No.W18.20.0458/IV 's-Gravenhage, 10 februari 2021

**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**.**

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[[1]](#footnote-1) (cyberbeveiligingsverordening). Met de cyberbeveiligingsverordening 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.[[2]](#footnote-2) 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.[[3]](#footnote-3)

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.[[4]](#footnote-4) 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.[[5]](#footnote-5)

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.

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.[[6]](#footnote-6) 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.[[7]](#footnote-7)

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.

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.[[8]](#footnote-8) 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.

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.[[9]](#footnote-9) 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.[[10]](#footnote-10)

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.

4. 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 vice-president van de Raad van State,

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.
1. Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (cyberbeveiligingsverordening), PbEU 2019, L 151. [↑](#footnote-ref-1)
2. Paragraaf 5.4 Uitvoering- en handhaafbaarheidstoets van Agentschap Telecom, voorstel. [↑](#footnote-ref-2)
3. Paragraaf 5.2 Advies van het Adviescollege Toetsing Regeldruk, voorstel. [↑](#footnote-ref-3)
4. Zie de Nederlandse Cyber Security Agenda, Nederland digitaal veilig, 21 april 2018, p. 27 – 28 en Voortgang Nederlandse Cyber Security Agenda, 18 juli 2019, p. 3. [↑](#footnote-ref-4)
5. Idem. [↑](#footnote-ref-5)
6. Artikel 52 van de cyberbeveiligingsverordening. [↑](#footnote-ref-6)
7. Vergelijk de subjectieve en objectieve conformiteitsvereisten bij levering aan consumenten van ICT-producten of -diensten: artikelen 7, onderdeel d, en 8, leden 2 en 3, van Richtlijn (EU) 2019/770 van het Europees Parlement en de Raad van 20 mei 2019 betreffende bepaalde aspecten van overeenkomsten voor de levering van digitale inhoud en digitale diensten, PbEU 2019, L 136, blz. 1, alsmede artikelen 6, onderdeel d, en 7, leden 3 en 4, van Richtlijn (EU) 2019/771 van het Europees Parlement en de Raad van 20 mei 2019 betreffende bepaalde aspecten van overeenkomsten voor de verkoop van goederen, PbEU 2019, L 136, blz. 28. [↑](#footnote-ref-7)
8. Paragraaf 5.1 Internetconsultatie, voorstel. [↑](#footnote-ref-8)
9. Artikel 58, achtste lid, onderdeel e, van de cyberbeveiligingsverordening. [↑](#footnote-ref-9)
10. Artikel 11 voorstel. [↑](#footnote-ref-10)