Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

35 838 Regels ter uitvoering van Verordening (EU) 2019/881 (Uitvoeringswet cyberbeveiligingsverordening)

Nr. 4

ADVIES AFDELING ADVISERING RAAD VAN STATE EN NADER RAPPORT[1]

Hieronder zijn opgenomen het advies van de Afdeling advisering van de Raad van State d.d. 10 februari 2021 en het nader rapport d.d. 11 mei 2021, aangeboden aan de Koning door Staatssecretaris van Economische Zaken en Klimaat. Het advies van de Afdeling advisering van de Raad van State is cursief afgedrukt.

Blijkens de mededeling van de Directeur van Uw kabinet van 11 februari 2021, nr. 2020002535, machtigde Uwe Majesteit de Afdeling advisering van de Raad van State haar advies inzake het bovenvermelde voorstel van wet rechtstreeks aan mij te doen toekomen. Dit advies, gedateerd 11 februari 2021, nr. W18.20.0458/IV, bied ik U hierbij aan.

Het voorstel heeft de Afdeling advisering van de Raad van State (hierna: de Afdeling) aanleiding gegeven tot opmerkingen over de gestelde ambities van de regering in relatie tot de uitvoering van het voorstel, de uitvoeringsproblematiek bij certificering in geval van updates en hacks en de voorgestelde bevoegdheid tot intrekking van goedkeuring voor afgifte van een cyberbeveiligingscertificaat. De Afdeling adviseert de toelichting, en waar nodig het wetsvoorstel, aan te passen. Graag ga ik op deze opmerkingen in het navolgende in. De tekst van het advies treft u hieronder aan, met tussengevoegd de reactie daarop.

Bij Kabinetsmissive van 10 december 2020, no. 2020002535, heeft Uwe Majesteit, op voordracht van de Staatssecretaris van Economische Zaken en Klimaat, bij de Afdeling advisering van de Raad van State ter overweging aanhangig gemaakt het voorstel van wet houdende regels ter uitvoering van Verordening (EU) 2019/881 (Uitvoeringswet cyberbeveiligingsverordening), met memorie van toelichting.

Het voorstel strekt tot uitvoering van de Europese verordening 2019/881 (cyberbeveiligingsverordening). Met de cyberbeveiligingsverordening

[1] De oorspronkelijke tekst van het voorstel van wet en van de memorie van toelichting zoals voorgelegd aan de Afdeling advisering van de Raad van State is ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer

kst-35838-4
ISSN 0921 - 7371
's-Gravenhage 2021

wordt een Europees kader voor cyberbeveiligingscertificering voor ICT-producten, -diensten, en -processen ingesteld. Gelet op de rechtstreekse toepasselijkheid van de verordening maakt deze automatisch deel uit van de nationale rechtsorde. Voor de operationalisering van de verordening voorziet het voorstel in bepalingen met betrekking tot procedures, handhaving, rechtsbescherming en de aanwijzing van uitvoeringsorganen.

De Afdeling advisering van de Raad van State maakt opmerkingen over de gestelde ambities van de regering in relatie tot de uitvoering van het voorstel, de uitvoeringsproblematiek bij certificering in geval van updates en hacks en de voorgestelde bevoegdheid tot intrekking van goedkeuring voor afgifte van een cyberbeveiligingscertificaat. In verband hiermee is aanpassing wenselijk van de toelichting, en waar nodig van het wetsvoorstel.

1. Gestelde ambities in relatie tot het voorstel

De cyberveiligheidsverordening biedt de mogelijkheid om op nationaal niveau certificering verplicht te stellen. Het advies van het Agentschap Telecom om een grondslag op te nemen waarin certificering op nationaal niveau kan worden verplicht wordt echter in het wetsvoorstel niet overgenomen omdat de regering inzet op verplichte certificering op Europees niveau om fragmentatie voorkomen. De regering merkt verder op dat de Europese Commissie uiterlijk einde 2023 een eerste afweging dient te maken over verplichte certificering van groepen ICT-producten, -diensten en -processen en dat de Europese gedachtewisseling daarover nog op gang moet komen.

Nu de ontwikkeling van verplichte certificering op Europees niveau mogelijk pas over enkele jaren wordt verwacht, roept dit de vraag op hoe dit zich verhoudt tot de inzet van de regering om voortvarend certificeringschema's te ontwikkelen en te implementeren. Ook roept dit de vraag op hoe in de tussentijd met de risico's van de afwezigheid van certificering wordt omgegaan. De regering onderkent immers dat standaarden en certificering een belangrijke bijdrage aan de digitale veiligheid van hard- en software leveren.

De Afdeling adviseert in het voorstel nader toe te lichten hoe in afwachting van verplichte certificering op Europees niveau tegemoet wordt gekomen aan de ambitie van de regering om voortvarend certificeringsschema's te ontwikkelen, en hoe wordt omgegaan met de gesignaleerde risico's van de afwezigheid van certificering.

Met het wetsvoorstel wordt uitvoering gegeven aan enkele bepalingen van de Europese cyberbeveiligingsverordening. Deze verordening biedt een kader om op Europees niveau cyberveiligheidscertificeringsregelingen te ontwikkelen en certificering uit te voeren.

Het kabinet is in Europees verband betrokken en ziet toe op de voortvarende ontwikkeling van cyberbeveiligingscertificeringsregelingen. Er worden momenteel twee Europese cyberbeveiligingscertificeringsregelingen ontwikkeld voor ICT-beveiligingsproducten respectievelijk cloudcomputingdiensten. In aanvulling hierop heeft de Europese Commissie via het werkprogramma aangekondigde prioriteiten geïdentificeerd voor de ontwikkeling van cyberbeveiligingsregelingen voor een breed palet aan ICT-producten, ICT-diensten en ICT-processen. Er is dan ook veel ambitie en het kabinet zal waakzaam zijn dat deze ambitie ook daadwerkelijk gerealiseerd wordt.

Op dit moment bestaan reeds verschillende nationale en internationale certificeringsregelingen. Een belangrijk voorbeeld hiervan is het Nederlandse Schema voor Certificatie op het gebied van IT-Beveiliging. Het doel van het schema is om in Nederland ICT-producten te kunnen evalueren en certificeren volgens de zogenaamde «Common Criteria», ook wel bekend als ISO-standaard 15408/18405. Het nationale schema zal vervangen worden door een Europees schema voor ICT-beveiligingsproducten. Ook bestaan reeds private certificeringsinitiatieven, zoals de certificering van clouddiensten via Zeker-OnLine. In afwachting van de Europese cyberbeveiligingscertificeringsregelingen op grond van de Europese cyberbeveiligingsverordening zal het kabinet de markt stimuleren om gebruik te blijven maken van deze bestaande certificeringstrajecten.

Daarnaast blijft het kabinet zich inzetten voor de ontwikkeling en gebruik van bestaande internationale en Europese standaarden en normen die betrekking hebben op de cyberbeveiliging (bijv. de ISO-normen) van ICT-producten, diensten, en processen.
Verder is van belang dat Nederland en Europa een integrale aanpak hebben om de digitale veiligheid te vergroten. Standaarden en certificering leveren daar een belangrijke bijdrage aan, maar op Europees niveau wordt er bijvoorbeeld ook diverse regelgeving ontwikkeld die betrekking heeft op de cyberbeveiliging van ICT-producten, diensten en processen.

Naar aanleiding van de opmerkingen van de Afdeling is de memorie van toelichting op diverse plaatsen aangevuld en verduidelijkt.

2. Certificering in geval van updates en hacks

Een cyberbeveiligingscertificaat biedt de zekerheid dat ICT-producten, -diensten en -processen voldoen aan de beveiligingsvoorschriften die bij een bepaald zekerheidsniveau passen. Noch uit de cyberbeveiligingsverordening noch uit de toelichting op het voorstel blijkt of de certificering mede betrekking heeft op de updates die de (eind)afnemer redelijkerwijs mag verwachten voor het behoud van de gebruiksfunctie en het zekerheidsniveau gedurende een bepaalde periode.

De Afdeling adviseert hier nader in de toelichting op in te gaan. Voorts wijst de Afdeling erop dat onduidelijk is welke invloed tussentijds opgetreden gegevenslekken of inbraken (hacks) en al dan niet naar aanleiding daarvan ad hoc uitgevoerde updates hebben voor het zekerheidsniveau van het betreffende ICT-product, -dienst of -proces en het daarvoor afgegeven cyberbeveiligingscertificaat.

Naar aanleiding van het advies is in de memorie van toelichting nader ingegaan op de vraag of de certificering mede betrekking heeft op de updates die redelijkerwijs mogen worden verwacht voor het behoud van de gebruiksfunctie en het zekerheidsniveau gedurende een bepaalde periode.

De cyberbeveiligingsverordening biedt een kader om Europese cyberbeveiligingscertificeringsregelingen te ontwikkelen voor ICT-producten, ICT-diensten en ICT-processen. De regels omtrent het beschikbaar stellen en uitvoeren van updates en de naleving ervan zullen een onderdeel van iedere certificeringsregeling zijn.
De op grond van de cyberbeveiligingsverordening vastgestelde certificeringsregelingen hebben onder meer als doelstelling dat ICT-producten, -diensten en – processen worden geleverd met actuele software en hardware die geen algemeen bekende kwetsbaarheden bevatten, en met mechanismen voor beveiligde updates (artikel 51, aanhef en onder j, van

de cyberbeveiligingsverordening). Daarnaast zal bij de uitwerking van deze certificeringsregelingen per regeling nader ingegaan worden op onder andere de wijze waarop voorheen onopgemerkte kwetsbaarheden in de cyberbeveiliging moeten worden aangepakt (artikel 54, eerste lid, aanhef en onder m, van de cyberbeveiligingsverordening).

Zoals gezegd moet er in iedere Europese cyberbeveiligingscertificeringsregeling regels worden opgenomen die ingaan op de wijze waarop kwetsbaarheden worden aangepakt, zoals bijvoorbeeld een hack. Daarnaast dient een certificeringsregeling regels te bevatten over de gevolgen voor een gecertificeerd ICT-product, -dienst of -proces dat niet voldoet aan de voorschriften van een cyberbeveiligingscertificeringsregeling (artikel 54, eerste lid, aanhef en onder l, van de cyberbeveiligingsverordening).
De passende regels inzake updates, hacks of patches en de gevolgen van de updates, hacks of patches voor het zekerheidsniveau en het afgegeven certificaat zullen dus per afzonderlijke Europese cyberveiligheidscertificeringsregeling moeten worden bepaald. Deze en andere regels kunnen per certificeringsregeling verschillen, aangezien deze betrekking zullen hebben op verschillende categorieën van ICT-producten, -diensten en -processen.

Overigens, indien er sprake is van een hack betekent dit niet per definitie dat een ICT-product, – dienst of – proces niet aan de voorschriften van de betreffende cyberveiligheidscertificeringsregeling voldoet. Het is immers denkbaar dat de gestelde veiligheidsvoorschriften niet zien op de «hackbaarheid» van een ICT-product, -dienst of -proces maar juist toezien op de aanwezigheid en werking van een proces dat kwetsbaarheden en cyberincidenten effectief aanpakt. Daarnaast kan het zo zijn dat de gestelde certificeringsvoorschriften door bijvoorbeeld nieuwe cyberdreigingen niet meer blijken te voldoen.

Bovenstaande is verduidelijkt in paragraaf 2 van de memorie van toelichting.

De Afdeling merkt verder op dat in het voorstel de (noodzakelijke) regels ontbreken over updates en hacks. Kiwa Nederland BV wijst hier in haar consultatiereactie ook op. Dat roept de vraag op waarvoor een certificaat precies geldt. Of eenzelfde certificaat blijft gelden na het vrijkomen van een update of een patch en voor welke versies het certificaat geldt. Onduidelijk is verder welk effect een hack heeft op de certificering, en volgens het huidige voorstel zijn er dan geen mogelijkheden tot intrekking van een certificaat. Dit acht de Afdeling problematisch omdat nu al voorzienbaar is dat deze problematiek onmiddellijk aan de orde zal zijn in geval van certificering. Onduidelijkheid hierover kan de uitvoerbaarheid van de verordening ernstig ondermijnen.

Volgens de regering is het niet de doelstelling van dit wetsvoorstel om dergelijke situaties in de uitvoeringswet te regelen, maar indien een Europese cyberbeveiligingscertificeringsregeling dit vereist kan dit middels een ministeriële regeling worden uitgewerkt. De Afdeling onderkent dat deze problematiek bij voorkeur op Europees niveau wordt geregeld. Dit ontslaat de regering er echter niet van initiatieven op dat vlak te ontplooien om duidelijkheid te creëren voor de uitvoeringspraktijk.

De Afdeling adviseert nader toe te lichten hoe de regering zich ervoor zal inzetten om binnen korte termijn duidelijkheid te verkrijgen hoe omgegaan dient te worden met de certificering in geval van updates en hacks.

Zoals reeds vermeld zal een Europese cyberveiligheidsregeling ook regels bevatten over de wijze waarop voorheen onopgemerkte kwetsbaarheden in de cyberbeveiliging moeten worden aangepakt (artikel 54, eerste lid, aanhef en onder m, van de cyberbeveiligingsverordening) en over de gevolgen voor een gecertificeerd ICT-product, -dienst of -proces dat niet voldoet aan de voorschriften van een Europese cyberbeveiligingscertificeringsregeling (artikel 54, eerste lid, aanhef en onder l, van de cyberbeveiligingsverordening). Dit betekent dat er ook ingegaan wordt op de gevolgen bij hacks en updates voor een certificaat. Het kabinet dat via de Europese Groep voor cyberbeveiligingscertificering betrokken is bij het opstellen van de certificeringsregelingen, zal zich inzetten dat dit per certificeringsregeling helder wordt bepaald.

Bovenstaande is verduidelijkt in paragraaf 2 van de memorie van toelichting.

3. Intrekking cyberbeveiligingscertificaten

Op grond van de cyberbeveiligingsverordening dient aan de nationale cyberbeveiligingscertificeringsautoriteit de bevoegdheid te worden toegekend om afgegeven Europese cyberbeveiligingscertificaten die niet voldoen aan de verordening of een Europese cyberbeveiligingscertificeringsregeling in te trekken. In het wetsvoorstel wordt aan deze verplichting invulling gegeven door de Minister van Economische Zaken en Klimaat de bevoegdheid toe te kennen een verleende goedkeuring op een onderzoeksrapport en bijbehorend certificaat in te trekken.

De Afdeling wijst erop dat uit het voorstel niet blijkt wat de consequenties van een dergelijke intrekking zijn voor de praktijk. Indien een cyberbeveiligingscertificaat niet voldoet aan de verordening of een Europese cyberbeveiligingscertificeringsregeling, kan dit betekenen dat een ICT-product, -dienst of -proces niet het zekerheidsniveau biedt waarvoor het certificaat is afgegeven. Niet duidelijk is hoe een eindafnemer er van op de hoogte kan zijn dat de goedkeuring van een certificaat, dat zijn leverancier eerder heeft laten zien, is ingetrokken en of dit certificaat nog wel een vermoeden van conformiteit met een bepaald zekerheidsniveau inhoudt.

De Afdeling adviseert nader toe te lichten hoe de intrekking van de goedkeuring zich verhoudt tot de afgegeven certificaten, en zo nodig het voorstel aan te passen.

Aan deze opmerking is gevolg gegeven door aan de artikelsgewijze toelichting bij artikel 11 een passage toe te voegen, waarin nader is toegelicht hoe de intrekking van de goedkeuring zich tot de afgegeven certificaten verhoudt.

De op grond van de cyberbeveiligingsverordening benodigde bevoegdheid voor de nationale cyberbeveiligingscertificeringsautoriteit om Europese cyberbeveiligingscertificaten in te trekken die niet aan de cyberbeveiligingsverordening of een Europese cyberbeveiligingscertificeringsregeling voldoen, heeft betrekking op Europese cyberbeveiligingscertificaten voor zekerheidsniveau hoog. In Nederland zal het Europees cyberbeveiligingscertificaat voor zekerheidsniveau hoog worden afgegeven door een conformiteitsbeoordelingsinstantie, nadat de nationale cyberbeveiligingscertificeringsautoriteit elk door de conformiteitsbeoordelingsinstantie af te geven individueel Europees cyberbeveiligingscertificaat heeft goedgekeurd. De bevoegdheid om de goedkeuring in te trekken kan de nationale autoriteit inzetten wanneer wordt vastgesteld dat een certificaat niet voldoet aan de Europese voorschriften voor

het certificaat. Deze bevoegdheid van de nationale autoriteit om de goedkeuring in te trekken geldt niet wanneer wordt vastgesteld dat een ICT- product, – dienst of -proces niet voldoet aan de cyberbeveiligingsverordening of een Europese cyberbeveiligingscertificeringsregeling. De gevolgen daarvan zullen in de desbetreffende certificeringsregeling worden uitgewerkt (artikel 54, eerste lid, aanhef en onder l, van de cyberbeveiligingsverordening).

De Europese voorschriften voor een certificaat kunnen worden afgeleid uit de cyberbeveiligingsverordening en de Europese cyberbeveiligingscertificeringsregelingen, en zullen betrekking hebben op de procedure van de totstandkoming van het certificaat als zodanig. Denk aan de inhoud en vorm, en de maximale geldigheidsduur van een certificaat (artikel 54, eerste lid, aanhef en onder p, respectievelijk r, van de cyberbeveiligingsverordening). De nationale cyberbeveiligingscertificeringsautoriteit zal bij de beoordeling van het certificaat kijken of het aan deze Europese voorschriften voldoet. Alleen indien het certificaat aan deze voorwaarden voldoet, keurt de nationale autoriteit het certificaat goed. Indien vervolgens blijkt dat het certificaat toch niet voldoet aan de Europese voorschriften, dan kan de nationale autoriteit de goedkeuring intrekken. In een dergelijk geval zal de goedkeuring voor het certificaat door de nationale cyberbeveiligingscertificeringsautoriteit onjuist zijn afgegeven.

Opgemerkt dient te worden dat een eindafnemer via de website van Enisa informatie kan vinden over Europese cyberbeveiligingscertificaten en EU-conformiteitsverklaringen die krachtens de cyberbeveiligingsverordening worden afgegeven, waaronder informatie over intrekking en verval van dergelijke Europese cyberbeveiligingscertificaten en EU-conformiteitsverklaringen.

4. Redactionele bijlage

De Afdeling verwijst naar de bij dit advies behorende redactionele bijlage

De Afdeling advisering van de Raad van State heeft een aantal opmerkingen bij het voorstel en adviseert daarmee rekening te houden voordat het voorstel bij de Tweede Kamer der Staten-Generaal wordt ingediend.

De redactionele opmerkingen van de Afdeling zijn allemaal overgenomen. De memorie van toelichting is dienovereenkomstig verduidelijkt.

5. Overige wijzigingen

Van de gelegenheid is gebruik gemaakt om artikel 11 van het wetsvoorstel aan te passen. Dat artikel voorziet in een bevoegdheid voor de Minister om een certificaat in te trekken indien het niet voldoet aan de Europese regelgeving. Aan deze bevoegdheid wordt thans zodanig vorm gegeven dat het mogelijk wordt om gebreken van ondergeschikt belang te (laten) corrigeren, zonder dat het certificaat dient te worden ingetrokken.
Tevens zijn nog enkele redactionele onvolkomenheden in de memorie van toelichting weggenomen.

De vice-president van de Raad van State,
Th.C. de Graaf

Ik moge U verzoeken het hierbij gevoegde gewijzigde voorstel van wet en de gewijzigde memorie van toelichting aan de Tweede Kamer der Staten-Generaal te zenden.

De Staatssecretaris van Economische Zaken en Klimaat,
M.C.G. Keijzer

Redactionele bijlage bij het advies van de Afdeling advisering van de Raad van State betreffende no. W18.20.0458/IV

– In de artikelsgewijze toelichting de toelichting bij artikel 8 en 9 van het voorstel toevoegen.
– In de toelichting aangeven hoe tegemoet zal worden gekomen aan de verplichting voor elke lidstaat om op grond van artikel 23(1) van de cyberbeveiligingsverordening één vertegenwoordiger voor het netwerk van nationale verbindingsfunctionarissen aan te wijzen.
– De summiere transponeringstabel van de cyberbeveiligingsverordening volledig aanvullen, uitgesplitst naar artikellid. Ook per artikellid uitsplitsen dat ofwel rechtstreekse werking volstaat, ofwel de bepaling al is geïmplementeerd, ofwel er sprake is van feitelijke uitvoering, ofwel met het voorstel wordt uitgevoerd. Als bestaand recht van toepassing is, concrete verwijzingen naar het bestaande recht opnemen.
– In de transponeringstabel, uitgesplitst naar artikellid, bij alle toepasselijke artikelen waarin beleidsruimte wordt gelaten aan de lidstaten toelichten of daar wel of geen gebruik van wordt gemaakt en wat de motivatie hiertoe is. Zie onder meer artikel 53, vierde lid, artikel 54, vierde lid en artikel 56, tweede lid van de cyberbeveiligingsverordening.]