Staatsblad
van het Koninkrijk der Nederlanden

Jaargang 2012

514

Besluit van 19 oktober 2012, houdende nadere regels met betrekking tot technische en organisatorische eisen ter beperking van risico's voor de veiligheid en de integriteit, de meldplicht van inbreuken op de veiligheid en verliezen van integriteit, de verstrekking van informatie voor de beoordeling van de veiligheid en de integriteit en de aanwijzing van inbreuken op de veiligheid en verliezen van integriteit van openbare elektronische communicatienetwerken en -diensten (Besluit continuïteit openbare elektronische communicatienetwerken en -diensten)

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

Op de voordracht van Onze Minister van Economische Zaken, Landbouw en Innovatie van 6 juli 2012, nr. WJZ / 12081040;
Gelet op de artikelen 13bis en 13ter van de Kaderrichtlijn, artikel 23, eerste volzin, van de Universeledienstenrichtlijn en de artikelen 11a.1, vierde lid, en 11a.2, vierde lid, van de Telecommunicatiewet;
De Afdeling advisering van de Raad van State gehoord (advies van 15 augustus 2012, nr. W15.0255/IV);
Gezien het nader rapport van Onze Minister van Economische Zaken, Landbouw en Innovatie van 17 oktober 2012, nr. WJZ / 12323356;

Hebben goedgevonden en verstaan:

§ 1. Begripsbepalingen

Artikel 1

In dit besluit en de daarop berustende bepalingen wordt verstaan onder:
a. *wet:* Telecommunicatiewet;
b. *aanbieder:* aanbieder van een openbaar elektronisch communicatienetwerk of van een openbare elektronische communicatiedienst;
c. *melding:* kennisgeving als bedoeld in artikel 11a.2, eerste lid, van de wet;
d. *meldpunt:* door Onze Minister aangewezen instantie waar de aanbieder een melding doet.

§ 2. Technische en organisatorische maatregelen

Artikel 2

1. De aanbieder beschikt over een continuïteitsplan dat in ieder geval de volgende onderdelen bevat:
a. de maatregelen, bedoeld in artikel 11a.1, eerste lid, van de wet, alsmede, voor zover van toepassing, de maatregelen, bedoeld in artikel 11a.1, tweede lid, van de wet;
b. de aanwijzing van een ter zake kundige functionaris die binnen zijn organisatie verantwoordelijk en beschikbaar is voor het nemen en uitvoeren van de maatregelen, bedoeld onder a;
c. de aanwijzing van de functionaris, bedoeld in artikel 9, eerste lid.
2. De aanbieder verstrekt de contactgegevens van de in het eerste lid, onder b, bedoelde functionaris en wijzigingen daarvan onverwijld aan Onze Minister.
3. Bij ministeriële regeling kunnen, ter uitvoering van bindende EU-rechtshandelingen, nadere regels worden gesteld omtrent de maatregelen, bedoeld in artikel 11a.1, eerste en tweede lid, van de wet.

Artikel 3

De aanbieder inventariseert, beoordeelt en evalueert regelmatig, mede aan de hand van de in artikel 11a.2, eerste lid, van de wet bedoelde meldingen, de risico's voor de veiligheid en voor de integriteit van zijn netwerken en diensten. Hij verwerkt de resultaten hiervan in het continuïteitsplan, bedoeld in artikel 2.

Artikel 4

De aanbieder zorgt ervoor dat bij hem werkzame personen die betrokken zijn bij de voor de veiligheid en de integriteit van zijn netwerk relevante processen op de hoogte zijn van de inhoud van het continuïteitsplan, bedoeld in artikel 2, en zorgt ervoor dat die personen te allen tijde over dit continuïteitsplan kunnen beschikken.

Artikel 5

1. De aanbieder zorgt voor een deugdelijke beveiliging van zijn netwerk of dienst door:
a. de fysieke toegang tot gebouwen of faciliteiten en
b. de elektronische toegang tot informatie en informatieverwerkende systemen die van belang zijn voor de veiligheid of integriteit van zijn netwerk of dienst uitsluitend toe te staan aan daartoe gemachtigde personen.
2. De aanbieder legt de voor hem werkzame personen die betrokken zijn bij de voor de veiligheid en integriteit van zijn netwerk relevante processen een geheimhoudingsverplichting op.

§ 3. Meldplicht en informatieplicht

Artikel 6

1. Bij ministeriële regeling kunnen inbreuken op de veiligheid of verliezen van integriteit als bedoeld in artikel 11a.2, eerste lid, van de wet, worden aangewezen waarvan Onze Minister in ieder geval onverwijld in kennis gesteld moet worden.
2. Bij deze aanwijzing neemt Onze Minister de aard en de omvang van de inbreuk of het verlies en de mogelijke gevolgen ervan in aanmerking, daarbij uitgaand van:

a. de bereikbaarheid van alarmnummers;
b. de aard en het aantal van de getroffen gebruikers;
c. de omvang van het getroffen gebied;
d. de verwachte duur van de inbreuk of het verlies.

Artikel 7

1. De aanbieder doet de in artikel 11a.2, eerste lid, van de wet bedoelde melding bij het meldpunt.
2. De melding bevat in ieder geval:
a. het tijdstip van aanvang van de inbreuk of het verlies;
b. de aard en de omvang van de inbreuk of het verlies;
c. op welk netwerk of bij welke dienst de inbreuk of het verlies heeft plaatsgevonden;
d. een prognose van de hersteltijd.
3. Bij ministeriële regeling kunnen nadere regels worden gesteld omtrent de wijze waarop de melding plaatsvindt.

Artikel 8

1. Indien de aanbieder melding heeft gedaan van een inbreuk op de veiligheid of een verlies van integriteit als bedoeld in artikel 11a.2, eerste lid, van de wet, verstrekt hij Onze Minister zo spoedig mogelijk doch in ieder geval binnen vier weken na beëindiging van de inbreuk of van het verlies van integriteit alle informatie omtrent:
a. wanneer de inbreuk of het verlies is beëindigd;
b. welke maatregelen zijn genomen om de inbreuk of het verlies te beëindigen;
c. welke maatregelen zijn genomen om herhaling van de inbreuk of het verlies te voorkomen.
2. Bij ministeriële regeling kunnen nadere regels worden gesteld omtrent de wijze waarop de in het eerste lid bedoelde verstrekking plaatsvindt.

Artikel 9

1. De aanbieder wijst een in Nederland gevestigde functionaris aan die verantwoordelijk is voor het doen van de in artikel 7 bedoelde melding en die tevens optreedt als eerste aanspreekpunt van de aanbieder voor het meldpunt in geval van een inbreuk op de veiligheid of een verlies van integriteit als bedoeld in artikel 11a.2, eerste lid, van de wet.
2. De in het eerste lid bedoelde functionaris is te allen tijde voor het meldpunt bereikbaar door middel van elektronische communicatie.
3. De aanbieder verstrekt de contactgegevens van de in het eerste lid bedoelde functionaris en wijzigingen daarvan onverwijld aan het meldpunt.

§ 4. Slotbepalingen

Artikel 10

Dit besluit treedt in werking met ingang van 1 januari 2013.

Artikel 11

Het advies van de Afdeling advisering van de Raad van State wordt niet openbaar gemaakt op grond van artikel 26, zesde lid jo vijfde lid van de Wet op de Raad van State, omdat het uitsluitend opmerkingen van redactionele aard bevat.

Dit besluit wordt aangehaald als: Besluit continuïteit openbare elektronische communicatienetwerken en -diensten.

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

's-Gravenhage, 19 oktober 2012

Beatrix

De Minister van Economische Zaken, Landbouw en Innovatie,
M. J. M. Verhagen

Uitgegeven de *dertigste* oktober 2012

De Minister van Veiligheid en Justitie,
I. W. Opstelten

stb-2012-514
ISSN 0920 - 2064
's-Gravenhage 2012

NOTA VAN TOELICHTING

I. Algemeen

1. Doel en aanleiding

In dit besluit worden nadere regels gegeven met betrekking tot het bepaalde in de artikelen 11a.1 en 11a.2 van de Telecommunicatiewet (verder te noemen: de wet). Deze artikelen strekken tot implementatie van de artikelen 13bis en 13ter van de Richtlijn 2002/21/EG van het Europees Parlement en de Raad van de Europese Unie van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronische-communicatie-netwerken en -diensten (Kaderrichtlijn) (PbEG L 108) alsmede van artikel 23, eerste volzin, van de Richtlijn 2002/22/EG van het Europees Parlement en de Raad van de Europese Unie van 7 maart 2002 inzake de universele dienst en gebruikersrechten met betrekking tot elektronische-communicatienetwerken en -diensten (Universeledienstrichtlijn) (PbEG L 108), het new regulatory framework (NRF). Doel van deze bepalingen is de continuïteit van de openbare elektronische communicatienetwerken of -diensten te waarborgen, teneinde de effecten van inbreuken op gebruikers en onderling verbonden netwerken zo gering mogelijk te houden.

Met de wijziging van het Europees regelgevend kader voor elektronische communicatie is een aantal verplichtingen geïntroduceerd vanuit de optiek van de continuïteit van de netwerken en de dienstverlening met behulp van deze netwerken. In een omgeving waarin de afhankelijkheid van elektronische communicatie almaar toeneemt, is de beschikbaarheid van netwerken en de daarover geleverde diensten van groot economisch en maatschappelijk belang.

2. Inhoud

De reikwijdte van het besluit wordt bepaald door de artikelen 11.a1 en 11.a2 van de wet, waarin de in paragraaf 1 bedoelde artikelen uit de NRF-richtlijnen zijn geïmplementeerd. Bij de uitwerking is bovendien, in het kader van de geharmoniseerde implementatie van deze richtlijnen binnen de EU, zoveel mogelijk aansluiting gezocht bij de daartoe door het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA) opgestelde Technical Guidelines, te weten: «Technical Guideline for Minimum Security Measures», Guidance on the security measures in Article 13a, Version 1.0 en «Technical Guideline on Reporting Incidents», Article 13a Implementation, Version 1.0, beide gepubliceerd op 13 december 2011 (http://www.enisa.europa.eu).

In artikel 11a.1, eerste lid, van de wet, is de verplichting opgenomen dat de aanbieders van openbare elektronische communicatienetwerken of -diensten passende technische en organisatorische maatregelen nemen om de veiligheid en de integriteit van deze netwerken en diensten te waarborgen. In artikel 11a.1, tweede lid, van de wet, is de verplichting opgenomen voor aanbieders van openbare telefoondiensten en aanbieders van openbare elektronische communicatienetwerken waarover openbare telefoondiensten worden aangeboden, om alle noodzakelijke maatregelen te nemen om de beschikbaarheid van de openbare telefoondiensten over de openbare elektronische communicatienetwerken zo volledig mogelijk te waarborgen in geval van een technische storing of uitval van het elektriciteitsnetwerk. In paragraaf 2 van het besluit is een en ander uitgewerkt.

Een andere verplichting die voortvloeit uit het gewijzigd Europees regelgevend kader, neergelegd in artikel 11a.2 van de wet, is de plicht tot het melden van veiligheidsinbreuken en het verlies van integriteit die een belangrijk effect hebben gehad op de continuïteit van het netwerk of de daarover geleverde diensten. Deze meldingen zullen plaatsvinden bij Agentschap Telecom van het Ministerie van Economische Zaken, Landbouw en Innovatie. Dit is uitgewerkt in paragraaf 3 van het besluit.

Agentschap Telecom is belast met het toezicht op de naleving van de bepalingen van hoofdstuk 11A van de wet. Hiertoe is het Besluit aanwijzing toezichthouders Telecommunicatiewet (Stcrt. 1998, 230) gewijzigd.

3. Relatie met andere onderdelen van de Telecommunicatiewet

Ernstige verstoringen van de continuïteit van de netwerken en van de dienstverlening die daarover plaatsvindt, spelen ook een rol in het kader van buitengewone omstandigheden. De meldplicht bij Agentschap Telecom van storingen in het kader van continuïteit op grond van artikel 11a.2 van de wet, sluit dan ook goed aan bij de in het kader van hoofdstuk 14 van de wet met de betrokken aanbieders gemaakte afspraken over het melden van verstoringen van de continuïteit van de dienstverlening.

Hoofdstuk 14 van de wet bevat regels die het mogelijk maken om, indien de regering dit nodig acht, aanwijzingen te geven over de verzorging van elektronische communicatie in buitengewone omstandigheden. Hoofdstuk 14 bevat onder meer een ook in andere noodwetgeving voorkomende standaardprocedure voor de inwerkingstelling van de desbetreffende bepalingen. De aanwijzingsbevoegdheden van hoofdstuk 14 zijn, anders dan in hoofdstuk 11A, gericht tot een beperkt aantal, nader aangewezen, aanbieders. Deze aanbieders zijn op grond van hoofdstuk 14 ook verplicht om organisatorische en personele maatregelen te treffen ter voorbereiding van buitengewone omstandigheden.

Bij het opstellen van het besluit is zoveel mogelijk aansluiting gezocht bij de reeds op grond van hoofdstuk 14 geldende verplichtingen en de in dat verband opgedane ervaringen. Het voorgaande betekent dat de desbetreffende aanbieders, op het moment van in werking treden van hoofdstuk 11A van de wet en de daarop gebaseerde regelingen, bekend zijn met verplichtingen zoals die op grond van hoofdstuk 11A zullen gaan gelden en grotendeels al aan deze verplichtingen zullen voldoen. De verwachting is overigens dat de meeste aanbieders op eenvoudige wijze aan deze verplichtingen zullen kunnen voldoen, omdat zij in het kader van hun dagelijkse bedrijfsvoering en om een serieuze rol op de markt voor elektronische communicatie te kunnen spelen, er uiteraard zelf alle belang bij hebben om te zorgen voor continuïteit van hun netwerken en diensten en daartoe al de nodige maatregelen hebben getroffen.

De op grond van hoofdstuk 14 aangewezen aanbieders zullen, na de inwerkingtreding van het onderhavige besluit, ook meldingen in het kader van hoofdstuk 14 bij het Agentschap Telecom dienen te doen. Het meldpunt zal in relevante gevallen zo nodig, in geval van buitengewone omstandigheden als bedoeld in hoofdstuk 14 van de wet, zorgen voor het doorgeleiden van de melding naar de crisisorganisatie van de overheid.

De meldplichten voor aanbieders van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten in verband met integriteit en veiligheid staan in beginsel naast de nieuw in te voeren meldplicht voor aanbieders van openbare elektronische communicatiediensten ten aanzien van veiligheidsinbreuken die leiden tot

het ongewenst vrijkomen van persoonsgegevens, bedoeld in hoofdstuk 11 van de wet. Dat wil echter niet zeggen dat er in de praktijk geen overlap kan zijn. Een veiligheidsinbreuk kan immers tegelijkertijd leiden tot een belangrijk effect op de continuïteit en het ongewild vrijkomen van persoonsgegevens. Mede om administratieve lasten zo veel mogelijk te beperken, kunnen beide meldingen bij hetzelfde meldpunt, in casu Agentschap Telecom, worden gedaan. Vanuit het meldpunt wordt er voor gezorgd dat de melding bij de Minister van Economische Zaken, Landbouw en Innovatie, het college van de Onafhankelijke post- en telecommunicatieautoriteit of, in geval van genoemde overlap, bij beide terecht komt.

4. Bedrijfseffecten

In de memorie van toelichting op het voornoemde wetsvoorstel ter implementatie van het NRF (Kamerstukken II, 32549, nr. 3, paragraaf 2) is een uitgebreide toelichting opgenomen op de toetsing van de administratieve lasten en van de bedrijfseffecten van dit wetsvoorstel. De voor het onderhavige besluit relevante passages uit deze toelichting betreffen het volgende:

«In opdracht van de toenmalige Minister van Economische Zaken is door het onderzoeksbureau EIM een zogenoemde quick scan naar de administratieve lasten verricht. Bij een quick scan kan worden volstaan met een beperkt aantal interviews met deskundigen aan de kant van de overheid en (indien nodig) het bedrijfsleven. Gekozen is voor een quick scan om de volgende redenen:
– een eerste oppervlakkige inventarisatie gaf het beeld dat de wijzigingen in de Telecommunicatiewet voor individuele bedrijven waarschijnlijk beperkte gevolgen hebben voor de administratieve lasten;
– dat de wijzigingen geen gevolgen hebben voor de administratieve lasten van burgers;
– dat de wetswijzigingen voorvloeien uit de één op één implementatie van de Europese richtlijnen, zonder «nationale koppen».

Bij de scan is ten aanzien van de meldingen van onderbrekingen van de continuïteit (artikel 11a.2, eerste lid, van de wet) uitgegaan van een tiental meldingen per jaar per aanbieder. Hierbij is geput uit de ervaringen die zijn opgedaan bij thans al (op vrijwillige basis) plaatsvindende meldingen van verstoringen in het kader van hoofdstuk 14 van de wet. Uitgangspunt hierbij is verder geweest dat in de praktijk bij verstoring van de continuïteit doorgaans kan worden volstaan met melding van deze verstoring door de netwerkexploitant en dat dienstaanbieders die gebruik maken van het netwerk en dus ook getroffen worden door de continuïteitsverstoring, die verstoring niet hoeven te melden. Hierdoor gaat het bij deze meldingen om een beperkt aantal aanbieders. Zo zijn in het kader van hoofdstuk 14 van de wet momenteel acht aanbieders door de minister aangewezen, die op grond van hoofdstuk 14 onder meer maatregelen ten behoeve van de continuïteit van hun dienstverlening moeten nemen. Voorts is uitgegaan van een gemiddelde tijdsbesteding van tien minuten per melding tegen een uurtarief van € 49. Op basis van deze aannames bedragen de totale kosten € 733 per jaar.

Verder is in de quick scan rekening gehouden met het feit dat de betrokken aanbieders gemiddeld genomen eenmaal per jaar een overleg hebben met het Ministerie van Economische Zaken, Landbouw en Innovatie of met Agentschap Telecom naar aanleiding van een melding of de gevolgen daarvan. Aangenomen is dat aanbieders hier acht uur aan besteden tegen een uurtarief van € 49, dat betekent in totaal € 3.136.

Behalve naar de in de memorie van toelichting vermelde administratieve lasten is bij het opstellen van dit besluit ook gekeken naar de zogenoemde inhoudelijke nalevingskosten. Op grond van dit besluit zouden deze kosten kunnen voortvloeien uit de verplichtingen voor de aanbieders om organisatorische en technische maatregelen te nemen om de continuïteit zo volledig mogelijk te waarborgen. Voorbeelden van dergelijke maatregelen zijn het aanwijzen van een contactfunctionaris, fysieke beveiliging van het netwerk en het opstellen van een continuïteitsplan. Zoals echter al in paragraaf 3 is aangegeven – en ook door aanbieders zelf tijdens de consultatie is bevestigd – voldoen de voor de continuïteit meest relevante aanbieders (dit zijn de aanbieders die beschikken over een eigen netwerk) nu reeds aan de desbetreffende verplichtingen. De nalevingskosten zijn in dit geval gelijk aan de «business as usual costs». Om een serieuze rol op de markt voor elektronische communicatie te kunnen spelen, heeft een aanbieder immers zelf alle belang bij continuïteit van zijn dienstverlening. Ook als de wettelijke verplichting niet zou bestaan, zou de aanbieder de in dit besluit voorgeschreven maatregelen nemen om de continuïteit van zijn diensten te waarborgen. Van «meerkosten» op grond van het besluit voor reeds bestaande aanbieders is dan ook geen sprake. Aanbieders die tot de markt toetreden na de inwerkingtreding van dit besluit zullen weliswaar moeten voldoen aan onder meer het besluit, maar ook voor deze aanbieders geldt dat de door hen te maken kosten ten behoeve van de continuïteit van hun dienstverlening in de eerste plaats in het belang van hun eigen businesscase gemaakt zullen worden.

Wat betreft de toezichtlasten wordt het volgende opgemerkt. Op grond van het voorgestelde artikel 11a.2, tweede lid, van de wet, zijn aanbieders gehouden op verzoek van de minister alle informatie te verstrekken die nodig is om de veiligheid en integriteit van hun netwerken en diensten te beoordelen. In de scan is ervan uitgegaan dat aanbieders hier gemiddeld één keer per jaar mee te maken krijgen en dat zij hier veertig uur tegen een uurtarief van € 49 aan kwijt zijn. Op basis hiervan bedragen deze kosten in totaal € 15.680 per jaar. Daarnaast kan een aanbieder op grond van artikel 11a.1, zesde lid, van de wet, verplicht worden om een veiligheidscontrole te laten uitvoeren door een onafhankelijke deskundige, waarbij de desbetreffende aanbieder de kosten draagt van deze controle. De verwachting is dat van deze bevoegdheid slechts sporadisch gebruik zal worden gemaakt, en dat de daaraan verbonden kosten niet significant zijn. Derhalve zijn deze kosten niet opgenomen in de hierboven vermelde quick scan.

Tenslotte zal bij de gebruikelijke evaluatie van de regelgeving uiteraard ook aandacht worden besteed aan de regeldrukaspecten, waaronder de administratieve lasten en de inhoudelijke nalevingskosten.

5. Uitvoeringstoets Agentschap Telecom

Dit besluit is voor een uitvoerbaarheids- en handhaafbaarheidstoets voorgelegd aan Agentschap Telecom. Het agentschap acht het besluit uitvoerbaar en handhaafbaar.

6. Consultatie

Dit besluit is geconsulteerd door middel van een internetconsultatie op Overheid.nl. Op de consultatie van het onderhavige besluit zijn in totaal 8 reacties ontvangen. Het merendeel van de reacties is positief en de doelstellingen van het besluit worden door de meeste partijen onderschreven. Enkele partijen benadrukken dat de voor de continuïteit meest relevante aanbieders (op grond van hoofdstuk 14 van de Telecommunica-

tiewet) reeds voldoen aan de in dit besluit gestelde verplichtingen en vinden dit besluit dan ook proportioneel. Daarnaast is er waardering voor het streven naar internationale harmonisatie van deze voorschriften. De volgende opmerkingen hebben aanleiding gegeven tot aanpassing van het besluit en de toelichting.

Een van de partijen wees er op dat de dienstverlening van de betrokken aanbieders vaak een internationaal karakter heeft en dat het in dit verband relevant is dat de onderliggende NRF-richtlijnen in de gehele EU consistent worden geïmplementeerd. Zij pleitte ervoor de invulling zoveel mogelijk over te laten aan de aanbieders en vond deze specifiek voor Nederland getroffen regeling mede vanwege de te plegen investeringen en te verwachten administratieve lasten disproportioneel. Zij was verder van mening dat de administratieve lasten te laag zijn ingeschat. Een andere partij stelde voor om een jaar na inwerkingtreding van dit besluit een evaluatie te houden van de administratieve lasten en bedrijfseffecten. De toelichting is op het punt van administratieve lasten verduidelijkt.

Een partij merkte op dat het besluit vanwege de huidige complexiteit in de organisatie van omroep-zendernetwerken ten aanzien van de niet-dupliceerbare omroepzenderinfrastructuur een dode letter zal zijn, tenzij deze organisatie eenvoudiger en transparanter zal worden georganiseerd. In de toelichting op artikel 1 is nader ingegaan op het begrip «aanbieders» van openbare netwerken.

Enkele partijen merkten op dat het onduidelijk is of en in welke mate de in deze regeling genoemde documenten, zoals het continuïteitsplan, informatie en de meldingen als vertrouwelijk moeten worden beschouwd en dat het niet wenselijk is dat met een beroep op de Wet openbaarheid van bestuur inzage in die stukken kan worden verkregen. In de toelichting op de artikelen 2 en 7 is aan dit punt aandacht geschonken.

Een partij gaf aan dat het niet duidelijk is wat met een «continuïteitsplan» wordt bedoeld; zij merkte op dat een aanbieder meerdere van deze plannen kan hebben en stelde voor dit plan te beperken tot de «vitale» diensten en netwerken. Het begrip «continuïteitsplan» is in de toelichting op artikel 2 nader toegelicht.

Wat betreft de meldplicht (paragraaf 3) merkte een partij op het te waarderen dat er één meldloket wordt ingericht voor zowel de meldingen als bedoeld in artikel 11a.2, eerste lid, van de wet (met betrekking tot continuïteit) als voor de meldingen als bedoeld in artikel 11.3a van de wet (met betrekking tot persoonsgegevens). Deze partij pleitte ervoor om in plaats van deze beide meldingen te volstaan met één enkele melding. Daarnaast merkte deze partij op dat het doorsturen van de meldingen ook nog zal moeten worden verwerkt in hoofdstuk 14 van de wet. In de toelichting op de artikelen 6 en 7 is aandacht geschonken aan de verschillende meldplichten.

Een partij was van mening dat de verplichting om eenmaal per jaar te evalueren en zo nodig de continuïteitsplannen aan te passen, niet realistisch en te statisch is, omdat aanbieders in de praktijk continu over de continuïteit nadenken en zelf onmiddellijk maatregelen nemen zodra daartoe aanleiding bestaat. Het besluit is in deze zin aangepast.

Een partij vond het niet nuttig om een eindverantwoordelijke aan te wijzen voor het continuïteitsplan, omdat deze functionaris mogelijk niet in Nederland werkzaam zal zijn. Een andere partij vond het niet duidelijk welke contactpersonen er voor welke taken moeten worden aangewezen. Op dit punt zijn zowel het besluit als de toelichting op artikel 9 aangepast.

Ten aanzien van beveiliging van netwerken en diensten merkte een partij op dat de zorgplicht van aanbieders zich niet moet beperken tot de fysieke beveiliging, maar dat ook de logische beveiliging moet worden gewaarborgd, met name met het oog op het voorkomen van inbreuken op het gebied van «cybercrime». Het besluit is op dit punt aangepast.

Door een aantal partijen werd opgemerkt dat de bepaling inzake geheimhouding te strikt is geformuleerd omdat aanbieders geen «garantie» van geheimhouding door de betrokken personen kunnen geven. Wel kunnen zij deze personen een geheimhoudingsverplichting opleggen. Het besluit is op dit punt aangepast.

Een partij vroeg waarom het besluit verplichtingen bevat die alleen gelden voor aanbieders van openbare telefoondiensten en dito netwerken. De bedoelde verplichting is geschrapt.

Meerdere partijen hebben opmerkingen gemaakt over het feit dat het moeilijk, zo niet onmogelijk is om, zeker voor grotere of internationale aanbieders, alle in dit verband relevante overeenkomsten op te nemen in het continuïteitsplan. Ook is opgemerkt dat dergelijke overeenkomsten vertrouwelijke informatie en geheimhoudingsbepalingen kunnen bevatten, waardoor deze niet zonder meer kunnen worden overgelegd. Deze bepaling is geschrapt.

Inwerkingtreding, vaste verandermomenten

Aan het beleid inzake Vaste verandermomenten, te weten: algemene maatregelen van bestuur treden in werking op 1 januari of 1 juli en bekendmaking geschiedt uiterlijk twee maanden voor inwerkingtreding, is gevolg gegeven.

II. Artikelen

Artikel 1

De in Hoofdstuk 11A van de wet neergelegde verplichtingen rusten op de aanbieders van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten. Onder dit begrip vallen onder meer aanbieders van openbare telefoondiensten over zowel openbare vaste als mobiele netwerken, aanbieders van de internettoegangsdienst, maar ook aanbieders van SIM-kaarten voor mobiele communicatie en aanbieders van telecommunicatiediensten en transmissiediensten op netwerken die voor omroep worden gebruikt.

Artikel 2

In het zogenoemde continuïteitsplan worden de technische en organisatorische maatregelen, bedoeld in artikel 11a.1, eerste lid, van de wet nader beschreven. Het gaat daarbij om maatregelen ter waarborging van de continuïteit, die geschikt en passend zijn gezien de risico's, de omvang van de aanbieder en diens netwerken en diensten en de stand van de techniek. Daarbij moet onder meer gedacht worden aan maatregelen ter bescherming van de instandhouding en exploitatie van de netwerken en diensten en maatregelen die moeten worden genomen in geval van technische storingen of bij elektriciteitsuitval, zoals het zorgen voor de beschikbaarheid van noodvoorzieningen en afspraken met relevante servicediensten of leveranciers.

De betrokken aanbieders van netwerken en diensten kunnen beschikken over meerdere netwerken waarover vanuit verschillende locaties diverse diensten worden verzorgd. Het is aan de aanbieder om te kiezen voor het

opstellen van een of meer continuïteitsplannen, bijvoorbeeld per netwerk of per dienst.

In het continuïteitsplan moet, in het belang van de interne bedrijfsvoering van de aanbieder, zijn vastgelegd, welke functionaris eindverantwoordelijk is voor de te nemen maatregelen. Om te voorkomen dat met wisseling van personeel van de aanbieder telkens het continuïteitsplan zou moeten worden gewijzigd, wordt op grond van dit artikel niet de voor het nemen en uitvoeren van de maatregelen verantwoordelijke persoon, maar de desbetreffende functionaris in het continuïteitsplan vastgelegd. Omdat deze functionaris tevens kan fungeren als aanspreekpunt voor de Minister van Economische Zaken, Landbouw en Innovatie en de toezichthouder, bijvoorbeeld voor het voeren van regulier of ad hoc overleg over beleidskwesties met betrekking tot de waarborging van de continuïteit, is het van belang dat de actuele contactgegevens van deze functionaris bij de minister en de toezichthouder bekend zijn. Dit is geregeld in het eerste lid, onder b, juncto het tweede lid van artikel 2. Deze functionaris kan uiteraard alleen verantwoordelijk zijn voor de uitvoering en naleving van het continuïteitsplan binnen de organisatie van de aanbieder. De verantwoordelijkheid voor de uitvoering en de naleving van de verplichtingen van dit besluit en van hoofdstuk 11A van de wet berust niet bij deze functionaris, maar bij de aanbieder.

Deze functionaris moet worden onderscheiden van de functionaris, bedoeld in het eerste lid, onder c, van dit artikel, die op grond van artikel 9 wordt aangewezen als de verantwoordelijke voor de meldingen, bedoeld in artikel 7. Dat deze functionarissen verschillende taken en verantwoordelijkheden hebben, hoeft er niet aan in de weg te staan dat een aanbieder een of meerdere personen aanwijst voor de uitvoering van deze taken en verantwoordelijkheden. Dit is afhankelijk van bijvoorbeeld de omvang, plaats van vestiging en organisatie van de onderneming en de beschikbaarheid van ter zake kundig personeel, mits dit uiteraard wordt vermeld in het continuïteitsplan en wordt gemeld aan de minister respectievelijk het meldpunt.

De in het continuïteitsplan neergelegde informatie betreft in het algemeen bedrijfs- en fabricagegegevens als bedoeld in artikel 10, eerste lid, onder c, van de Wet openbaarheid van bestuur.

De in het derde lid opgenomen mogelijkheid om bij ministeriële regeling nadere regels te stellen, is met name bedoeld om zo nodig snel uitvoering te kunnen geven aan de eerder genoemde Technical Guidelines van ENISA. De verwachting is dat deze Guidelines, die gedetailleerde (technische) voorschriften en verwijzingen naar verschillende internationale standaarden bevatten, regelmatig gewijzigd zullen worden.

Artikel 3

Dit artikel bevat de verplichting voor de aanbieder om het continuïteitsplan regelmatig te evalueren. Hiervoor is geen minimumtermijn voorgeschreven omdat artikel 11a.1, eerste lid, van de wet reeds impliceert dat de te nemen maatregelen «passend» moeten zijn, wat wil zeggen dat de maatregelen «up to date» en geschikt zijn gezien de stand van de techniek. De eerder genoemde Guidelines van ENISA zijn hiervoor een bruikbaar hulpmiddel. Evaluatie en zo nodig aanpassing van het continuïteitsplan dient vanzelfsprekend ook plaats te vinden aan de hand van de door de aanbieder gemelde inbreuken.

Inherent aan deze verplichting is uiteraard dat de aanbieder ervoor zorgt dat de benodigde maatregelen onmiddellijk kunnen worden uitgevoerd,

door de desbetreffende voorzieningen goed te onderhouden, regelmatig testen en oefeningen te houden en te zorgen voor bekwaam personeel.

Artikel 5

De in het tweede lid bedoelde geheimhoudingsverplichting geldt niet alleen voor het eigen personeel van de aanbieder, maar ook voor door de aanbieder ingeschakelde derde partijen, zoals onderhoudsbedrijven of servicediensten.

Artikelen 6 en 7

Op grond van artikel 11a.2, eerste lid, van de wet moet een inbreuk op de veiligheid en een verlies van integriteit onverwijld worden gemeld indien de continuïteit in belangrijke mate wordt onderbroken. Gelet op het belang van deze meldingen, de mogelijke gevolgen van een inbreuk en om te zorgen voor een snelle verwerking, zal het meldpunt van het Agentschap Telecom 7 dagen per week en 24 uur per dag bereikbaar zijn.

Het is niet mogelijk en niet zinvol om een uitputtende omschrijving van alle mogelijk voorkomende gevallen van dergelijke inbreuken of verliezen te geven. De uitvoeringspraktijk zal daarover duidelijkheid moeten verschaffen. Gelet op de almaar toenemende afhankelijkheid van elektronische communicatie, zal daarbij in elk geval het economische en maatschappelijke belang van de beschikbaarheid van de netwerken en diensten in ogenschouw worden genomen. Het vierde lid van artikel 11a.2 van de wet geeft de Minister van Economische Zaken, Landbouw en Innovatie de mogelijkheid om een ondergrens te bepalen van inbreuken of verliezen die in elk geval moeten worden gemeld. Daarbij zullen telkens de aard en de omvang van de inbreuk of het verlies en de mogelijke gevolgen ervan centraal staan, aan de hand van de aspecten bereikbaarheid van alarmnummers, aard en aantal van de getroffen gebruikers, omvang van het getroffen gebied, verwachte duur van de inbreuk of het verlies. Deze aspecten en de wijze waarop de aspecten de ondergrens bepalen zijn ontleend aan de Technical Guidelines van ENISA.

Op het moment dat de melding wordt gedaan, zal het niet altijd eenvoudig zijn om een onderbouwde prognose van de hersteltijd te geven. Desalniettemin is deze prognose een verplicht onderdeel van de melding, omdat deze wezenlijk kan zijn in het geval dat de inbreuk dermate ernstig is of kan worden, dat er moet worden opgeschaald naar de crisisorganisatie van de overheid of dat sprake kan zijn van buitengewone omstandigheden als bedoeld in hoofdstuk 14 van de wet.

Op grond van het derde lid van artikel 7 zal in een ministeriële regeling een model worden vastgesteld voor de in dit besluit bedoelde meldingen. Daarbij zal zoveel mogelijk worden aangesloten bij de Technical Guidelines van ENISA, mede met het oog op de op de Minister van Economische Zaken, Landbouw en Innovatie rustende rapportageverplichtingen aan ENISA en de Europese Commissie over de meldingen en genomen maatregelen.

De met betrekking tot de melding verstrekte informatie betreft in het algemeen bedrijfs- en fabricagegegevens als bedoeld in artikel 10, eerste lid, onder c, van de Wet openbaarheid van bestuur.

Artikel 9

De in dit artikel bedoelde functionaris is in feite het «loket» van de aanbieder die de feitelijke melding doet. Deze functionaris is dan ook het eerste aanspreekpunt van de aanbieder voor het meldpunt in geval van een storingsmelding. Wie deze functie binnen de aanbieder vervult, wordt aan de aanbieder overgelaten en zal onder meer afhankelijk zijn van de omvang en de organisatie van de betrokken aanbieder. Gelet op deze loketfunctie bij verstoringen, moet deze functionaris in Nederland gevestigd en permanent bereikbaar zijn. Ook moet het meldpunt op de hoogte zijn, respectievelijk onverwijld in kennis worden gesteld van de contactgegevens van de functionaris en eventuele wijzigingen daarvan, zodat het meldpunt ten behoeve van eventuele vervolgacties direct contact met de aanbieder kan leggen. Verder is de actualiteit van deze gegevens relevant voor het kunnen nagaan van de authenticiteit van de melding.

De Minister van Economische Zaken, Landbouw en Innovatie,
M. J. M. Verhagen