Staatsblad
van het Koninkrijk der Nederlanden

Jaargang 2003

472

Besluit van 28 oktober 2003, houdende regels betreffende door aanbieders van openbare telecommunicatienetwerken of openbare telecommunicatiediensten te treffen beveiligingsmaatregelen ten aanzien van gegevens betreffende het aftappen en opnemen van telecommunicatie (Besluit beveiliging gegevens aftappen telecommunicatie)

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

Op de voordracht van de Staatssecretaris van Economische Zaken van 15 mei 2003, nr. WJZ/03/02344 gedaan mede namens Onze Minister van Justitie, Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties en Onze Minister van Defensie;

Gelet op de artikelen 13.2, derde lid, 13.5, tweede lid, van de Telecommunicatiewet;

De Raad van State gehoord (advies van 10 juli 2003, nr. W10.03.0182/II);

Gezien het nader rapport van de Minister van Economische Zaken van 22 oktober 2003, nr. WJZ 3057391, uitgebracht mede namens Onze Minister van Justitie, Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties en Onze Minister van Defensie;

Hebben goedgevonden en verstaan:

Artikel 1

In dit besluit wordt verstaan onder:

a. wet: Telecommunicatiewet;

b. aanbieder: aanbieder van een openbaar telecommunicatienetwerk of van een openbare telecommunicatiedienst;

c. bevoegde autoriteit:

1°. de officier van justitie of de door de korpsbeheerder voor zijn korps, dan wel door het hoofd van een andere opsporingsdienst voor zijn dienst aangewezen opsporingsambtenaar;

2°. het hoofd van de Algemene Inlichtingen- en Veiligheidsdienst, of de door hem aangewezen ambtenaar;

3°. het hoofd van de Militaire Inlichtingen- en Veiligheidsdienst, of de door hem aangewezen ambtenaar;

d. bijzondere last: last tot het aftappen of opnemen van telecommunicatie.

Artikel 2

1. De aanbieder draagt zorg voor het treffen van alle noodzakelijke beveiligingsmaatregelen om kennisneming door onbevoegden te voorkomen van de navolgende gegevens en informatie:

a. de gegevens welke in het kader van het verlenen van medewerking aan de uitvoering van een bevoegd gegeven bijzondere last dan wel een toestemming op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2002 tot het aftappen of opnemen van telecommunicatie door een bevoegde autoriteit aan de aanbieder zijn verstrekt;

b. 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 het aan deze verstrekking ten grondslag liggende verzoek of in de aan deze verstrekking ten grondslag liggende vordering om informatie van de desbetreffende bevoegde autoriteit.

2. De maatregelen, bedoeld in het eerste lid, dienen ten minste te bestaan uit:

a. maatregelen gericht op de personen die werkzaam zijn voor de aanbieder;

b. maatregelen gericht op de toegang tot de gebouwen en ruimten waarin de gegevens en informatie aanwezig zijn;

c. maatregelen gericht op een deugdelijke werking en beveiliging van het informatiesysteem waarin de gegevens en informatie worden verwerkt;

d. maatregelen gericht op het voorkomen, vaststellen en onderzoeken van een ongeoorloofde inbreuk op de vertrouwelijkheid van de gegevens en informatie;

e. maatregelen in het geval van calamiteiten.

3. Tot de maatregelen, bedoeld in het eerste en tweede lid worden in ieder geval gerekend de maatregelen, bedoeld in de bijlage bij dit besluit.

Artikel 3

1. De aanbieder draagt zorg voor een beveiligingsplan, waarin hij aangeeft op welke wijze door hem uitvoering is gegeven aan zijn beveiligingsplicht. In het beveiligingsplan wordt ten minste aangegeven op welke wijze uitvoering is gegeven aan de maatregelen, bedoeld in de bijlage.

2. Op een daartoe strekkend verzoek van de bevoegde autoriteit wordt door de aanbieder inzage verleend in het beveiligingsplan.

Artikel 4

1. De aanbieder draagt er zorg voor dat aan de uitvoering van:

a. de in artikel 13.2, eerste en tweede lid, van de wet bedoelde toestemming op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2002, en

b. de in artikel 13.4, eerste en tweede lid, van de wet bedoelde verplichting tot het verstrekken van informatie in het belang van de veiligheid van de staat,

uitsluitend personen, die een vertrouwensfunctie als bedoeld in de Wet veiligheidsonderzoeken uitoefenen en ten aanzien van wie een verklaring als bedoeld in die wet is afgegeven, medewerking verlenen.

2. De aanbieder draagt er zorg voor dat aan de uitvoering van de in artikel 13.2, eerste en tweede lid, van de wet bedoelde bevoegd gegeven bijzondere last en de in 13.4, eerste en tweede lid, van de wet neergelegde verplichting tot het verstrekken van informatie in andere gevallen dan in het belang van de veiligheid van de staat, de medewerking uitsluitend wordt verleend door personen, die aan hem een verklaring omtrent het gedrag als bedoeld in de Wet op de justitiële documentatie en op de

verklaringen omtrent het gedrag hebben overgelegd. De eerste volzin is niet van toepassing, indien de betrokken persoon een vertrouwensfunctie uitoefent als bedoeld in het eerste lid.

Artikel 5

De aanbieder stelt de desbetreffende bevoegde autoriteit terstond op de hoogte, indien op de vertrouwelijkheid van enigerlei gegevens of informatie als bedoeld in artikel 2, eerste lid, een ongeoorloofde inbreuk is gemaakt. Hierbij vermeldt de aanbieder:

a. welke informatie of gegevens het betreft;

b. de wijze waarop de inbreuk heeft plaatsgevonden;

c. de maatregelen welke zijn genomen om verdere verspreiding van bedoelde informatie of gegevens tegen te gaan en herhaling van het gebeurde te voorkomen.

Artikel 6

De aanbieder draagt er zorg voor dat de personeelsleden die belast zijn met:

a. de werkzaamheden ter uitvoering van een bevoegd gegeven bijzondere last dan wel een toestemming op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2002 als bedoeld in artikel 13.2, eerste en tweede lid, van de wet en

b. de werkzaamheden verbonden aan de informatieverstrekking als bedoeld in artikel 13.4 van de wet,

met betrekking tot deze werkzaamheden en de gegevens en informatie waarvan zij in dat kader kennis nemen, geheimhouding betrachten.

Artikel 7

1. Indien de aanbieder de uitvoering van werkzaamheden uitbesteedt aan een derde en in dat kader de derde kennis neemt of kan nemen van gegevens en informatie als bedoeld in artikel 2, eerste lid, draagt de aanbieder er zorg voor dat de derde zich verplicht:

a. de desbetreffende gegevens en informatie te beveiligen tegen kennisneming door onbevoegden;

b. met betrekking tot de desbetreffende gegevens en informatie geheimhouding te betrachten;

c. de ingevolge dit besluit gestelde maatregelen na te leven;

d. alle informatie te verstrekken die voor het toezicht op de naleving van de beveiligings- en geheimhoudingsverplichting noodzakelijk is.

2. De verplichtingen van de derde als bedoeld in het eerste lid worden geregeld in een schriftelijke overeenkomst tussen aanbieder en derde. Op een daartoe strekkend verzoek van de bevoegde autoriteit wordt inzage verleend in de overeenkomst.

3. De aanbieder is verantwoordelijk voor de naleving door de derde van de verplichtingen, bedoeld in het eerste lid.

Artikel 8

Dit besluit treedt in werking op een bij koninklijk besluit te bepalen tijdstip.

Artikel 9

Dit besluit wordt aangehaald als: Besluit beveiliging gegevens aftappen telecommunicatie.

Het advies van de Raad van State wordt niet openbaar gemaakt op grond van artikel 25a, vijfde lid j° vierde lid onder b, van de Wet op de Raad van State, omdat het uitsluitend opmerkingen van redactionele aard bevat.

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

's-Gravenhage, 28 oktober 2003

Beatrix

De Minister van Economische Zaken,
L. J. Brinkhorst

De Minister van Justitie,
J. P. H. Donner

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
J. W. Remkes

De Minister van Defensie,
H. G. J. Kamp

Uitgegeven de *vijfentwintigste* november 2003

De Minister van Justitie,
J. P. H. Donner

STB8060
ISSN 0920 - 2064
Sdu Uitgevers
's-Gravenhage 2003

BIJLAGE

ALS BEDOELD IN ARTIKEL 2, DERDE LID, VAN HET BESLUIT BEVEILIGING GEGEVENS AFTAPPEN TELECOMMUNICATIE

I. Beveiligingseis algemeen

Er is een functionaris, belast met het toezicht op de uitvoering en naleving van de beveiligingsmaatregelen. De functionaris voert daartoe regelmatig controles uit en legt de resultaten daarvan vast.

II. Beveiligingseisen ten aanzien van personeel

a. In de functiebeschrijving van personeel dat belast is met de verwerking van de informatie en gegevens wordt de verantwoordelijkheid voor de beveiliging daarvan beschreven.

b. Personeel dat in aanraking komt met de informatie en gegevens tekent een geheimhoudingsverklaring.

c. Uitsluitend personeel dat overeenkomstig de functiebeschrijving belast is met de verwerking van de informatie en gegevens heeft toegang tot de informatie en de gegevens.

III. Fysieke beveiliging en beveiliging van de omgeving

a. De informatie en de gegevens worden zoveel mogelijk binnen één ruimte geconcentreerd.

b. De ruimte waarbinnen de informatie en de gegevens aanwezig zijn is deugdelijk fysiek beveiligd.

c. De fysieke beveiliging is zodanig ingericht dat ongeautoriseerde toegang en pogingen daartoe worden gedetecteerd en dat tijdige interventie plaatsvindt.

d. Toegang tot de ruimte waar de gegevens of de informatie zich bevindt is uitsluitend toegestaan aan daartoe geautoriseerde personen voorzover dit voor hun functie noodzakelijk is.

e. Het binnentreden en verlaten van de ruimte moet zodanig zijn geregeld dat er sprake is van gecontroleerde en achteraf herleidbare toegang op individueel niveau.

f. Documenten waarin, dan wel verwisselbare gegevensdragers waarop, de informatie en de gegevens zijn vastgelegd worden in deugdelijk beveiligde opbergmiddelen bewaard.

g. Personen belast met onderhouds- en reparatiewerkzaamheden in de ruimte waarin de informatie en de gegevens zich bevinden worden door eigen geautoriseerd personeel begeleid.

IV. Beheer van communicatie- en bedieningsprocessen

a. De status/rubricering van de informatie en de gegevens (staatsgeheim of vertrouwelijk) dient te allen tijde kenbaar te zijn.

b. Reproductie van de informatie of de gegevens is alleen toegestaan door daartoe geautoriseerde personen en uitsluitend voor zover dat nodig is voor de goede uitvoering van de bijzondere last dan wel toestemming op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2002 als bedoeld in artikel 13.2, eerste en tweede lid, van de wet dan wel een verzoek op grond van artikel 13.4 van de wet.

c. De informatie of de gegevens worden niet buiten de normale ruimte gebracht, tenzij dat voor de goede voortgang van de werkzaamheden noodzakelijk is. In dat geval wordt de verblijfplaats van de informatie of de gegevens geregistreerd.

d. De verwijdering en vernietiging van de informatie en gegevens geschiedt op een onomkeerbare wijze. Van de verwijdering en vernietiging wordt een rapport opgemaakt, dat in afschrift wordt gezonden aan

de bevoegde autoriteit wie het aangaat dan wel een door deze aangewezen instantie.

V. Toegangsbeveiliging van geautomatiseerde informatiesystemen

a. De toegang tot geautomatiseerde informatiesystemen waarin de informatie en de gegevens worden verwerkt is op deugdelijke wijze beveiligd, onder meer door middel van persoonsgebonden authenticatie.

b. De logische beveiliging is zodanig ingericht dat ongeautoriseerde toegang en pogingen daartoe worden gedetecteerd en dat tijdige interventie plaatsvindt.

c. Het aantal foutieve inlogpogingen is beperkt tot drie. Overschrijding van het aantal foutieve inlogpogingen leidt tot definitieve blokkering, welke uitsluitend door de functionaris, bedoeld in onderdeel I van deze bijlage, kan worden opgeheven. Het voorgaande is niet van toepassing op de systeembeheerder, met dien verstande dat bij drie foutieve inlogpogingen een hernieuwde inlogpoging slechts kan plaatsvinden via een voor noodsituaties ingericht account en persoonsgebonden authenticatie voor het gebruik waarvan door de functionaris, bedoeld in onderdeel I van deze bijlage toestemming moet worden verleend.

d. Het geautomatiseerde systeem, waarin de gegevens en de informatie worden verwerkt, wordt niet eerder verlaten dan nadat een (handmatig of automatisch) toegangsbeveiligingsmechanisme in werking is gesteld.

e. Alle handelingen met betrekking tot de verwerking van de informatie en de gegevens in het geautomatiseerde informatiesysteem worden persoonsgebonden vastgelegd teneinde onderzoek mogelijk te maken.

f. Toegang tot het geautomatiseerde informatiesysteem is uitsluitend voorbehouden aan daartoe geautoriseerd personeel.

g. De toegangsrechten van de gebruikers worden periodiek geëvalueerd.

h. De autorisaties van alle gebruikers worden vastgelegd.

VI. Ontwikkeling, onderhoud en reparatie van geautomatiseerde informatiesystemen

a. Alle wijzigingen in apparatuur, software of procedures die de beveiliging van de gegevens en informatie kunnen beïnvloeden zijn controleerbaar, dat wil zeggen bekend en beoordeeld door of namens de aanbieder als zijnde aanvaardbaar.

b. Het onderhouden van geautomatiseerde informatiesystemen, voor zover deze nog toegang verschaffen tot gegevens en informatie, vindt op locatie plaats.

c. In afwijking van onderdeel b, is het op afstand onderhouden van geautomatiseerde informatiesystemen slechts toegestaan, indien dit wordt uitgevoerd door daartoe geautoriseerde personen als bedoeld in onderdeel II van deze bijlage, en slechts op tijdstippen waarvoor door de functionaris, bedoeld in onderdeel I, onder a, van deze bijlage, toestemming is verleend en er aantoonbaar voldoende waarborgen bestaan voor het handhaven van het beveiligingsniveau van de gegevens en informatie.

d. Reparatie aan het geautomatiseerde informatiesysteem waarin de informatie en de gegevens worden verwerkt vindt op locatie plaats. Van de eerste volzin kan worden afgeweken indien de informatie en gegevens zijn verwijderd en niet te achterhalen zijn.

NOTA VAN TOELICHTING

1. Algemeen

Hoofdstuk 13 van de Telecommunicatiewet (Tw) geeft regels inzake het bevoegd aftappen. Zo wordt aldaar voorzien in de verplichting voor aanbieders van openbare telecommunicatienetwerken en van openbare telecommunicatiediensten om medewerking te verlenen aan de uitvoering van een bevoegd gegeven bijzondere last dan wel een toestemming op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2002 (WIV 2002) tot het aftappen en opnemen van telecommunicatie (artikel 13.2, eerste en tweede lid, Tw). Dergelijke taplasten kunnen door de daartoe bevoegd verklaarde instanties worden afgegeven in het belang van de strafvordering of in het belang van de veiligheid van de staat. Voor de genoemde aanbieders bestaat voorts onder meer de verplichting om aan de autoriteiten de informatie te verstrekken die noodzakelijk is om die autoriteiten in staat te stellen de bij de wet in het belang van de strafvordering of in het belang van de veiligheid van de staat geregelde bevoegdheden tot het aftappen of opnemen van telecommunicatie, dan wel tot het vorderen van gegevens ter zake van alle verkeer dat over een openbaar telecommunicatienetwerk dan wel met gebruikmaking van openbare telecommunicatiediensten plaatsvindt, te kunnen uitoefenen (artikel 13.4, eerste lid, Tw).

Gaat het bij artikel 13.2 Tw om het verlenen van medewerking aan de daadwerkelijke uitvoering van een taplast, bij artikel 13.4 gaat het om de verplichting tot verstrekking van informatie aan de desbetreffende autoriteiten die zij nodig hebben om een dergelijke taplast op te kunnen stellen dan wel een vordering tot het verstrekken van verkeersgegevens te kunnen doen. Het is evident dat in beide gevallen de desbetreffende gegevens en informatie een uiterst gevoelig karakter hebben. Indien de gegevens bekend zouden worden met betrekking tot wie een taplast is afgegeven, komt – al naar gelang het doel waarvoor de taplast is afgegeven – het welslagen van een strafrechtelijk onderzoek of de veiligheid van de staat in ernstige mate in het geding. Dit geldt evenzeer voor de informatie die benodigd is om een taplast op te kunnen stellen; ook dan wordt immers kenbaar wie in het belang van het strafrechtelijk onderzoek of de veiligheid van de staat de aandacht van de met opsporing en vervolging van strafbare feiten belaste autoriteiten onderscheidenlijk de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) of de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) heeft. Het is dan ook noodzakelijk dat ter zake van de hier bedoelde gegevens en informatie wordt voorzien in adequate beveiligingsmaatregelen teneinde een inbreuk op de vertrouwelijkheid van deze gegevens en informatie te voorkomen en, voor zover een dergelijke inbreuk wel plaats heeft gevonden, in maatregelen waarmee op een snelle en adequate wijze daarop kan worden gereageerd.

In artikel 13.5, eerste lid, Tw is voor de aanbieders de basisverplichting neergelegd om de gegevens welke aan de aanbieders worden verstrekt om uitvoering te kunnen geven aan een bijzondere last dan wel een toestemming op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2002 als bedoeld in artikel 13.2, eerste en tweede lid, Tw, alsmede de informatie welke de aanbieders binnen het kader van artikel 13.4 Tw verstrekken aan de tot aftappen bevoegde instanties, te beveiligen tegen kennisneming door onbevoegden; voorts wordt hen verplicht geheimhouding te betrachten met betrekking tot deze gegevens. De wijze waarop de aanbieders invulling geven aan deze beveiligingsverplichting is in beginsel een eigen aangelegenheid. De wetgever heeft echter gemeend dat het noodzakelijk kan zijn dat ter zake van de door de aanbieder te nemen beveiligingsmaatregelen regels worden gesteld. In artikel 13.5, tweede lid, Tw, is daarvoor de grondslag gelegd. Door het stellen van dergelijke regels kan worden bewerkstelligd dat bij elke aanbieder in ieder

geval een op de aard van de gegevens toegesneden minimum-niveau van beveiligingsmaatregelen wordt getroffen. Nu – in vergelijking met vroeger, toen er immers slechts één aanbieder op de Nederlandse telecommunicatiemarkt werkzaam was – als gevolg van de liberalisering van deze markt een veelvoud van aanbieders werkzaam is, waardoor ook de kans op inbreuken op de vertrouwelijkheid ter zake van de hier bedoelde informatie of gegevens is toegenomen, is het noodzakelijk bevonden om van de in artikel 13.2, derde lid, en 13.5, tweede lid, Tw voorziene mogelijkheid tot regelstelling gebruik te maken. De aanbieder is overigens zelf verantwoordelijk voor het treffen van de in dit besluit voorgeschreven maatregelen alsmede voor andere, uit de in artikel 13.5, eerste lid, Tw voor hem geldende algemene beveiligingsplicht, voortvloeiende maatregelen.

Bij de invulling van de beveiligingsmaatregelen dient onderscheid gemaakt te worden tussen de gevallen waarin de te beveiligen gegevens en informatie betrekking hebben op de veiligheid van de staat enerzijds en strafvordering anderzijds. Voor zover de veiligheid van de staat in het geding is, gaat het om (formeel) als staatsgeheim gerubriceerde gegevens en informatie waarop binnen de rijksdienst een verzwaard regime van toepassing is. Dergelijke gegevens en informatie dienen bij de rijksdienst immers beveiligd te worden overeenkomstig de Aanwijzingen voor de beveiliging van staatsgeheimen en vitale onderdelen bij de Rijksdienst ((AAR 9)(Stcrt. 1989, 26)). Voor zover dergelijke, als staatsgeheimen gerubriceerde gegevens buiten de rijksdienst worden gebracht schrijft aanwijzing 45.1 voor dat daarvoor toestemming dient te worden verleend door de secretaris-generaal of een door hem aangewezen ambtenaar (in de praktijk is dat het hoofd van de AIVD dan wel het hoofd van de MIVD). Een dergelijke toestemming wordt echter eerst dan verleend, nadat is vastgesteld dat het buiten de rijksdienst brengen van staatsgeheimen noodzakelijk is voor een goede voortgang der werkzaamheden en dat voldoende waarborgen aanwezig zijn dat de staatsgeheimen overeenkomstig het bepaalde in deze aanwijzingen zullen worden beveiligd. Tot op heden wordt dit voor een deel ad hoc, te weten op het moment dat een bepaalde aanbieder een taplast dient uit te voeren, vastgesteld en wordt bij de desbetreffende aanbieder waar nodig voorzien in (aanvullende) beveiligingsmaatregelen; daarnaast zijn reeds bij bepaalde aanbieders in overleg met de inlichtingen- en veiligheidsdiensten op voorhand structurele beveiligingsmaatregelen getroffen. Overigens wordt opgemerkt dat ondanks het feit dat een aanbieder de in dit besluit voorgeschreven beveiligingsmaatregelen heeft getroffen, de inlichtingen- en veiligheidsdiensten, gelet op het bepaalde in aanwijzing 45.1 niet ontslagen zijn van hun plicht zich te vergewissen of er in casu, gelet op de specifieke situatie bij de desbetreffende aanbieder, voldoende (andere) waarborgen aanwezig zijn. Mochten deze diensten van oordeel zijn dat bij de aanbieder aanvullende maatregelen nodig zijn, dan kunnen zij daarover in overleg treden met die aanbieder. De diensten zelf beschikken evenwel niet over de bevoegdheid om deze extra maatregelen af te dwingen. Waar nodig kan echter de met handhaving belaste instantie worden geïnformeerd, die vervolgens kan onderzoeken of de situatie bij de desbetreffende aanbieder inderdaad tot aanvullende beveiligingsmaatregelen noopt. Zie voorts hetgeen in onderdeel 3 omtrent toezicht is gesteld.

2. Kernelementen van het besluit

Het besluit kent een aantal kernelementen:

a. een explicitering van verschillende aspecten waarop de door de aanbieder te treffen beveiligingsmaatregelen zich dienen te richten (artikel 2, tweede lid);

b. een bijlage met verplicht te treffen beveiligingsmaatregelen (artikel 2, derde lid jo. bijlage);

c. de verplichting tot vastlegging van de beveiligingsmaatregelen in een beveiligingsplan (artikel 3);

d. de eis dat de aanbieder uitsluitend «gescreend» personeel inschakelt bij de uitvoering van taplasten dan wel verzoeken om informatie en dat deze er voor zorgt dat het personeel de vereiste geheimhouding betracht (artikel 4 en artikel 6);

e. maatregelen die genomen moeten worden bij ongeoorloofde inbreuken op de vertrouwelijkheid (artikel 5);

f. een regeling voor de situatie dat door een aanbieder werkzaamheden zijn uitbesteed aan een derde («outsourcing») (artikel 7).

Ad a: een explicitering van verschillende aspecten waarop de door de aanbieder te treffen beveiligingsmaatregelen zich dienen te richten

In artikel 2, eerste lid, wordt aan de aanbieder de plicht opgelegd om alle noodzakelijke maatregelen van technische en organisatorische aard te treffen om kennisneming door onbevoegden te voorkomen van – kort gezegd – de gegevens welke aan een aanbieder worden verstrekt ten behoeve van het ten uitvoer kunnen leggen van een taplast en de informatie welke door de aanbieder aan de tot aftappen bevoegde instanties wordt verstrekt. Dergelijke maatregelen dienen ten minste te bestaan uit maatregelen gericht op de personen die werkzaam zijn voor de aanbieder, maatregelen gericht op de toegang tot gebouwen en ruimten waarin de gegevens en informatie, bedoeld in artikel 2, eerste lid, aanwezig zijn, maatregelen gericht op een deugdelijke werking en beveiliging van het informatiesysteem waarin de desbetreffende gegevens en informatie worden verwerkt, maatregelen voor het geval op de vertrouwelijkheid van de desbetreffende gegevens en informatie een inbreuk wordt gemaakt alsmede maatregelen voor het geval dat er calamiteiten optreden (artikel 2, tweede lid). Het is aan elke aanbieder afzonderlijk om – met inachtneming van hetgeen overigens in het besluit is bepaald – te bepalen op welke wijze invulling wordt gegeven aan de zorgplicht voor beveiliging en de daarin onderscheiden beveiligingsaspecten. Daarbij zal deze rekening kunnen houden met de specifieke omstandigheden van zijn organisatie. Een en ander zal naast implementatie van de daaruit voortvloeiende concrete maatregelen in de organisatie, tevens zijn weerslag dienen te krijgen in het in artikel 3 voorgeschreven beveiligingsplan.

Ad b: de bijlage met beveiligingsmaatregelen

In de bijlage bij het besluit is een aantal maatregelen voorgeschreven, die door iedere aanbieder *ten minste* dienen te worden getroffen. De maatregelen zijn onderverdeeld in een zestal categorieën. De aanduiding van de verschillende categorieën sluit weliswaar niet geheel aan op de in artikel 2, tweede lid, geformuleerde aspecten, maar laten zich daar wel degelijk inpassen. Bij de formulering van de verschillende maatregelen is nadrukkelijk gelet op de aspecten relevantie en uitvoerbaarheid. Relevantie spreekt voor zich; de maatregelen dienen bij te dragen aan het doel van het besluit, te weten het bewerkstelligen van een minimumniveau aan beveiliging. Uitvoerbaarheid is nadrukkelijk aandachtspunt geweest vanwege het feit dat de maatregelen door verschillende soorten aanbieders met uiteenlopende omvang en organisatievorm dienen te worden geïmplementeerd.

Met betrekking tot enkele onderdelen van de bijlage wordt ter verduidelijking het navolgende opgemerkt.

In onderdeel II van de bijlage worden enkele eisen gesteld met betrekking tot de functiebeschrijving van personeel. Het begrip functiebeschrijving moet hier ruim worden geïnterpreteerd in die zin, dat ingeval personeel op een later tijdstip met werkzaamheden wordt belast in het

kader waarvan van de hier bedoelde gegevens en informatie moet worden kennisgenomen, dit niet per se vergt dat een geheel nieuwe functiebeschrijving wordt opgemaakt, maar dat met een aanvulling op de bestaande functiebeschrijving (bijvoorbeeld in de vorm van een aantekening) kan worden volstaan. Duidelijk dient te zijn dat de desbetreffende taak is toebedeeld aan een persoon en dat de taak tot zijn functie behoort.

In onderdeel IV, onder d, van de bijlage is aangegeven dat het rapport dat van de verwijdering en vernietiging van de gegevens en informatie is opgemaakt, in afschrift dient te worden gezonden aan de bevoegde autoriteit wie het aangaat dan wel een door deze aangewezen instantie. In de praktijk kan een aanbieder met vele bevoegde autoriteiten te maken krijgen. Het moeten toezenden van een afschrift van het rapport aan de bevoegde autoriteit wie het aangaat levert naast de daardoor veroorzaakte administratieve lasten ook risico's op met betrekking tot de vertrouwelijkheid van de inhoud van die rapporten; de kans op het zoekraken van dergelijke rapporten is immers groter dan in het geval er slechts één of een beperkt aantal instanties zou zijn, waaraan de afschriften gezonden zouden moeten worden. Voorzien is in de mogelijkheid om de afschriften te zenden aan een door de bevoegde autoriteit aangewezen instantie, hetgeen ook één instantie voor alle bevoegde autoriteiten kan zijn. Daarbij moet meer concreet worden gedacht aan de Landelijke Interceptie Organisatie (LIO). De Minister van Justitie zal in overleg met het College van PG's treden teneinde te bewerkstelligen dat het LIO als zodanig door de bevoegde autoriteiten wordt aangewezen.

In onderdeel V, onder a, is bepaald dat de beveiliging van geautomatiseerde informatiesystemen onder meer door middel van persoonsgebonden authenticatie dient plaats te vinden. Authenticatie is erop gericht vast te stellen of de betrokkene rechtmatig toegang heeft tot het systeem; uit de eis dat deze persoonsgebonden dient te zijn, vloeit voort dat deze altijd herleidbaar dient te zijn tot een identificeerbare persoon. Voor authenticatie kan bijvoorbeeld gebruik gemaakt worden van een PKI (Public key Infrastructuur)-mechanisme.

In onderdeel VI worden enkele eisen gesteld met betrekking tot het onderhoud en de reparatie van geautomatiseerde informatiesystemen. Onder onderhoud moet in dit kader onder andere worden verstaan bestandsreparatie en het (reguliere) systeemonderhoud. Dit moet – onder bepaalde voorwaarden – ook op afstand kunnen worden gedaan. In het geval dat bij onderhoud op afstand niet in het vereiste beveiligingsniveau kan worden voorzien, zal dit onderhoud op locatie dienen plaats te vinden. Reparatie betreft fysieke reparatie, dat wil zeggen aan het apparaat zelf.

Ad c: het beveiligingsplan

De door de aanbieder te treffen c.q. getroffen maatregelen dienen te worden vastgelegd in een beveiligingsplan. In het beveiligingsplan dienen alle beveiligingsaspecten welke aan de orde zijn ten aanzien van de bedrijfsprocessen waaraan de gegevens en informatie zijn onderworpen op een gestructureerde wijze te worden behandeld. Het beveiligingsplan kan door elke aanbieder – zij het met inachtneming van de in het besluit reeds geëxpliciteerde eisen – op de specifieke situatie van de eigen organisatie worden toegesneden. Het beveiligingsplan dient op een daartoe strekkend verzoek van de bevoegde autoriteit, aan deze ter inzage te worden gegeven. Overigens dient het beveiligingsplan niet alleen ter inzage te worden gegeven aan de bevoegde autoriteit die daarom verzoekt. Ook de met toezicht op de naleving van artikel 13.5 Tw belaste instantie kan in het kader van de uitvoering van die taak – onder gebruikmaking van de in artikel 5:16 en 5:17 van de Algemene wet bestuursrecht aan toezichthouders toekomende bevoegdheden – het beveiligingsplan opvragen dan wel inzage daarin vorderen. Op het toezicht op de naleving van de beveiligingsmaatregelen zal in het onderstaande nog nader worden ingegaan.

Ad d: «gescreend» personeel en geheimhouding

In artikel 4 van het besluit wordt aan de aanbieder voorgeschreven dat hij de uitvoering van taplasten dan wel de verstrekking van informatie aan de bevoegde autoriteiten, slechts mag opdragen aan personen die – kort gezegd – zijn «gescreend». Deze «screening» varieert naar gelang het gaat om de uitvoering van taplasten en (daaraan gerelateerde) informatieverstrekkingen in het belang van de veiligheid van de staat dan wel om de uitvoering van taplasten en (daaraan gerelateerde) informatieverstrekking in het kader van een strafvorderlijk onderzoek. In het eerste geval zal met betrekking tot het personeelslid een veiligheidsonderzoek dienen plaats te vinden. In het tweede geval kan worden volstaan met het vaststellen of door het desbetreffende personeelslid aan de werkgever een verklaring omtrent het gedrag is overgelegd.

De gegevens betreffende taplasten van inlichtingen- en veiligheidsdiensten gelden als (formele) staatsgeheimen; dat geldt ook voor de informatie die op grond van artikel 13.4 Tw door een aanbieder aan de AIVD of de MIVD wordt verstrekt. De veiligheid (en andere gewichtige belangen) van de staat kan worden geschaad, indien van deze gegevens door onbevoegden kennis wordt genomen. Voorts geldt ingevolge aanwijzing 45.1 van de Aanwijzingen voor de beveiliging van staatsgeheimen en vitale onderdelen bij de rijksdienst, dat toestemming voor het buiten de rijksdienst brengen van staatsgeheimen slechts dan wordt verleend (door de secretaris-generaal of een door hem aangewezen ambtenaar) indien is vastgesteld dat dit noodzakelijk is voor een goede voortgang van de werkzaamheden en dat er voldoende waarborgen aanwezig zijn dat de staatsgeheimen overeenkomstig het bepaalde in deze aanwijzingen zullen worden behandeld. Nu de hier in het geding zijnde gegevens als staatsgeheim zijn gerubriceerd en ingevolge aanwijzing 24 van dergelijke staatsgeheimen uitsluitend kennis mag worden genomen door personen die een vertrouwensfunctie vervullen, zullen de functies bij een aanbieder waarbij van de hier bedoelde staatsgeheimen dient te worden kennis genomen – met inachtneming van hetgeen bij de Wet veiligheidsonderzoeken (Wvo) is bepaald – als vertrouwensfunctie dienen te worden aangewezen. De desbetreffende functies worden als vertrouwensfunctie aangewezen door de Minister van Economische Zaken in overeenstemming met de Minister van Binnenlandse Zaken en Koninkrijksrelaties (artikel 3, eerste lid, Wvo). Het is daarbij niet noodzakelijk dat iedere individuele functie in een aanwijzingsbesluit wordt aangeduid. Er zullen categorieën van functies (kunnen) worden aangewezen, waarbij duidelijk zal blijken welke functie(s) het zal betreffen.

Personen die in aanmerking komen om met de desbetreffende vertrouwensfunctie te worden belast, dienen eerst aan een veiligheidsonderzoek te worden onderworpen. De aanbieder zal de betrokken persoon daartoe dienen aan te melden bij het hoofd van de AIVD; voor deze aanmelding is schriftelijke toestemming vereist van de betrokken persoon, die door de werkgever (in casu de aanbieder) dient te worden geïnformeerd over de betekenis en de rechtsgevolgen van de aanmelding. De werkgever belast de betrokken persoon pas met de vervulling van de vertrouwensfunctie, nadat door de Minister van Binnenlandse Zaken en Koninkrijksrelaties ten aanzien van de betrokkene een verklaring is afgegeven, dat vanuit het oogpunt van de veiligheid of van andere gewichtige belangen van de staat geen bezwaar tegen de vervulling van de desbetreffende vertrouwensfunctie door de betrokkene bestaat (artikel 3 Wvo).

Opgemerkt wordt dat de lasten tot aftappen die worden afgegeven in het kader van strafvordering – anders dan die in het kader van de veiligheid van de staat – niet als staatsgeheim zijn gerubriceerd. De extra eisen die derhalve worden gesteld aan de omgang met staatsgeheimen, gelden dan ook in beginsel niet voor de gegevens die betrekking hebben

op deze bijzondere lasten alsmede voor de informatieverstrekking ex artikel 13.4 Tw waar het gaat om verstrekking ten behoeve van strafvordering. Niettemin moet ook met betrekking tot de uitvoering van de hier bedoelde lasten en informatieverstrekkingen verzekerd zijn dat uitsluitend personeel dat aan bepaalde betrouwbaarheidseisen voldoet, daarbij door de aanbieder wordt ingeschakeld. In artikel 4, tweede lid, van het besluit wordt dan ook als beveiligingsmaatregel voorgeschreven dat het desbetreffende personeelslid aan de aanbieder (diens werkgever) een verklaring omtrent het gedrag als bedoeld in de Wet op de justitiële documentatie en op de verklaringen omtrent het gedrag heeft overgelegd. Deze eis geldt niet voor zover het betrokken personeelslid reeds een vertrouwensfunctie uitoefent, waarbij hij is belast met de uitvoering van taplasten en informatieverstrekkingen in het kader van de veiligheid van de staat. De betrouwbaarheid van de betrokkene is dan immers reeds anderszins vastgesteld.

In artikel 13.5, eerste lid, Tw wordt niet alleen bepaald dat de aanbieders verplicht zijn de gegevens met betrekking tot een bijzondere last dan wel een toestemming als bedoeld in artikel 13.2 en de informatieverstrekkingen als bedoeld in artikel 13.4 te *beveiligen* tegen kennisneming door onbevoegden, maar ook *geheimhouding* te betrachten met betrekking tot deze gegevens. Deze geheimhoudingsplicht, die zich primair richt tot de aanbieder, kan niet los gezien worden van het geheel van te treffen beveiligingsmaatregelen. In artikel 6 van het besluit wordt dan ook bepaald dat de aanbieder er voor zorg dient te dragen dat de personeelsleden die belast zijn met de werkzaamheden ter uitvoering van een bevoegd gegeven bijzondere last dan wel een toestemming op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2002 als bedoeld in artikel 13.2, eerste en tweede lid, Tw alsmede met de werkzaamheden verbonden aan de informatieverstrekking als bedoeld in artikel 13.4 Tw, met betrekking tot deze werkzaamheden en de gegevens en informatie waarvan zij in dat verband kennis nemen, geheimhouding betrachten. Deze zorgplicht kan op verschillende wijzen worden ingevuld. Een adequate voorlichting aan de betrokken personeelsleden waarbij zij worden doordrongen van het gevoelige karakter van de door hen te verrichten werkzaamheden alsmede van de gegevens en informatie waarvan zij in dat kader kennisnemen en de noodzaak ter zake geheimhouding te bewaren is daarbij een allereerste vereiste. In dat verband ware zeker te wijzen op de wettelijke geheimhoudingsverplichtingen die er bestaan; denk daarbij aan de artikelen 98 en 272 van het Wetboek van Strafrecht (schending van geheimen) en – waar het gaat om de veiligheid van de staat – artikel 85 van de Wet op de inlichtingen- en veiligheidsdiensten 2002 (een taplast strekt ter uitvoering van de in deze wet neergelegde taak voor de AIVD of MIVD en daarmee ter uitvoering van deze wet, waarvoor de aangescherpte geheimhoudingsverplichting ex artikel 85 geldt). Overigens geldt voor de werkgever, in casu de aanbieder, die een persoon wil belasten met een vertrouwensfunctie, op grond van artikel 4, tweede lid, Wvo de verplichting de betrokken persoon te informeren over de betekenis en de rechtsgevolgen van het feit dat deze voor een veiligheidsonderzoek wordt aangemeld; daartoe behoort op zijn minst ook een aanduiding van de redenen waarom in casu sprake is van een vertrouwensfunctie. Als sluitstuk van het voorlichtingstraject is het wenselijk om de betrokken personeelsleden een geheimhoudingsverklaring te laten ondertekenen. In de bijlage bij het besluit, onderdeel II, onder b, is laatstgenoemde maatregel voorgeschreven. Het moge duidelijk zijn dat de zorgplicht voor de aanbieder in dezen geen eenmalige activiteit behelst, doch een duurzaam karakter heeft.

Ad e: Maatregelen in geval van ongeoorloofde inbreuken op de vertrouwelijkheid

Het is evident dat voorkomen dient te worden dat niet daartoe gerechtigde personen kennis kunnen nemen van de gegevens of de informatie, bedoeld in artikel 2. Geschiedt dat wel, dan is er sprake van een ongeoorloofde inbreuk op de vertrouwelijkheid van die gegevens en informatie. Als gevolg daarvan kan onder meer schade ontstaan voor het desbetreffende strafrechtelijk onderzoek of voor de veiligheid van de staat. Het is dan ook van groot belang dat wordt voorzien in maatregelen die erop gericht zijn te voorkomen dat een dergelijke ongeoorloofde inbreuk kan plaatsvinden en waar deze wel plaatsvindt, deze zo spoedig mogelijk wordt ontdekt. Ingevolge artikel 2, tweede lid, onder d, van het besluit dient de aanbieder daartoe beveiligingsmaatregelen te treffen; in de bijlage bij het besluit is een aantal van deze maatregelen reeds geëxpliciteerd (vergelijk onderdeel V, onder b en e). De door de aanbieder getroffen maatregelen dienen in het in artikel 3 bedoelde beveiligingsplan te worden vastgelegd.

Indien door een aanbieder wordt vastgesteld dat een ongeoorloofde inbreuk heeft plaatsgevonden, dan is deze verplicht de desbetreffende bevoegde autoriteit terstond daaromtrent te informeren. Immers, opsporingsonderzoeken of onderzoeken in het kader van de veiligheid van de staat kunnen door het bekend raken van de vertrouwelijke gegevens buiten de kring van personen die tot kennisneming gerechtigd zijn worden gefrustreerd met alle gevolgen van dien. Daarbij dient hij aan te geven welke gegevens of informatie het betreft. Verder dient de aanbieder te vermelden op welke wijze de inbreuk heeft plaatsgevonden en welke maatregelen hij heeft genomen om verdere verspreiding van de bedoelde gegevens of informatie tegen te gaan en herhaling van het gebeurde te voorkomen. Op basis van de aldus verstrekte informatie kan de bevoegde autoriteit de maatregelen nemen die deze aangewezen acht om de gevolgen voor bedoelde onderzoeken tot een minimum te beperken. In het geval de inbreuk heeft plaatsgevonden ten aanzien van staatsgeheimen zal er een gericht onderzoek dienen plaats te vinden; onderdeel G van de Aanwijzingen voor de beveiliging van staatsgeheimen en vitale onderdelen bij de rijksdienst voorziet daartoe in een procedure, waarnaar zoveel als mogelijk is zal worden gehandeld. In het onderhavige geval zal het desbetreffende onderzoek door het hoofd van de AIVD dan wel het hoofd van de MIVD (in casu door de door hem daartoe gemandateerde ambtenaren van de dienst) worden verricht. Voor het welslagen van dit onderzoek is medewerking door de desbetreffende aanbieder van het grootste belang.

Tot slot wordt opgemerkt, dat indien het vermoeden rijst dat er sprake is van een strafbaar feit (artikel 98 e.v. alsmede 272 Wetboek van Strafrecht) er ook een strafrechtelijk onderzoek zal dienen te worden geëntameerd.

Ad f: een regeling voor de situatie dat door een aanbieder werkzaamheden zijn uitbesteed aan een derde («outsourcing»).

Artikel 7 van het besluit geeft een voorziening voor het geval dat door een aanbieder (een deel van zijn) werkzaamheden zijn uitbesteed aan een derde en in het kader van de uitvoering van die werkzaamheden door die derde kennis kan c.q. dient te worden genomen van de gegevens en de informatie, bedoeld in artikel 2, eerste lid. Het is evident dat ook in die situatie voorzien dient te zijn in de noodzakelijke maatregelen ter beveiliging van de gegevens en informatie en dat er de noodzakelijke geheimhouding wordt betracht. Artikel 13.5 Tw biedt niet de grondslag om aan dergelijke derden, niet zijnde aanbieders van openbare telecommunicatienetwerken of -diensten, rechtstreeks verplichtingen ter zake van de noodzakelijk geachte beveiligingsmaatregelen op te leggen. Niettemin moet het tot de zorgplicht van de aanbieder worden gerekend, dat in het geval dat hij werkzaamheden als hier bedoeld uitbesteedt, hij er

op toeziet dat de noodzakelijke beveiligingsmaatregelen worden getroffen. In artikel 7 wordt deze zorgplicht nader geëxpliciteerd en wel in die zin, dat de aanbieder wordt verplicht om in een schriftelijke overeenkomst met de derde vast te leggen dat deze zich onder meer ertoe verplicht om de in het besluit gestelde maatregelen na te leven. Bovendien wordt bepaald dat in die overeenkomst vastgelegd dient te worden dat de derde alle informatie dient te verstrekken die voor het toezicht op de naleving van de beveiligings- en geheimhoudingsverplichting noodzakelijk is. Deze informatieplicht is in het bijzonder van belang voor zover de toezichthoudende bevoegdheden jegens de aanbieder worden uitgeoefend en deze om informatie wordt gevraagd over de wijze waarop de derde diens beveiligingsplicht heeft ingevuld. Dit laat overigens onverlet de bevoegdheid van de toezichthoudende instantie, waarop in paragraaf 3 nader wordt ingegaan, om zich rechtstreeks tot de derde te wenden; de toezichthoudende bevoegdheden zijn gelet op de formulering van artikel 15.1, eerste lid, Tw immers ook jegens deze aan te wenden. Artikel 15.1, eerste lid, aanhef en onder e, doet immers het toezicht uitstrekken tot het bepaalde bij of krachtens de wet dat betrekking heeft op bevoegd aftappen.

Voor de goede orde wordt opgemerkt dat ook bij de hier bedoelde derden vertrouwensfuncties kunnen worden aangewezen. Voor de aanwijzing van vertrouwensfuncties biedt immers niet artikel 13.5 Tw, maar – in casu artikel 3 van – de Wet veiligheidsonderzoeken de juridische basis.

3. Toezicht op de beveiligingsplicht van de aanbieder

Ingevolge artikel 15.1, eerste lid, aanhef en onder e, Tw berust het toezicht op de naleving van hetgeen bij of krachtens hoofdstuk 13 Tw (Bevoegd aftappen) is gesteld, bij de door de Minister van Economische Zaken[1] daartoe aangewezen ambtenaren. Tot 1 september 2002 betrof het hier de (aangewezen) ambtenaren werkzaam bij de Afdeling Veiligheid en Nummering van het Directoraat-Generaal Telecommunicatie en Post; met ingang van 1 september 2002 berust de toezichthoudende taak bij de (aangewezen) ambtenaren van het agentschap Telecom[2]. Met de overgang van de toezichthoudende taak naar het agentschap Telecom zal tegelijkertijd een intensivering van het handhavingstoezicht, zowel preventief als repressief, plaatsvinden. Dat geldt niet alleen voor de wijze waarop door de aanbieder – met inachtneming van de bepalingen van dit besluit – invulling is gegeven aan de ingevolge artikel 13.5 Tw op hem rustende zorgplicht tot het treffen van beveiligingsmaatregelen, maar ook voor de overige in hoofdstuk 13 Tw geformuleerde verplichtingen. Preventief handhavingstoezicht betekent dat actief toezicht wordt gehouden op de naleving van de bij of krachtens de wet gestelde regels los van de situatie dat er een vermoeden bestaat dat door een aanbieder in strijd met de regels is gehandeld. Repressief toezicht vindt plaats, indien er wel sprake is van een dergelijk vermoeden. Dit laatste kan onder meer blijken uit meldingen die door de bevoegde autoriteiten bij de toezichthouder worden gedaan naar aanleiding van hetgeen zij in de uitvoeringspraktijk van het bevoegd aftappen bij een aanbieder tegenkomen.

Aan de toezichthouders komen de bevoegdheden uit hoofdstuk 5 van de Algemene wet bestuursrecht (Awb) toe. De bestuursrechtelijke sanctioneringsmogelijkheden die kunnen worden toegepast, indien door een toezichthouder 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 Tw e.v.). Daarnaast bestaat de mogelijkheid dat de overtreding strafrechtelijk

[1] In de wettekst staat nog Minister van Verkeer en Waterstaat, echter op 22 juli 2002 is de verantwoordelijkheid voor het beleidsterrein telecommunicatie en post naar de Minister van Economische Zaken overgegaan.
[2] Voorheen de Divisie Telecom van de Inspectie Verkeer en Waterstaat (IVW-T).

wordt gesanctioneerd. De overtreding van de voorschriften, gesteld bij of krachtens de artikelen 13.2 en 13.5 Tw, is immers in artikel 1 van de Wet op de economische delicten (Wed) als economisch delict aangemerkt en uit dien hoofde strafbaar. Overtreding van de voorschriften zoals deze zijn neergelegd in artikelen 13.2 en 13.5 Tw, indien opzettelijk gepleegd, zijn bovendien aan te merken als een misdrijf in de zin van de Wed. Hieraan is ingevolge de Wed een strafmaat verbonden van ten hoogste twee jaar gevangenisstraf en een geldboete van € 11 250. 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.

4. Bedrijfseffecten en administratieve lasten

De verplichting voor aanbieders van openbare telecommunicatie-netwerken en- diensten om zorg te dragen voor een adequate beveiliging van de gegevens en informatie, waarop ook dit besluit betrekking heeft, vloeit reeds rechtstreeks voort uit artikel 13.5, eerste lid, van de wet. Dat zou strikt genomen moeten betekenen dat die aanbieders, die al bij de uitvoering van een bijzondere last ex artikel 13.2 van de wet betrokken zijn (geweest) of op basis van artikel 13.4 Tw informatie aan de bevoegde autoriteiten hebben moeten verstrekken, ter invulling van deze zorgverplichting reeds de nodige beveiligingsmaatregelen hebben genomen. Zeker voor die gevallen, waarbij de veiligheid van de staat in het geding is; zie hetgeen in paragraaf 2 omtrent het buiten de rijksdienst brengen van staatsgeheimen is gesteld.

Andere aanbieders zullen òf al wel òf nog niet specifieke maatregelen hebben getroffen en voor zover deze nog niet zijn genomen, de intentie hebben om daartoe pas over te gaan op het moment dat medewerking door de bevoegde autoriteit wordt verlangd. Dat is echter op een te laat moment en kan aan een tijdige uitvoering van een taplast of informatie-verstrekking in de weg staan. De toepassing van opsporings-bevoegdheden dan wel bevoegdheden in het kader van de veiligheid van de staat dient niet afhankelijk te zijn van de vraag of er wel of niet door de aanbieder de noodzakelijke beveiligingsmaatregelen zijn getroffen. Met het onderhavige besluit wordt de op zich abstract geformuleerde zorgplicht uit artikel 13.5, eerste lid, Tw naar een aantal concrete – door de aanbieder te ondernemen – acties vertaald; explicitering en implementatie van de te onderscheiden maatregelen alsmede vastlegging daarvan in een beveiligingsplan vormen in dezen de essentie.

Uitvoering van het besluit brengt voor de aanbieder lasten met zich mee; afgezet tegen het doel waarvoor de maatregelen worden voorge-schreven, worden deze gerechtvaardigd geacht. De specifiek in het besluit en de bijlage voorgeschreven maatregelen zijn van dien aard dat verwacht wordt dat de daarmee gepaard gaande kosten, mede doordat de aanbieder zelf de nodige ruimte is gelaten om daaraan op een specifiek op zijn organisatie toegesneden wijze invulling te geven, binnen redelijke grenzen kunnen worden gehouden. Een kwantificering van deze kosten is echter moeilijk te geven, gelet op het feit dat de beveiligingsplicht diverse soorten aanbieders raakt met verschillen in omvang en organisatievorm.

De kosten welke verbonden zijn aan de implementatie van de technische en organisatorische beveiligingsmaatregelen komen voor rekening van de netwerk- en dienstenaanbieders. Dit vloeit voort uit artikel 13.6 Tw. Op basis van dit artikel komen de investerings-, exploitatie- en onderhoudskosten voor de technische voorzieningen welke door de aanbieders van openbare telecommunicatienetwerken- of diensten worden gemaakt om te kunnen voldoen aan (onder meer) artikel 13.5 Tw te hunner laste. Hierbij dient bijvoorbeeld te worden gedacht aan de

kosten die moeten worden gemaakt om in geautomatiseerde systemen – hardwareen softwarematige – maatregelen te treffen die toegang tot de hier in het geding zijnde gegevens beperkt tot de daartoe geautoriseerde personen.

Naast de hiervoor aangeduide kosten voor de aanbieders, verbonden aan de implementatie van de in dit besluit voorgeschreven beveiligingsmaatregelen in de organisatie van de aanbieder, brengt de uitvoering van het besluit voor de aanbieder tevens administratieve lasten met zich mee. Het gaat dan om de kosten die verbonden zijn aan de volgende informatieverplichtingen:

– het opstellen van een beveiligingsplan, waarin wordt aangegeven op welke wijze door de aanbieder uitvoering is gegeven aan zijn beveiligingsplicht (artikel 3);

– het informeren van de bevoegde autoriteit indien op de vertrouwelijkheid van enigerlei gegevens of informatie als bedoeld in artikel 2, eerste lid, een ongeoorloofde inbreuk is gemaakt (compromittering) (artikel 5);

– het vastleggen van de verblijfplaats van gegevens en informatie in de gevallen dat deze buiten de werkruimte worden gebracht (bijlage onder IV, onderdeel c);

– het opmaken van een rapport van de verwijdering en vernietiging van gegevens alsmede het toezenden van een afschrift ervan aan de bevoegde autoriteit wie het aangaat dan wel een door deze aangewezen instantie (bijlage onder IV, onderdeel d).

Van de genoemde informatieverplichtingen levert de verplichting tot het opstellen van een beveiligingsplan naar verwachting de meeste administratieve lasten op. Het gaat daarbij om eenmalige en structurele kosten; de eenmalige kosten betreffen het opstellen van een beveiligingsplan, de structurele kosten zien op het actueel houden van het beveiligingsplan. Het beveiligingsplan is niet aan bijzondere vormvereisten gebonden; de aanbieder is dan ook vrij om te bepalen in welke vorm en omvang hij het beveiligingsplan giet. Dat betekent dat per aanbieder de daarmee gepaard gaande eenmalige kosten kunnen verschillen.

Uitgaande van 300 aanbieders[1] en een geschatte werklast van gemiddeld 5 werkdagen per beveiligingsplan, wordt de totale omvang van de administratieve lasten verbonden aan de verplichting tot het opstellen van een beveiligingsplan geraamd op (afgerond) € 660 000[2]. Kostenbesparing op dit onderdeel is overigens denkbaar in het geval dat er modellen voor beveiligingsplannen beschikbaar komen, waarmee een deel van de ontwikkelingskosten die de aanbieder moet maken voor een dergelijk plan (wat betreft inrichting en vormgeving) kunnen worden bespaard. Het initiatief daartoe ligt overigens bij de (brancheorganisaties van de) aanbieders zelf. Naast de eenmalige kosten die aan het opstellen van een beveiligingsplan zijn verbonden, dienen ook kosten te worden gemaakt om de plannen actueel te houden, waarbij wordt uitgegaan van een jaarlijkse up-date; de totale omvang van deze kosten wordt geschat op 10% van de kosten van het opstellen van een beveiligingsplan, te weten € 66 000. Met betrekking tot de kosten verbonden aan de overige informatieverplichtingen, wordt het volgende opgemerkt. De kosten verbonden aan de informatieplicht in het geval dat sprake is van compromittering, zijn moeilijk in te schatten aangezien op voorhand niet aan te geven is hoe vaak deze daadwerkelijk toepassing zal vinden. Naar wordt verwacht (en gehoopt) zal een dergelijke situatie niet tot zeer zelden voor komen en zal een melding daarvan in beginsel langs telefonische weg kunnen plaatsvinden. De daaraan verbonden administratieve lasten dienen dan ook als verwaarloosbaar te worden aangemerkt. Ook waar het gaat om de verplichting tot het vastleggen van de verblijfplaats van gegevens en informatie in de gevallen dat deze buiten de werkruimte worden gebracht, laat de omvang van de daaraan verbonden kosten zich moeilijk inschatten, temeer daar het hier gaat om een afwijking van de

[1] In het door Cap Gemini Ernst & Young in 2001 ten behoeve van het ministerie van Verkeer en Waterstaat uitgevoerde onderzoek naar de administratieve lasten (zogenaamde nulmeting) wordt waar het gaat om hoofdstuk 13 van de Telecommunicatiewet uitgegaan van 296 aanbieders van openbare telecommunicatienetwerken en -diensten, waarop de daarin neergelegde verplichtingen van toepassing zijn.

[2] Gehanteerde uitgangspunten: aantal bedrijven 300, betreft een eenmalige operatie, tijdsbesteding wordt ingeschat op gemiddeld 40 uur tegen een gemiddeld uurtarief van 55. Deze uitgangspunten zijn voor commentaar aan enkele aanbieders van openbare telecommunicatienetwerken en -diensten (zowel telefonie als internet) voorgelegd en worden door hen – op een enkele partij na – onderschreven.

hoofdregel dat dit juist niet mag. Wat het opmaken van een rapport van de verwijdering en de vernietiging van de gegevens betreft (inclusief de toezending van een afschrift aan de bevoegde autoriteit dan wel aan de door deze aangewezen instantie), wordt de omvang van de (jaarlijks terugkerende kosten) geraamd op € 33 000[1]. De kosten van toezending van afschriften van het rapport van verwijdering en vernietiging kunnen overigens beduidend lager uitvallen in het geval dat de toezending van deze rapporten aan één aan te wijzen instantie, naar verwachting de Landelijke Interceptie Organisatie, kan plaatsvinden en daarvoor ook elektronische mogelijkheden worden ontwikkeld. Voorts wordt bij dit onderdeel nog de kanttekening geplaatst dat in de berekening er vanuit gegaan is, dat iedere aanbieder met de uitvoering van taplasten of informatieverzoeken wordt geconfronteerd; in de praktijk gaat het echter om een over het algemeen beperkte groep aanbieders.

De kosten die zijn gemoeid met het uitvoeren van veiligheids-onderzoeken op grond van de Wet veiligheidsonderzoeken worden door de Staat gedragen.

Het ontwerp-besluit is voor advies voorgelegd aan het Adviescollege toetsing administratieve lasten (Actal). Het College heeft aangegeven het ontwerp-besluit niet te selecteren voor een Actal-toets op de gevolgen hiervan voor de administratieve lasten voor het bedrijfsleven. De reden daarvoor is dat de omvang van de door dit besluit veroorzaakte administratieve lasten beperkt is.

5. Notificatie

Het ontwerp-besluit is op 23 mei 2003 gemeld aan de Commissie van de Europese Gemeenschappen (notificatienummer 2003/184/NL) ter voldoening aan artikel 8, eerste lid, van richtlijn 98/34/EG van het Europees Parlement en de Raad van de Europese Unie van 22 juni 1998 betreffende een informatieprocedure op het gebied van normen en technische voorschriften en regels betreffende diensten van de informatiemaatschappij (PbEG L 204), zoals gewijzigd bij richtlijn nr. 98/48/EG van 20 juli 1998 (PbEG L 217). Na afloop van de notificatietermijn (25 augustus 2003) heeft de Commissie nog een mededeling van opmerkingen uitgebracht als bedoeld in artikel 8, tweede lid, van de richtlijn. De Commissie geeft daarin aan in het kader van de procedure als vastgelegd in richtlijn nr. 98/34/EG geen bezwaren naar voren te brengen.

6. Overleg en -adviesverplichtingen

Een ontwerp van het onderhavige besluit is bij brief van 26 april 2002 voorgelegd aan het deelorgaan aftappen van het Permanent overleg-orgaan post en telecommunicatie (OPT/DAF). Het ontwerp is in het overlegorgaan op 15 mei en 26 juni 2002 aan de orde gesteld. Voorts is – naar aanleiding van de uitvoerige bespreking in het OPT/DAF – een aangepast ontwerp in augustus 2002 nog voor een schriftelijke commentaarronde aan de leden van OPT/DAF voorgelegd. Bij brief van 23 september 2002 heeft het OPT/DAF uiteindelijk zijn rapport van bevindingen uitgebracht. Daarin wordt aangegeven dat de leden van het OPT/DAF kunnen instemmen met het ontwerp-besluit.

De Minister van Economische Zaken,
L. J. Brinkhorst

[1] Gehanteerde uitgangspunten: aantal bedrijven 300, frequentie van toezending van het bericht wordt gesteld op eenmaal per kwartaal (4) met een gemiddelde tijds-besteding van 0,5 uur tegen een gemiddeld uurtarief van 55. Deze uitgangspunten zijn voor commentaar aan enkele aanbieders van openbare telecommunicatienetwerken en -diensten (zowel telefonie als internet) voorgelegd en worden door hen – op een enkele partij na – onderschreven.