Besluit van – datum - , houdende wijziging van het Besluit beveiliging gegevens aftappen telecommunicatie in verband met het bewaren van telecommunicatiegegevens

Wij Beatrix, bij de gratie Gods, Koningin der Nederlanden, Prinses van Oranje-Nassau, enz. enz. enz.

Op de voordracht van Onze Minister van Justitie van ..., nr. ..., gedaan mede namens de Ministers van Economische Zaken, van Binnenlandse Zaken en Koninkrijksrelaties en van Defensie.
Gelet op artikel 13.5 van de Telecommunicatiewet;
De Raad van State gehoord (advies van – datum -);
Gezien het nader rapport van Onze Minister van Justitie van – datum -;

Hebben goedgevonden en verstaan:

ARTIKEL I

Het Besluit beveiliging gegevens aftappen telecommunicatie wordt als volgt gewijzigd:

A. Artikel 2, eerste lid, wordt als volgt gewijzigd:

a. In onderdeel b wordt “artikel 13.4 van de wet” vervangen door: de artikelen 13.2b en 13.4 van de wet.
b. Een nieuw onderdeel c wordt ingevoegd, dat komt te luiden:

c. de gegevens welke door een aanbieder ingevolge artikel 13.2a, tweede lid, van de wet worden bewaard.

B. Onder vernummering van de artikelen 5 tot en met 9 tot respectievelijk 6 tot en met 10 wordt een nieuw artikel ingevoegd, dat komt te luiden:

Artikel 5

1. De aanbieder draagt er zorg voor dat de gegevens, die ingevolge artikel 13.2a, tweede lid, van de wet, worden bewaard, uiterlijk binnen acht dagen na afloop van de termijn, bedoeld in artikel 13.2a, derde lid, van de wet, worden vernietigd.
2. Artikel 5, eerste lid, van het Besluit bewaren en vernietigen niet-gevoegde stukken is van overeenkomstige toepassing.

C. Artikel 9 komt te luiden:

Artikel 9

Dit besluit wordt aangehaald als: Besluit beveiliging gegevens telecommunicatie.

Artikel II

Dit besluit treedt in werking met ingang van de dag na de datum van uitgifte van het Staatsblad waarin het wordt geplaatst.

Lasten en bevelen dat dit besluit met de daarbij behorende nota van toelichting in het Staatsblad zal worden geplaatst.

’s-Gravenhage, - datum -

De Minister van Justitie,

De Minister van Economische Zaken,

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,

De Minister van Defensie,

NOTA VAN TOELICHTING

ALGEMEEN

Op 3 mei 2006 is Richtlijn nr. 06/24/EG van het Europees Parlement en de Raad van de Europese Unie van 15 maart 2006 in werking getreden, betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of openbare communicatienetwerken en tot wijziging van Richtlijn nr. 02/68/EG (PbEU, L105/54) in werking getreden (PbEU L 105). (hierna ook te noemen: de richtlijn dataretentie). De richtlijn dataretentie voorziet in een verplichting voor aanbieders van openbare communicatienetwerken en aanbieders van openbare elektronische communicatiediensten tot het bewaren van telecommunicatiegegevens gedurende een bepaalde periode. Ter implementatie van de richtlijn dataretentie worden in de Wet bewaarplicht telecommunicatiegegevens regels gesteld voor de verplichting tot bewaring van gegevens door de aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten. Deze regels hebben betrekking op de verplichting tot het bewaren van bepaalde gegevens, de bewaartermijnen en de bescherming en beveiliging van de bewaarde gegevens. De wet biedt de mogelijkheid om bij algemene maatregel van bestuur regels te stellen met betrekking tot de te nemen maatregelen in verband met de beveiliging van, de toegang tot, en de vernietiging van de gegevens (artikel 13.4 Tw). In dit besluit worden die regels nader uitgewerkt. Deze algemene maatregel van bestuur geeft regels voor de bescherming, beveiliging en vernietiging van de gegevens die door de aanbieders worden bewaard ten behoeve van het onderzoeken, opsporen of vervolgen van strafbare feiten, op grond van artikel 13.2a, derde lid, van de wet.
Mede namens mijn ambtgenoten van Economische Zaken, van Binnenlandse Zaken en Koninkrijksrelaties en van Defensie licht ik het Besluit tot wijziging van het Besluit beveiliging gegevens aftappen telecommunicatie in deze nota van toelichting toe.

Op grond van de Telecommunicatiewet geldt voor de aanbieders van openbare elektronische communicatienetwerken en van openbare elektronische communicatiediensten (hierna ook te noemen: de aanbieder) reeds de verplichting om, onverminderd de Wet bescherming persoonsgegevens, zorg te dragen voor de bescherming van de persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers van hun netwerk, onderscheidenlijk hun dienst (art. 11.2 Tw). Ook zijn de aanbieders verplicht in het belang van de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers passende technische en organisatorische maatregelen te treffen ten behoeve van de veiligheid en beveiliging van de door hen aangeboden netwerken en diensten (art. 11.3, eerste lid, Tw). 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. In de Wet bewaarplicht telecommunicatiegegevens worden, aanvullend aan de meer algemene normen op basis van de Wet bescherming persoonsgegevens (Wbp) en de Telecommunicatiewet, aan de aanbieders specifieke verplichtingen opgelegd ten aanzien van de bescherming en de beveiliging van de gegevens die worden bewaard ten behoeve van het onderzoeken, opsporen en vervolgen van ernstige misdrijven. Bij de bewaring van telecommunicatiegegevens is de bescherming van de persoonlijke levenssfeer aan de orde, omdat aan de hand van de te bewaren gegevens inzicht kan worden verkregen in de gedragingen van personen. Voorgesteld wordt om voor de nadere uitwerking van de te treffen maatregelen in verband met de beveiliging van, de toegang tot, en de vernietiging van de gegevens aan te sluiten bij de regeling van het bestaande Besluit

beveiliging gegevens aftappen telecommunicatie (Staatsblad 2003, 472) (hierna ook te noemen: BBGAT). Een dergelijke aansluiting ligt voor de hand omdat dit besluit thans reeds regels kent voor de beveiliging van gegevens die de aanbieders verwerken in het kader van het verlenen van medewerking aan de uitvoering van een vordering of een verzoek tot het aftappen of opnemen van telecommunicatie (artikel 2, eerste lid, onderdeel a, BBGAT) en het verstrekken van informatie aan een bevoegde autoriteit naar aanleiding van een vordering dan wel een verzoek tot het verstrekken van verkeersgegevens (artikel 2, eerste lid, onderdeel b, BBGAT). Nu de beveiliging van gegevens in verband met de verstrekking van verkeersgegevens reeds onder de reikwijdte van het Besluit beveiliging gegevens aftappen telecommunicatie valt, ligt het voor de hand om ook voor de bewaring van dergelijke gegevens de bepalingen van dit besluit toe te passen. De aanbieders zijn inmiddels goed bekend met deze regels en hebben deze kunnen integreren in hun bedrijfsvoering. Deze regels voldoen ook voor de beveiliging van gegevens in verband met de bewaarplicht. Aansluiting bij dit besluit is goed mogelijk en is, bezien vanuit het oogpunt van heldere regelgeving en de efficiency van de bedrijfsvoering van de aanbieders, ook wenselijk.

Het Besluit beveiliging gegevens aftappen telecommunicatie bevat een aantal kernelementen. Dit betreft een verduidelijking van verschillende aspecten waarop de door de aanbieder te treffen beveiligingsmaatregelen zich dienen te richten (artikel 2, tweede lid), een bijlage met de verplicht te treffen beveiligingsmaatregelen (artikel 2, derde lid, jo. bijlage), de verplichting tot vastlegging van de beveiligingsmaatregelen in een beveiligingsplan (artikel 3), de eis dat de aanbieder ‘gescreend’ personeel inschakelt bij de uitvoering van taplasten dan wel verzoeken om informatie en dat deze ervoor zorgt dat het personeel de vereiste geheimhouding betracht (artikelen 4 en 6), maatregelen die genomen moeten worden bij geoorloofde inbreuken op de vertrouwelijkheid (artikel 5) en een regeling voor de situatie dat door een aanbieder werkzaamheden zijn uitbesteed aan een derde (artikel 7). Voorgesteld wordt deze bepalingen tevens van toepassing te doen zijn op de verwerking van de gegevens die de aanbieders ingevolge artikel 13.2a van de wet moeten bewaren. Dit is geregeld in artikel 2, eerste lid, onderdeel c.

Inzake de reikwijdte van de wettelijke verplichtingen voor de aanbieders geldt dat de Wet bescherming persoonsgegevens van toepassing is op de verwerking van persoonsgegevens in het kader van activiteiten van een vestiging van een verantwoordelijke in Nederland (art. 4, eerste lid, Wbp). De Telecommunicatiewet is van toepassing op aanbieders die in Nederland openbare elektronische communicatiediensten of openbare elektronische communicatienetwerken aanbieden. De betreffende begrippen zijn in de wet omschreven (artikel 1.1, onderdelen f, g, h, i, ee en ff Tw). Dit brengt met zich mee dat de eisen op het gebied van de bescherming van persoonsgegevens bij het aanbieden van openbare telecommunicatiediensten of openbare telecommunicatienetwerken, zoals uitgewerkt in de Wbp en in de Telecommunicatiewet (hoofdstukken 11 en 13), onverkort gelden indien het telecommunicatieverkeer wordt afgehandeld door middel van netwerkfaciliteiten in het buitenland.

De Wet bewaarplicht telecommunicatiegegevens bevat geen verplichting om de te bewaren gegevens gescheiden te bewaren van het netwerk. De richtlijn dataretentie bevat hierover evenmin nadere regels, behoudens het richtsnoer dat de gegevens op zodanige wijze zouden moeten worden opgeslagen dat voorkomen wordt dat deze meermalen worden bewaard (Overweging 13). Wel bevat de richtlijn de verplichting voor de aanbieders om ervoor te zorgen dat de bewaarde gegevens dezelfde kwaliteit hebben en worden onderworpen aan dezelfde beveiligings- en beschermingseisen als de gegevens in het netwerk (artikel 7,

onderdeel a). Op dit punt kan onderscheid worden gemaakt in de fase waarin de gegevens op het netwerk aanwezig zijn en de fase waarin de gegevens uit het netwerk worden gehaald en worden vastgelegd en opgeslagen ('gelogd'), om te kunnen voldoen aan vorderingen of verzoeken door de bevoegde autoriteiten. De gegevens die op het netwerk aanwezig zijn, zijn (nog) niet direct bruikbaar voor de verdere verwerking met het oog op zakelijke doeleinden van de aanbieders dan wel voor het voldoen aan een vordering of een verzoek van een bevoegde autoriteit tot verstrekking van gegevens omtrent telecommunicatie. Zodra de gegevens ten behoeve van verdere verwerking voor bepaalde doeleinden uit het netwerk worden opgehaald, samengebracht en vastgelegd, opgeslagen of gelogd is er doorgaans sprake van gegevens die op individuele personen herleidbaar zijn. Voor het samenbrengen, vastleggen, opslaan of loggen van deze gegevens, al dan niet in een afzonderlijk gegevensbestand, gelden vooraleerst de meer algemene verplichtingen op grond van de Wet bescherming persoonsgegevens en de Telecommunicatiewet (artikelen 11.2 en 11.3 Tw). Daar de betreffende gegevens inzicht kunnen bieden in de gedragingen van personen (de gegevens kunnen betrekking hebben op de communicatiediensten die door een persoon worden gebruikt, de aansluitnummers waarmee verbinding is geweest en de duur van de verbinding) bestaat een bijzonder belang bij de bescherming en beveiliging van de gegevens. Daarom zijn aanvullend de verplichtingen van het Besluit beveiliging gegevens aftappen telecommunicatie van toepassing op de verdere verwerking van de gegevens. Artikel 2, eerste lid, onderdeel c, van het Besluit beveiliging gegevens aftappen telecommunicatie is van toepassing op het bewaren van de gegevens, het bestaande onderdeel b is reeds van toepassing op de verstrekking van de gegevens aan een bevoegde autoriteit, op grond van artikel 13.4 van de wet.

De richtlijn dataretentie bevat naast de verplichting om bepaalde categorieën van gegevens gedurende een bepaalde termijn te bewaren ook specifieke verplichtingen ten aanzien van de bescherming en de beveiliging van de gegevens die door de aanbieders worden bewaard ten behoeve van het onderzoeken, opsporen en vervolgen van ernstige misdrijven. Deze verplichtingen hebben betrekking op het treffen van passende technische en organisatorische maatregelen op het gebied van de beveiliging van, de toegang tot en de vernietiging van de bewaarde gegevens. Daarnaast geldt dat de aanbieders ervoor zorg moeten dragen dat de bewaarde gegevens dezelfde kwaliteit hebben en worden onderworpen aan dezelfde maatregelen als de gegevens in het netwerk.

Het Besluit beveiliging gegevens aftappen telecommunicatie bevat reeds gedetailleerde en uitgebreide normen ten aanzien van technische en organisatorische maatregelen ten behoeve van de beveiliging van, en de toegang tot, de gegevens. Zoals hierboven reeds opgemerkt, kunnen deze normen ongewijzigd worden toegepast op de gegevens die door de aanbieders op grond van artikel 13.2a van de wet worden bewaard. Daarvoor is wel een aanvulling van artikel 2 van dit besluit vereist. Verder bevat het Besluit beveiliging gegevens aftappen telecommunicatie geen specifieke regels over de vernietiging van gegevens door de aanbieders. Op dit punt is aanvulling noodzakelijk. Zie hiertoe artikel 5 van het besluit.

Het is thans niet uitgesloten dat met het oog op het toezicht in de nabije toekomst blijkt dat aanvullend nadere regels vereist zijn voor de bescherming en beveiliging van de gegevens die door de aanbieders worden gegenereerd en verwerkt, bijvoorbeeld inzake de wijze van de opslag van de gegevens.

Voor wat betreft de verstrekking van gegevens kan hier worden vermeld dat gewerkt wordt aan de ontwikkeling van een gemeenschappelijke standaard voor de verstrekking van de te

bewaren gegevens in Europees verband. Dit betreft de zogenaamde ETSI-standaard. Het European Telecommunications Standards Institute is in 1988 opgericht en is actief op het terrein van wereldwijd toepasbare standaarden op het gebied van telecommunicatie. Binnen ETSI wordt door vertegenwoordigers van rechtshandhavingsdiensten, aanbieders en producenten van telecommunicatieapparatuur gewerkt aan een gemeenschappelijke standaard voor het, door middel van een interface, langs elektronische weg verstrekken van de bewaarde telecommunicatiegegevens. De standaard zal naar verwachting voor het eind van dit jaar toegepast kunnen worden. Ingeval een aanbieder kiest voor het langs elektronische weg overdragen van de gegevens, dan ligt het voor de hand dat de ETSI-standaard wordt gevolgd. Zodra deze standaard is vastgesteld kan dit aanleiding vormen tot het stellen van nadere regels bij algemene maatregel van bestuur. Artikel 13.4, vierde lid, van het wetsvoorstel biedt hiertoe een basis.

II ARTIKELEN

Artikel I, onderdeel A

Artikel 2 bevat, in het eerste lid, de verplichting voor de aanbieder om alle noodzakelijke technische en organisatorische maatregelen te treffen om kennisneming door onbevoegden te voorkomen van de in dit lid aangewezen gegevens en informatie. Dit betreft de gegevens welke in het kader van – kort gezegd – het aftappen of opnemen van telecommunicatie door een bevoegde autoriteit aan de aanbieder zijn verstrekt (onderdeel a) en de informatie welke door de aanbieder aan een bevoegde autoriteit is verstrekt op grond van artikel 13.4 van de wet alsmede de gegevens welke zijn vervat in de aan deze verstrekking ten grondslag liggende vordering om informatie van de desbetreffende autoriteit (onderdeel b).

Artikel 2, eerste lid, onderdeel b
In dit onderdeel is de verplichting voor de aanbieder neergelegd tot beveiliging van de informatie welke aan een bevoegde autoriteit is verstrekt op grond van artikel 13.4 van de wet alsmede de gegevens welke zijn vervat in het aan deze verstrekking grondslag liggende verzoek of in de aan deze verstrekking ten grondslag liggende vordering om informatie van de desbetreffende bevoegde autoriteit. Dit betreft de verstrekking van verkeersgegevens (gegevens over een gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker). Deze bepaling verdient echter aanvulling vanwege twee recente wijzigingen van het Wetboek van Strafvordering, die tevens consequenties hebben voor de verplichtingen van de aanbieders op grond van de Telecommunicatiewet.

De Wet bevoegdheden vorderen gegevens (Staatsblad 2005, 390) voorziet in de bevoegdheid voor de opsporingsambtenaar tot het vorderen van identificerende gegevens van degene die daarvoor redelijkerwijs in aanmerking komt (art. 126nc Sv). De officier van justitie is bevoegd van degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot bepaalde opgeslagen of vastgelegde gegevens, te vorderen deze gegevens te verstrekken (art. 126nd Sv). Een dergelijke vordering kan worden gericht tot de aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst, voorzover de vordering betrekking heeft op andere gegevens dan verkeersgegevens en identificerende gegevens (art. 126ng Sv). Deze beperking vloeit voort uit de omstandigheid dat laatstbedoelde gegevens reeds gevorderd kunnen worden door toepassing van de artikelen 126n en 126na Sv. De aanbieder van een openbare telecommunicatiedienst of een openbaar telecommunicatienetwerk is verplicht aan een dergelijke vordering te voldoen (art. 13.2b Tw).

Ingeval andere dan verkeersgegevens en identificerende gegevens van de aanbieders worden gevorderd ligt het, mede vanuit het oogpunt van de systematiek, in de rede het Besluit beveiliging gegevens aftappen telecommunicatie ook op de verstrekking van deze gegevens van toepassing te doen zijn. Met de aanpassing van artikel 2, eerste lid, onderdeel b wordt daarin voorzien.

In de Wet van 20 november 2006 tot wijziging van het Wetboek van Strafvordering, het Wetboek van Strafrecht en enige andere wetten ter verruiming van de mogelijkheid tot opsporing en vervolging van terroristische misdrijven (Staatsblad 2006, 580) is de bevoegdheid van de officier van justitie opgenomen om, indien een verkennend onderzoek de voorbereiding van de opsporing van terroristische misdrijven tot doel heeft, van degene die daarvoor redelijkerwijs in aanmerking komt en die anders dan ten behoeve van persoonlijk gebruik gegevens verwerkt, te vorderen bepaalde opgeslagen of vastgelegde identificerende gegevens van een persoon te verstrekken (art. 126ii Sv). Daarnaast kan de officier van justitie, ingeval van een dergelijk onderzoek, van degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot een geautomatiseerd gegevensbestand schriftelijk vorderen dit bestand of delen daarvan, te verstrekken teneinde de hierin opgenomen gegevens te doen bewerken (art. 126hh Sv). De aanbieder van een openbare telecommunicatiedienst of een openbaar telecommunicatienetwerk is verplicht aan een dergelijke vordering te voldoen (art. 13.2b Tw). Gelet op de aard van de gegevens en de achtergrond van de inzet van de bevoegdheid door de officier van justitie is het wenselijk dat het Besluit beveiliging gegevens aftappen telecommunicatie ook op de verstrekking van deze gegevens van toepassing is. Met de aanpassing van dit onderdeel wordt daarin voorzien.

Artikel 2, eerste lid, onderdeel c
De verplichtingen van dit onderdeel hebben betrekking op de gegevens die door de aanbieders in het kader van de door hun aangeboden openbare telecommunicatienetwerken of openbare telecommunicatiediensten worden gegenereerd of verwerkt en vervolgens samengebracht en vastgelegd, opgeslagen of gelogd teneinde te kunnen voldoen aan de verplichting tot bewaring van de gegevens, bedoeld in artikel 13.2a, derde lid, van de wet. Daartoe zullen de gegevens doorgaans in eerste instantie op een harde schijf worden bewaard en, voorzover zij meerdere maanden bewaard worden, overgebracht op CD's . Zoals hierboven reeds opgemerkt hebben deze verplichtingen dus geen betrekking op de gegevens die in ruwe vorm op het netwerk aanwezig zijn en die (nog) niet bruikbaar zijn voor de verdere verwerking met het oog op de doelen, als bedoeld in de hoofdstukken 11 en 13 van de Telecommunicatiewet.

Artikel I, onderdeel B.

Artikel 5, eerste lid
In de wet is de verplichting voor de aanbieders vastgelegd ervoor zorg te dragen dat de bewaarde gegevens na afloop van de wettelijke bewaartermijn onverwijld worden vernietigd (artikel 13.5, derde lid, onderdeel b, Tw). Het is de bedoeling dat na afloop van de bewaartermijn geen gebruik meer gemaakt kan worden van de gegevens. De verplichting tot onverwijlde vernietiging van de gegevens brengt met zich mee dat de gegevens, zo mogelijk, direct na afloop van de wettelijke bewaartermijn worden vernietigd. In de wet is de verplichting voor de aanbieders vastgelegd om zodanige passende technische en organisatorische maatregelen te nemen teneinde de gegevens te kunnen vernietigen na afloop van de bewaarperiode. Worden de gegevens geautomatiseerd opgeslagen en bewaard, bijvoorbeeld op een harde schijf, dan zal het vanuit technisch oogpunt niet onoverkomelijk zijn om de gegevens direct na afloop van de wettelijke bewaartermijn te vernietigen. In dit

verband kan het begrip ‘onverwijld’ – in navolging van de memorie van toelichting bij de Wet bewaarplicht telecommunicatiegegevens - worden opgevat als ‘zo spoedig mogelijk als de inrichting van de bedrijfsvoering en de stand der techniek van het betreffende bedrijf dat mogelijk maakt’. Ingeval de aanbieder kiest voor niet volledig geautomatiseerde opslag en verwerking bijvoorbeeld doordat de gegevens worden bewaard op een DVD, tape of CD, dan dienen de betreffende gegevensdragers te worden geselecteerd en de daarop aangebrachte gegevens te worden overgeschreven of anderszins te worden vernietigd. Mede gelet op de noodzaak om deskundig personeel met deze taak te belasten en het feit dat kleinere aanbieders wellicht zullen kiezen voor niet volledig geautomatiseerde opslag van de gegevens, is het aangewezen om te voorzien in een iets langere periode voor de vernietiging van de gegevens. Zo wordt in het voorstel tot wijziging van de Duitse Telecommunicatiewet (‘Telekommunikationsgesetz’) in verband met de implementatie van de richtlijn dataretentie, dat thans in Duitsland aanhangig is, een termijn van uiterlijk een maand na afloop van de wettelijke bewaartermijn voorgesteld (art. 113a, elfde lid, TKG). In Nederland lijkt een dergelijk lange termijn echter niet nodig. Mede gelet op de tekst van de richtlijn, die strekt tot vernietiging van de gegevens aan het einde van de bewaarperiode, lijkt het aangewezen te bepalen dat de bewaarde gegevens binnen een periode van uiterlijk acht dagen daadwerkelijk zijn vernietigd.

Tweede lid

De vernietiging houdt in dat geen kennis meer kan worden genomen van de vernietigde gegevens. De wijze van vernietiging kan verschillen, afhankelijk van de gebruikte systemen en materialen voor de bewaring van de gegevens. Worden de gegevens bijvoorbeeld bewaard op een gegevensdrager (CD-rom, CD, DVD, diskette, tape, harde schijf of server), dan is fysieke vernietiging van de gegevensdrager niet altijd vereist. Het wissen van bestanden of van gegevens is echter niet voldoende indien de gegevens door middel van het verrichten van betrekkelijk eenvoudige technische handelingen en anders dan slechts met disproportionele inzet van tijd, kosten en arbeid, kunnen worden teruggehaald. De gegevensdrager dient op zodanige wijze te worden bewerkt dat van de te vernietigen gegevens geen kennis meer kan worden genomen Evenmin is het anonimiseren van de gegevens voldoende, in de betekenis dat de gegevens zodanig worden bewerkt dat bijzonderheden inzake personele of materiële omstandigheden niet of slechts met disproportionele inzet van tijd, kosten en arbeid, kunnen worden herleid tot een geïdentificeerde of te identificeren persoon. Anonimisering is slechts toegestaan voor de gegevens die op grond van artikel 11.5 en 11.5a van de wet worden verwerkt. Deze bepalingen hebben betrekking op de gegevensverwerking ten behoeve van de zakelijke doeleinden van de aanbieders. De bewaarplicht, als neergelegd in hoofdstuk 13 van die wet, geschiedt echter voor andere doeleinden. Anonimisering van de gegevens is slechts mogelijk indien de bewaarde gegevens dezelfde gegevens zijn als die welke onder de voorwaarden, genoemd in de artikelen 11.5 en 11.5a van de wet kunnen worden verwerkt voor de aldaar genoemde doeleinden. In de praktijk zal de lengte van de termijn van artikel 13.2a van die wet de termijn, gedurende welke de verdere verwerking van gegevens op grond van de artikelen 11.5 en 11.5a van de wet is toegestaan, naar alle waarschijnlijkheid voor het merendeel der verwerkingen overstijgen, zodat na afloop van de wettelijke bewaartermijn uitsluitend vernietiging aan de orde is.

Voor de uitvoering van de verplichting tot vernietiging van de bewaarde gegevens en de uitoefening van het toezicht op de naleving daarvan zijn voorschriften opgenomen in het Besluit bewaren en vernietigen niet-gevoegde stukken (Staatsblad 1999, 548). Dit besluit bevat verplichtingen voor de officier van justitie met betrekking tot processen-verbaal en andere voorwerpen die informatie bevatten die is vastgelegd door middel van het opnemen van vertrouwelijke communicatie en het onderzoek van telecommunicatie. In artikel 5, eerste

lid, van dat besluit wordt bepaald dat met de vernietiging (van het proces-verbaal) gelijk staat het op zodanige wijze bewerken van de gegevensdrager dat de gegevens die daaraan voor de bewerking konden worden ontleend, niet meer kenbaar zijn. Hierbij wordt in dit lid aangesloten.

Artikel I, onderdeel C**.**

Artikel 9
Door de voorgestelde wijzigingen geeft het besluit nu niet alleen regels over de bescherming en beveiliging van (a) de gegevens die door de bevoegde autoriteit aan de aanbieder zijn verstrekt met het oog op het aftappen en opnemen van telecommunicatie, bedoeld in artikel 13.2a van de wet, en (b) de verkeersgegevens, inclusief gebruikersgegevens, die door de aanbieder aan een bevoegde autoriteit zijn verstrekt op grond van de bevoegdheid, bedoeld in de artikelen 13.2b en 13.4 van de wet evenals de gegevens die zijn vervat in het aan deze verstrekking ten grondslag liggende vordering of verzoek van de bevoegde autoriteit. Het besluit geeft nu ook regels voor (c) de gegevens die door de aanbieders worden bewaard ten behoeve van het onderzoeken, opsporen en vervolgen van ernstige misdrijven, op grond van artikel 13.2a, tweede lid, van de wet. Gelet hierop ligt het in de rede om de citeertitel dienovereenkomstig aan te passen. In het licht van de Aanwijzingen voor de regelgeving (Ar 185) wordt voorgesteld de citeertitel in te korten tot: *Besluit beveiliging gegevens telecommunicatie*.

Artikel II

De eerdergenoemde richtlijn dataretentie moet uiterlijk op 15 september 2007 zijn geïmplementeerd in de nationale wetgeving (artikel 15, eerste lid). De Wet bewaarplicht telecommunicatiegegevens zal dan ook, zo mogelijk, op die datum in werking treden. Gelet op het belang dat de Nederlandse wetgeving, ter implementatie van de richtlijn dataretentie, op tijd van kracht is ligt het in de bedoeling dit besluit spoedig na plaatsing in het Staatsblad in werking te laten treden.

De Minister van Justitie,