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 Staatssecretaris van Economische Zaken en Onze Ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Defensie.
Gelet op artikel 13.5, vierde lid, 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 die door de aanbieder worden geraadpleegd en verder worden verwerkt met het oog op het voldoen aan een verzoek of vordering op grond van de artikelen 13.2b en 13.4 van de wet.

B. Artikel 4 wordt als volgt gewijzigd:

In het tweede lid wordt “artikel 13.4, eerste en tweede lid van de wet” vervangen door: de artikelen 13.2b en 13.4 van de wet.

C. 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.

D. Artikel 7 wordt gewijzigd als volgt:

In onderdeel b wordt “artikel 13.4 van de wet” vervangen door: de artikelen 13.2b en 13.4 van de wet.

E. Artikel 10 komt te luiden:

Artikel 10

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 Staatssecretaris van Economische Zaken,

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,

De Minister van Defensie,

NOTA VAN TOELICHTING

ALGEMEEN

I. Inleiding

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 13.5 Tw). In dit besluit worden die regels nader uitgewerkt. Hiermee wordt uitvoering gegeven aan de verplichtingen, zoals die voortvloeien uit artikel 7 van de richtlijn dataretentie. Mede namens de Staatssecretaris van Economische Zaken en de Ministers 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.

II. Verplichtingen richtlijn

De richtlijn dataretentie bevat, naast de verplichting om bepaalde categorieën van gegevens gedurende een bepaalde termijn te bewaren, 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 (artikel 7). Tenslotte bevat de richtlijn het richtsnoer dat de gegevens op zodanige wijze zouden moeten worden opgeslagen dat voorkomen wordt dat deze meermalen worden bewaard (Overweging 13).

De verwerking van persoonsgegevens door de aanbieders in het kader van het aanbieden van openbare telecommunicatienetwerken en openbare telecommunicatiediensten valt onder de reikwijdte van de Wet bescherming persoonsgegevens (Wbp). De verantwoordelijke dient de nodige maatregelen te treffen opdat de persoonsgegevens, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens verder verwerkt, juist en nauwkeurig zijn (artikel 11, tweede lid, Wbp). Ook is de verantwoordelijke verplicht passende technische en organisatorische maatregelen te treffen om persoonsgegevens te beveiligen tegen verlies of enige andere vorm van onrechtmatige gegevensverwerking (artikel 13 Wbp). Op grond van de Telecommunicatiewet geldt voor de

aanbieders van openbare elektronische communicatienetwerken en van openbare elektronische communicatiediensten (hierna ook te noemen: de aanbieder) 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. Hoofdstuk 13 van de Telecommunicatiewet geeft regels inzake het bevoegd aftappen. De aanbieders zijn verplicht medewerking te verlenen aan de uitvoering van een vordering of verzoek tot het opnemen van telecommunicatie en aan de bevoegde autoriteiten de informatie te verstrekken die noodzakelijk is om hun bevoegdheden op dat gebied te kunnen uitoefenen (artikelen 13.2 en 13.4 Tw). De desbetreffende gegevens hebben een uiterst gevoelig karakter vanwege het risico dat deze ter kennis komen van onbevoegden waardoor het welslagen van het opsporingsonderzoek of de veiligheid van de staat in ernstige mate in het geding kan komen. Het tot nu toe geldende Besluit beveiliging gegevens aftappen telecommunicatie (hierna ook te noemen: het oude Besluit of de afkorting Bbgat) gaf nadere regels voor de beveiliging van de gegevens ter uitvoering van een vordering of een verzoek op grond van de artikelen 13.2 of 13.4 van de Telecommunicatiewet, teneinde te voorkomen dat inbreuk wordt gemaakt op de vertrouwelijkheid van deze gegevens en, voor zover een dergelijke inbreuk heeft plaatsgevonden, in maatregelen waarmee op een snelle en adequate wijze daarop kan worden gereageerd. Het besluit verplichtte de aanbieder tot het treffen van maatregelen ter voorkoming van kennisneming door onbevoegden van de informatie welke door de aanbieder aan de bevoegde autoriteit is verstrekt alsmede de gegevens welke zijn vervat in het aan deze verstrekking ten grondslag liggende verzoek of vordering van de bevoegde autoriteit.

In de Wet bewaarplicht telecommunicatiegegevens worden, aanvullend aan de meer algemene normen op basis van de Wet bescherming persoonsgegevens 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 niet alleen de bescherming van de persoonlijke levenssfeer aan de orde maar ook de afscherming van gevoelige informatie, omdat het welslagen van het opsporingsonderzoek of de veiligheid van de staat in ernstige mate in het geding kan komen als deze informatie ter kennis komt van onbevoegden. Voor de nadere uitwerking van de te treffen maatregelen in verband met de beveiliging van, de toegang tot, en de vernietiging van de gegevens wordt aangesloten bij de regeling van het oude Besluit. Een dergelijke aansluiting ligt voor de hand omdat dit besluit reeds regels kende voor de beveiliging van gegevens die de aanbieders verstrekken 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). 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 oude Besluit bevatte een aantal kernelementen. Dit betrof een verduidelijking van verschillende aspecten waarop de door de aanbieder te treffen beveiligingsmaatregelen zich dienen te richten (artikel 2, tweede lid, Bbgat), een bijlage met de verplicht te treffen beveiligingsmaatregelen (artikel 2, derde lid, jo. bijlage, Bbgat), de verplichting tot vastlegging van de beveiligingsmaatregelen in een beveiligingsplan (artikel 3 Bbgat), 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 Bbgat), maatregelen die genomen moeten worden bij geoorloofde inbreuken op de vertrouwelijkheid (artikel 5 Bbgat) en een regeling voor de situatie dat door een aanbieder werkzaamheden zijn uitbesteed aan een derde (artikel 7 Bbgat).
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, j, 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. Indien de gegevensverwerking in Nederland wordt uitgevoerd in het kader van de activiteiten van vestigingen van de verantwoordelijke in verschillende EU-lidstaten, dient de verantwoordelijke de noodzakelijke maatregelen te treffen om te waarborgen dat met de gegevensverwerking van iedere vestiging wordt voldaan aan de regels van het betreffende land. Dit doet echter niet af aan de toepasselijkheid van de Nederlandse regels terzake.

III. Gevolgen voor de gegevensverwerking door de aanbieders

De gegevens die worden gegenereerd of verwerkt naar aanleiding van een communicatie zijn aanwezig op het netwerk van de aanbieders. 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. Onverminderd het bepaalde in de Wet politiegegevens en de Wet op de inlichtingen- en veiligheidsdiensten 2002, voor zover de gegevens verder worden verwerkt op grond van die wet, hebben de regels van de Wet bescherming persoonsgegevens en van de Telecommunicatiewet betrekking op alle vormen van verwerking van persoonsgegevens, zoals het samenbrengen, vastleggen, opslaan of loggen van deze gegevens, al dan niet in een afzonderlijk gegevensbestand (artikelen 11.2 en 11.3 Tw). Deze regels zijn van toepassing op de gegevens die door de aanbieders worden bewaard met het oog op de wettelijke bewaarplicht.

De artikelen 11.5 en 11.5a Tw bieden de grondslag voor de verdere verwerking van de gegevens ten behoeve van doeleinden die samenhangen met hun eigen bedrijfsvoering. Dit betreft doelen als de facturering, verkeersbeheer, het opsporen van fraude en marktonderzoek. Daarbij wordt doorgaans onderscheid gemaakt tussen klantgegevens en verkeersgegevens. De bestanden zijn toegankelijk voor medewerkers die belast zijn met taken of werkzaamheden op het gebied van de eerdergenoemde zakelijke doeleinden, zoals de klantenservice (vragen over abonnementen of facturering). Op grond van de algemene eisen van de Wet

bescherming persoonsgegevens en de Telecommunicatiewet dienen deze gegevens te zijn beveiligd tegen kennisneming door onbevoegden. De gegevens die met het oog op zakelijke doeleinden worden verwerkt kunnen echter tevens onder de wettelijke bewaarplicht vallen. Het doel van de wettelijke regeling is te waarborgen dat zowel het feit dat de behoeftestellers hun interesse voor het telecommunicatieverkeer rond bepaalde personen kenbaar hebben gemaakt, alsook de raadpleging en het bijeenbrengen van de gegevens dan wel het verrichten van andere handelingen met het oog op de verstrekking van de betreffende telecommunicatiegegevens, alsmede de verstrekking zelf ten behoeve van de opsporing en vervolging van strafbare feiten dan wel de bescherming van de veiligheid van de staat, adequaat worden afgeschermd. Vanwege het feit dat een deel van de gegevens tevens verder kan worden verwerkt met het oog op de zakelijke doeleinden van de aanbieder is het wenselijk dat de te stellen eisen niet zozeer betrekking hebben op de bewaring van de gegevens als zodanig, als wel op de raadpleging en de verdere verwerking daarvan met het oog op het voldoen aan een vordering of verzoek op grond van de artikelen 13.2b en 13.4 van de Telecommunicatiewet. Met de aanvulling van het oude Besluit wordt aanvullend geregeld dat ook de verdere verwerking met het oog op dat doel onder de reikwijdte van het Besluit beveiliging gegevens telecommunicatie zal vallen. Daardoor wordt verzekerd dat niet alleen de informatie die door de aanbieder aan de bevoegde autoriteit is verstrekt maar ook de raadpleging van de bewaarde gegevens en de verdere verwerking daarvan met het oog op het voldoen aan de vordering op grond van de artikelen 13.2b en 13.4 van de wet, zoals het ophalen van de gegevens en het samenbrengen van de gegevens, ook onder de reikwijdte van het Besluit beveiliging gegevens telecommunicatie valt. Hiermee wordt uitvoering gegeven aan de verplichtingen tot beveiliging van de gegevens, zoals die voortvloeien uit artikel 7 van de richtlijn dataretentie.

Het oude Besluit bevatte 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. De normen hebben betrekking op de beveiliging van de toegang tot de gegevens. Dit omvat zowel de personen als de processen (toepassingen, applicaties, informatiesystemen e.d.). Indien nodig kan hieraan door middel van een beleidsregel van de minister van Economische Zaken nadere uitwerking worden gegeven. Op grond van het besluit is de aanbieder verplicht tot het opstellen van een beveiligingsplan, waarin hij aangeeft op welke wijze door hem uitvoering is gegeven aan zijn beveiligingsplicht (artikel 3). In de bijlage bij dit besluit zijn de te treffen maatregelen uitgewerkt. In het beveiligingsplan moet worden aangegeven op welke wijze uitvoering is gegeven aan de bescherming en beveiliging van de gegevens die worden verstrekt ten behoeve van het onderzoeken, opsporen of vervolgen van strafbare feiten en de gegevens die in het belang van de nationale veiligheid worden verstrekt aan de inlichtingen- en veiligheidsdiensten. Daarbij dient specifieke aandacht te worden besteed aan het onderscheid in de verschillende beveiligingsregimes, omdat dezelfde gegevens gebruikt kunnen worden ten behoeve van zakelijke doeleinden van de aanbieders als ten behoeve van het voldoen aan een vordering op grond van de artikelen 13.2b en 13.4 van de Telecommunicatiewet. De gegevens die de aanbieders voor eigen doeleinden verwerken, dienen afdoende beschermd zijn in het licht van de eisen die op grond van de Wet bescherming persoonsgegevens en de Telecommunicatiewet van toepassing zijn. In het beveiligingsplan dienen de aanbieders inzichtelijk te maken welke organisatorische of technische maatregelen aanvullend zijn getroffen ten aanzien van de gegevens die onder de bewaarplicht vallen, inclusief de toegang daartoe, om te waarborgen dat ten aanzien van het raadplegen en verder verwerken van die gegevens wordt voldaan aan de eisen van het Besluit beveiliging gegevens telecommunicatie.

Het oude Besluit bevatte geen specifieke regels over de vernietiging van gegevens door de aanbieders. Op dit punt is aanvulling noodzakelijk; daartoe dient het nieuwe artikel 5 van het besluit. De verplichting tot vernietiging

heeft betrekking op de gegevens die op grond van artikel 13.2a van de Telecommunicatiewet worden bewaard. Zoals hierboven reeds opgemerkt, is het niet uitgesloten dat deze gegevens ook voor zakelijke doeleinden worden verwerkt, zoals bedoeld in de artikelen 11.5 en 11.5a van de Telecommunicatiewet. Dit betreft doeleinden als facturering en marktonderzoek. Ingeval de bewaarde gegevens op grond van de Telecommunicatiewet verder kunnen worden verwerkt met het oog op andere doeleinden, dan zijn de voor die doeleinden geldende verplichtingen tot anonimisering of vernietiging op die verdere verwerking van toepassing.

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.

De huidige regels staan er niet aan in de weg dat een aanbieder ervoor zou kiezen de te bewaren gegevens bij een derde partij op te slaan die dan vervolgens als bewerker van die gegevens fungeert. Ook zouden de aanbieders kunnen besluiten om gezamenlijk de gegevens op een centraal punt op te slaan, bijvoorbeeld door middel van opslag bij een derde partij die dan vervolgens als bewerker fungeert. In beide gevallen zijn de verplichtingen van het Besluit beveiliging gegevens telecommunicatie echter onverkort van toepassing en blijft de aanbieder verantwoordelijk voor de gegevensverwerking door de bewerker, ook jegens de toezichthoudende autoriteiten.

Voor wat betreft de verstrekking van gegevens ten behoeve van de opsporing en vervolging van strafbare feiten 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 in de loop 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 de Telecommunicatiewet biedt hiervoor een basis.

IV. Financiële gevolgen; administratieve lasten voor burgers en bedrijven

De beveiligingseisen die in artikel 7 van de Europese Richtlijn in algemene bewoordingen zijn gesteld, geven aan de lidstaten ruimte voor tactische en operationele keuzen. Er wordt onder andere gesproken over de verplichting van de lidstaten tot nemen van adequate technische en organisatorische maatregelen. Derhalve diende nader bepaald te worden in welke risicoklasse het proces van dataretentie moet worden ingedeeld en daarvan afgeleid, tot een juiste specificatie van beveiligingsmensen te komen. In het onderzoek van Verdonck, Klooster & Associates is met betrekking tot het niveau van beveiliging en de kostenberekening aansluiting gevonden bij de eisen met betrekking tot een op essentiële punten vergelijkbaar proces dat de overheid op een eerder moment heeft geformuleerd en vastgelegd namelijk in de bijlage van het oude Besluit. Hierbij is overwogen dat:
1. de actoren die betrokken zijn bij dit proces vrijwel dezelfde actoren zijn als die welke betrokken zijn bij het proces van de bewaring van telecommunicatiegegevens;
2. het betreft eveneens zeer gevoelige persoonsgegevens die ingeval van misbruik tot grote

schade kunnen leiden voor het object van onderzoek en het imago van de betrokken actoren in het proces van de bewaring van telecommunicatiegegevens;
3. het belang van de actoren bij de juistheid en bescherming van de gegevens vergelijkbaar is;
4. het belang van de behoeftestellers bij de bescherming van bron van de vordering, identiteit van het object van onderzoek en de vergaarde informatie vergelijkbaar is.
In de bijlage van het tot oude Besluit zijn concrete beveiligingseisen opgenomen die, zij het met andere formuleringen en terminologie, inhoudelijk niet echt afwijken van de betreffende (selectie) beveiligingseisen uit de ISO normering. In de informatiearchitectuur van de door VKA weergegeven implementatieopties zijn de relevante maatregelen opgenomen om de te nemen beveiligingsmaatregelen in te vullen. Daarbij is uitgegaan van het hoogste beveiligingsniveau (staatsgeheim). De daarmee gemoeide investerings- en personele kosten zijn door middel van een rekenmodel toegevoegd aan de kosten voor acquisitie, opslag en bevraging.
De marktwerking wordt niet of nauwelijks beïnvloed. Enerzijds omdat het voorliggende Besluit beveiliging gegevens telecommunicatie voor alle aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten geldt, anderzijds omdat dit besluit nauw aansluit bij het oude Besluit, waarin reeds regels zijn opgenomen rond de beveiliging van gegevens en de verstrekking van informatie. De aanbieders dienden zich reeds aan die eisen te conformeren. De grote(re) aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten zullen naar alle waarschijnlijkheid geen extra investeringen terzake behoeven te doen. Voor de echt kleine aanbieders is het afhankelijk van de wijze van opslag en daarbij mogelijke wijzen van vernietiging.

Met de voorgestelde regeling wordt nauw aangesloten bij het oude Besluit. Mede gelet op de totale financiële consequenties in verband met de Wet bewaarplicht telecommunicatiegegevens - daarvoor kan worden verwezen naar de memorie van toelichting bij deze wet - vloeien uit de voorgestelde regeling geen extra lasten van zodanig substantiële aard voort, dat deze een afzonderlijke begroting en dekking zouden rechtvaardigen. Aldus kan worden geconcludeerd dat uit het besluit geen andere financiële gevolgen voortvloeien dan de kosten die al zijn voorzien bij de Wet bewaarplicht telecommunicatiegegevens.

V. Handhaving van de regels

Op de naleving van de in dit besluit gestelde regels wordt toezicht uitgeoefend door Agentschap Telecom. Hierop is nader ingegaan in de memorie van toelichting bij de Wet bewaarplicht telecommunicatiegegevens. Aan de toezichthouder komen de bevoegdheden uit hoofdstuk 5 van de Algemene wet bestuursrecht (Awb) toe. Dit is reeds beschreven in de nota van toelichting bij het oude Besluit. De bestuursrechtelijke sanctioneringsmogelijkheden die kunnen worden toegepast indien wordt geconstateerd dat in strijd wordt gehandeld met hetgeen bij of krachtens artikel 13.5 Tw is bepaald, betreffen de mogelijkheden tot het toepassen van bestuursdwang (artikel 15.2 Tw), het opleggen van een last onder dwangsom (artikel 15.2 Tw jo. artikel 5:32 Awb) of het opleggen van een bestuursrechtelijke boete (artikel 15.4 ev. Tw) Daarnaast bestaat de mogelijkheid dat de overtreding strafrechtelijk wordt gesanctioneerd. De overtreding van de voorschriften, gesteld bij of krachtens artikel 13.5 Tw is in artikel 1 van de Wet op de economische delicten als economisch delict aangemerkt en uit dien hoofde strafbaar. In geval van overtreding kan een geldboete worden opgelegd van de vierde categorie (18 500 euro). Overtreding van de voorschriften zoals deze zijn neergelegd in artikel 13.5 Tw, indien opzettelijk gepleegd, zijn bovendien aan te merken als een misdrijf in de zin van de Wed. Overigens is het niet mogelijk dat bij een geconstateerde overtreding gelijktijdig zowel een bestuursrechtelijke boete als een strafrechtelijke sanctie ingevolge de Wed wordt opgelegd. Dubbele vervolging en bestraffing van hetzelfde feit is niet mogelijk; artikel 15.4, vierde en vijfde lid, Tw geeft daarvoor een voorziening.

VI. De adviezen

Het openbaar ministerie, de politie – verenigd in het Nederlands Politie Instituut (NPI) – het College bescherming persoonsgegevens (CBP), Agentschap Telecom en de Nederlandse Orde van Advocaten (NOvA) zijn om advies gevraagd over het ontwerpbesluit. Het ontwerpbesluit is tevens voorgelegd aan het Adviescollege toetsing administratieve lasten (Actal). Daarnaast is het ontwerpbesluit gepubliceerd op de website van het Ministerie van Economische Zaken en is een ieder gedurende een termijn van vier weken in de gelegenheid gesteld een reactie in te brengen.

Naar aanleiding van het ontwerpbesluit beveiliging gegevens telecommunicatie is advies uitgebracht door de ACT, KPN, @Home, de Raad van Hoofdcommissarissen (mede namens het korpsbeheerdersberaad), het College bescherming persoonsgegevens, Agentschap Telecom en de Nederlandse Orde van Advocaten.

De Associatie van Competitieve Telecomoperators (ACT) kan zich niet vinden in de gekozen opzet en vraagt aandacht door een aantal punten. Dit betreft in de eerste plaats de voorgenomen aanpassing van het (oude) Besluit beveiliging gegevens aftappen telecommunicatie, deze uitbreiding van dit besluit tot het bewaren van gegevens in het kader van de dataretentie is volgens de ACT ongewenst en niet nodig. Het bewaren van gegevens is thans reeds onderhevig aan bestaande verplichtingen op basis van artikel 13 Wbp en de artikelen 11.2 en 11.3 Tw, het lijkt niet nodig om voor het bewaren van gegevens in het kader van dataretentie extra beveiligingseisen te stellen. De ACT bepleit de regelgeving te beperken tot het verstrekken van gegevens in het kader van dataretentie. Daarbij zou ernaar moeten worden gestreefd dat de eventuele beveiligingseisen en vernietigingstermijnen op Europees niveau maximaal worden geharmoniseerd, ten behoeve van de werkbaarheid van de regels voor de aanbieders die in meerdere Europese landen diensten aanbieden. De ACT acht de voorgestelde vernietigingstermijn van acht dagen veel te kort en adviseert eerst nader te onderzoeken wat de mogelijkheden zijn van een Europees geharmoniseerde termijn, bijvoorbeeld in het kader van de Informal Electronic Dataretention Group van de Europese Commissie. Tenslotte steunt de ACT in beginsel het uitgangspunt dat op de verstrekking van gegevens een ETSI standaard van toepassing dient te zijn maar kan de ACT zich op voorhand nog niet committeren aan een standaard die nog niet is vastgesteld. Voorzover door Nederland vooruit wordt gelopen op een ETSI-standaard, moet dat geschieden in zeer nauw overleg met de aanbieders.

KPN wijst er eveneens op dat het van toepassing verklaren van het (oude) Besluit beveiliging gegevens aftappen telecommunicatie op de bewaarplicht een fundamentele en nodeloze verandering aanbrengt. Voor de bedrijfsvoering beschikt de aanbieder van telecommunicatie over telecommunicatiegegevens van haar klanten. Voor verschillende verwerkingsgrondslagen zijn specifiek per verwerkingsgrondslag bewaartermijnen gesteld. In essentie betreft het in alle gevallen dezelfde gegevens. Door voor de bewaring aanvullende eisen te stellen ten aanzien van de gegevens als zodanig zouden de facto ook voor de andere toegestane toepassingen de strengere eisen gaan gelden ten aanzien van de verwerking van die gegevens. Hierdoor wordt de efficiency van de bedrijfsvoering in ernstige mate verstoord. Tenslotte wijst KPN op de bescherming van de persoonlijke levenssfeer indien telecommunicatiediensten worden afgehandeld door middel van netwerkfaciliteiten in het buitenland. Om de vrijheid van het economisch verkeer te waarborgen dient de verwijzing in de nota van toelichting te worden aangevuld met de woorden “met inachtneming van de in het betreffende land vigerende wetgeving”.

@home acht onverkorte toepassing van het (oude) Besluit beveiliging gegevens aftappen telecommunicatie op de bestanden, waar de bewaarplicht zich op richt, niet voor de hand liggend en ongewenst. Het opleggen van eisen aan het gehele bestand is niet als proportioneel te beschouwen, toegevoegde waarde aan de informatie ontstaat slechts wanneer een selectie uit dit bestand wordt gemaakt. Het is dan ook redelijk om uitsluitend extra eisen te stellen aan deze selectie uit het bestand van opgeslagen gegevens. Verder acht @Home het wenselijk om voor de verplichting tot vernietiging van de gegevens een uitzondering te maken voor gegevens die voor een langere termijn met het oog op andere doelen, zoals de facturering, kunnen worden verwerkt.

Agentschap Telecom acht het ontwerpbesluit uitvoerbaar en handhaafbaar als de opmerkingen uit het advies worden verwerkt in het conceptbesluit. Daarbij wijst Agentschap Telecom erop dat de aanbieders ervoor kunnen kiezen om de te bewaren gegevens in het buitenland op te slaan. Agentschap Telecom gaat er echter vanuit dat op dit moment het houden van toezicht alleen op Nederlandse bodem mogelijk en toegestaan is en acht het onduidelijk hoe de controle in het buitenland vorm gegeven en geregeld gaat worden. Verder beveelt Agentschap Telecom aan om aan artikel 2 van het ontwerpbesluit een nieuw derde lid toe te voegen waarin de aanbieder wordt verplicht in het beveiligingsplan aan te geven hoe hij waarborgt dat de bij of krachtens de Telecommunicatiewet en de Wet bescherming persoonsgegevens gestelde regels worden toegepast op de te bewaren gegevens. Voorts wijst Agentschap Telecom op mogelijk onvoorziene consequenties van een dergelijke toepassing, zoals de verplichting voor de aanbieders om van iedere vernietiging van gegevens een rapport naar de bevoegde autoriteit te zenden. Voor het begrip openbare aanbieder vormen afspraken tussen DGET, OPTA en het agentschap de basis voor de invulling van dit begrip. Het ligt voor de hand de lijst van aanbieders, die door OPTA wordt gehanteerd, als uitgangspunt te nemen. Tenslotte wijst Agentschap Telecom op de mogelijke consequenties van de bewaarplicht voor de personele capaciteit van de dienst en meent dat zonder de benodigde extra financiële middelen en formatie-uitbreiding deze nieuwe taak niet uitvoerbaar en handhaafbaar is.

De Raad van Hoofdcommissarissen vraagt aandacht voor het feit dat uit een passage uit de nota van toelichting de indruk zou kunnen ontstaan dat geen nadere regels worden gesteld aan de wijze waarop de aanbieders aan een vordering of verzoek voldoen. De Raad wijst erop dat het voor de politie van zeer groot belang is dat de aanlevering van de gegevens gestandaardiseerd via elektronische weg en bovendien in een uniform format plaatsvindt. Verder wordt erop gewezen dat de nota van toelichting het besluit van toepassing verklaart op de gegevens die door de aanbieders worden bewaard ten behoeve van het onderzoeken, opsporen of vervolgen van strafbare feiten. De Raad gaat er verder vanuit dat, indien een aanbieder zou besluit om de gegevens door de overheid of een derde partij (een zogenaamde ‘trusted third party’) te laten bewaren, genoemd besluit van overeenkomstige toepassing is. Tenslotte spreekt hij zijn zorg uit ten aanzien van de mogelijkheden van handhaving van de eisen als gesteld in de Telecommunicatiewet en de Wet bescherming persoonsgegevens indien telecommunicatieverkeer wordt afgehandeld door middel van netwerkfaciliteiten in het buitenland. Diezelfde zorg heeft hij voor de gevallen waarin de aanbieders de verkeersgegevens in het buitenland opslaan.

Het College bescherming persoonsgegevens wijst erop dat uit het wetsvoorstel blijkt dat de regering vooralsnog kiest voor decentrale opslag van verkeersgegevens, dat wil zeggen bij de aanbieders zelf. Dit is in lijn met het advies van het CBP van 22 januari 2007, waarbij het onontkoombaar is om een strikt logische scheiding voor te schrijven tussen de data die ten behoeve van de opsporing worden bewaard en de operationele data. Deze scheiding is naar het oordeel van het CBP nog onvoldoende uitgewerkt in het ontwerpbesluit beveiliging gegevens telecommunicatie. In de uitwerking van de beveiligingsverplichting die voorgesteld wordt in (de toelichting bij) Artikel I, onder A, onderdeel b, dient scherper onderscheid gemaakt te worden tussen het

beveiligingsregime voor gegevens die aanbieders voor eigen bedrijfsdoeleinden (mogen) bewaren en anderzijds het (hogere) beveiligingsregime voor de set gegevens die de aanbieders uitsluitend bewaren met het oog op de opsporing en de staatsveiligheid. Allereerst is het van belang dat de verplichtingen uit de Wbp en de Tw van toepassing zijn op het moment dat de gegevens ontstaan, en dus niet pas nadat ze ten behoeve van verdere verwerking uit het netwerk worden opgehaald. De vereisten op het gebied van de beveiliging van gegevens zijn dus van toepassing op alle telecommunicatiegegevens die de aanbieders genereren of ontvangen. Daarnaast verplicht de richtlijn dataretentie de lidstaten om specifieke beveiligingsmaatregelen voor te schrijven voor gegevens die uitsluitend ten behoeve van de bewaarplicht worden bewaard. Om te voorkomen dat er onduidelijkheid ontstaat acht het CBP het noodzakelijk om te preciseren wanneer het 'zwaarste' regime van beveiliging precies geldt en hoe technisch gewaarborgd kan worden dat de aanbieders daadwerkelijk onderscheid maken in het beveiligingsniveau van de gegevens die voor de eigen bedrijfsvoering (mogen) worden ingezet en van de gegevens die uitsluitend worden bewaard om te kunnen voldoen aan de bewaarplicht. Daarbij moet wel inzichtelijk worden gemaakt wat de implicaties zijn van de gekozen benadering in het besluit voor de bedrijfsvoering van de aanbieders.

De Nederlandse Orde van Advocaten constateert dat het ontwerpbesluit enkele technische veranderingen doorvoert en heeft te kennen gegeven geen aanleiding te zien voor commentaar.

Naar aanleiding van de adviezen van de ACT, KPN, @Home en het College bescherming persoonsgegevens is de opzet van de voorgestelde regeling verhelderd. In de oorspronkelijke opzet, die in consultatie is gegeven, is voorgesteld de op grond van artikel 13.2a van de wet te bewaren gegevens onder de reikwijdte van het Besluit beveiliging gegevens telecommunicatie te brengen. De inhoud van de ingebrachte adviezen heeft echter tot het inzicht geleid dat een dergelijke benadering, strikt genomen, niet goed verenigbaar is met de bedrijfsvoering van de aanbieders en vanuit het oogpunt van de bescherming en beveiliging van de gegevens en de belangen van de behoeftestellers ook niet strikt noodzakelijk is. Gegevens, die door de aanbieders op grond van de wettelijke bewaarplicht worden verwerkt, worden doorgaans niet in een afzonderlijke database opgeslagen maar vormen onderdeel van een bestand van gegevens welke door de aanbieders ook met het oog op zakelijke doeleinden worden verwerkt. De toepassing van de regels van het besluit op de bewaring van de gegevens met het oog op de bewaarplicht kan aanleiding geven tot onduidelijkheid over de verhouding tussen de regels van dit besluit en de bedrijfsvoering van de aanbieders. Gelet op de adviezen van de aanbieders lijken zij uit de voorgestelde regeling af te leiden dat deze strekt tot separate opslag van de gegevens. Een dergelijke consequentie wordt met dit besluit echter niet beoogd, omdat een separate opslag van de gegevens risico's in zich draagt ten aanzien van de bescherming en de beveiliging van de gegevens en bovendien de bedrijfsvoering van de aanbieders ernstig zou kunnen belemmeren, zonder dat het belang van gegevensbescherming en –beveiliging tot een dergelijke maatregel noodzaakt.
Het voorgaande heeft geleid tot wijziging van het voorgestelde onderdeel c van artikel 2 en aanpassing c.q. aanvulling van de nota van toelichting, ter verheldering van de reikwijdte van de verplichtingen voor de aanbieders. Uitgangspunt daarbij is dat op grond van de bestaande normen van de Wbp en de Telecommunicatiewet reeds een voldoende niveau van bescherming en beveiliging van de te bewaren gegevens wordt geboden en dat dan ook niet zozeer de bewaring van de gegevens als zodanig relevant is voor de noodzaak van de aanvullende maatregelen ter bescherming en beveiliging als wel het verband tussen die gegevens en de opsporing en vervolging van strafbare feiten. Omdat de aanbieders te bewaren gegevens onder omstandigheden ook voor andere doeleinden kunnen gebruiken dienen de aanvullende specifieke verplichtingen voor de aanbieders op het gebied van de bescherming en de beveiliging van de bewaarde gegevens te zijn gericht op de raadpleging en de verdere verwerking daarvan ten behoeve van opsporing en vervolging. De

toegang tot de gegevens dient te zijn voorbehouden aan daartoe geautoriseerde personen voorzover dit voor hun functie noodzakelijk is. Met deze benadering wordt nauw aangesloten bij de bestaande verplichtingen van de aanbieders op grond van het tot oude Besluit. Een dergelijke benadering verhoudt zich ook beter met de verplichting tot vernietiging van de bewaarde gegevens. Deze verplichting kan bezwaarlijk van absolute aard zijn omdat de Telecommunicatiewet niet uitsluit dat die gegevens in bepaalde gevallen, al dan niet in geanonimiseerde vorm, verder worden verwerkt met het oog op andere doelen die verband houden met zakelijke doeleinden van de aanbieders. Mede naar aanleiding van het advies van @Home is hier in de artikelsgewijze toelichting bij artikel 5, tweede lid, nader op in gegaan.

In zijn advies heeft het College bescherming persoonsgegevens er daarentegen op gewezen dat de scheiding tussen de data die ten behoeve van de opsporing worden verwerkt en de operationele data onvoldoende is uitgewerkt in het conceptbesluit beveiliging gegevens telecommunicatie. Met de voorgestelde wijziging wordt een scherper onderscheid gemaakt tussen het beveiligingsregime voor de gegevens die de aanbieders voor eigen bedrijfsdoeleinden gebruiken en de gegevens die de aanbieders verstrekken met het oog op de opsporing en de staatsveiligheid. Anders dan het Cbp kennelijk veronderstelt kan echter geen eenduidig onderscheid worden gemaakt tussen gegevens die uitsluitend voor de eigen bedrijfsdoeleinden worden bewaard en gegevens die uitsluitend worden bewaard met het oog op de opsporing en de staatsveiligheid. Verder geldt dat de aanvullende eisen van het Besluit beveiliging gegevens telecommunicatie zijn gericht op de toegang tot de gegevens en niet op de bewaring daarvan. Naar aanleiding van het advies van het Cbp is in de nota van toelichting verhelderd dat de beveiligingsverplichtingen, die voortvloeien uit de Wbp en de Telecommunicatiewet, van toepassing zijn op de bewaarde gegevens en wordt er op gewezen dat de aanbieders in het beveiligingsplan inzichtelijk dienen te maken op welke wijze wordt voldaan aan de maatregelen van de bijlage bij het Besluit beveiliging gegevens telecommunicatie. Daarbij moet onderscheid worden gemaakt in de verschillende beveiligingsregimes die van toepassing zijn op de verdere verwerking van de gegevens voor de verschillende doeleinden, inclusief de toegang tot die gegevens. Daarmee wordt tevens tegemoet gekomen aan de wens van de ACT. Opneming van een afzonderlijke verplichting daartoe in een nieuw derde lid van artikel 3, zoals door Agentschap Telecom bepleit, ligt minder in de rede omdat dit reeds voortvloeit uit het bestaande eerste lid.

Zowel de ACT als de Raad van Hoofdcommissarissen hebben in hun advies aandacht geschonken aan de toepassing van de zogenaamde ETSI- standaard op de verstrekking van de gegevens door de aanbieders. Naar verwachting zal deze standaard in de loop van 2008 kunnen worden vastgesteld en ingevoerd. Voor alle duidelijkheid kan echter worden benadrukt dat het voorliggende besluit niet voorziet in toepassing van deze gemeenschappelijke standaard. Ingeval daarover in de nabije toekomst overeenstemming mocht bestaan tussen de betrokken partijen, dan kan dit aanleiding vormen om bij algemene maatregel van bestuur te bepalen dat een dergelijke standaard wordt gehanteerd. Op dit punt dienen de ontwikkelingen echter te worden afgewacht.

Naar aanleiding van de opmerkingen van de Raad van Hoofdcommissarissen over de bewaring van gegevens door een ‘trusted third party’ is in de nota van toelichting op dit punt aangevuld.

Naar aanleiding van de opmerking van KPN over de bescherming van de persoonlijke levenssfeer bij de afhandeling van telecommunicatieverkeer via netwerkfaciliteiten in het buitenland is de nota van toelichting op dit punt aangevuld. Ten aanzien van het door Agentschap Telecom en de Raad van Hoofdcommissarissen naar voren gebrachte punt van zorg inzake de handhaving van de eisen van de Telecommunicatiewet en de Wet bescherming persoonsgegevens als telecommunicatieverkeer wordt afgehandeld door middel van netwerkfaciliteiten in het buitenland geldt het volgende. Indien telecommunicatieverkeer wordt afgehandeld door

middel van netwerkfaciliteiten in het buitenland is het risico aan de orde dat gevoelige gegevens over personen, wier gedragingen door de behoeftestellers worden gevolgd in verband met mogelijke betrokkenheid bij ernstige strafbare feiten of activiteiten die een inbreuk maken op de staatsveiligheid, ter kennis komen van een bredere kring van personen dan op grond van het Besluit beveiliging gegevens telecommunicatie is voorzien. De uitoefening van adequaat toezicht op een strikte naleving van de regels van dit besluit zal echter kunnen worden belemmerd doordat de gegevensverwerking niet in Nederland plaatsvindt. Dit is ook thans reeds het geval en vloeit als zodanig niet voort uit de invoering van een bewaarplicht voor telecommunicatiegegevens. Ook thans wordt, naar aanleiding van een verzoek of vordering van de behoeftestellers, door de aanbieders medewerking verleend aan het aftappen of opnemen van telecommunicatie dan wel het verstrekken van verkeersgegevens. Zoals ook uit de adviezen van Agentschap Telecom en de Raad van Hoofdcommissarissen blijkt, wordt met de invoering van de wettelijke bewaarplicht voor telecommunicatiegegevens de aandacht op dit risico gevestigd. Mede naar aanleiding van het door de adviesorganen naar voren gebrachte punt zal op korte termijn, in overleg met alle betrokken partijen, nader onderzoek worden verricht naar de bescherming van de verwerking van gegevens door de aanbieders naar aanleiding van het verlenen van medewerking aan het aftappen of opnemen van telecommunicatie dan wel het verstrekken van verkeersgegevens. De consequenties van dergelijke maatregelen voor de bedrijfsvoering van de aanbieders dienen nader in kaart te worden gebracht. Daarnaast stelt de regelgeving van de Europese Gemeenschap ten aanzien van het vrije verkeer van diensten restricties aan het opleggen van beperkingen aan de afhandeling van telecommunicatiediensten via netwerkfaciliteiten in het buitenland. Bij het formuleren van eventuele aanvullende maatregelen, zoals een verplichting tot opslag van de bewaarde gegevens in Nederland dan wel een verplichting tot verdere verwerking van de door de behoeftestellers verstrekte gegevens in Nederland, dienen deze aspecten dan ook nadrukkelijk betrokken te worden.

Naar aanleiding van de opmerking van de ACT over de vernietigingstermijn kan het volgende worden opgemerkt. De richtlijn verplicht tot vernietiging van de gegevens aan het einde van de bewaarperiode. Hieruit zou voortvloeien dat de gegevens, na afloop van de wettelijke bewaartermijn, direct worden vernietigd. De termijn van acht dagen beoogt echter de aanbieders enige ruimte te bieden. Daaraan liggen de volgende overwegingen ten grondslag. In de eerste plaats zal de directe vernietiging van de gegevens eenvoudiger zijn te realiseren wanneer deze geautomatiseerd worden vernietigd dan wanneer dit handmatig wordt verricht. In de tweede plaats biedt een dergelijke termijn de mogelijkheid voor de beoordeling of er aanleiding bestaat tot verdere verwerking van de bewaarde gegevens met het oog op zakelijke doeleinden van de aanbieder, op grond van hoofdstuk 11 van de wet. Tenslotte wordt met deze termijn rekening gehouden met de inrichting van het bedrijfsproces van de aanbieders, omdat de gegevens dan wekelijks langs geautomatiseerde weg kunnen worden gecontroleerd. Met de termijn van acht dagen wordt een goed evenwicht gevonden tussen de uit de richtlijn voortvloeiende verplichting tot directe vernietiging van de gegevens en het belang van de bescherming van de persoonlijke levenssfeer enerzijds en de belangen rond de bedrijfsvoering van de aanbieders anderzijds. Een termijn van dertig dagen, zoals opgenomen in de Duitse wet, leidt tot een substantiële verlenging van de bewaartermijn en lijkt niet goed verenigbaar met de verplichting van de richtlijn. De termijn van acht dagen is dan ook gehandhaafd.

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 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 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 telecommunicatie ook op de verstrekking van deze gegevens van toepassing is. Met de aanpassing van dit onderdeel wordt daarin voorzien.

Artikel I, onderdeel B

De aanpassing van artikel 4, tweede lid, betreft een technische wijziging in verband met het gestelde in de toelichting bij artikel I, onderdeel A. Met toevoeging van artikel 13.2b van de wet is dit artikel ook van toepassing op de verstrekking van telecommunicatiegegevens naar aanleiding van een vordering op grond van de artikelen 126hh, 126ii, 126nc tot en met ni en 126uc tot en met 126ui van het Wetboek van Strafvordering. De artikelen 126hh en 126ii van het Wetboek van Strafvordering hebben betrekking op de vordering tot overdracht van een geautomatiseerd gegevensbestand en van identificerende gegevens door de officier van justitie, indien een verkennend onderzoek de voorbereiding van de opsporing van terroristische misdrijven tot doel heeft. De artikelen 126nc tot en met 126ni en 126uc tot en met 126ui van het Wetboek van Strafvordering hebben betrekking op het vorderen van gegevens van aanbieders van telecommunicatiediensten, voorzover de vordering betrekking heeft op andere gegevens dan die welke gevorderd kunnen worden op grond van de artikelen 126n en 126na van het Wetboek van Strafvordering (verkeers- en gebruikersgegevens).

Artikel I, onderdeel C

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, dat wil zeggen 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 kunnen worden verwerkt voor de aldaar genoemde doelen. Deze bepalingen hebben betrekking op de gegevensverwerking ten behoeve van de zakelijke doeleinden van de aanbieders. Niet uitgesloten is dat de bewaarde gegevens na het verstrijken van de wettelijke bewaartermijn op grond van de Telecommunicatiewet verder kunnen worden verwerkt voor de in de artikelen 11.5 en 11.5a van de Telecommunicatiewet genoemde doeleinden. Dan zijn de voor die doelen geldende verplichtingen tot anonimisering of vernietiging op de verdere verwerking van toepassing. 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 zal zijn.
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. 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 D

Dit betreft eveneens een technische wijziging, in verband met het gestelde in de toelichting bij artikel 2, eerste lid, onderdeel b. Voor de nadere toelichting wordt verwezen naar het gestelde onder artikel I, onderdeel B, van deze nota van toelichting.

Artikel I, onderdeel E

Artikel 10
Het besluit geeft niet alleen regels over de bescherming en beveiliging van 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 13.2 van de wet, maar tevens over 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. 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 zou uiterlijk op 15 september 2007 moeten zijn geïmplementeerd in de nationale wetgeving (artikel 15, eerste lid). De Wet bewaarplicht telecommunicatiegegevens zal dan ook zo spoedig mogelijk in werking moeten treden. Gelet op het belang van een tijdige implementatie van de richtlijn dataretentie ligt het in de bedoeling dit besluit spoedig na plaatsing in het Staatsblad in werking te laten treden.

De Minister van Justitie,