Adviescollege toetsing regeldruk

> **Retouradres** Postbus 16228 2500 BE Den Haag

Aan de minister van Economische Zaken en Klimaat
De heer ir. E.D. Wiebes
Postbus 20401
2500 EK DEN HAAG

ATR, Adviescollege toetsing regeldruk
Rijnstraat 50
2515 XP Den Haag

Postbus 16228
2500 BE Den Haag

T 070 310 86 66
E info@atr-regeldruk.nl
www.atr-regeldruk.nl

Onze referentie MvH/RvZ/SH/bs/ATR0821/2020-U110
Uw referentie

Datum 5 augustus 2020
Betreft Uitvoeringswet Cyberbeveiligingsverordening

Geachte heer Wiebes,

Op 24 juni 2020 is de Uitvoeringswet Cyberbeveiligingsverordening voor advies aan het Adviescollege toetsing regeldruk (ATR) aangeboden. Het voorstel is ook voor internetconsultatie aangeboden.[1] De adviestermijn verloopt in overeenstemming met de reactietermijn van de internconsultatie op 16 augustus 2020.

Inhoud van het voorstel

De Uitvoeringswet Cyberbeveiligingsverordening introduceert het wettelijk kader voor Europese cyberbeveiligingscertificering van ICT-producten, -diensten en -processen. Tot op heden bestaat een dergelijk certificeringskader niet. Voorliggend voorstel beoogt hiermee om de digitale weerbaarheid van ICT-producten, -diensten en -processen te verbeteren en het vertrouwen in deze producten, diensten en processen te vergroten door Europese cyberbeveiligingscertificaten te verstrekken. Het voorstel legt tenslotte de aanwijzing van de nationale cyberbeveiligingscertificeringsautoriteit vast. De nationale cyberbeveiligingscertificeringsautoriteit is belast met het toezicht op het wettelijk kader. In Nederland is dit Agentschap Telecom. De basis van het wettelijk kader is de set aan Europese afspraken die middels een verordening rechtstreekse werking heeft in Nederland. Nederland is verplicht om de afspraken te implementeren. In de verordening is echter ook nationale beleidsruimte. Hierdoor is het mogelijk de implementatie aan te laten sluiten bij de nationale context.

De Europese Commissie (EC) wordt bevoegd om Europese cyberbeveiligings-certificeringsregelingen (ook wel: certificatieschema's) voor categorieën van ICT-producten, -diensten en -processen vast te stellen. In deze schema's worden de minimumvereisten en -elementen vastgesteld waaraan een ICT-product, -dienst- of proces moet voldoen. De EC gaat onder andere eisen stellen aan de beschikbaarheid en vertrouwelijkheid. Om maatwerk mogelijk te maken worden de certificatieschema's opgesteld voor verschillende typen producten, diensten en processen. Het is nog niet definitief bekend welke schema's worden ontwikkeld, maar veel genoemde voorbeelden zijn: Cloud, Internet of things, en Smartcards. De uitgifte van certificaten geschiedt nationaal. De verordening maakt

[1] https://www.internetconsultatie.nl/uitvoeringswetcyberbeveiligingsverordening.

onderscheid tussen drie typen certificaten. Een certificaat met een basis, een substantieel en een hoog zekerheidsniveau. Vanuit het oogpunt van regeldruk is slechts de laatste categorie van belang omdat Nederland hier beleidsruimte heeft om bij de implementatie rekening te houden met de nationale context.

Bij de uitgifte van certificaten zijn vier partijen betrokken: (1) de fabrikant of leverancier die een aanvraag voor een certificaat wil indienen, (2) een conformiteitsbeoordelingsinstantie die de aanvraag controleert en het Europees cyberbeveiligingscertificaat verstrekt, (3) de Raad voor Accreditatie die de conformiteitsbeoordelingsinstanties accrediteert om certificaten te verstrekken, en (4) de nationale cyberbeveiligingscertificeringsautoriteit Agentschap Telecom (AT). AT fungeert in deze rol als toezichthouder, maar toetst bij certificaten met zekerheidsniveau hoog de aanvraag van een certificaat ook vooraf.

Tot op heden is certificering nog niet verplicht. De EC zal echter voor eind 2023 besluiten welke certificatieschema's verplicht worden.

Toetsingskader

ATR beoordeelt de gevolgen voor de regeldruk aan de hand van het volgende toetsingskader:

1. Nuloptie (nut en noodzaak): is er een taak voor de overheid en is wetgeving het meest aangewezen instrument?
2. Zijn er minder belastende alternatieven mogelijk?
3. Is gekozen voor een uitvoeringswijze die werkbaar is voor de doelgroepen die de wetgeving moeten naleven?
4. Zijn de gevolgen voor de regeldruk volledig en juist in beeld gebracht?

1. Nut en noodzaak

Voorliggend voorstel beoogt de digitale weerbaarheid van ICT-producten, -diensten en -processen te verbeteren en het vertrouwen in deze producten, diensten en processen te vergroten door Europese cyberbeveiligingscertificaten te verstrekken. Aanvullend krijgt Agentschap Telecom de rol van nationale cyberbeveiligingscertificeringsautoriteit aangewezen waarmee het agentschap een actieve rol krijgt in het toezicht op de cyberbeveiligingscertificaten.

De commissie is voornemens certificering eerst op vrijwillige basis te introduceren. Dit is een logische stap aangezien het tot op heden nog niet bekend is voor welke ICT-producten, -diensten en -processen certificatieschema's worden opgesteld. De toepassing is potentieel heel breed, waardoor de regeldrukgevolgen heel groot kunnen zijn. Een voorzichtige grondhouding ten aanzien van wettelijke verplichtingen is daarom gepast. Nederland zet zich echter proactief in als voorstander van verplichte certificering, zonder dat de gevolgen daarvan in te schatten zijn. Het college onderkent dat deze positie naar aanleiding van een Kamermotie is ingenomen[2], maar benadrukt dat de consequenties van verplichte certificering mogelijk zeer substantieel zijn (zie toetsvraag 4). De toelichting bij het voorstel maakt overigens geen melding van de Kamermotie.
Het college heeft geen verdere opmerkingen en adviespunten bij nut en noodzaak.

[2] https://www.tweedekamer.nl/kamerstukken/moties/detail?id=2018Z03963&did=2018D18120

2. *Minder belastende alternatieven*

Nederland kiest bij de uitgifte van de Europese cyberbeveiligingscertificaten met zekerheidsniveau hoog voor het goedkeuringsmodel. In dit model is Agentschap Telecom als nationale cyberbeveiligingscertificeringsautoriteit in een vroeg stadium al betrokken bij de uitgifte van certificaten. Dit betekent concreet dat conformiteitsbeoordelingsinstanties al in een vroeg stadium aan informatieverplichtingen moeten voldoen.

De verordening geeft ruimte om te kiezen uit twee andere modellen waarbij het niet noodzakelijk is om in een vroeg stadium al aan informatieverplichtingen te voldoen:

1. De nationale cyberbeveiligingscertificeringsautoriteit geeft zelf het certificaat voor zekerheidsniveau hoog uit (in plaats van particuliere conformiteitsbeoordelingsinstanties). Volgens de toelichting is niet voor dit alternatief gekozen omdat conformiteitsbeoordelingsinstanties efficiënter kunnen inspelen op de behoeftes van fabrikanten en leveranciers en wegens hun deskundigheid in staat zijn om de meest recente ontwikkelingen op het gebied van cyberbeveiliging bij te houden. Ook meldt de toelichting dat certificering door marktpartijen een kostenbesparend effect heeft op de rijksbegroting. Het college merkt hierbij op dat publieke instanties een (mogelijk kostendekkende) vergoeding vragen aan partijen die profijt hebben van de publieke dienstverlening i.c. de ontvangers van een certificaat).
2. De nationale cyberbeveiligingscertificeringsautoriteit verleent delegatie aan een conformiteitsbeoordelingsinstantie om de certificaten uit te geven. Deze optie acht Nederland niet wenselijk omdat de overheid een vinger aan de pols wil houden bij cyberbeveiligingsrisico's die kleven aan ICT-producten, -diensten of -processen met zekerheidsniveau hoog.

Bovenstaande alternatieven zijn vanuit de optiek van regeldruk minder belastend. Het voorstel kiest beargumenteerd voor een ander model. Het college heeft geen verdere opmerkingen en adviespunten bij deze keuze.

3. *Werkbaarheid*

Een fabrikant of leverancier moet aan informatieverplichtingen voldoen om een aanvraag in te kunnen dienen voor een cyberbeveiligingscertificaat. Bij zekerheidsniveau hoog moet de conformiteitsbeoordelingsinstantie aan informatieverplichtingen voldoen. De toelichting meldt dat daarbij gebruik zal worden gemaakt van een online procedure met een e-formulier. Het is raadzaam om te testen of deze procedure en dit formulier werkbaar zijn voor de fabrikanten en leveranciers die er gebruik van moeten maken.

4. *Gevolgen regeldruk*

De toelichting bevat een regeldrukparagraaf waarin is aangegeven aan welke algemene openbaarmakingsverplichtingen fabrikanten en leveranciers moeten voldoen. De informatie die openbaar gemaakt moet worden, betreft onder andere de periode gedurende welke de fabrikanten en leveranciers beveiligingsondersteuning aanbieden, en richtsnoeren om eindgebruikers te helpen met de beveiligde configuratie. Een fabrikant of leverancier moet daarnaast, na toekenning van een cyberbeveiligingscertificaat, een melding doen bij het *European Union agency for cybersecurity* (Enisa) dat namens de EC alle certificaten registreert en publiceert. De fabrikant of leverancier kan tenslotte nog te maken krijgen met een periodieke inspectie. Naar verwachting zal een inspectie gemiddeld niet meer dan 1 keer per jaar plaatsvinden.

De regeldrukgevolgen voor fabrikanten en leveranciers die volgen uit het indienen van een aanvraag bij conformiteitsbeoordelingsinstanties, zijn niet berekend. Aanvullend moeten fabrikanten en leveranciers conformiteitsbeoordelingsinstanties betalen voor het verstrekken van een Europees cyberbeveiligingscertificaat. De regeldrukgevolgen hiervan zijn ook niet in kaart gebracht.

4.1 Het college adviseert om de regeldrukberekening voor fabrikanten en leveranciers aan te vullen, conform de rijksbrede methodiek.

Ook conformiteitsbeoordelingsinstanties ondervinden regeldrukgevolgen. Zij moeten in het goedkeuringsmodel voldoen aan informatieverplichtingen. Daarnaast is het mogelijk dat zij aanvullend toelichting moeten geven bij het onderzoeksrapport op basis waarvan zij een certificaat willen toekennen. Het college heeft geen opmerkingen bij de berekening van de regeldrukgevolgen voor conformiteitsbeoordelingsinstanties.

De toelichting bevat geen ramingen van het aantal certificaten dat zal worden aangevraagd. De totale regeldrukgevolgen zijn daarom nog onbekend. De reden hiervoor is dat de reikwijdte van de certificatieschema's nog niet is vastgesteld. Potentieel zijn die regeldrukgevolgen zeer substantieel, met name als de stap wordt gezet naar verplichte certificering van ICT-producten, -diensten en -processen. Voor gewogen besluitvorming over een dergelijke stap is het cruciaal dat een beeld wordt geschetst van de mogelijke gevolgen voor de regeldruk.

4.2 Het college adviseert om aan de hand van scenario's een indicatie van de totale regeldrukgevolgen te geven van een verplichte certificering van ICT-producten, -diensten en -processen.

Dictum

Gelet op bovengenoemde bevindingen is het eindoordeel ten aanzien van de consultatieversie van dit voorstel:

Niet indienen tenzij met de adviespunten rekening is gehouden.

Het college merkt hierbij op dat dit advies geen oordeel bevat over de wenselijkheid van certificering van ICT-producten, -diensten en -processen. Het advies volgt uit het ontbreken van een adequate kwantitatieve onderbouwing (aan de hand van scenario's) van de gevolgen van die certificering.

In de verwachting u hiermee voldoende te hebben geïnformeerd,

Hoogachtend,

w.g.

M.A. van Hees
Voorzitter

R.W. van Zijp
Secretaris