep is gedaan Als de oproeper niet in staat is om zelf door te geven waar hij zich bevindt, kunnen vervolgens de zoekinspanningen naar de juiste locatie door de hulpverlenende instanties meer gericht plaatsvinden Verder kunnen de locatiegegevens nuttig zijn bij de bestrijding van misbruik van het alarmnummer (MvT, Kamerstukken II 2002/03, 28 851, nr 3, p 162)

4. Vastlegging en verstrekking gegevens (leden 3-6). De nummers en andere gegevens moeten worden vastgelegd ten behoeve van de hulpverlening onderscheidenlijk de misbruikbestrijding De verschillende gegevens mogen vervolgens alleen ten behoeve van deze doeleinden worden verstrekt aan de aangewezen diensten Voorzover het persoonsgegevens betreft geeft de bepaling een invulling aan art 9 Wbp dat verlangt dat de gegevens niet verder worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verzameld *Verantwoordelijke in de zin van de Wbp* In het tweede lid staat dat de beheerders, voorzover het de vastlegging van deze gegevens betreft, worden aangemerkt als 'verantwoordelijke' in de zin van de Wbp Dit begrip wordt in art 1, onder d, Wbp gedefinieerd als 'de natuurlijke persoon of rechtspersoon die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt' De aanwijzing van de beheerders als verantwoordelijken stelt buiten twijfel dat zij zich dienen te houden aan de desbetreffende bepalingen van de Wbp

5. Bewaartermijnen (lid 7). Voor de onderscheiden gevallen worden verschillende bewaartermijnen gehanteerd Voorzover het persoonsgegevens betreft (gegevens betreffende een geïdentificeerde of identificeerbare natuurlijk personen) wordt daarmee invulling gegeven aan art 10 Wbp dat verlangt dat de gegevens niet langer worden bewaard dan noodzakelijk voor de doeleinden waarvoor ze zijn verzameld (zie art 10 Wbp, aant 1). *Voorontwerp van wet* In een voorontwerp voor een Wet kleine wijzigingen Telecommunicatiewet 2005, dat in de zomer van 2004 voor bespreking in het OPT is verspreid, wordt voorgesteld de bewaartermijn van één maand, genoemd onder a, te verlengen tot twee maanden Dit omdat in de praktijk is gebleken dat de termijn van één maan te kort is om het doel waarvoor de gegevens worden bewaard te realiseren

6. Kostenvergoeding (lid 8). De in het eerste lid genoemde aanbieders hebben aanspraak op vergoeding van de kosten die verband houden met het verstrekken van het nummer en de naam-, adres-, postcode en woonplaatsgegevens of de locatie van de openbare betaaltelefoon van waaruit de oproep is gemaakt.

7. Bekendmaking aanwijzing (lid 9). De aanwijzing heeft plaatsgevonden in het Besluit 1-1-2 alarmcentrales (Stb. 1998, 235). Aangewezen zijn de korpsbeheerders, bedoeld in art. 23 Politiewet 1993, en de Minister van Justitie als beheerder van het Korps landelijke politiediensten.

8. Vastleggen oproepen (lid 10). Art. 5, eerste lid, Richtlijn privacy en elektronische communicatie (bijlage A5) verbiedt het opnemen van gesprekken, maar art. 15, eerste lid, staat een uitzondering toe wanneer het belang van de openbare orde in het geding is. Daaronder valt het goed functioneren van de noodhulpverlening. De vastgelegde gesprekken mogen niet worden gebruikt voor andere doeleinden dan de kwaliteitscontrole op de noodhulpverlenning. Het is derhalve niet toegestaan de opnames te gebruiken voor de misbruikbestrijding. De opnames mogen een maand worden bewaard. Deze bewaartermijn correspondeert met de in het zevende lid onder a opgenomen termijn voor de nummers en gegevens die betrekking hebben op gevallen waarin kennelijk sprake is van een verzoek om hulpverlenning in een noodsituatie (Toel. NvW, Kamerstukken II 1997/98, 25 533, nr. 6, p. 9-10, Parl. Gesch., p. 462). *Voorontwerp van wet.* In een voorontwerp voor een Wet kleine wijzigingen Tele communicatiewet 2005, dat in de zomer van 2004 voor bespreking in het OPT is verspreid, wordt voorgesteld de in dit onderdeel opgenomen bewaartermijn van één maand te verlengen tot twee maanden. Dit omdat in de praktijk is gebleken dat de termijn van één maan te kort is om het doel waarvoor de ingekomen gesprekken worden bewaard, te realiseren.

[Hinderlijke of kwaadwillige oproepen]

Artikel 11.11. — 1. Een abonnee die last heeft van hinderlijke of kwaadwillige oproepen, waarbij de verstrekking van het nummer van het oproepende netwerkaansluitpunt is geblokkeerd, kan aan de aanbieder van een openbaar elektronisch communicatienetwerk of van een openbare elektronische communicatiedienst verzoeken om het nummer van de oproepende abonnee en de beschikbare daarop betrekking hebbende naam-, adres-, postcode- en woonplaatsgegevens, te verstrekken.

— 2. Een verzoek als bedoeld in het eerste lid voldoet aan de volgende vereisten:

***a.* het verzoek is schriftelijk en bevat de naam-, adres-, postcode- en woonplaatsgegevens van de verzoeker alsmede het nummer waarop de oproepen betrekking hebben, en**

***b.* het verzoek bevat een indicatie van de data en tijdstippen waarop de desbetreffende oproepen hebben plaatsgevonden.**

— 3. De verzoeker informeert de aanbieder onverwijld omtrent hinderlijke of kwaadwillige oproepen, die plaats hebben gevonden na indiening van het verzoek, bedoeld in het eerste lid.

— 4. De aanbieder stelt naar aanleiding van het verzoek een onderzoek in, teneinde vast te stellen of tot verstrekking van de gegevens, bedoeld in het eerste lid, dient te worden overgegaan.

— 5. Indien bij het onderzoek blijkt dat het oproepende nummer toebehoort aan een abonnee van een andere aanbieder, verleent de desbetreffende aanbie-

der op een daartoe strekkend verzoek van de met het onderzoek belaste aanbieder medewerking aan het onderzoek en verstrekt, indien het onderzoek daartoe aanleiding geeft, de beschikbare op het oproepende nummer betrekking hebbende naam-, adres-, postcode- en woonplaatsgegevens aan de aanbieder die met het onderzoek belast is.

— 6. Van de gegevensverstrekking aan een verzoeker wordt door de aanbieder mededeling gedaan aan de abonnee, wiens gegevens het betreft.

— 7. Bij algemene maatregel van bestuur kunnen nadere regels worden gesteld met betrekking tot:

***a.* het onderzoek, bedoeld in het vierde lid;**

***b.* de gegevensverstrekking, bedoeld in het vierde lid;**

***c.* de medewerkingsverplichting, bedoeld in het vijfde lid;**

***d.* de kennisgeving van de verstrekking van de gegevens, bedoeld in het zesde lid.**

1. Algemeen. Het artikel implementeert art 10, onder a, Richtlijn privacy en elektronische communicatie (bijlage A5) en voorziet in een regeling op grond waarvan aanbieders tijdelijke nummerblokkering kunnen opheffen om tegemoet te komen aan verzoeken van abonnees die worden lastig gevallen door hinderlijke of kwaadwillige oproepen Bij dergelijke oproepen moet worden gedacht aan de veelal veelvuldig gepleegde oproepen waarbij de opgeroepene wordt lastig gevallen (onder meer in de vorm van bedreigingen of liederlijke taal) Veelal wordt in zo een geval gebruik gemaakt van nummerblokkering (art. 11 9 eerste lid, onder a), zodat de identiteit van de oproeper niet kan worden achterhaald In dat geval heeft de opgeroepene de mogelijkheid om oproepen, waarbij de weergave van het nummer door de oproeper is geblokkeerd, te weigeren (art. 11 9, eerste lid, onder b, onderdeel 2°). Echter dat biedt geen bevredigende oplossing, omdat er ook veel andere, niet hinderlijke of niet kwaadwillige oproepen plaatsvinden, die de opgeroepene wel degelijk zou willen beantwoorden Om deze reden voorziet het artikel in een regeling op grond waarvan de abonnee het geblokkeerde nummer en andere gegevens van de hinderlijke of kwaadwillige oproeper kan opvragen bij de desbetreffende aanbieder (MvT, Kamerstukken II 2002/03, 28 851, nr 3, p 162-163) *Verstrekking naw-gegevens als geen gebruik is gemaakt van nummerblokkering* Er kan er ook behoefte zijn aan verstrekking van naw-gegevens als de oproepende abonnee geen gebruik maakt van nummerblokkering In dat geval zal de desbetreffende aanbieder aan de hand van de regels in de Wbp (m.n art 8, onder f, daarvan) moeten beoordelen of hij overgaat tot verstrekking van de hem beschikbare identificerende gegevens uit zijn abonnee-administratie (MvT, Kamerstukken II 2002/03, 25 581, nr 3, p 85)

2. Verzoek verstrekking geblokkerd nummer (lid 1). Een abonnee die last heeft van hinderlijke of kwaadwillige oproepen, waarbij gebruik wordt gemaakt van nummerblokkering (art 11.9, tweede lid onder b, onderdeel 2°) kan zijn aanbieder het verzoek doen het geblokkeerde oproepende nummer te verstrekken alsmede de daarop betrekking hebbende naw-gegevens van de abonnee Dit verzoek moet erop zijn gericht om de oproepende abonnee te identificeren, zodat de opgeroepen abonnee of gebruiker aan de hand van de door de aanbieder te verstrekken gegevens nadere actie tegen betrokkene kan ondernemen Daarbij kan worden gedacht aan een civielrechtelijke actie of het indienen van een klacht als bedoeld in art. 285b, tweede lid, Sr (MvT, Kamerstukken II 2002/03, 28 851, nr 3, p 163) *Beschikbare gegevens* Het verzoek van de abonnee heeft betrekking op de gegevens waarover de aanbieder beschikt Er is geen sprake van impliciete identificatieplicht met betrekking tot prepaidklanten (NV, Kamer-

stukken II 2002/03, 28 851, nr, 7, p 83, NvW, Kamerstukken II 2002/03, 28 851, nr, 13, p 20)

3. Vereisten van het verzoek (lid 2). Het in te dienen verzoek moet aan een aantal eisen voldoen Allereerst moet het in schriftelijke vorm worden ingediend en moet het de naw-gegevens van de abonnee bevatten, alsmede het nummer waarop de oproepen betrekking hebben Dit laatste is wenselijk, omdat een abonnee meer nummers tot zijn beschikking kan hebben, zoals bijvoorbeeld bij een ISDN-aansluiting Verder dient het verzoek een omschrijving te bevatten van de aard en ernst van de ondervonden last Daarmee kan de aanbieder vervolgens beoordelen of er sprake is van hinderlijke of kwaadwillige oproepen Daarnaast dient het verzoek een zo nauwkeurig mogelijke opgave te bevatten van de data en tijdstippen waarop de oproepen hebben plaatsgevonden Één en ander beoogt mede te voorkomen dat dergelijke verzoeken lichtvaardig worden gedaan Van belang is dat door de verstrekking van de gegevens van de oproepende abonnee aan de verzoeker een inbreuk wordt gemaakt op de persoonlijke levenssfeer van de oproepende abonnee (MvT, Kamerstukken II 2002/03, 28 851, nr 3, p 163)

4. Informeren over nieuwe hinderlijke of kwaadwillige oproepen (lid 3). Behalve de verstrekking van gegevens bij de indiening van het verzoek dient de verzoeker de aanbieder onverwijld op de hoogte te stellen van hinderlijke of kwaadwillige oproepen, die hebben plaatsgevonden na indiening van het verzoek Dit is met name van belang voor die gevallen, waarbij de aanbieder niet meer de beschikking heeft over gegevens terzake van de desbetreffende oproepen (MvT, Kamerstukken II 2002/03, 28 851, nr 3, p 163-164)

5. Onderzoek door aanbieder (lid 4). De aanbieder moet onderzoeken of de abonnee een zodanige last ondervindt dat verstrekking van gegevens van de oproeper is gerechtvaardigd Of daarvan sprake is, zal van geval tot geval dienen te worden vastgesteld De aanbieder heeft daarbij enige beoordelingsruimte Zijn onderzoek zal zich concentreren op objectief vaststelbare feiten, zoals onder andere het belpatroon en de frequentie van de gemaakte oproepen Het onderzoek zal primair dienen plaats te vinden aan de hand van de gegevens die door de verzoeker zijn verstrekt, en wel in het bijzonder aan de hand van de door de verzoeker verstrekte data en tijdstippen waarop de oproepen hebben plaatsgevonden (d w z de gegevens als bedoeld in het tweede lid, onder c) alsmede de meldingen als bedoeld in het derde lid Als er nog (verkeers)gegevens uit de desbetreffende periode beschikbaar zijn, kan de aanbieder, door vergelijking van de gegevens die door de verzoeker zijn aangeleverd met zijn eigen (verkeers)gegevens vaststellen of op de genoemde data en tijdstippen de gemaakte oproepen hebben plaatsgevonden en of het inderdaad om een situatie gaat waarbij sprake is van oproepen afkomstig van een en hetzelfde nummer die meer dan een incidenteel karakter dragen (MvT, Kamerstukken II 2002/03, 28 851, nr 3, p 164)

6. Medewerking andere aanbieder (lid 5). Als uit het onderzoek van de aanbieder blijkt dat het nummer van de hinderlijke of kwaadwillige oproeper toebehoort aan een eigen abonnee, zal de aanbieder zelf beschikken over de naw-gegevens van deze abonnee Maar als het oproepende nummer toebehoort aan een abonnee van een andere aanbieder, is medewerking van de andere aanbieder noodzakelijk In verband daarmee is bepaald dat de desbetreffende aanbieder op een daartoe strekkend verzoek van de met het onderzoek belaste aanbieder de gevraagde medewerking verleent en, indien het onderzoek daartoe aanleiding geeft, de op het oproepende nummer betrekking hebbende gegevens verstrekt aan de aanbieder die met het onderzoek is belast En als blijkt dat op de door de verzoeker aangegeven data en tijdstippen inderdaad vanuit een bepaald num-

mer de gewraakte oproepen zijn gepleegd, dan zal verstrekking van de in het eerste lid bedoelde gegevens kunnen plaatsvinden Overigens staat het artikel er niet aan in de weg dat de aanbieder, voordat hij tot verstrekking overgaat, eerst met degene aan wie het oproepende nummer toebehoort contact opneemt en daarbij de betrokkene confronteert met zijn bevindingen (MvT, Kamerstukken II 2002/03, 28 851, nr 3, p 164)

7. Mededeling aan de oproepende abonnee (lid 6). Als sluitstuk van de regeling is voorzien in de verplichting om de abonnee over wie de gegevens in het kader van een verzoek op grond van het eerste lid, zijn verstrekt, van deze verstrekking op de hoogte te stellen Dit omdat het aan deze abonnee ingevolge art 11 9 toekomende recht op nummerblokkering opzij wordt gezet Verder wordt de abonnee op deze wijze voorbereid op eventuele acties zijdens de verzoeker en kan wellicht worden bewerkstelligd dat deze zijn gewraakte gedrag voor de toekomst achterwege laat (MvT, Kamerstukken II 2002/03, 28 851, nr 3, p 164)

8. AMvB (lid 7). In art 11 11, zevende lid, is ten slotte nog voorzien in de mogelijkheid om bij AMvB nadere regels te stellen met betrekking tot enkele daarin benoemde onderwerpen (MvT, Kamerstukken II 2002/03, 28 851, nr 3, p 165) Een dergelijke AMvB is nog niet vastgesteld

§ 11 3 Ontheffing

[Ontheffingen betreffende doorschakeling en nummeridentificatie]

Artikel 11.12. — 1. Aan een aanbieder van een openbaar elektronisch communicatienetwerk en een aanbieder van een openbare elektronische communicatiedienst kan door het college ontheffing worden verleend van de verplichtingen die voortvloeien uit de artikelen 11.4, eerste lid, onderdeel *b*, en 11.9 tot en met 11.11.

— 2. Een ontheffing als bedoeld in het eerste lid kan uitsluitend worden verleend, indien:

***a.* deze betrekking heeft op abonneelijnen verbonden met analoge centrales, en**

***b.* nakoming van de desbetreffende verplichtingen technisch niet haalbaar is of onevenredig veel financiële lasten voor de aanbieder met zich meebrengt.**

— 3. Een ontheffing kan onder beperkingen worden verleend. Aan een ontheffing kunnen voorschriften worden verbonden.

Betekenis. Op grond van het artikel kan OPTA in individuele gevallen ontheffing verlenen van de verplichtingen van achtereenvolgens art 11 4, eerste lid, onder b, (doorschakeling) en art 11 9 tot en met 11 11 (nummeridentificatie) Deze ontheffingsbevoegdheid is geclausuleerd Overeenkomstig art 3, tweede lid, Richtlijn privacy en elektronische communicatie (bijlage A5) is ontheffing alleen mogelijk als is voldaan aan twee voorwaarden, namelijk (a) dat de ontheffing betrekking heeft op abonneelijnen verbonden met analoge centrales en (b) dat nakoming van de desbetreffende verplichtingen technisch niet haalbaar is of onevenredig veel financiele lasten voor de aanbieder met zich meebrengt OPTA kan een ontheffing onder beperkingen verlenen en kan daaraan voorschriften verbinden (MvT, Kamerstukken II 2002/03, 28 851, nr 3, p 162) Zie art 11.9, aant 2

§ 11 4 Uitzonderingen

[Uitzonderingen betreffende verkeers- en locatiegegevens en nummeridentificatie]

Artikel 11.13. — 1. Aanbieders van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten kunnen de artikelen 11.5, 11.5*a* en 11.9, eerste lid, buiten toepassing laten, indien dit noodzakelijk is in het belang van:

***a*. de nationale veiligheid;**

***b*. de voorkoming, opsporing en vervolging van strafbare feiten.**

— 2. Aanbieders van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten mogen, in afwijking van artikel 11.5, eerste lid, verkeersgegevens verwerken, indien en voor zolang dat noodzakelijk is voor een onderzoek als bedoeld in artikel 11.11, vierde en vijfde lid. De verkeersgegevens mogen voor een periode van ten hoogste drie maanden na beëindiging van een onderzoek als bedoeld in artikel 11.11, vierde lid, door de desbetreffende aanbieders worden bewaard. Na afloop van deze periode worden de verkeersgegevens verwijderd.

1. Uitzondering (lid 1) Art 15, eerste lid, Richtlijn privacy en elektronische communicatie (bijlage A5) voorziet in de mogelijkheid dat lidstaten wettelijke maatregelen treffen waarbij de reikwijdte van de rechten en plichten van enkele in de richtlijn opgenomen bepalingen worden beperkt in verband met (o a) de nationale veiligheid en de opsporing van strafbare feiten Bij de soort maatregelen waar art 15 van de richtlijn op ziet, moet onder andere worden gedacht aan het aftappen en opnemen van telecommunicatie en de vordering van verkeersgegevens Dergelijke maatregelen vergen (veelal) de medewerking van de aanbieders van elektronische communicatienetwerken en openbare elektronische communicatiediensten, waarbij deze in strijd kunnen komen met de verplichtingen die op grond van de genoemde bepalingen in dit hoofdstuk op deze aanbieders rusten In verband daarmee bepaalt het artikel dat aanbieders van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten, als dit noodzakelijk is in het belang van de nationale veiligheid of de voorkoming, opsporing en vervolging van strafbare feiten, art 11 5, 11 5a en 11 9, eerste lid, van de wet buiten toepassing kunnen laten (MvT, Kamerstukken II 2002/03, 28 851, nr 3, p 165)

2. Verwerking verkeersgegevens voor onderzoek naar hinderlijke en kwaadwillige oproepen (lid 2). Verder is bepaald dat aanbieders van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten bevoegd zijn om, in afwijking van het bepaalde in art 11 5, eerste lid, verkeersgegevens te verwerken, als dat nodig is voor onderzoek naar hinderlijke of kwaadwillige oproepen, zoals bedoeld in art 11 11, vierde en vijfde lid Verwerking van verkeersgegevens bij een dergelijk onderzoek is noodzakelijk om op een verantwoorde wijze op het verzoek om verstrekking van de in art 11 1, eerste lid, bedoelde gegevens aan een verzoeker te kunnen beslissen Art 10, onder a, Richtlijn privacy en elektronische communicatie (bijlage A5) biedt daarvoor de ruimte Daarin staat dat de identificatiegegevens van de oproepende abonnee overeenkomstig de nationale wetgeving kunnen worden opgeslagen en beschikbaar gesteld Na de verstrekking van de gegevens, bedoeld in art 11 11, eerste lid, worden de verkeersgegevens verwijderd (MvT, Kamerstukken II 2002/03, 28 851, nr 3, p 165)