Besluit van , houdende nadere regels betreffende de veiligheid en integriteit van openbare elektronische communicatienetwerken en -diensten (Besluit veiligheid en integriteit telecommunicatie)

Op de voordracht van de Staatssecretaris van Economische Zaken en Klimaat van 14 oktober 2019, nr. WJZ / 19232889;

Gelet op artikel 11a.1, vierde lid, van de Telecommunicatiewet;

De Afdeling advisering van de Raad van State gehoord (advies van nr.);

Gezien het nader rapport van de Staatssecretaris van Economische Zaken en Klimaat van , nr. WJZ / ;

Hebben goedgevonden en verstaan:

Artikel 1

In dit besluit en de daarop gebaseerde regelgeving wordt verstaan onder:

- beheer: onderhoud of aansturing van apparatuur of programmatuur van een aanbieder van een openbaar elektronisch communicatienetwerk of een openbare elektronische communicatiedienst,
- producten of diensten: apparatuur, programmatuur, beheer en aanverwante dienstverlening.

Artikel 2

1. Bij ministeriële regeling kunnen nadere regels worden gegeven met betrekking tot de in artikel 11a.1 van de wet bedoelde technische en organisatorische maatregelen en kunnen technische en organisatorische eisen worden gesteld aan aanbieders van openbare elektronische communicatienetwerken of openbare elektronische communicatiediensten.

2. Indien dat naar het oordeel van Onze Minister noodzakelijk is om risico's voor de veiligheid en integriteit van diens netwerk of dienst die de nationale veiligheid of de openbare orde raken te beheersen, legt Onze Minister een aanbieder van een openbaar elektronisch communicatienetwerk of -dienst een verplichting op om in de daarbij aangewezen onderdelen van diens netwerk of bijbehorende faciliteiten, uitsluitend gebruik te maken van producten of diensten van anderen dan een door Onze Minister op grond van het derde lid aangewezen partij.

3. Een partij wordt door Onze Minister aangewezen indien deze:

a. een staat, entiteit of persoon is waarvan bekend is of waarvoor gronden zijn te vermoeden dat deze de intentie heeft een in Nederland aangeboden elektronisch communicatienetwerk of -dienst te misbruiken of uit te laten vallen, of

b. nauwe banden heeft met of onder invloed staat van een staat, entiteit of persoon als bedoeld onder a, of een entiteit of persoon is ten aanzien van wie er gronden zijn om dergelijke banden of invloed te vermoeden.

4. Indien een verplichting op grond van het tweede lid betrekking heeft op reeds in gebruik zijnde producten en diensten ten behoeve van de daarbij aangewezen onderdelen, stelt Onze Minister in het belang van de continuïteit van dienstverlening een termijn vast voor het vervangen respectievelijk beëindigen van de betreffende producten en diensten.

5. De aanwijzing van een partij op grond van het derde lid wordt meegedeeld aan de aanbieder aan wie een verplichting op grond van het tweede lid is opgelegd.

Artikel 3

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

Artikel 4

Dit besluit wordt aangehaald als: Besluit veiligheid en integriteit telecommunicatie.

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

De Staatssecretaris van Economische Zaken en Klimaat,

TOELICHTING

Aanleiding en inhoud besluit

Op 21 februari 2019 is een interdepartementale Taskforce Economische Veiligheid onder leiding van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) van het ministerie van Justitie en Veiligheid opgericht (hierna: de Taskforce). Aanleiding hiervoor waren de waarschuwingen van de inlichtingen- en veiligheidsdiensten voor infiltratie van statelijke actoren ten behoeve van spionage in de telecomsector. Misbruik van producten en diensten van leveranciers in de telecomsector biedt statelijke actoren spionagemogelijkheden ten aanzien van vertrouwelijke bedrijfs- en overheidsinformatie, persoonsgegevens en andere gevoelige informatie en kan daarmee de nationale veiligheid van Nederland in het geding brengen. Daarnaast is geconstateerd dat er meerdere landen zijn waar wetgeving van kracht is die dienstverleners kan dwingen mee te werken aan inlichtingenactiviteiten. Hierdoor kan gebruik worden gemaakt van de toegang die bedrijven die producten en diensten leveren voor de aanleg en beveiliging van telecominfrastructuren, hebben tot netwerken in de telecomsector. De risico's voor de nationale veiligheid worden significant vergroot als dienstverleners tot die medewerking kunnen worden verplicht door landen met een offensief cyberprogramma gericht tegen Nederlandse belangen. Verwacht wordt dat met de introductie van 5G de maatschappelijke afhankelijkheid van mobiele telecommunicatienetwerken, en daarmee de kwetsbaarheid bij misbruik door statelijke actoren, verder zal toenemen.

De Taskforce heeft onderzocht of de huidige beveiligingsmaatregelen die de aanbieders van mobiele netwerken op grond van de zorgplicht in artikel 11a.1 van de Telecommunicatiewet (hierna: Tw) nemen, voldoende zijn, gelet op het actuele dreigingsbeeld. De conclusie was dat aanvullende maatregelen nodig zijn, zowel ten aanzien van de beveiligingsmaatregelen als ten aanzien van de door netwerkaanbieders gebruikte producten en diensten. Bovendien moet, om aan te blijven sluiten bij de veranderingen in dreiging en technologische ontwikkeling, in samenwerking met de telecomaanbieders een structureel proces worden ingericht passend bij de huidige verantwoordelijkheden en rollen. In dit proces wordt doorlopend dreigingsinformatie gedeeld, op basis waarvan een gezamenlijke risicobeoordeling wordt verricht door telecomaanbieders, EZK/Agentschap Telecom en veiligheidspartners. Naar aanleiding van de risicobeoordeling kunnen, na overleg met de telecomaanbieders, op basis van nationale veiligheidsbelangen waar nodig adviezen worden opgesteld of maatregelen worden voorgeschreven.

Deze algemene maatregel van bestuur vormt de basis voor de maatregelen die ter uitwerking van de rapportage van de Taskforce dienen te worden genomen, zowel nu als in de toekomst. De grondslag is artikel 11a.1, vierde, Tw: de in artikel 2, tweede en derde lid, uitgewerkte maatregelen vormen een nadere uitwerking van wat gelet op het dreigingsniveau passende organisatorische beveiligingseisen zijn, in casu: om in de door de minister aangewezen, meest gevoelige onderdelen van het netwerk uitsluitend gebruik te maken van vertrouwde leveranciers.

Op dit moment staan telecompartijen voor belangrijke investeringsbeslissingen. Zij staan op het punt om hun huidige netwerken (verder) klaar te maken voor 5G. Met de komst van 5G zal in belangrijke mate worden voortgebouwd op het huidige netwerk. Het is daarom van belang dat aanbieders snel duidelijkheid krijgen over de maatregelen die zij moeten nemen, zodat zij door kunnen gaan met de modernisering van hun netwerken en de uitrol van 5G. Ook met het oog op de aanstaande frequentieveiling van 700, 1400 en 2100 MHz-vergunningen is het belangrijk om snel duidelijkheid te geven over beveiligingsverplichtingen die van invloed kunnen zijn op investeringsbeslissingen.

De Taskforce heeft met medewerking van de aanbieders van mobiele telecommunicatienetwerken een risicoanalyse uitgevoerd naar de kwetsbaarheid van hun netwerken voor misbruik van leveranciers van producten en diensten (apparatuur, programmatuur, beheer en aanverwante

dienstverlening). Hierbij is in kaart gebracht welke maatregelen de telecomaanbieders reeds treffen om hun netwerk te beschermen en is onderzocht welke aanvullende maatregelen nodig zijn om de weerbaarheid van het huidige netwerk te verhogen in het licht van de actuele dreiging. Artikel 2, eerste lid, van dit besluit biedt de grondslag om deze aanvullende beveiligingsmaatregelen op te kunnen leggen bij ministeriële regeling.

Voorts is gebleken dat ook aanvullende beveiligingsmaatregelen onvoldoende bescherming bieden tegen spionage wanneer in bepaalde onderdelen van het netwerk of de bijbehorende faciliteiten, de zogenoemde 'kritieke onderdelen', gebruik wordt gemaakt van producten of diensten van een leverancier die onder invloed staat van een kwaadwillende partij. Gelet op het actuele dreigingsbeeld en de risico's voor de nationale veiligheid en openbare orde is de Taskforce tot de conclusie gekomen dat in aanvulling op de aangescherpte beveiligingsmaatregelen aanbieders van mobiele communicatienetwerken in deze kritieke onderdelen van hun netwerken uitsluitend gebruik zouden moeten maken van vertrouwde leveranciers. De Taskforce heeft per aanbieder een technische analyse uitgevoerd waarin de kritieke onderdelen van diens netwerk in kaart zijn gebracht. Het dreigingsbeeld en nieuwe technologieën, zoals rondom 5G, zijn echter continu in ontwikkeling, waardoor er op termijn mogelijk andere onderdelen als kritiek moeten worden aangewezen. In artikel 2, tweede lid, van dit besluit is ter uitwerking van deze conclusie van de Taskforce een grondslag opgenomen op grond waarvan de minister van EZK een aanbieder van een openbaar elektronisch communicatienetwerk of -dienst bij beschikking kan verplichten om in de daarbij aangewezen onderdelen van diens netwerk of bijbehorende faciliteiten (de kritieke onderdelen bedoeld door de Taskforce), uitsluitend gebruik te maken van producten of diensten van vertrouwde leveranciers. Vanwege de gevoeligheid van deze informatie zal uitsluitend in de beschikking gericht aan de aanbieder worden meegedeeld welke onderdelen van diens netwerk als kritiek worden aangewezen.

Het zal niet altijd mogelijk zijn voor een aanbieder van een elektronisch communicatienetwerk of -dienst om per direct gevolg te geven aan de beschikking op grond van het tweede lid, zonder hiermee uitval van het netwerk te riskeren. In zo'n geval zal de minister op grond van artikel 2, vierde lid, in de beschikking een termijn opnemen waarbinnen de reeds in gebruik zijnde producten of diensten dienen te worden vervangen respectievelijk beëindigd.

De criteria op grond waarvan de minister kan bepalen wanneer al dan niet sprake is van een vertrouwde leverancier van producten of diensten, zijn opgenomen in artikel 2, derde lid, van het besluit. Dit lid geeft de minister de bevoegdheid een leverancier aan te wijzen, als gevolg waarvan diens producten en/of diensten niet langer mogen worden gebruikt in kritieke onderdelen. De aanwijzing is een beschikking gericht aan de betreffende leverancier. Omdat de aanbieder van een telecommunicatienetwerk voor de naleving van diens beschikking op grond van het tweede lid, moet weten welke leveranciers zijn aangewezen, zal de aanwijzing van dergelijke partijen ook aan de aanbieder worden meegedeeld (artikel 2, vijfde lid). De aanwijzing is, evenals de aan de telecomaanbieder krachtens het tweede lid op te leggen beschikking, met inbegrip van de daarin opgenomen aanwijzing van kritieke onderdelen, een besluit in de zin van de Algemene wet bestuursrecht en als zodanig vatbaar voor bezwaar en beroep.

De criteria in het derde lid zijn ontleend aan het wetsvoorstel ongewenste zeggenschap telecommunicatie (het voorgestelde artikel 14a.4, tweede lid, van de Telecommunicatiewet). Het gaat om leveranciers die ofwel zelf de intentie hebben om een in Nederland aangeboden elektronisch communicatienetwerk te misbruiken of uit te laten vallen, dan wel nauwe banden hebben met of onder invloed staan van een dergelijke partij. Hierbij is het niet van belang of dit een (erkende) staat is of een andere entiteit, zoals een terroristische organisatie of een niet-erkende mogendheid. Bij misbruik valt te denken aan spionage: ongeoorloofde toegang tot communicatiegegevens (zowel verkeersgegevens als inhoud van communicatie). Het bestaan van nauwe banden of invloed kan zich bijvoorbeeld uiten in de aanwezigheid van wetgeving die bedrijven verplicht medewerking te verlenen aan buitenlandse inlichtingendiensten. Bij de voorbereiding van een aanwijzing van een leverancier op grond van het derde lid zal afstemming

plaatsvinden met de NCTV en kan de minister van EZK uiteraard gebruik maken van informatie van de veiligheidsdiensten.

Bij de beoordeling van risico's ten aanzien van spionage, beïnvloeding of sabotage door statelijke actoren of andere partijen bij digitale producten hanteert het kabinet de overwegingen die zijn vermeld in de brief aan de Tweede Kamer over C2000 (Kamerstukken II 2018/19, 25 124, nr. 96). De criteria in het derde lid zijn in lijn met de overwegingen genoemd in voornoemde Kamerbrief:

1. Is de partij die de dienst of product levert afkomstig, of staat hij onder controle van een partij, uit een land met wetgeving die commerciële of particuliere partijen verplicht samen te werken met de overheid van dat land, in het bijzonder met staatsorganen die zijn belast met een inlichtingen- of militaire taak, of is de partij een staatsbedrijf?
2. Is de partij die de dienst of product levert afkomstig uit een land met een actief offensief inlichtingenprogramma gericht op Nederland en Nederlandse belangen of een land waarmee de Nederlandse relatie dusdanig gespannen is dat acties die Nederlandse belangen aantasten voorstelbaar zijn?
Indien het antwoord op de in bovenstaande overwegingen geformuleerde vragen positief is, zal er sprake zijn van een partij die nauwe banden heeft met of onder invloed staat van een staat of entiteit die de intentie heeft een in Nederland aangeboden elektronisch communicatienetwerk of -dienst te misbruiken of uit te laten vallen, of waarvoor gronden zijn om dergelijke banden of invloed te vermoeden.

3. A. Krijgt de partij die de dienst of product levert uitgebreide toegang tot gevoelige locaties, gevoelige ICT-systemen en vitale infrastructurele installaties of werken, waarbij misbruik een nationaal veiligheidsrisico kan vormen?
B. Zijn er beheersmaatregelen mogelijk en realiseerbaar die de nationale veiligheidsrisico's die in het geding zijn voldoende beschermen?
De reikwijdte van de beschikking op grond van het tweede lid is beperkt tot die onderdelen die daarin worden aangewezen. Bij de afweging, welke onderdelen in de beschikking worden aangewezen, komen bovenstaande overweging als volgt aan bod. Eerst worden de kritieke onderdelen in kaart gebracht. Dit zijn de onderdelen waarvoor geldt dat de leverancier uitgebreide toegang tot gevoelige locaties, gevoelige ICT-systemen, vitale infrastructurele installaties of werken krijgt, waarbij misbruik een nationaal veiligheidsrisico kan vormen (overweging 3A). Vervolgens wordt beoordeeld of het opleggen van een beschikking als bedoeld in het tweede lid in relatie tot die onderdelen noodzakelijk is om risico's die de nationale veiligheid of de openbare orde raken te beheersen: dit houdt in dat er geen beheersmaatregelen mogelijk en realiseerbaar zijn om deze risico's voldoende te beschermen (overweging 3B). De kritieke onderdelen waar dit voor geldt worden vervolgens aangewezen in de beschikking op grond van artikel 2, tweede lid, waarmee de reikwijdte van de verplichting om uitsluitend gebruik te maken van vertrouwde leveranciers tot die aangewezen onderdelen is beperkt.

Aanbeveling cybersecurity

Deze algemene maatregel van bestuur geeft tevens uitvoering aan de Aanbeveling Cyberbeveiliging van 5G-netwerken van de Europese Commissie (PbEU 2019, L 88/42), waarin ook naar de Europeesrechtelijke basis van artikel 11a.1 Tw (artikel 13 bis van richtlijn 2002/21, Kaderrichtlijn) wordt verwezen als bruikbaar instrument om de in de aanbeveling beschreven belangen te beschermen.

Eigendomsregulering

Dit besluit biedt de grondslag om beschikkingen op te leggen die leiden tot eigendomsregulering. Van eigendomsregulering is sprake wanneer de gebruiksmogelijkheden van de eigendom worden beperkt, zonder dat de beschikking over het eigendom verloren gaat. Bij een beschikking op basis van artikel 2, tweede lid, is sprake van *regulering* van eigendom en geen (de facto) onteigening:

het leidt immers niet tot verlies van eigendom dan wel dat de beschikking over het eigendom verloren gaat. De apparatuur behoudt waarde, blijft eigendom van de aanbieders en kan door hen te gelde worden gemaakt.

Artikel 1 van het Eerste Protocol bij het Europees Verdrag tot bescherming van de Rechten van de Mens en de Fundamentele Vrijheden (hierna: artikel 1 EP EVRM) beschermt het recht op eigendom.[1] Een beschikking op grond van artikel 2, tweede lid, van dit besluit vormt een inmenging in het eigendomsrecht van deze aanbieders als bedoeld in artikel 1 EP EVRM. Het Europees Hof voor de Rechten van de Mens en de Fundamentele vrijheden (EHRM) erkent dat een Staat ter borging van het algemeen belang (het gebruik van) eigendom mag reguleren en aan beperkingen mag onderwerpen als aan een aantal voorwaarden wordt voldaan. Een inbreuk op het eigendomsrecht is gerechtvaardigd wanneer er sprake is van regulering van eigendom en deze aan de legaliteitstoets, de legitimiteitstoets en de evenredigheidstoets ("fair balance") voldoet.

De toets van *legaliteit* brengt mee dat de inmenging in het eigendomsrecht voorzien moet zijn bij wet of daarop gebaseerde regelgeving. Met deze algemene maatregel van bestuur wordt mede beoogd invulling te geven aan het legaliteitsvereiste. De zorgplicht voor aanbieders om passende technische en organisatorische maatregelen te nemen om de risico's voor de veiligheid en de integriteit van hun netwerken en diensten te beheersen is neergelegd in artikel 11a.1 van de Telecommunicatiewet. In de nadere uitwerking van deze wettelijke bepaling in deze algemene maatregel van bestuur wordt onder meer geconcretiseerd dat deze zorgplicht in bepaalde, in artikel 2 van het besluit genoemde gevallen, kan leiden tot eigendomsregulering.

Daarnaast moeten de regels voldoende toegankelijk, precies en voorzienbaar zijn. Aan de toegankelijkheid (bekendmaking via de gebruikelijke weg) en nauwkeurigheid (precies) zal aandacht moeten worden besteed bij de formulering van de uiteindelijk op te leggen beschikkingen aan de aanbieders bedoeld in artikel 2 van het besluit. Daarbij zal tevens aandacht moeten worden besteed aan de vraag of de opgelegde maatregelen voorzienbaar zijn geweest. Met name waar een beschikking een aanbieder dwingt een product dat hij rechtmatig heeft aangeschaft vroegtijdig (voor afloop van de afschrijftermijn) te vervangen door een product van een andere leverancier zal de voorzienbaarheid van een dergelijke maatregel per geval moeten worden onderzocht. Waar deze maatregel niet voorzienbaar was, en de daaruit voortvloeiende kosten het normale ondernemersrisico te boven gaan, kunnen deze omstandigheden nopen tot compenserende maatregelen om de maatregelen verenigbaar te maken met artikel 1 EP EVRM (zie 'Fair balance').

De *legitimiteitstoets* houdt in dat de inmenging enkel mag plaatsvinden in het algemeen belang en dat deze een legitiem doel dient. Het EHRM laat de lidstaten een ruime beoordelingsmarge bij het vaststellen van wat als een legitieme doelstelling in het kader van het algemeen belang kan gelden, nationale veiligheid kan daar ook onder geschaard worden. Hierbij is wel van belang dat wordt overwogen of de ingrijpendheid van de maatregel in redelijke verhouding staat tot het ermee beoogde legitieme doel (proportionaliteit) en of er geen andere, minder ingrijpende maatregelen mogelijk zijn om ditzelfde doel te bereiken (subsidiariteit). De Taskforce heeft onderzocht of met de aanvullende beveiligingsmaatregelen, een minder ingrijpende maatregel, kan worden volstaan, hetgeen niet het geval bleek. Vervolgens is met het oog op de subsidiariteit bekeken tot welke onderdelen van het netwerk het voorschrift om uitsluitend vertrouwde leveranciers te gebruiken zou moeten uitstrekken, de zogenoemde kritieke onderdelen. Deze maatwerkaanpak is overgenomen in artikel 2, tweede lid, van deze amvb. Ook bij de beschikking op grond van artikel 2, tweede lid, waarbij tevens de kritieke onderdelen worden aangewezen, en bij de aanwijzing van een partij op grond van artikel 2, derde lid, van deze amvb, zal de minister van EZK aandacht moeten besteden aan de proportionaliteit en de subsidiariteit van dat besluit.

[1] De bescherming die deze bepaling biedt komt overeen met de bescherming van artikel 17 van het Handvest van de Grondrechten van de Europese Unie. Hierna wordt gemakshalve enkel nog over artikel 1 EP EVRM gesproken.

De *evenredigheidstoets* vraagt tot slot om een beoordeling of met de maatregelen sprake is van een rechtvaardig en evenwichtig resultaat, oftewel 'fair balance', tussen het algemeen belang en de belangen van het individu dat wordt geraakt door de inmenging in zijn eigendomsrecht.

Fair balance
Bij de beoordeling of sprake is van een 'fair balance' dienen verschillende aspecten in ogenschouw te worden genomen. De wijze waarop de maatregel wordt toegepast mag niet leiden tot een individuele en buitensporige last voor de betrokken aanbieders. Er moet bovendien een redelijke mate van evenredigheid bestaan tussen de gebruikte middelen en het nagestreefde doel.

Een van de aspecten die een belangrijke rol speelt in het kader van de 'fair balance' is de voorzienbaarheid van de maatregel. Hiermee wordt bedoeld of de maatregel in de lijn der verwachting ligt, ook al bestond er nog geen concreet zicht op de omvang waarin, de plaats waar en het moment waarop de ontwikkeling zich zou voordoen. Aanbieders zijn op grond van artikel 11a.1 Tw al sinds 2012 verplicht om passende technische en organisatorische maatregelen te nemen om de risico's voor de veiligheid en de integriteit van hun netwerken en diensten te beheersen. Echter, dat deze risico's ondanks de reeds genomen (en eventuele aanvullende) veiligheidsmaatregelen naar het oordeel van de regering niet voldoende kunnen worden beheerst wanneer in kritieke onderdelen van het netwerk niet uitsluitend producten of diensten van vertrouwde leveranciers worden gebruikt (en welke leveranciers als vertrouwd worden gezien) is pas sinds kortere tijd bekend. Een maatregel die leidt tot het moeten vervangen van producten en diensten uit (kritieke onderdelen van) het netwerk was daarmee ook pas sinds kortere tijd voorzienbaar. Voor schade die voortvloeit uit het (vroegtijdig, voor afloop van de afschrijvingstermijn) moeten vervangen van producten waarvan dit op het moment van aanschaf niet voorzienbaar was, kan het noodzakelijk zijn nadeelcompensatie te bieden, om de vereiste 'fair balance' te bereiken.

Nadeelcompensatie

Niet alleen artikel 1, Eerste Protocol bij het EVRM, leidt tot een verplichting tot het bieden van nadeelcompensatie. Een bestuursorgaan is bovendien op grond van het égalitébeginsel gehouden tot compensatie van onevenredige – buiten het normale maatschappelijk risico vallende en op een beperkte groep burgers of instellingen drukkende – schade als gevolg van het op de behartiging van het openbaar belang gerichte optreden van de overheid.

Alleen schade als direct gevolg van de opgelegde maatregel komt voor vergoeding in aanmerking. Toekomstige inkomsten vallen volgens vaste jurisprudentie van het EHRM niet onder het eigendomsbegrip van artikel 1 EP EVRM, het als gevolg van een aanwijzing op grond van artikel 2, derde lid, mislopen van toekomstige inkomsten door een aangewezen partij komt om die reden niet voor vergoeding in aanmerking. Bovendien komt schade op grond van het égalitébeginsel alleen voor vergoeding in aanmerking voor zover de schade onevenredig is. Van onevenredige schade is sprake indien de schade op een beperkte groep burgers of bedrijven drukt (speciale last) en de schade boven het normaal maatschappelijke of ondernemersrisico uitstijgt (abnormale last).

Bij de beoordeling van het deel van de schade dat niet tot het normale ondernemersrisico behoort is, zoals in de vorige paragraaf beschreven, van belang vanaf wanneer het voorzienbaar was voor de aanbieders van de mobiele communicatienetwerken dat de maatregel zou worden opgelegd. Voor investeringen die voor die tijd zijn gemaakt en die door de maatregel niet de afschrijftermijn kunnen volmaken zal steeds in overleg met de betrokken aanbieders moeten worden onderzocht in hoeverre deze behoren tot het eigen ondernemersrisico. Investeringen die na die tijd zijn gemaakt worden in beginsel niet vergoed, tenzij een aanbieder (bijvoorbeeld met het oog op de continuïteit van zijn netwerk) genoodzaakt is deze investeringen te doen en de aanbieder voldoende schadebeperkende maatregelen heeft genomen. Hierover zal duidelijkheid moeten worden geboden op het moment dat de beschikking op grond van het tweede lid wordt opgelegd.

EU-recht

Kaderrichtlijn
Deze algemene maatregel van bestuur geeft een nadere uitwerking aan de algemene zorgplicht in artikel 11a.1 Tw, waarmee artikel 13 bis, eerste en tweede lid, van richtlijn 2002/21 (de Kaderrichtlijn) is geïmplementeerd. De Kaderrichtlijn verplicht lidstaten ervoor te zorgen dat aanbieders van openbare communicatienetwerken of -diensten passende technische en organisatorische maatregelen nemen om de risico's voor de veiligheid van hun netwerken of diensten goed te beheersen. Deze maatregelen moeten, gezien de stand van de techniek, zorgen voor een veiligheidsniveau dat is afgestemd op de risico's die zich voordoen. Bovendien dienen aanbieders van openbare communicatienetwerken alle nodige maatregelen te nemen om te zorgen voor de integriteit van hun netwerken, met het oog op de continuïteit van de diensten die via deze netwerken worden geleverd. Zoals beschreven in de paragraaf Aanleiding en inhoud besluit leiden de momenteel geconstateerde spionagerisico's in ieder geval tot de noodzaak de in dit besluit mogelijk gemaakte maatregelen op te leggen om de risico's voor de veiligheid van de netwerken goed te kunnen beheersen. Indien dit in de toekomst bijvoorbeeld met het oog op sabotagerisico's tevens nodig blijkt te zijn voor de integriteit van de netwerken biedt deze algemene maatregel van bestuur daarvoor tevens de nodige grondslag.

Notificatierichtlijn en vrij verkeer van goederen
Bij de totstandkoming van de ministeriële regeling op grond van artikel 2, eerste lid, zal worden overgegaan tot notificatie onder richtlijn 1535/2015 en – voor zover van toepassing - de Dienstenrichtlijn (richtlijn 2006/123/EG) van de gestelde eisen, standaarden en voorschriften. In de toelichting bij de regeling zal ook de onderbouwing van de noodzakelijkheid, geschiktheid en proportionaliteit van de gestelde eisen en voorschriften worden gegeven overeenkomstig de eisen die deze richtlijnen en de Europese jurisprudentie hieraan stellen.

Een verplichting om in de kritieke onderdelen uitsluitend gebruik te maken van producten en/of diensten van vertrouwde leveranciers is een maatregel die het vrij verkeer van goederen belemmert in de zin van artikel 34 VWEU (een kwantitatieve invoerbeperking of maatregel van gelijke werking). Dit is slechts toegestaan indien dit gerechtvaardigd kan worden wegens een dwingende reden van algemeen belang of in geval van discriminatoire maatregelen een van de belangen opgesomd in artikel 36 VWEU, waaronder de bescherming van de openbare orde en openbare veiligheid (hetgeen ook de nationale veiligheid omvat). De maatregelen dienen voorts geschikt te zijn om het beoogde doel te bereiken en niet verder gaan dan noodzakelijk is.

Zoals toegelicht in de paragraaf Aanleiding en inhoud besluit vindt de maatregel zijn rechtvaardiging in het beschermen van de nationale veiligheid en openbare orde. Onderzocht is of deze belangen ook met minder vergaande maatregelen kunnen worden beschermd. Gelet op het actuele dreigingsbeeld en de huidige stand van techniek zijn de geconstateerde spionagerisico's echter niet afdoende te ondervangen met alleen aangescherpte beveiligingsmaatregelen. Volgens deze analyse worden de spionagerisico's aanzienlijk beter beheersbaar wanneer in bepaalde, zogenoemde kritieke onderdelen van het netwerk, uitsluitend gebruik wordt gemaakt van vertrouwde leveranciers. De maatregel gaat daarmee niet verder dan nodig voor het beoogde doel en is geschikt om het beoogde doel te bereiken.

Aangezien de algemene maatregel van bestuur betrekking heeft op elektronische-communicatiediensten en -netwerken en bijbehorende faciliteiten en diensten, en met de algemene maatregel van bestuur uitvoering wordt gegeven aan artikel 13 bis van de Kaderrichtlijn valt deze volgens artikel 2, tweede lid, onderdeel c, van de Dienstenrichtlijn (richtlijn 2006/123/EG) buiten de werkingssfeer van laatstgenoemde richtlijn (zie in deze zin voor een ruime uitleg van deze uitzondering op het toepassingsbereik van de Dienstenrichtlijn: arrest HvJEU van 30 januari 2018, gevoegde zaken C-360/15 en C-31/16, Amersfoort/X en Visser Vastgoed, overwegingen 60-82).

Internationale handels- en investeringsafspraken
Bij een beschikking op basis van artikel 2 die betrekking heeft op reeds in gebruik zijnde producten en diensten ten behoeve van de daarbij aangewezen onderdelen is tevens van belang dat de internationale afspraken tussen het Koninkrijk en derde landen over investeringsbescherming in acht worden genomen. Onder deze afspraken wordt een buitenlandse investeerder in Nederland (en worden Nederlandse investeerders in het betreffende derde land) beschermd tegen onder meer onredelijk en/of discriminatoir handelen van de overheid. Daarnaast bieden deze afspraken voorwaarden op basis waarvan onteigend mag worden, namelijk indien de maatregel die tot (de-facto) onteigening leidt non-discriminatoir, in het publiek belang is en waartegenover een gepaste schadevergoeding wordt geboden. Indien een overheid jegens die investeerder niet redelijk heeft gehandeld of de voorwaarden voor onteigening heeft geschonden, kan de investeerder daartegen compensatie eisen. Dit is alleen van belang waar het gaat om een reeds bestaande investering.
Uit hetgeen hiervoor ten aanzien van de eigendomsregulering en nadeelcompensatie is besproken (vraagstukken waarop de toetsing dezelfde beginselen volgt), kan worden geconcludeerd dat deze beschikkingen in beginsel geen schending opleveren van de internationale investeringsbeschermingsafspraken op dit terrein. De minister zal bij het opleggen van een beschikking op grond van artikel 2, tweede lid, steeds per geval toetsen aan de genoemde specifieke vereisten.

Verder is van belang dat een dergelijke beschikking op grond van nationale veiligheid en behoud van de openbare orde geen afbreuk doet aan de handelsafspraken over diensten en goederen aangegaan onder de WTO (GATS en GATT) en bilaterale/regionale handelsakkoorden van de EU met derde landen. Deze akkoorden voorzien onder bepaalde voorwaarden in een uitzondering op de regels van markttoegang en non-discriminatoire behandeling. Zo kan de beschikking gezien het doel van de maatregel gerechtvaardigd worden met een beroep op de algemene uitzondering voor de handhaving van de openbare orde en de bescherming van de nationale veiligheid. Bij het opleggen van de beschikking zal moeten worden getoetst of dergelijke beperkende maatregelen noodzakelijk zijn om deze doelstelling te verwezenlijken, en er dus geen alternatieve maatregel bestaat die de handel minder beperkt en waarvan redelijkerwijs geacht wordt dat een staat die maatregel neemt. Uit artikel 2, tweede lid, van het besluit blijkt al dat de beschikking uitsluitend wordt opgelegd indien deze maatregelen noodzakelijk zijn om risico's die de nationale veiligheid of de openbare orde raken te beheersen. Hieruit volgt tevens dat een dergelijke maatregel alleen wordt opgelegd indien andere beheersmaatregelen, zoals de beveiligingsvoorschriften op grond van artikel 2, eerste lid, de risico's voor de nationale veiligheid of openbare orde onvoldoende beschermen. Daarnaast geldt wat betreft de uitzonderingen op de handelsafspraken op grond van handhaving van de openbare orde dat de maatregel niet op willekeurige of ongerechtvaardigd discriminerende wijze mag worden toegepast en geen verkapte beperking van de internationale handel mag zijn. De inzet van deze maatregel zal daar aan moeten voldoen.

Wat betreft een beroep op de uitzonderingen ter bescherming van de nationale veiligheid geldt nog specifiek dat een staat maatregelen kan nemen die het nodig acht ter bescherming van het wezenlijke belang van haar veiligheid en die (voorzover hier relevant) enkel worden toegepast in tijd van oorlog of van gevaarlijke internationale spanningen. Daarnaast kan een staat maatregelen nemen tot handhaving van de internationale vrede en veiligheid ingevolge haar verplichtingen krachtens het Handvest van de Verenigde Naties.

Gezien het doel van en de onderbouwing voor de onderhavige beschikkingen, bescherming van de openbare orde en nationale veiligheid, is deze maatregel – afhankelijk van de specifieke situatie - in beginsel te rechtvaardigen onder de geldende uitzonderingsgronden van de handelsafspraken. De minister zal bij het opleggen van een beschikking op grond van artikel 2, tweede lid, steeds per geval toetsen aan de genoemde specifieke vereisten.

Regeldruk

Dit besluit heeft geen administratieve lasten tot gevolg. De nalevingskosten zullen voortvloeien uit de maatregelen die bij ministeriële regeling op grond van artikel 2, eerste lid, worden opgelegd en uit de beschikkingen die op grond van artikel 2, tweede lid, zullen worden opgelegd. Een deel van de kosten als gevolg van de beschikkingen op grond van artikel 2, tweede lid, zal onder omstandigheden worden vergoed als nadeelcompensatie. Andere nalevingskosten bestaan uit het (toekomstige) prijsverschil tussen producten en diensten van aangewezen partijen en die van hun concurrenten.

Deze algemene maatregel van bestuur is niet geselecteerd voor advisering door het Adviescollege toetsing regeldruk.

Inwerkingtreding

Voor de inwerkingtreding van dit besluit wordt afgeweken van de vaste verandermomenten omdat het spoedregelgeving betreft. De redenen hiervoor zijn enerzijds de door de Taskforce vastgestelde noodzaak om zo snel mogelijk de in de aanleiding beschreven maatregelen op te leggen en anderzijds de noodzaak om de daarbij betrokken aanbieders van openbare elektronische communicatiediensten nog voor aanvang van de aanstaande veiling van frequenties voor onder meer 5G hierover de vereiste duidelijkheid te bieden.

De Staatssecretaris van Economische Zaken en Klimaat,