Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

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

Nr. 3

MEMORIE VAN TOELICHTING

ALGEMEEN

1. Inleiding

Dit wetsvoorstel strekt tot uitvoering van Verordening (EU) nr. 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 (hierna: de cyberbeveiligingsverordening). De cyberbeveiligingsverordening is op 27 juni 2019 in werking getreden.

Een Europese verordening werkt rechtstreeks en lidstaten van de Europese Unie zijn verplicht om alle maatregelen te nemen die nodig zijn voor de volledige verwezenlijking van een verordening. Gelet op het rechtstreekse karakter, maakt een verordening automatisch deel uit van de nationale rechtsorde en is het verboden om bepalingen ervan in het nationale recht over te nemen. Wel kan het en in dit geval is het voor de operationalisering van een verordening nodig om bepalingen met betrekking tot procedures, handhaving, rechtsbescherming en aanwijzing van uitvoeringsorganen op te nemen in nationale regelgeving. Daarin voorziet dit wetsvoorstel, waarbij het uitgangspunt van de rechtstreekse werking van de verordening en minimumomzetting wordt gerespecteerd.

Een transponeringstabel is opgenomen in hoofdstuk III van deze memorie van toelichting.

2. De hoofdlijnen van de cyberbeveiligingsverordening

De cyberbeveiligingsverordening is een Europese verordening, die enerzijds het mandaat van Enisa versterkt en anderzijds een Europees kader introduceert op het gebied van cyberbeveiligingscertificering. Het doel van de cyberbeveiligingsverordening is om door middel van een geharmoniseerde certificatiesystematiek de cyberbeveiliging in de Europese Unie te vergroten en de (digitale) interne markt te versterken.

kst-35838-3
ISSN 0921 - 7371
's-Gravenhage 2021

Deze verordening biedt een kader om op Europees niveau cyberveiligheidscertificeringsregelingen te ontwikkelen en certificering uit te voeren.

Cyberbeveiliging is gedefinieerd als de activiteiten die nodig zijn om netwerk- en informatiesystemen, de gebruikers van dergelijke systemen, en andere personen die getroffen worden door cyberdreigingen, te beschermen. Europese regelingen voor cyberbeveiligingscertificering moeten tot doel hebben te waarborgen dat ICT-producten, -diensten en -processen die door middel van een dergelijke regeling zijn gecertificeerd, aan gespecificeerde voorschriften voldoen met als doel de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of de daaraan gerelateerde diensten die via die producten, diensten en processen, worden aangeboden of toegankelijk zijn, gedurende hun levenscyclus te beschermen.

De cyberbeveiligingsverordening maakt het mogelijk om op Europees niveau cyberbeveiligingscertificeringsregelingen (in de praktijk ook wel aangeduid als «certificatieschema's») vast te stellen voor categorieën van ICT-producten, -diensten en -processen.

a) Reikwijdte

De cyberbeveiligingsverordening bestaat uit een tweetal onderdelen.

De cyberbeveiligingsverordening richt zich allereerst op de versterking van het mandaat van Enisa (Titel II van de cyberbeveiligingsverordening). Enisa verkrijgt een permanent en meer uitgebreid mandaat op het gebied van cyberbeveiliging. De verordening beschrijft uitvoerig haar mandaat, de taken, de organisatie, de werkwijze en de wijze van budgettering. Enisa heeft de taak om lidstaten te ondersteunen bij beleidsontwikkeling inzake cyberbeveiliging en biedt ondersteuning bij de implementatie van de Europese richtlijn inzake netwerk- en informatiebeveiliging. Ook heeft Enisa een aantal operationele taken verkregen en speelt het een belangrijke en centrale rol in het Europese cyberbeveiligingscertificatiekader.

De cyberbeveiligingsverordening richt zich daarnaast op het bewerkstelligen van een Europees kader voor de vaststelling van cyberbeveiligingscertificeringsregelingen van ICT-producten, -diensten en -processen (Titel III van de cyberbeveiligingsverordening). Ook gaat de cyberbeveiligingsverordening nader in op de conformiteitsbeoordeling en de inrichting van het toezicht op de verordening.

Een ICT-product is een element of groep van elementen van een netwerk- of informatiesysteem (artikel 2, twaalfde lid, van de cyberbeveiligingsverordening). Een ICT-dienst is een dienst die volledig of hoofdzakelijk bestaat in de verzending, opslag, opvraging of verwerking van data door middel van netwerk- en informatiesystemen (artikel 2, dertiende lid, van de cyberbeveiligingsverordening). Een ICT-proces is een reeks activiteiten die wordt uitgevoerd om een ICT-product of ICT-dienst te ontwerpen, ontwikkelen, leveren of onderhouden (artikel 2, veertiende lid, van de cyberbeveiligingsverordening).

De Europese Commissie wordt bevoegd om Europese cyberbeveiligingscertificeringsregelingen voor categorieën van ICT-producten, -diensten en -processen vast te stellen. De verordening somt de minimumvereisten en -elementen op waaraan cyberbeveiligingscertificeringsregelingen moeten voldoen. Dit zijn vereisten op het gebied van beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit van producten, processen en diensten.

Een geharmoniseerd kader voor het ontwikkelen van certificeringsregelingen voorkomt fragmentatie en vergroot de weerbaarheid van de Europese digitale interne markt. Dit leidt tot een verbetering van het vertrouwen in de beveiliging in ICT-producten, -diensten en -processen. De ICT-producten, -diensten en -processen die zijn gecertificeerd op basis van een vastgestelde Europese cyberbeveiligingscertificeringsregeling worden weerbaar geacht tegen acties gericht op het aantasten van de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van data en/of functionaliteiten.

Het onderhavige Uitvoeringswetsvoorstel richt zich op de uitvoering van de wettelijke bepalingen uit titel III van de cyberbeveiligingsverordening.

De cyberbeveiligingsverordening heeft geen betrekking op bevoegdheden van lidstaten betreffende de activiteiten inzake openbare beveiliging, defensie, nationale veiligheid en strafrecht. Deze thema's vallen immers onder de nationale competenties van de lidstaten. De verordening laat lidstaten hiermee vrij om aanvullende maatregelen te nemen om het gebruik van de in beginsel voor de commerciële markt bedoelde gecertificeerde ICT-producten, -diensten en -processen in de voornoemde domeinen te beperken, te verbieden of hieraan aanvullende eisen te stellen.

b) Nationale cyberbeveiligingscertificeringsautoriteit

De cyberbeveiligingsverordening stelt dat iedere lidstaat een (of meerdere) nationale cyberbeveiligingscertificeringsautoriteit(en) moet aanwijzen die met toezichthoudende taken wordt belast. Het voornemen is om in Nederland één nationale cyberbeveiligingscertificeringsautoriteit (hierna ook: nationale autoriteit) aan te wijzen. De werkzaamheden van de nationale autoriteit in het kader van toezicht dienen organisatorisch strikt gescheiden te zijn van de werkzaamheden in kader van de uitgifte van cyberbeveiligingscertificaten (zie paragraaf d voor een toelichting) en onafhankelijk van elkaar verricht te worden (artikel 58, vierde lid, van de cyberbeveiligingsverordening).

Artikel 58 van de cyberbeveiligingsverordening gaat nader in op de taken en bevoegdheden van de nationale cyberbeveiligingscertificeringsautoriteit. De taken van de nationale autoriteit staan nader omschreven in artikel 58, zevende lid, van de cyberbeveiligingsverordening. Deze taken houden het volgende in:

- De nationale autoriteiten zien toe op en handhaven in cyberbeveiligingscertificeringsregelingen opgenomen regels voor toezicht op de conformiteit van ICT-producten, -diensten en -processen met de voorschriften van de cyberbeveiligingscertificaten die zijn afgegeven binnen hun respectieve grondgebieden.
- De nationale autoriteiten monitoren en handhaven de naleving van verplichtingen van op hun grondgebieden gevestigde fabrikanten of aanbieders ten aanzien van de conformiteitszelfbeoordelingen.
- De nationale autoriteiten verlenen bijstand en ondersteuning aan de nationale accreditatie-instanties bij de monitoring van en het toezicht op de werkzaamheden van de conformiteitsbeoordelingsinstanties.
- Indien van toepassing, monitoren de nationale autoriteiten en houden zij toezicht op de werkzaamheden van de overheidsinstanties als bedoeld in artikel 56, vijfde lid, van de cyberbeveiligingsverordening.
- De nationale autoriteiten laten – indien van toepassing – conformiteitsbeoordelingsinstanties toe.
- De nationale autoriteiten behandelen klachten van natuurlijke personen of rechtspersonen over de afgegeven Europese cyberbeveiligingscertificaten, of over afgegeven EU-conformiteitsverklaringen.

– De nationale autoriteiten stellen een jaarverslag op.
– De nationale cyberbeveiligingscertificeringsautoriteiten werken samen met andere nationale autoriteiten voor cyberbeveiligingscertificering of andere overheidsinstanties, door informatie uit te wisselen over de mogelijke non-conformiteit van ICT-producten, -diensten en -processen met de voorschriften van de cyberbeveiligingsverordening of met voorschriften van specifieke Europese cyberbeveiligingscertificeringsregelingen.
– De nationale autoriteiten volgen de ontwikkelingen op het gebied van cyberbeveiligingscertificering.

Op grond van artikel 58, achtste lid, van de cyberbeveiligingsverordening beschikt elke nationale autoriteit ten minste over de volgende bevoegdheden:
– het verzoeken van conformiteitsbeoordelingsinstanties, houders van Europese cyberbeveiligingscertificaten en afgevers van EU-conformiteitsverklaringen om alle informatie te verstrekken die zij nodig heeft voor de uitvoering van haar taken;
– het verrichten van onderzoeken, in de vorm van audits, naar conformiteitsbeoordelingsinstanties, houders van Europese cyberbeveiligingscertificaten en afgevers van EU-conformiteitsverklaringen om hun naleving van deze titel te verifiëren;
– het nemen van passende maatregelen, overeenkomstig het nationale recht, om ervoor te zorgen dat conformiteitsbeoordelingsinstanties, houders van Europese cyberbeveiligingscertificaten en afgevers van EU-conformiteitsverklaringen deze verordening of een Europese regeling voor cyberbeveiligingscertificering naleven;
– het overeenkomstig het Europese of nationale procesrecht toegang krijgen tot de gebouwen en terreinen van een conformiteitsbeoordelingsinstantie of houders van Europese cyberbeveiligingscertificaten voor het verrichten van onderzoeken;
– het verkrijgen van toegang tot de gebouwen en terreinen van een conformiteitsbeoordelingsinstantie of houders van Europese cyberbeveiligingscertificaten voor het verrichten van onderzoeken overeenkomstig het procesrecht van de Unie of lidstaat;
– het overeenkomstig nationaal recht intrekken van door de nationale autoriteit of overeenkomstig artikel 56, zesde lid, van de cyberbeveiligingsverordening door conformiteitsbeoordelingsinstanties afgegeven Europese cyberbeveiligingscertificaten die niet voldoen aan de verordening of een Europese cyberbeveiligingscertificeringsregeling;
– de oplegging overeenkomstig nationaal recht van sancties en het eisen dat onmiddellijk een einde wordt gemaakt aan de niet-nakoming van de verplichtingen van de cyberbeveiligingsverordening.

De nationale cyberbeveiligingscertificeringsautoriteiten van de lidstaten moeten ten minste eens per 5 jaar een collegiale toetsing ondergaan, hiermee wordt getracht om meer gelijkwaardige normen te creëren ten aanzien van cyberbeveiligingscertificaten en EU-conformiteitsverklaringen. Artikel 59 van de cyberbeveiligingsverordening gaat nader in op de wijze van toetsing. Collegiale toetsing omvat procedures voor het toezicht op de conformiteit van ICT-producten, -diensten en -processen van Europese cyberbeveiligingscertificaten, op de verplichtingen van fabrikanten en aanbieders van ICT-producten, -diensten en -processen die een conformiteitszelfbeoordeling doen, op conformiteitsbeoordelingsinstanties, evenals op de relevantie van de expertise van het personeel van de organen die cyberbeveiligingscertificaten voor zekerheidsniveau hoog afgeven. De Europese Commissie kan, door middel van een uitvoeringshandeling, een plan voor collegiale toetsing dat een periode van ten minste vijf jaar beslaat opstellen, alsmede criteria

en methoden vastleggen voor de werking van het systeem van collegiale toetsing.

c) Europese cyberbeveiligingscertificeringsregelingen

De verordening richt ook een EU-breed kader op, waarbinnen de vaststelling van Europese cyberbeveiligingscertificeringsregelingen tot stand moet gaan komen, waarbij de Europese Commissie, Enisa en stakeholders (inclusief lidstaten) een belangrijke rol vervullen.

De Europese Commissie stelt in haar voortschrijdend werkprogramma (artikel 47 van de cyberbeveiligingsverordening) de strategische prioriteiten vast voor toekomstige Europese cyberbeveiligingscertificeringsregelingen. Het voortschrijdend werkprogramma wordt opgesteld door de Europese Commissie. Daarbij houdt de Europese Commissie rekening met de adviezen van de Europese Groep voor cyberbeveiligingscertificering (de «EGC», een adviesgremium bestaande uit de lidstaten) en de Groep van belanghebbenden (een stakeholdersadviesgremium) bij cyberbeveiligingscertificering. Vervolgens publiceert de Europese Commissie het werkprogramma.

Aan de hand van het werkprogramma zullen cyberbeveiligingscertificeringsregelingen worden vastgesteld. Ook de EGC kan Enisa hierom verzoeken. De Europese Commissie doet voor het opstellen van een certificeringsregeling een verzoek aan Enisa. Bij de uitwerking van de certificeringsregelingen vindt nauwe samenwerking plaats met de EGC, zie de artikelen 49 en 62 van de cyberbeveiligingsverordening. Ook wordt bij de ontwikkeling van een certificeringsregeling een ad-hoc werkgroep ingericht (artikel 49 van de cyberbeveiligingsverordening). Vervolgens stelt de Europese Commissie de certificeringsregelingen vast door middel van uitvoeringshandelingen (artikel 49, zevende lid, van de cyberbeveiligingsverordening). Enisa evalueert ten minste om de vijf jaar elke vastgestelde Europese cyberbeveiligingscertificeringsregeling.

Op dit moment bestaan reeds verschillende nationale en internationale certificeringsregelingen voor ICT-producten, -diensten of -processen. De nationale cyberbeveiligingscertificeringsregelingen die hetzelfde onderwerp regelen als een Europese cyberbeveiligingscertificeringsregelingen, zullen vanaf een bij de certificeringsregeling vastgestelde datum vervallen (artikel 57, eerste lid, van de cyberbeveiligingsverordening). Een voorbeeld hiervan is het Nederlandse Schema voor Certificatie op het gebied van IT-Beveiliging (NSCIB). Het doel van het schema is om in Nederland ICT-beveiligingsproducten te kunnen evalueren en certificeren volgens de zogenaamde «Common Criteria», ook wel bekend als ISO-standaard 15408/18405. Er wordt momenteel een Europese cyberbeveiligingscertificeringsregelingen van dezelfde strekking ontwikkeld. Het nationale schema zal dan ook vervangen worden door deze Europese cyberbeveiligingscertificeringsregeling voor ICT-beveiligingsproducten. De cyberbeveiligingsverordening regelt de beveiligingsdoelstellingen van de Europese cyberbeveiligingscertificeringsregelingen (artikel 51 van de cyberbeveiligingsverordening) en ook de elementen die de regelingen ten minste moeten omvatten (artikel 54 van de cyberbeveiligingsverordening). De Europese cyberbeveiligingscertificeringsregelingen zullen onder meer regels bevatten omtrent het beschikbaar stellen en uitvoeren van updates en de naleving ervan. De 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). 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. 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.

De cyberbeveiligingsverordening introduceert een onderscheid tussen cyberbeveiligingscertificering op drie zekerheidsniveaus: basis, substantieel en hoog. Het zekerheidsniveau is een basis voor vertrouwen dat een ICT-product, -dienst of -proces aan de beveiligingsvoorschriften van een specifieke Europese cyberbeveiligingscertificeringsregeling voldoet. Het zekerheidsniveau geeft aan op welk niveau een betrokken ICT-product, -dienst, of -proces is geëvalueerd, maar is als zodanig geen maatstaf voor de beveiliging van het betrokken ICT-product, -dienst of -proces; Deze zekerheidsniveaus staan in verhouding tot het niveau van het risico dat verbonden is aan het gebruik van het ICT-product, -dienst, of -proces. Een certificeringsregeling kan één of meerdere zekerheidsniveaus bevatten (artikel 52 van de cyberbeveiligingsverordening).
Deelname van fabrikanten en aanbieders aan de cyberbeveiligingscertificeringsregelingen is vooralsnog vrijwillig. De Europese Commissie kan echter een regeling verplicht stellen. De Europese Commissie beoordeelt regelmatig de efficiëntie en het gebruik van de vastgestelde Europese cyberbeveiligingscertificeringsregelingen en beoordeelt of er door middel van het relevante Unierecht een specifieke Europese cyberbeveiligingscertificeringsregeling verplicht moet worden gesteld. De eerste zulke beoordeling vindt uiterlijk op 31 december 2023 plaats en daaropvolgende beoordelingen vinden ten minste om de twee jaar daarna plaats (artikel 56, derde lid, van de cyberbeveiligingsverordening).

d) Verstrekking van Europese cyberbeveiligingscertificaten en EU-conformiteitsverklaringen

De cyberbeveiligingscertificeringsregelingen vormen de basis van de uitgifte van de cyberbeveiligingscertificaten en EU-conformiteitsverklaringen. Deze uitgifte geschiedt nationaal. Cyberbeveiligingscertificaten met zekerheidsniveaus basis en substantieel worden in beginsel afgegeven door een daartoe geaccrediteerde en – indien van toepassing – toegelaten conformiteitsbeoordelingsinstantie, nadat deze een succesvolle conformiteitsbeoordeling van een ICT-product, -dienst, of -proces heeft uitgevoerd (artikel 56, vierde lid, van de cyberbeveiligingsverordening). Een conformiteitsbeoordeling is een procedure waarbij wordt geëvalueerd of aan gespecificeerde (technische) voorschriften voor een ICT-product, -dienst of -proces is voldaan.

Daarnaast is er de mogelijkheid van een conformiteitszelfbeoordeling, waarbij de conformiteitsbeoordeling niet wordt verricht door een conformiteitsbeoordelingsinstantie, maar door een fabrikant of aanbieder (artikel 2 van de cyberbeveiligingsverordening). Met een conformiteitszelfbeoordeling verklaart de fabrikant of aanbieder dat er aan de voorschriften van de certificeringsregeling is voldaan. De fabrikant of aanbieder is verantwoordelijk voor de conformiteit van het ICT-product, de ICT-dienst of het ICT-proces met de in die regeling bepaalde voorschriften (artikel 53, tweede lid, van de cyberbeveiligingsverordening) en geeft daarover een EU-conformiteitsverklaring af. Het toezichthoudende kader is onverkort van toepassing op dergelijke EU-conformiteitsverklaringen. De mogelijkheid van conformiteitszelfbeoordeling wordt bepaald in een Europese cyberbeveiligingscertificeringsregeling en wordt uitsluitend toegestaan voor ICT-producten, -diensten en -processen met een laag risico of voor Europese cyberbeveiligingscertificeringsregelingen met zekerheidsniveau basis.

Voor cyberbeveiligingscertificaten voor zekerheidsniveau hoog geldt een zwaarder conformiteitsbeoordelingsregime. Uitgangspunt is dat de nationale cyberbeveiligingscertificeringsautoriteit dit type certificaten zelf verstrekt. De lidstaat kan er echter ook voor kiezen om de cyberbeveiligingscertificaten te laten verstrekken door een conformiteitsbeoordelingsinstantie in de volgende twee gevallen:
– een conformiteitsbeoordelingsinstantie verstrekt het cyberbeveiligingscertificaat, maar voor ieder individueel af te geven certificaat dient zij goedkeuring te hebben van de nationale autoriteit; of
– de conformiteitsbeoordelingsinstantie is in algemene zin gedelegeerd door de nationale autoriteit om cyberbeveiligingscertificaten te verstrekken.

Voor cyberbeveiligingscertificaten voor zekerheidsniveaus basis en substantieel kan in gemotiveerde gevallen in een cyberbeveiligingscertificeringsregeling worden bepaald dat een nationale autoriteit zelf deze cyberbeveiligingscertificaten verstrekt (artikel 56, vijfde lid, van de cyberbeveiligingsverordening).

Europese cyberbeveiligingscertificaten en EU-conformiteitsverklaringen worden in alle lidstaten wederzijds erkend.

e) Conformiteitsbeoordelingsinstanties

Een conformiteitsbeoordelingsinstantie is een onafhankelijke derde partij, die niet de fabrikant of de aanbieder van de geëvalueerde ICT-producten, -diensten of -processen is. Conformiteitsbeoordelingsinstanties dienen op grond van artikel 60, eerste lid, van de cyberbeveiligingsverordening geaccrediteerd te zijn door de betreffende nationale accreditatie-instantie. De cyberbeveiligingsverordening bevat een bijlage waarin de vereisten vermeld staan waaraan een conformiteitsbeoordelingsinstantie moet voldoen om te worden geaccrediteerd om Europese cyberbeveiligingscertificaten op grond van deze verordening te kunnen verstrekken.

Artikel 54, eerste lid 1, onderdeel f, van de cyberbeveiligingsverordening brengt mee dat een cyberbeveiligingscertificeringsregeling ook aanvullende vereisten kan stellen aan conformiteitsbeoordelingsinstanties, om zo te garanderen dat zij beschikken over de benodigde technische bekwaamheid.

Artikel 61 van de cyberbeveiligingsverordening brengt met zich mee dat iedere conformiteitsbeoordelingsinstantie aangemeld moet worden bij de Europese Commissie. De aanmelding betreft een administratieve handeling.

f) Fabrikanten/aanbieders

Fabrikanten of aanbieders van ICT-producten, -diensten of -processen worden middels de cyberbeveiligingsverordening aangespoord om beveiligingsmaatregelen te nemen. Met Europese cyberbeveiligingscertificaten en EU-conformiteitsverklaringen kunnen zij het beveiligingsniveau van hun ICT-producten, -diensten of -processen aantonen. Artikel 55 van de cyberbeveiligingsverordening bepaalt dat de fabrikant of aanbieder van ICT-producten, -diensten en -processen met een cyberbeveiligingscertificaat of een EU-conformiteitsverklaring bepaalde aanvullende cyberbeveiligingsinformatie openbaar moeten maken.

g) Rechtsbescherming

Natuurlijke personen en rechtspersonen hebben op grond van de cyberbeveiligingsverordening het recht om een klacht in te dienen bij een conformiteitsbeoordelingsinstantie. Indien de klacht verband houdt met een Europees cyberbeveiligingscertificaat met zekerheidsniveau hoog, moet de klacht worden ingediend bij de nationale cyberbeveiligingscertificeringsautoriteit. De conformiteitsbeoordelingsinstantie respectievelijk nationale autoriteit neemt de klacht in behandeling. De natuurlijke persoon of rechtspersoon die de klacht heeft ingediend dient hierbij goed geïnformeerd te worden over de behandeling en uitkomst, en dient tevens gewezen te worden op eventuele rechtsmiddelen. Tegen de (besluiten in het kader van) afhandeling van de klacht dient een doeltreffende voorziening in rechte open te staan.

3. Hoofdlijnen van het wetsvoorstel

Met de inwerkingtreding van de cyberbeveiligingsverordening wordt certificering van cyberbeveiliging in het publieke domein gebracht. Het betreft een nieuw beleidsterrein, waarvoor nog geen nationale wet- en regelgeving is. Er is daarom gekozen voor de uitvoering van de cyberbeveiligingsverordening vorm te geven in een nieuwe nationale wet: de Uitvoeringswet cyberbeveiligingsverordening.

Het onderhavige wetsvoorstel geeft waar nodig uitvoering aan de cyberbeveiligingsverordening en regelt de aanwijzing van de nationale cyberbeveiligingscertificeringsautoriteit, de verstrekking van Europese cyberbeveiligingscertificaten met zekerheidsniveau hoog en een kader voor de handhaving en toezicht op de verordening, cyberbeveiligingscertificeringsregelingen, de uitvoeringswet en de lagere regelgeving. Voor zover er op grond van de cyberbeveiligingsverordening ruimte is om keuzes te maken hebben deze keuzes als doelstelling om een aantrekkelijk en kwalitatief hoogwaardig klimaat op het gebied van cyberbeveiligingscertificering in te richten in Nederland. Hierbij gaat het in bijzonder om de beleidskeuzes die gemaakt zijn voor het stelsel van de verstrekking van cyberbeveiligingscertificaten met zekerheidsniveau hoog.

De voortvarende ontwikkeling van cyberbeveiligingscertificeringsregelingen is van essentieel belang om een geharmoniseerde certificatiesystematiek in de Europese Unie te creëren. Er worden momenteel twee Europese specifieke cyberbeveiligingscertificeringsregelingen ontwikkeld voor ICT-beveiligingsproducten respectievelijk cloudcomputingdiensten. In aanvulling hierop heeft de Europese Commissie via het werkpro-

gramma aangekondigd 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.

a) Nationale cyberbeveiligingscertificeringsautoriteit

Artikel 58, eerste lid, van de cyberbeveiligingsverordening verplicht iedere lidstaat om een nationale cyberbeveiligingscertificeringsautoriteit aan te wijzen. Met de onderhavige Uitvoeringswet wordt de Minister van Economische Zaken en Klimaat aangewezen als nationale cyberbeveiligingscertificeringsautoriteit. De Minister van Economische Zaken en Klimaat is voornemens om de uitvoering van de genoemde taken onder te brengen bij Agentschap Telecom.

Vanuit het oogpunt van effectiviteit en efficiëntie wordt de nationale autoriteit ondergebracht bij een bestaande organisatie die geruime ervaring heeft met zowel uitvoerende als, afdoende daarvan gescheiden, toezichthoudende werkzaamheden binnen het digitale domein.

b) Conformiteitsbeoordelingsinstantie en accreditatie

Conformiteitsbeoordelingsinstanties dienen op grond van de cyberbeveiligingsverordening geaccrediteerd te zijn. In Nederland worden de conformiteitsbeoordelingsinstanties geaccrediteerd door de Raad voor Accreditatie (RvA). De RvA opereert geheel onafhankelijk. Middels een accreditatie geeft de RvA aan dat een conformiteitsbeoordelingsinstantie voor het specifieke onderwerp waarvoor accreditatie is afgegeven competent is om onafhankelijk Europese cyberbeveiligingscertificaten te verstrekken aan opdrachtgevers (fabrikanten/leveranciers). De Raad voor Accreditatie heeft enkel een verhouding tot conformiteitsbeoordelingsinstanties. De accreditatie van conformiteitsbeoordelingsinstanties voor de activiteiten waarop de cyberbeveiligingsverordening ziet, vergt geen aanvullende wijziging van nationale wet- en regelgeving. Ook fabrikanten en aanbieders gevestigd in andere lidstaten en derde landen kunnen een conformiteitsbeoordeling laten uitvoeren in Nederland. De Nederlandse conformiteitsbeoordelingsinstanties dienen in Nederland geaccrediteerd te zijn.

c) Verstrekking van Europese cyberbeveiligingscertificaten met zekerheidsniveau hoog: het nationale stelsel

Voor verstrekking van Europese cyberbeveiligingscertificaten voor zekerheidsniveau hoog geldt een zwaarder regime. Zoals in Hoofdstuk 2 uiteen is gezet, kunnen lidstaten kiezen uit drie opties. Nederland heeft gekozen voor een model waarin het Europees cyberbeveiligingscertificaat wordt afgegeven door een conformiteitsbeoordelingsinstantie, nadat de nationale cyberbeveiligingscertificeringsautoriteit elk door de conformiteitsbeoordelingsinstantie af te geven individueel Europees cyberbeveiligingscertificaat heeft goedgekeurd (artikel 56, zesde lid, onderdeel a, van de cyberbeveiligingsverordening). De nationale autoriteit zal goedkeuring geven, indien de conformiteitsbeoordeling en het cyberbeveiligingscertificaat voldoen aan de voorliggende cyberbeveiligingscertificeringsregeling. Deze systematiek van voorafgaande goedkeuring door de nationale autoriteit wordt hier ook wel het goedkeuringsmodel genoemd.

Bij dit goedkeuringsmodel zijn zowel de markt als de nationale autoriteit actief betrokken bij de conformiteitsbeoordeling. De reden voor de keuze van dit model is als volgt. Binnen dit goedkeuringsmodel geven conformiteitsbeoordelingsinstanties de Europese cyberbeveiligingscertificaten af.

Het voordeel van het benutten van conformiteitsbeoordelingsinstanties is dat deze efficiënt kunnen inspelen op 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. Daarbij werkt dit kostenbesparend ten aanzien van het overheidsbudget: de conformiteitsbeoordelingsinstanties verrichten immers de conformiteitsbeoordeling en geven het certificaat af. Nederland heeft goede ervaringen met modellen waarbij de markt ingezet wordt. Tegelijkertijd blijft de overheid betrokken binnen dit model, aangezien de nationale autoriteit goedkeuring verleent aan een conformiteitsbeoordelingsinstantie om een cyberbeveiligingscertificaat te verstrekken. De betrokkenheid van de overheid wordt nodig geacht wegens de hoge cyberbeveiligingsrisico's die er kleven aan ICT-producten, -diensten of -processen bij zekerheidsniveau hoog. Dergelijke cyberbeveiligingsrisico's kunnen aanzienlijke schadelijke gevolgen teweeg brengen, die de gehele maatschappij en economie kunnen raken. Nederland heeft dan ook dit goedkeuringsmodel gekozen, omdat het een goede balans biedt van zowel het benutten van de markt als betrokkenheid van de overheid.

Het goedkeuringsmodel is nader uitgewerkt, waarbij is gekozen voor het opzetten van een systeem van stapsgewijze goedkeuring door de nationale autoriteit. In de invulling van dit model hebben de belangen van opdrachtgevers (de fabrikanten en leveranciers) en de uitvoerbaarheid voor alle betrokken partijen, inclusief de nationale autoriteit, een belangrijke rol gespeeld. Opdrachtgevers en conformiteitsbeoordelingsinstanties hebben belang bij zo veel mogelijk zekerheid en voorspelbaarheid in het certificatietraject voor zekerheidsniveau hoog. Het certificatietraject voor zekerheidsniveau hoog is doorgaans een langdurig en kostbaar traject, waarbij aanzienlijke investeringen van de opdrachtgevers worden gevraagd. Gelet hierop is gekozen voor een model dat een hoge mate van zekerheid aan opdrachtgevers biedt dat het cyberbeveiligingscertificaat verstrekt zal worden, dan wel in een zo vroeg mogelijk stadium duidelijk wordt dat dit niet het geval zal zijn en het traject om die reden kan worden afgebroken. Op deze manier kunnen onnodige kosten worden beperkt. Deze hoge mate van zekerheid en voorspelbaarheid wordt bereikt door de nationale autoriteit een actieve rol te geven gedurende het traject van de conformiteitsbeoordeling voor zekerheidsniveau hoog. Als er geen tussentijdse rol van de nationale autoriteit zou zijn, dan zouden de conformiteitsbeoordelingsinstanties en opdrachtgevers mogelijk pas aan het einde van het certificatietraject horen dat geen goedkeuring wordt gegeven voor het afgeven van een certificaat. Het Nederlandse model met stapsgewijze goedkeuring stelt de nationale autoriteit bovendien in staat om informatie te ontvangen en kennis rondom de betreffende conformiteitsbeoordeling op te bouwen, waardoor de nationale autoriteit aan het einde van de conformiteitsbeoordelingsprocedure sneller en goed geïnformeerd een goedkeuringsbesluit kan nemen, dan wanneer de nationale autoriteit pas aan het einde van het traject de informatie zou ontvangen. Artikel 56, zesde lid, van de cyberbeveiligingsverordening biedt de ruimte aan lidstaten om het goedkeuringsmodel op een dergelijke wijze in te vullen.

De goedkeuringsprocedure houdt in de kern in dat het Europees cyberbeveiligingscertificaat wordt afgegeven door een conformiteitsbeoordelingsinstantie, nadat de nationale cyberbeveiligingscertificeringsautoriteit elk door de conformiteitsbeoordelingsinstantie afgegeven individueel Europees cyberbeveiligingscertificaat heeft goedgekeurd (artikel 56, zesde lid, onderdeel a, van de cyberbeveiligingsverordening). In het Nederlandse model is dit opgedeeld in meerdere stappen. De conformiteitsbeoordelingsinstantie (1) doet melding bij de nationale autoriteit dat een certificeringstraject wordt gestart, (2) legt de conformiteitsbeoordelingsin-

stantie – behoudens in bij ministeriële regeling bepaalde gevallen – het onderzoeksplan ter goedkeuring voor aan de nationale autoriteit en (3) legt het onderzoeksrapport en het bijhorende Europese cyberbeveiligingscertificaat dat de conformiteitsbeoordelingsinstantie voornemens is af te geven aan het einde van het traject ter goedkeuring voor aan de nationale autoriteit. Na goedkeuring door de nationale autoriteit, kan de conformiteitsbeoordelingsinstantie het Europese cyberbeveiligingscertificaat afgeven. Het gaat hierbij om een beperkt aantal cruciale momenten in de conformiteitsbeoordeling. De eerste stap is een melding. De tweede en derde stap betreffen momenten waarbij de conformiteitsbeoordelingsinstantie een besluit vraagt aan de nationale autoriteit. Om op de aanvraag te kunnen beslissen ontvangt de nationale autoriteit de nodige informatie van de conformiteitsbeoordelingsinstantie omtrent onderdelen van de conformiteitsbeoordeling. De besluiten van de nationale autoriteit zijn besluiten in de zin van de Algemene wet bestuursrecht, waartegen bezwaar en beroep open staat. Hieronder volgt een toelichting op de verschillende stappen.

De manier waarop de nationale autoriteit zal gaan toetsen dient voorspelbaar, zorgvuldig en transparant te zijn. Het inhoudelijk toetsingskader van de nationale autoriteit is de betreffende cyberbeveiligingscertificeringsregeling en de cyberbeveiligingsverordening. Dit betekent dat de nationale autoriteit beoordeelt of de conformiteitsbeoordelingsinstantie in overeenstemming handelt met de voorschriften van de betreffende certificeringsregeling en de cyberbeveiligingsverordening. De nationale autoriteit controleert of er sprake is van een onvolkomenheid, te weten een handeling, interpretatie of nalaten van een conformiteitsbeoordelingsinstantie, welke niet in overeenstemming is met de betreffende cyberbeveiligingscertificeringsregeling of de cyberbeveiligingsverordening.

Als eerste stap in het proces, is een conformiteitsbeoordelingsinstantie op grond van deze Uitvoeringswet verplicht om aan de nationale cyberbeveiligingscertificeringsautoriteit te melden dat zij voornemens is om een conformiteitsbeoordeling uit te voeren. De conformiteitsbeoordelingsinstantie verricht deze melding nadat opdrachtgever en conformiteitsbeoordelingsinstantie een certificatieovereenkomst hebben gesloten. De nationale autoriteit wordt met deze melding geïnformeerd dat er een certificatietraject zal gaan starten en kan het traject procedureel voorbereiden.

Bij de tweede stap in het goedkeuringsproces legt de conformiteitsbeoordelingsinstantie het onderzoeksplan ter goedkeuring voor aan de nationale autoriteit. Hiermee wordt aangesloten bij de gebruikelijke procedure voor conformiteitsbeoordeling. Een conformiteitsbeoordelingsinstantie stelt een onderzoeksplan op als onderdeel van het proces bij een conformiteitsbeoordeling, en deelt dit onderzoeksplan met de opdrachtgever. Dit is een cruciaal moment in het proces, omdat het onderzoeksplan (1) goed de relatie weergeeft tussen de eisen uit de cyberbeveiligingscertificeringsregeling en de eigenschappen van het ICT-product, -dienst of -proces, en (2) beschrijft op welke wijze wordt getoetst of het ICT-product, de ICT-dienst of het ICT-proces voldoet aan de in een Europese cyberbeveiligingscertificeringsregeling aan dat product, die dienst of dat proces gestelde eisen. Het onderzoeksplan vormt de grondslag voor de uitvoering van de conformiteitsbeoordeling. De nationale autoriteit toetst of het voorliggende onderzoeksplan voor de evaluatie van het product, proces of dienst voldoet aan de voorliggende cyberbeveiligingscertificeringsregeling en de cyberbeveiligingsverordening. Indien de nationale autoriteit besluit dat het onderzoeksplan niet voldoet, dan wijst de autoriteit de aanvraag tot goedkeuring af. De conformiteitsbeoordelingsinstantie kan een nieuwe aanvraag doen en

wederom ter goedkeuring voorleggen aan de nationale autoriteit. De uitvoeringswet geeft een grondslag om bij ministeriële regeling te bepalen dat in bepaalde gevallen een onderzoeksplan geen goedkeuring behoeft.

Bij de derde en laatste stap in het goedkeuringsproces legt de conformiteitsbeoordelingsinstantie het onderzoeksrapport en het Europese cyberbeveiligingscertificaat dat de conformiteitsbeoordelingsinstantie voornemens is af te geven ter goedkeuring voor aan de nationale cyberbeveiligingscertificeringsautoriteit. Een conformiteitsbeoordelingsinstantie stelt op grond van de voor hem geldende vereisten van betreffende certificeringsregeling een onderzoeksrapport op als onderdeel van het proces bij een conformiteitsbeoordeling, en deelt dit onderzoeksrapport met de opdrachtgever. In het Nederlandse model legt de conformiteitsbeoordelingsinstantie dit onderzoeksrapport ter goedkeuring voor aan de nationale autoriteit, samen met het Europese cyberbeveiligingscertificaat dat de conformiteitsbeoordelingsinstantie voornemens is te verstrekken. Dit is een cruciaal moment in het proces, omdat het onderzoeksrapport de resultaten van het onderzoek samenvat, en de onderbouwing bevat waarom het ICT-product, -dienst, of -proces voldoet aan de voorschriften van de cyberbeveiligingscertificeringsregeling en de cyberbeveiligingsverordening. Enkel het concept-certificaat en de conclusie dat het ICT-product, -dienst, of -proces voldoet zou onvoldoende zijn voor de nationale autoriteit om dit goed te kunnen beoordelen. De nationale autoriteit toetst of het onderzoek is uitgevoerd conform het goedgekeurde plan, en of de conclusies herleidbaar zijn naar de onderzoeksbevindingen en of het daarmee voldoet aan de voorliggende cyberbeveiligingscertificeringsregeling. Indien er geen onvolkomenheden zijn, dan moet de nationale autoriteit besluiten om goedkeuring te verlenen aan het onderzoeksrapport en het concept-certificaat, waarop de conformiteitsbeoordelingsinstantie het cyberbeveiligingscertificaat zal verstrekken aan de opdrachtgever. Indien de nationale autoriteit besluit om geen goedkeuring te verlenen wegens geconstateerde onvolkomenheden, dan kan de conformiteitsbeoordelingsinstantie een nieuwe aanvraag doen en wederom ter goedkeuring voorleggen aan de nationale autoriteit.

Het is mogelijk dat er per Europese certificeringsregeling verschillende voorschriften worden gesteld aan de vormvereisten en procedurele vereisten voor de melding, het onderzoeksplan en het onderzoeksrapport. Het wetsvoorstel maakt het dan ook mogelijk dat deze vereisten, indien nodig, verder uitgewerkt kunnen worden via lagere regelgeving.

De nationale autoriteit kan ten behoeve van haar besluitvorming advies vragen van andere (overheids-)organisaties. Dit advies is niet-bindend van aard. De nationale autoriteit zal in ieder geval in overleg treden met de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) over mogelijke advisering. Vanuit haar wettelijke taakstelling heeft de AIVD specifieke technische expertise op het gebied van beveiligingsaspecten van ICT-producten. De AIVD benut deze expertise in het gerubriceerde domein en in de vitale sectoren, en deze kan nuttig zijn bij de beoordeling van aanvragen tot goedkeuring van cyberbeveiligingscertificaten voor zekerheidsniveau hoog.

Tenslotte bevat de uitvoeringswet regels over het waarborgen van de vertrouwelijkheid van gegevens die worden aangeleverd bij de nationale autoriteit. Deze gegevens die de autoriteit in het kader van het goedkeuringsproces en het uitoefenen van een beperkt aantal toezichthoudende taken (artikel 58, zevende lid, onder a en h van de Verordening) verkrijgt met betrekking tot cyberbeveiligingscertificaten voor zekerheidsniveau

hoog zijn uitgezonderd van de toepassing van de Wet openbaarheid van bestuur. De redenen daarvoor zijn gelegen in de bescherming van de openbare veiligheid. De ICT-producten, -processen en -diensten die gecertificeerd zijn voor zekerheidsniveau hoog dienen op grond van de verordening aan hoge beveiligingsvereisten te voldoen wegens de veiligheidsrisico's die er kleven bij het gebruik van dergelijke producten, processen en diensten. Zo dienen dergelijke ICT-producten, -processen en -diensten onder meer weerbaar te zijn tegen geavanceerde cyberaanvallen van statelijke actoren. Dergelijke veiligheidsinformatie dient daarom beschermd te worden tegen misbruik door derden. Daarnaast speelt het zo veel mogelijk voorkomen van schade bij fabrikanten en aanbieders en benadeling van de concurrentiepositie in het Europese speelveld een rol. Overigens bestaat de mogelijkheid dat gegevens waarop de Wet openbaarheid van bestuur wel van toepassing is, op grond van artikel 10 eerste of tweede lid, evenmin openbaar gemaakt kunnen worden.

De nationale autoriteit verkrijgt via zowel het goedkeuringsproces als de uitoefening van toezichthoudende taken genoemd in artikel 58, zevende lid, onder a en h van de verordening vertrouwelijke informatie over de ICT-producten, -diensten en -processen van opdrachtgevers. Onder het verkrijgen van deze gegevens wordt ook verstaan het in het kader van de uitoefening van deze bevoegdheden gegenereerde gegevens. Deze gegevens zullen naar verwachting informatie bevatten over de werkingen en de cyberbeveiliging van ICT-producten, -diensten of -processen. In het bijzonder gaat het om informatie in hoeverre de ICT-producten, -diensten en -processen aan de hoge beveiligingsvereisten van de betreffende cyberbeveiligingscertificeringsregeling (voor zekerheidsniveau hoog) voldoen.
De cyberbeveiligingsverordening noopt tot het bijdragen aan een groter vertrouwen in ICT-producten, -diensten en -processen die zijn gecertificeerd. Door certificering wordt onder meer bijgedragen aan het vertrouwen in een digitaal veilige infrastructuur en het weerbaar maken van de maatschappij tegen cyberrisico's, zoals de georganiseerde cybermisdaad en ongewenste inmenging van buitenlandse diensten.

Certificering is vooralsnog op basis van vrijwilligheid, zodat fabrikanten en partijen niet verplicht zijn de conformiteitsbeoordeling (in Nederland) te doen om ICT-producten, -diensten of -processen op de markt aan te bieden. In verband met het eerder aangehaalde doel en het daaruit voortvloeiende effect betreffende cyberveiligheid, digitale weerbaarheid en de toenemende digitalisering is het wenselijk dat fabrikanten en aanbieders zich conformeren aan de cyberbeveiligingseisen en zij daar vervolgens de erkenning middels een Europees cyberbeveiligingscertificaat voor krijgen. Hierdoor kan een positieve marktwerking ontstaan, waarbij gestreefd kan worden naar een gecertificeerd product.

Bij de conformiteitsbeoordeling zullen fabrikanten en aanbieders gegevens aanleveren, waardoor een inzicht ontstaat in de werking, technische (beveiligings-)informatie en cyberkwetsbaarheden van de betreffende ICT-producten, -diensten en -processen. De nationale autoriteit kan deze gegevens verkrijgen in verband met de toezichthoudende taak, dan wel haar uitvoerende taak bij de goedkeuring van certificaten met zekerheidsniveau hoog. Zoals reeds is aangehaald, gaat het bij deze groep om ICT-producten, -diensten en -processen met hoge cyberbeveiligingsrisico's welke, bij de verwezenlijking daarvan, aanzienlijke schadelijke gevolgen teweeg brengen en die de gehele maatschappij en economie kunnen raken.

Bij de conformiteitsbeoordeling zal een fabrikant of aanbieder geschaad kunnen worden door openbaarmaking van de gegevens, welke technische (beveiligings-)informatie en kwetsbaarheden kunnen bevatten. Voor fabrikanten en aanbieders zal openbaarmaking, alsmede het risico daarop, een afschrikwekkende werking kunnen hebben. Een risico op openbaarmaking van deze informatie zou ertoe kunnen leiden dat fabrikanten en aanbieders minder geneigd zijn om hun ICT-producten, -diensten of -processen in Nederland te laten certificeren, en eerder zouden kiezen voor een andere lidstaat. Dat is niet in het belang van de Nederlandse positie op het gebied van cyberveiligheid, gelet op de bijdrage die certificering daaraan levert en de kwaliteit van de certificering in Nederland.

De openbare veiligheid kan in het geding komen bij openbaarmaking van deze veiligheidsinformatie omtrent ICT-producten, ICT-processen en ICT-diensten die aan hoge beveiligingsvereisten behoren te voldoen. Wanneer aanbieders terughoudend worden met het delen van vertrouwelijke informatie, kan dat de beoogde ontwikkeling van veilige ICT-producten, -diensten en -processen benadelen.

In het kader van de uitoefening van de toezichthoudende taken kan de nationale autoriteit gegevens op het gebied van de cyberbeveiliging verkrijgen. Zo houdt de nationale autoriteit toezicht op en handhaaft in cyberbeveiligingscertificeringsregelingen opgenomen regels voor toezicht op de conformiteit van ICT-producten, -diensten en -processen met de voorschriften van de cyberbeveiligingscertificaten die zijn afgegeven binnen Nederland (artikel 58, zevende lid onder a van de Verordening). De nationale autoriteit wisselt verder informatie uit over de mogelijke niet-conformiteit van ICT-producten, -diensten en -processen met autoriteiten uit andere lidstaten (artikel 58, zevende lid onder h van de Verordening). Het is van belang dat de vertrouwelijkheid van de gegevens gewaarborgd blijft, voor zover er bij de uitoefening van deze toezichthoudende taken informatie omtrent de cyberbeveiliging gemoeid gaat.

Hoewel een weigering om deze gegevens op grond van de Wet openbaarheid van bestuur openbaar te maken, naar verwachting wel bij de rechter in stand blijft, zijn de veiligheidsinformatie uit de conformiteitsbeoordeling en de bij de uitoefening van de toezichthoudende taken verkregen gegevens uitgezonderd van de toepassing van de Wet openbaarheid van bestuur om genoemde vertrouwelijkheid buiten twijfel te stellen.

Bij de uitoefening van alle overige toezichthoudende taken met betrekking tot cyberbeveiligingscertificaten met zekerheidsniveau hoog genoemd in artikelen 58, zevende lid, onderdelen b (toezicht op de zelfconformiteitsbeoordeling), c (ondersteunen van nationale accreditatie-instanties), d (indien van toepassing monitoren en toezicht op overheidsinstanties), e (toelaten conformiteitsbeoordelingsinstanties), f (behandeling klachten), g (jaarverslagen opstellen) en i (volgen ontwikkelingen inzake cyberbeveiligingscertificering) van de cyberbeveiligingsverordening, is de Wet openbaarheid van bestuur wel van toepassing. Ook is de Wet openbaarheid van bestuur onverkort van toepassing op alle toezichthoudende taken inzake cyberbeveiligingscertificaten met zekerheidsniveaus basis en substantieel.

d) Toezicht en handhaving

De cyberbeveiligingsverordening kent een limitatieve opsomming van de toezichthoudende taken die de nationale cyberbeveiligingscertificeringsautoriteit moet verrichten. Om deze taken te kunnen verrichten geeft de

verordening de nationale autoriteit een aantal bevoegdheden. Het merendeel van deze bevoegdheden heeft rechtstreekse werking en vereist geen nadere omzetting. De inspecteurs van Agentschap Telecom zullen gebruik maken van de handhavingsmogelijkheden van hoofdstuk 5 van de Algemene wet bestuursrecht. De cyberbeveiligingsverordening bevat echter een aantal bevoegdheden die via nationaal recht nader uitgewerkt moet worden.

Het gaat hierbij om de bevoegdheid om passende maatregelen te nemen die zorgdragen voor de naleving van de verordening en de cyberbeveiligingscertificeringsregelingen (artikel 58, achtste lid, onderdeel c, van de cyberbeveiligingsverordening). Om aan deze bepaling invulling te geven in het nationale recht, krijgt de nationale autoriteit de bevoegdheid om bindende aanwijzingen te geven in het geval dat de cyberbeveiligingsverordening, de regelingen of de onderhavige uitvoeringswet niet worden nageleefd.

Verder wordt er een grondslag voorzien voor de nationale autoriteit om het goedkeuringsbesluit voor de verstrekking van het Europese cyberbeveiligingscertificaat met zekerheidsniveau hoog weer in te trekken indien het certificaat niet voldoet aan de cyberbeveiligingsverordening of de voorliggende cyberbeveiligingscertificeringsregeling (artikel 58, achtste lid, onderdeel e, van de cyberbeveiligingsverordening).

Daarnaast wordt er een bevoegdheid voorzien voor de nationale autoriteit om (1) sancties op te kunnen leggen en (2) te eisen dat onmiddellijk een einde wordt gemaakt aan de niet-nakoming van de verplichtingen van deze verordening (artikel 58, achtste lid, onderdeel f, en artikel 65 van de cyberbeveiligingsverordening). De Uitvoeringswet geeft immers een grondslag voor de nationale autoriteit om een last onder bestuursdwang, last onder dwangsom en een bestuurlijke boete op te leggen. De boete kan ten hoogste 900.000 Euro bedragen. Door Onze Minister de bevoegdheid toe te kennen bestuursdwang toe te passen, kan indien de situatie daar aanleiding toe geeft, ogenblikkelijk worden opgetreden.

e) Uitvoeringshandelingen

Zoals in Hoofdstuk 2 is vermeld, worden de Europese cyberbeveiligingscertificeringsregelingen door middel van uitvoeringshandelingen vastgesteld. In de cyberbeveiligingsverordening zijn de verplichte en facultatieve elementen van een cyberbeveiligingscertificeringsregeling niet-limitatief opgesomd (artikel 54, eerste lid, van de cyberbeveiligingscertificeringsverordening). In deze Europese cyberbeveiligingscertificeringsregelingen zullen de aspecten rondom specifieke certificeringen nader worden ingevuld. De cyberbeveiligingscertificeringsregelingen zullen naar verwachting rechtstreekse werking hebben en technisch en gedetailleerd van aard zijn. Hierdoor zal naar verwachting bij de uitvoering van de cyberbeveiligingscertificeringsregelingen weinig tot geen ruimte zijn voor het maken van beleidsmatige keuzes. Het is tevens te verwachten dat deze cyberbeveiligingscertificeringsregelingen snel in werking zullen treden. Dit wetsvoorstel bevat daarom een rechtsgrondslag om bepaalde zaken naar aanleiding van de cyberbeveiligingscertificeringsregelingen uit te werken in lagere regelgeving.

Verder kunnen er op grond van artikel 61, vijfde lid, van de cyberbeveiligingsverordening uitvoeringshandelingen vastgesteld worden voor de aanmelding door de nationale autoriteit van conformiteitsbeoordelingsinstanties bij de Europese Commissie. Dit wetsvoorstel bevat daarom een rechtsgrondslag om dergelijke zaken uit te (kunnen) werken in nadere regelgeving.

f) Rechtsbescherming

Zoals hierboven is toegelicht, kent het Nederlandse model twee procedures voor de uitgifte van Europese cyberbeveiligingscertificaten. De eerste procedure is dat cyberbeveiligingscertificaten met zekerheidsniveau basis of substantieel worden uitgegeven door een conformiteitsbeoordelingsinstantie. De tweede procedure is dat cyberbeveiligingscertificaten met zekerheidsniveau hoog worden uitgegeven door een conformiteitsbeoordelingsinstantie na goedkeuring door de nationale autoriteit.

Derhalve zijn er ook twee klachtenprocedures te onderscheiden waarbij natuurlijke personen en rechtspersonen de klacht kunnen richten tot de conformiteitsbeoordelingsinstantie of de nationale autoriteit welke belast is met de uitgifte van het certificaat waarover de klacht zich richt.
Een klacht, welke verband houdt met de uitgifte van een cyberbeveiligingscertificaat met zekerheidsniveau «basis» of «substantieel» dient bij de conformiteitsbeoordelingsinstantie ingediend te worden. Conform de cyberbeveiligingsverordening dient deze instantie de mogelijkheid te bieden een klacht in te dienen en te behandelen.

Tevens kan een klacht over het handelen van een conformiteitsbeoordelingsinstantie bij de uitgifte van certificaten met zekerheidsniveau basis of substantieel, volgens reeds bestaande procedures, middels een melding worden ingediend bij de Raad voor Accreditatie. Op gelijke wijze kan bij de Raad voor Accreditatie een klacht worden ingediend indien het gaat om de uitgifte van een cyberbeveiligingscertificaat met zekerheidsniveau hoog, maar slechts voor zover zij een klacht over de beoordeling van de conformiteitsbeoordelingsinstantie betreft of een geschil betreft over het handelen van een conformiteitsbeoordelingsinstantie.

Een klacht, welke verband houdt met de uitgifte van een cyberbeveiligingscertificaat van een Europees cyberbeveiligingscertificaat met zekerheidsniveau hoog, dient bij de nationale autoriteit ingediend te worden voor zover deze klacht verband houdt met een besluit welke betrekking heeft op de uitgifte van een certificaat of nadat het goedkeuringsbesluit is genomen. Zoals reeds uiteengezet is, zijn goedkeuringsbesluiten van de nationale autoriteit besluiten in de zin van de Algemene wet bestuursrecht. Indien een klacht is gericht tegen een besluit van de nationale autoriteit, dient de klacht ingediend en behandeld te worden als bezwaar of beroep in de zin van de Algemene wet bestuursrecht.

Voorts schrijft de cyberbeveiligingsverordening voor om, onverminderd de bestuurlijke of buitengerechtelijke rechtsmiddelen, een doeltreffende voorziening te bieden voor klachten die verband houden met de (onjuiste) afgifte van een certificaat, en voor het verzuim om gevolg te geven aan deze klachten. In Nederland bestaan reeds deze mogelijkheden in het civiele recht.
Voor de afhandeling van klachten door een conformiteitsbeoordelingsinstantie geldt het civiele recht. Conformiteitsbeoordelingsinstanties zijn op grond van de voor hen geldende normen voor accreditatie verplicht een klachtenprocedure in te richten.[1]

Besluiten van de nationale autoriteit zijn besluiten in de zin van de Algemene wet bestuursrecht, waartegen bezwaar en beroep open zal staan. Indien bij de nationale autoriteit klachten worden ingediend over

[1] De verplichting voor een CBI en testlaboratorium om een klachtenprocedure in te richten is als gemeenschappelijke ISO/CASCO-element in de relevante normen die voor accreditatie worden gebruikt (w.o., EN-ISO/IEC 17065, EN-ISO/IEC 17021-1 en EN-ISO/IEC 7025) opgenomen.

het ten onrechte wel of niet afgeven van een certificaat op zekerheidsniveau hoog kan dit worden aangemerkt als een bezwaar tegen het goedkeuringsbesluit van de nationale autoriteit of de weigering daarvan. Daarnaast kan door een ieder een klacht, ook buiten de termijn voor bezwaar en beroep worden ingediend, welke een signalerende werking kan hebben en kan nopen tot het verrichten van nader onderzoek door de autoriteit. Deze klacht zal worden beschouwd als een handhavingsverzoek.

Geschillen, welke vatbaar zijn voor beroep worden voorgelegd aan de bestuursrechter in de Rechtbank Rotterdam en in hoger beroep aan het College van Beroep voor het bedrijfsleven. De nationale autoriteit stelt de klager binnen een redelijke termijn in kennis van de voortgang en het resultaat van het onderzoek.

4. Regeldruk

Zoals hierboven reeds is toegelicht, is hier sprake van de implementatie van een Europese verordening, waarbij de nationale beleidsruimte beperkt is. In hoofdstuk III is de transponeringstabel opgenomen.

Met de cyberbeveiligingsverordening en onderhavige Uitvoeringswet wordt een Europees kader voor cyberbeveiligingscertificering voor ICT-producten, -diensten, en -processen opgericht. De verordening richt ook een EU-breed kader op, waarbinnen de vaststelling van Europese cyberbeveiligingscertificeringsregelingen tot stand moet gaan komen, en waarbij de Europese Commissie, Enisa en stakeholders (inclusief lidstaten) een rol vervullen. Op dit moment zijn er nog geen Europese cyberbeveiligingscertificeringsregelingen vastgesteld, en is het nog niet duidelijk hoe veel Europese cyberbeveiligingscertificeringsregelingen er zullen komen, op welke ICT-producten, -processen, of -diensten deze cyberbeveiligingscertificeringsregelingen betrekking zullen hebben, of hoe deze regelingen er uit zullen zien, en hoe veel er gebruik van zal worden gemaakt. Deze regeldruktoets richt zich op de regeldrukeffecten van de uitvoeringswet en het kader voor cyberbeveiligingscertificering binnen Nederland. Indien er lagere regelgeving wordt vastgesteld, onder meer naar aanleiding van Europese cyberbeveiligingscertificeringsregelingen, zullen daarbij de regeldrukeffecten in kaart worden gebracht.

De cyberbeveiligingsverordening en onderhavige Uitvoeringswet leidt niet tot extra regeldruk voor burgers. Voor bedrijven ligt dat iets anders. De cyberbeveiligingsverordening gaat in eerste instantie uit van certificering op basis van vrijwilligheid. Als bedrijven er voor kiezen hun ICT-producten, -diensten en -processen te laten certificeren, dan is daar wel tijd en geld mee gemoeid.

Het aantal bedrijven (en daarmee de totale kosten voor bedrijven) dat ICT-producten, -diensten en -processen in Nederland zal laten certificeren is op dit moment niet realistisch te schatten. Afhankelijk van de te ontwikkelen Europese cyberbeveiligingscertificeringsregelingen zijn de partijen die hun ICT-producten, -diensten of -processen kunnen laten certificeren in potentie zeer uiteenlopend. Het kunnen onder meer fabrikanten, importeurs of gebruikersorganisaties zijn van uiteenlopende groepen ICT-producten, -diensten en -processen. Deze aanbieders kunnen in Nederland gevestigd zijn, of in een andere lidstaat of buiten de Europese Unie. Daarnaast kunnen deze aanbieders kiezen voor certificering conform de uitvoeringsregelingen in een willekeurige lidstaat. Dus een Nederlandse aanbieder kan kiezen voor certificering in Nederland of in een andere lidstaat.

De specifieke kosten voor een certificering voortkomend uit de inschakeling van een conformiteitsbeoordelingsinstantie zijn niet op voorhand in te schatten. Deze kosten zijn afhankelijk de nog te ontwikkelen cyberbeveiligingscertificeringsregelingen en de aard en complexiteit van het te certificeren ICT-product, -dienst en -proces. Wel kan per certificering een indicatie worden gegeven van de kosten die voortkomen uit de generieke verplichtingen die de cyberbeveiligingsverordening oplegt. Overigens is ook bij de impact assessment op Europees niveau gekozen voor een kwalitatieve beschrijving van de impact.

a) Aanbieders

Op het moment dat een aanbieder kiest voor een cyberbeveiligingscertificaat van ICT-producten, -diensten en -processen, zijn er verplichtingen waaraan hij moet voldoen. Een deel van de verplichtingen komt mogelijk bovenop verplichtingen waar de aanbieder bij certificeringen in een ander kader aan moet voldoen.

Op grond van artikel 55 van de cyberbeveiligingsverordening dienen aanbieders de volgende informatie rondom hun ICT-producten, -diensten en -processen openbaar te maken:

a) richtsnoeren en aanbevelingen om eindgebruikers te helpen met de beveiligde configuratie, installatie, inzet, exploitatie en onderhoud van de ICT-producten of -diensten;
b) de periode gedurende welke beveiligingsondersteuning zal worden aangeboden aan eindgebruikers, met name wat betreft de beschikbaarheid van actualiseringen in verband met cyberbeveiliging;
c) contactgegevens van de fabrikant of aanbieder en aanvaarde methoden voor het ontvangen, van eindgebruikers en beveiligingsonderzoekers, van kwetsbaarheidsinformatie;
d) een verwijzing naar online registers van openbaar gemaakte kwetsbaarheden met betrekking tot het ICT-product, de ICT-dienst of het ICT-proces en met betrekking tot relevante cyberbeveiligingsadviesorganen.

Deze informatie wordt in elektronische vorm beschikbaar gesteld, blijft beschikbaar en wordt indien nodig bijgewerkt, ten minste tot het verstrijken van het overeenkomstige Europese cyberbeveiligingscertificaat of de overeenkomstige EU-conformiteitsverklaring. Aangenomen mag worden dat de aanbieder reeds beschikt over de bedoelde informatie en de extra handelingen de gestructureerde publicatie ervan betreft. De tijdsbesteding hiervan wordt ingeschat op 24 uur voor het eerste product en voor alle volgende producten 8 uur. Uitgaande van een standaarduurtarief (volgens het Handboek Meting Regeldrukkosten) van € 54,– komt dit neer op € 1.296,– voor het eerste product en € 432,– per volgend product. Aangezien het niet te voorspellen is hoeveel producten die aanbieders jaarlijks laten certificeren, kan geen schatting gemaakt worden van de totale kosten per aanbieder.

Ten behoeve van de Europese geldigheid van een Europees cyberbeveiligingscertificaat zijn aanbieders verplicht om na het voltooien van een traject voor certificering, het uitgereikte Europese cyberbeveiligingscertificaat of EU-conformiteitsverklaring aan te melden bij Enisa. Enisa registreert en publiceert namens de Europese Commissie het Europese cyberbeveiligingscertificaat of de EU-conformiteitsverklaring. Uitgaande van het idee dat aanmelding online via een e-formulier tezamen met het uploaden van een kopie-certificaat of EU-conformiteitsverklaring zal plaats vinden, wordt verwacht dat deze melding aan Enisa niet meer dan een uur in beslag neemt. Bij een standaarduurtarief (volgens het Handboek Meting Regeldrukkosten) van € 54,– komt dit neer op € 54,– per aanmelding.

Aangezien het niet voorspelbaar is hoeveel producten die aanbieders jaarlijks laten certificeren kan geen schatting gemaakt worden van de totale kosten per aanbieder.

De nationale cyberbeveiligingscertificeringsautoriteit ziet toe op de naleving van eisen door de certificaathouders. Dit betekent dat de aanbieder, naast de activiteiten die een conformiteitsbeoordelingsinstantie normaliter en periodiek uitvoert in het kader van een certificering, te maken kan krijgen met verzoeken van de nationale autoriteit tot verantwoording en eventuele inspecties. De mate van deze toezichtlast is afhankelijk van het doel van de inspectie, het aantal Europese cyberbeveiligingscertificaten dat wordt gehouden en de complexiteit van het gecertificeerde ICT-product, -dienst of -proces. De omvang van deze toezichtlast voor de aanbieder kan daarom variëren van een halve werkdag tot meerdere werkdagen. Bij een standaarduurtarief (volgens het Handboek Meting Regeldrukkosten) van € 54,– komt dit neer op een last variërend van € 216,– tot € 2.160,– per inspectie. Aangenomen wordt dat er onder normale omstandigheden niet meer dan één keer per jaar een inspectie bij een aanbieder plaatsvindt, waarmee dit ook de totale lasten per jaar per aanbieder betreft.

Aan de hand van voorbeelden kan een indicatie worden gegeven van de mogelijke bandbreedtes van kosten van een individuele certificering ten aanzien van aanbieders. Daarbij moet worden opgemerkt dat de aanbieder de kosten van certificering doorgaans opneemt in de kosten van het aanbod en dat de afnemers van dit aanbod zich ook grotendeels buiten Nederland en Europa zullen bevinden. Daarbij geldt ook de verwachting dat naarmate het aanbod meer afnemers kent, het kostenverhogende effect per afnemer lager zal worden. Immers, het aanbod is onderhevig aan de normale marktwerking.

Aan de hand van de huidige praktijk rondom certificering van ICT-beveiligingsproducten kan er op basis van enkele aannames een grove inschatting gemaakt worden van de kosten van een individuele certificering van een ICT-product op de zekerheidsniveaus substantieel en hoog. Deze aannames zijn gebaseerd op ervaringen met certificeringen conform het huidig Nederlandse Schema voor de Certificatie van IT-beveiliging (NSCIB). NSCIB is erop gericht om in Nederland IT-producten te evalueren en certificeren volgens de zogenaamde internationale «Common Criteria», ook wel bekend als ISO-standaard 15408/18405. De certificering van ICT-beveiligingsproducten aan de hand van NSCIB kan worden vergeleken met de certificering van ICT-producten met zekerheidsniveaus substantieel en hoog van de verordening. Het gaat om de volgende grove inschatting:

– 20% van de certificatietrajecten zijn van het niveau substantieel en minder complex. De kosten daarvan variëren van € 100.000 tot € 250.000.
– 80% van de certificatietrajecten zijn van het niveau hoog en complexer. De kosten daarvan variëren van € 250.000 tot € 500.000.

Er is een opwaartse ontwikkeling zichtbaar van het aantal certificeringen dat in Nederland wordt uitgevoerd.

Een ander voorbeeld voor een indicatie van de mogelijke bandbreedtes van kosten van een individuele certificering door aanbieders van clouddiensten. Hier worden de aannames gebaseerd op de Nederlandse praktijk, waarbij sinds 2016 een vrijwillig keurmerk voor clouddiensten (een particulier initiatief) is. Er zijn op dit moment 10 aanbieders met een keurmerk en er is nog geen duidelijke groei. Hoewel de verwachting is dat de Europese cyberbeveiligingsregeling onder de cyberbeveiligingsveror-

dening zal afwijken van het Nederlandse keurmerk, is de verwachting ook dat er belangrijke elementen worden overgenomen en op grond hiervan een inschatting van de kosten van het certificatietraject kan worden gemaakt. Het is de verwachting dat de kosten van een certificeringstraject voor een clouddienst beduidend lager uitvallen dan de hiervoor beschreven certificering van ICT-beveiligingsproducten met zekerheidsniveau substantieel en hoog.

De kosten van een certificeringstraject van een clouddienst zijn afhankelijk van meerdere factoren, waaronder de complexiteit van de dienst, de omvang van de organisatie van de aanbieder en het volwassenheidsniveau van de organisatie ten aanzien van externe verantwoording. Interne kosten zijn inspanningen die de organisatie moet leveren om bewijs te leveren van conformiteit en zijn voornamelijk afhankelijk van de omvang van een organisatie en het volwassenheidsniveau van de organisatie ten aanzien van externe verantwoording. Deze interne kosten laten zich in algemene zin berekenen. Wel is de verwachting dat een certificatietraject voor zekerheidsniveau substantieel lagere interne kosten met zich mee zal brengen dan voor het certificatietraject voor zekerheidsniveau hoog. De verwachting is daarom dat het merendeel van de aanbieders van clouddiensten zal kiezen voor een certificaat met zekerheidsniveau substantieel.

Het is op dit moment niet met zekerheid te zeggen of en in welke mate de externe kosten zullen verschillen voor een certificaat met zekerheidsniveau substantieel en een certificaat met zekerheidsniveau hoog. Voor het inschatten van de kosten kan daarom alleen gekeken worden naar complexiteit van de dienst. Het type onderzoek dat wordt gedaan door de conformiteitsbeoordelingsinstantie is naar verwachting enigszins vergelijkbaar met het onderzoek van de relevante ICT-omgeving in het kader van de jaarrekening van organisaties.

Een zachte raming van de externe certificeringskosten is gebaseerd op ervaringen betreffende vergelijkbare trajecten en op de volgende grove inschattingen:
- 80% van de certificeringen betreft minder complexe clouddiensten (zekerheidsniveau substantieel). De externe kosten van een initiële- en her-certificering van een eenvoudige clouddienst bedragen € 15.000 tot € 25.000.
- 20% van de certificeringen betreft een complexere clouddienst (zekerheidsniveau hoog). De externe kosten van een initiële- en her-certificeringen voor een meer complexe dienst bedragen € 25.000,– tot € 35.000,–.
- De kosten van een tussenliggende audit bedragen ongeveer de helft van een initiële certificering.

Er is nog geen uitspraak te doen over de mate waarin de markt gebruik zal gaan maken van een Europese cyberbeveiligingscertificeringsregeling inzake clouddiensten.

De twee voorbeelden geven aan dat de kosten per certificering sterk kunnen verschillen. De daadwerkelijke kosten van een certificering worden bepaald door de eisen die een cyberbeveiligingscertificeringsregeling bevat per zekerheidsniveau, de complexiteit van een product, dienst of het proces dat wordt gecertificeerd, de aard van het product, dienst of proces dat moet worden gecertificeerd en de geldigheidsduur van een certificaat.

b) Conformiteitsbeoordelingsinstanties

De nationale keuze voor het goedkeuringsmodel (artikel 56, zesde lid, onderdeel a, van de cyberbeveiligingsverordening), voegt voor certificeringen op het zekerheidsniveau hoog enige verplichtingen voor een conformiteitsbeoordelingsinstantie toe.

In het goedkeuringsmodel doet de conformiteitsbeoordelingsinstantie (1) melding bij de nationale cyberbeveiligingscertificeringsautoriteit dat een certificeringstraject wordt gestart, (2) legt de conformiteitsbeoordelingsinstantie het onderzoeksplan ter goedkeuring voor aan de nationale autoriteit en (3) legt de conformiteitsbeoordelingsinstantie aan het einde van het traject het onderzoeksrapport en het bijhorende Europese cyberbeveiligingscertificaat dat zij voornemens is te verstrekken ter goedkeuring voor aan de nationale cyberbeveiligingscertificeringsautoriteit. Op deze momenten moet door de conformiteitsbeoordelingsinstantie bijbehorende en voor de goedkeuring noodzakelijke informatie worden verstrekt. Dit is echter informatie die gangbaar is voor een willekeurig certificeringstraject en dus niet specifiek voor die momenten moet worden vergaard of geproduceerd. Uitgaande van het idee dat de melding en de verzoeken om goedkeuring online via een e-formulier tezamen met het uploaden van de noodzakelijke informatie plaats zal vinden, zullen deze momenten ieder afzonderlijk naar verwachting niet meer dan een 1 uur in beslag nemen. Bij een standaarduurtarief (volgens het Handboek Meting Regeldrukkosten) van € 54,– komt dit neer op € 54,– per aanmelding en per verzoek om goedkeuring. Voor een volledig certificeringstraject komt dat neer op € 162,–.

Daarnaast wordt verwacht dat het in sommige gevallen noodzakelijk zal zijn om een conformiteitsbeoordelingsinstantie om toelichting te vragen op het onderzoeksrapport. Uitgaande van een gemiddelde over alle certificeringen op zekerheidsniveau hoog van 2 uur toelichting inclusief reistijd door de conformiteitsbeoordelingsinstantie per onderzoeksrapport en bij een standaarduurtarief (volgens het Handboek Meting Regeldrukkosten) van € 54,– komt dit neer op € 108,– per onderzoeksrapport.

De totale extra last voor een conformiteitsbeoordelingsinstantie wordt dan bij certificeringen op zekerheidsniveau hoog € 270,–. Het is een keuze van de conformiteitsbeoordelingsinstantie om deze kosten aan de aanbieder door te berekenen.

5. Advies en consultatie

5.1 Internetconsultatie

Een eerdere versie van dit wetsvoorstel is opengesteld voor consultatie op

www.internetconsultatie.nl en voor commentaar toegezonden aan belanghebbende organisaties. Hieronder volgt een globale bespreking van de reacties.

Goedkeuringsprocedure

Een aantal organisaties hadden een aantal opmerkingen over de goedkeuringsprocedure. Hieronder worden de opmerkingen op hoofdlijnen behandeld.

Een organisatie stelt dat artikel 3 van de uitvoeringswet, de melding, geen toegevoegde waarde heeft en tot vertraging kan leiden. In reactie hierop wil het kabinet benadrukken dat de nationale autoriteit met deze melding

voorbereidingen kan treffen voor de stapsgewijze goedkeuringsprocedure en dat dit naar verwachting ten goede komt aan de doorlooptijd van de goedkeuringsprocedure.

Een organisatie stelt voor om de nationale autoriteit het onderzoeksplan a priori te laten goedkeuren, en pas na het uitbrengen van de conformiteitsverklaring te laten toetsen. Het kabinet acht aanpassing van het ontwerpwetsvoorstel hierop niet wenselijk. In het wetsvoorstel is bewust gekozen voor het goedkeuringsmodel met stapsgewijze goedkeuring, waarbij de nationale autoriteit het onderzoeksplan niet zonder beoordeling goedkeurt. Het gaat immers om ICT-producten, -diensten, en -processen met hoge veiligheidsrisico's. Dit neemt niet weg dat er voor bepaalde categorieën ICT-producten, -diensten, en -processen omstandigheden kunnen zijn die aanleiding kunnen geven om van deze hoofdregel af te wijken. Dit dient bij ministeriële regeling geregeld te worden (artikel 4 lid 2 van de uitvoeringswet).

Kiwa Nederland BV ziet toegevoegde waarde in de procedure rondom het goedkeuringsbesluit, de autoriteit kan immers, indien nodig, tijdig interveniëren in het certificatietraject. Kiwa Nederland BV suggereert om vormvereisten verder te regelen in artikel 4 van de uitvoeringswet. Het kabinet merkt op dat het de voorkeur heeft om vormvereisten niet in een formele wet, maar in lagere regelgeving te regelen. Dit komt onder meer tot uitdrukking in artikel 4, vijfde lid van de uitvoeringswet. Tevens kunnen vormvereisten rechtstreeks uit een Europese cyberbeveiligingscertificeringsregeling volgen.

Twee organisaties merken op dat de beslistermijnen van de goedkeuringsprocedure (artikelen 4 en 5 van de uitvoeringswet) tot onnodige vertraging zullen leiden. Hierdoor kan mogelijk negatieve marktwerking in Nederland optreden. Daarbij roepen de organisaties op om voor bepaalde categorieën van ICT-producten, -diensten en -processen standaardprocedures te ontwikkelen met een vlotte doorlooptijd. Met betrekking tot de beslistermijnen merkt het kabinet op dat de gekozen termijnen maximale termijnen betreffen. De Awb stelt dat een besluit binnen een redelijke termijn genomen dient te worden en dat een termijn van acht weken als een redelijke termijn beschouwd kan worden. De nationale autoriteit dient binnen de gestelde termijn een besluit te nemen. Dit betekent dat de autoriteit eerder een besluit kan nemen. Het is daarbij de insteek dat de besluitvormingsprocessen binnen de autoriteit niet tot onnodige vertraging zullen gaan leiden. Verder zal de autoriteit standaardprocedures ontwikkelen, voor zover dit mogelijk is gelet op de betreffende certificeringsregeling.

Een organisatie vraagt of er gedurende de goedkeuringsprocedure contact kan plaatsvinden tussen de conformiteitsbeoordelingsinstantie en de nationale autoriteit. Hierop geeft het kabinet mee dat het mogelijk moet zijn dat een conformiteitsbeoordelingsinstantie en de nationale autoriteit informeel contact kunnen hebben.

Overig

Kiwa Nederland BV stelt dat artikel 7 van de uitvoeringswet zou moeten worden aangevuld met aanvullende regels waarbij wordt vastgesteld hoe er omgegaan wordt met bepaald situaties, zoals *updates*, *hacks* of *patches*. Het kabinet acht aanpassing van de uitvoeringswet niet wenselijk. Het is niet de doelstelling om dergelijke situaties in de uitvoeringswet te regelen, maar indien een Europese cyberbeveiligingscertificeringsregeling dit vereist kan dit middels een ministeriële regeling. Ook brengt Kiwa Nederland BV op dat hoofdstuk 4 van de uitvoeringswet

niet ingaat op concepten zoals *continuous compliance* en *market surveillance activities*. Ten aanzien hiervan merkt het kabinet op dat de cyberbeveiligingsverordening de nationale autoriteit niet beperkt in haar methodiek omtrent toezicht. De nationale autoriteit zal dan ook onverkort de hedendaagse methodes kunnen toepassen.

Cyberveilig Nederland merkt op dat de nationale autoriteit over voldoende personele middelen dient te beschikken. Ook merkt Cyberveilig Nederland op dat kwaliteitseisen aan certificaten zoveel mogelijk in wet- en regelgeving vastgelegd moeten worden. Daarnaast dient certificering van zekerheidsniveau hoog verplicht te worden. Met betrekking tot personele middelen spant het kabinet zich in om de nationale autoriteit over voldoende capaciteit te laten beschikken. De kwaliteitseisen van certificaten zullen naar verwachting volgen uit de betreffende Europese cyberbeveiligingscertificeringsregelingen. Verder zal het kabinet in Europees verband zich ertoe inspannen dat de betreffende cyberbeveiligingscertificeringsregelingen een verplicht karakter krijgen. Hierbij moet opgemerkt worden dat de Europese Commissie ook eerder dan 31 december 2023 certificeringsregelingen verplicht kan stellen.

5.2 Advies van het Adviescollege Toetsing Regeldruk

Het Adviescollege Toetsing Regeldruk (ATR) heeft advies uitgebracht[2]. ATR heeft geadviseerd om de regeldrukberekening voor fabrikanten en leveranciers aan te vullen. De regeldrukparagraaf is hierop aangepast.

Daarnaast heeft ATR geadviseerd om aan de hand van scenario's een indicatie van de totale regeldrukgevolgen in kaart te brengen van verplichte certificering van ICT-producten, -diensten en -processen. Ten aanzien hiervan merkt het kabinet ten eerste op dat de Europese Commissie uiterlijk einde 2023 een eerste afweging dient te maken over verplichte certificering van groepen ICT-producten, -diensten en -processen. De Europese gedachtewisseling daarover moet nog op gang komen. In Europees verband zal het kabinet zich ertoe inspannen dat de betreffende certificeringsregelingen zo lastenluw mogelijk zullen worden vormgegeven. Verder dient opgemerkt te worden dat het in deze fase niet mogelijk is om de totale regeldrukgevolgen van verplichte certificering in kaart te brengen wegens een groot aantal onbekende variabelen. Zo is onder meer de reikwijdte van de cyberbeveiligingscertificeringsregelingen die ontwikkeld worden nog niet bekend, zodat het niet mogelijk is om aan te geven welke ICT-producten, -diensten en -processen hieronder vallen of welke aanbieders hier gebruik van zullen maken.

De cyberbeveiligingsverordening maakt het mogelijk om cyberbeveiligingscertificeringsregelingen te ontwerpen voor alle ICT-producten, -diensten en -processen. Dit betekent dat de verordening betrekking kan hebben op alle aanbieders van ICT-producten, -diensten en -processen met commerciële activiteiten op het grondgebied van de Europese Unie, nu en in de toekomst.

5.3 Advies van de Raad voor de rechtspraak

De Raad voor de rechtspraak heeft advies uitgebracht[3]. De Raad heeft geen zwaarwegende bezwaren, maar verzoekt om verduidelijking van enkele onderdelen op het gebied van rechtsbescherming. Kort samengevat vraagt de Raad verduidelijking over welke rechter wanneer bevoegd

[2] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.
[3] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.

is, waarover de rechter een oordeel dient te vellen (de rechtsgrond), en wat het toepasselijke toetsingskader is.

De paragraaf rechtsbescherming in het wetsvoorstel is aangepast om dit te verduidelijken voor de civielrechtelijke en bestuursrechtelijke rechtsbescherming.

5.4 Uitvoering- en handhaafbaarheidstoets van Agentschap Telecom

Agentschap Telecom (AT), de beoogde autoriteit, heeft het voorstel getoetst op uitvoerbaarheid en handhaafbaarheid[4]. AT acht het voorstel uitvoerbaar en handhaafbaar. AT merkt op dat het noodzakelijk is dat het wetsvoorstel een bepaling bevat waarin wordt bepaald dat die de informatie welke de autoriteit verkrijgt in het kader van haar taakuitvoering niet onder de Wet openbaarheid van bestuur en Wet Open Overheid valt. Het wetsvoorstel is daarop aangepast. De uitzondering op de Wet Openbaarheid van Bestuur en de Wet Open Overheid is beperkt tot documenten verkregen op grond van de taakuitvoering voor certificaten met zekerheidsniveau «hoog». Tevens adviseert AT een grondslag op te nemen waarin certificering op nationaal niveau kan worden verplicht. Dit voorstel wordt niet overgenomen. Ten aanzien hiervan dient opgemerkt te worden dat Nederland inzet op verplichte certificering op Europees niveau, hiermee wordt fragmentatie voorkomen.

ARTIKELSGEWIJZE TOELICHTING

Artikel 1

De begrippen conformiteitsbeoordelingsinstantie, Europees cyberbeveiligingscertificaat en Europese cyberbeveiligingscertificeringsregeling hebben dezelfde betekenis als in de cyberbeveiligingsverordening. Hoewel de verordening rechtstreeks werkt en dus ook de uitleg van de begrippen bij toepassing van de verordening rechtstreeks werkt, is, omdat deze begrippen zelfstandig in dit wetsvoorstel worden gebruikt en om misverstanden te voorkomen, aangegeven dat de uitleg dezelfde is als in de cyberbeveiligingsverordening.

Onder conformiteitsbeoordelingsinstantie verstaat de cyberbeveiligingsverordening een conformiteitsbeoordelingsinstantie als gedefinieerd in artikel 2, punt 13, van Verordening (EG) nr. 765/2008. In de laatstgenoemde verordening is het begrip conformiteitsbeoordelingsinstantie gedefinieerd als «een instantie die conformiteitsbeoordelingsactiviteiten verricht, zoals onder meer ijken, testen, certificeren en inspecteren. Conformiteitsbeoordelingen zijn beoordelingen van producten, processen, diensten, systemen, personen en instanties aan de hand van vastgestelde eisen» (artikel 2, punt 12, van Verordening (EG) nr. 765/2008).

Onder Europees cyberbeveiligingscertificaat verstaat de cyberbeveiligingsverordening «een door een bevoegde instantie afgegeven document waarin wordt bevestigd dat is geëvalueerd of een bepaald ICT-product, een bepaalde ICT-dienst of een bepaald ICT-proces voldoet aan de specifieke, in een Europese cyberbeveiligingscertificeringsregeling vastgestelde beveiligingsvoorschriften» (artikel 2, onderdeel 11, van de cyberbeveiligingsverordening).

Onder Europese cyberbeveiligingscertificeringsregeling verstaat de cyberbeveiligingsverordening «een uitvoerige reeks voorschriften, technische vereisten, normen en procedures die door een nationale

[4] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.

overheidsinstantie zijn ontwikkeld en vastgesteld en die van toepassing zijn op de certificering of conformiteitsbeoordeling van ICT-producten, -diensten en -processen die onder het toepassingsgebied van de specifieke regeling vallen». Europese cyberbeveiligingscertificeringsregelingen zullen door de Europese Commissie als uitvoeringshandelingen worden vastgesteld op grond van artikel 49, zevende lid, van de cyberbeveiligingsverordening.

Artikel 2

Onze Minister van Economische Zaken en Klimaat wordt aangewezen als nationale cyberbeveiligingscertificeringsautoriteit in Nederland. Zie hoofdstuk I, punt 2, paragraaf b, voor nadere toelichting over de taken en bevoegdheden van een nationale cyberbeveiligingscertificeringsautoriteit.

Artikelen 3 tot en met 6

Zoals eerder toegelicht in hoofdstuk 1, punt 3, paragraaf c, is in Nederland gekozen voor de afgifte van Europese cyberbeveiligingscertificaten voor zekerheidsniveau hoog door de conformiteitsbeoordelingsinstanties nadat elk individueel certificaat door de nationale autoriteit is goedgekeurd (artikel 56, zesde lid, onderdeel a, van de cyberbeveiligingsverordening). In het wetsvoorstel wordt de verantwoordelijkheid voor de goedkeuring van cyberbeveiligingscertificaten voor zekerheidsniveau hoog gelegd bij Onze Minister van Economische Zaken en Klimaat. De artikelen 3 tot en met 6 hebben betrekking op diverse aspecten van de goedkeuring van een af te geven Europees cyberbeveiligingscertificaat door Onze Minister van Economische Zaken en Klimaat.

De artikelen 3 tot en met 5 bevatten de grondslag om, indien nodig, nadere regels te stellen ter uitvoering van de goedkeuringsprocedure.

Artikel 4, tweede lid, geeft een grondslag om bij ministeriële regeling te bepalen dat in bepaalde gevallen een onderzoeksplan geen goedkeuring behoeft. Van deze bevoegdheid zal gebruik worden gemaakt wanneer uit de Europese cyberbeveiligingscertificeringsregeling al ondubbelzinnig volgt hoe de aanpak van het onderzoek eruit moet zien. Het goedkeuren van het onderzoeksplan heeft dan geen toegevoegde waarde en zorgt voor onnodige vertraging.

Met artikel 6 wordt uitvoering gegeven aan artikel 56, zesde lid, onderdeel a, van de cyberbeveiligingsverordening.

Artikel 7

De cyberbeveiligingsverordening geeft de Europese Commissie de bevoegdheid om door middel van uitvoeringshandelingen Europese cyberbeveiligingscertificeringsregelingen vast te stellen en de omstandigheden, vormen en procedures vast te leggen waarmee de nationale cyberbeveiligingscertificeringsautoriteiten de Commissie in kennis moeten stellen van de conformiteitsbeoordelingsinstanties die geaccrediteerd en, waar nodig, toegelaten zijn om Europese cyberbeveiligingscertificaten af te geven. Dit artikel voorziet in een delegatiegrondslag voor regels ter uitvoering van deze uitvoeringshandelingen indien en voor zover dat nodig is voor een goede uitvoering van de cyberbeveiligingsverordening of een Europese cyberbeveiligingscertificeringsregeling.

Artikel 8

Voor de uitvoering van de cyberbeveiligingsverordening en de Europese cyberbeveiligingscertificeringsregelingen, die naar verwachting in de vorm van een verordening zullen worden vastgesteld, is in het wetsvoorstel een aparte voorziening getroffen. Verordeningen zijn een rechtstreekse bron van rechten en plichten binnen de Europese lidstaten en mogen daarom niet worden geïmplementeerd in de nationale regelgeving. Wel is het nodig dat overtreding van die voorschriften strafbaar wordt gesteld. Het voorgestelde artikel 8 regelt dit. De Minister van Economische Zaken en Klimaat wijst op grond van deze bepaling de desbetreffende voorschriften aan.

Artikel 9

Het voorgestelde artikel 9 voorziet in de aanwijzing van toezichthouders.

Artikel 10

Met dit artikel wordt uitvoering gegeven aan artikel 58, achtste lid, onderdeel c, van de cyberbeveiligingsverordening. Op grond daarvan moet de nationale autoriteit over de bevoegdheid beschikken om passende maatregelen te nemen om ervoor te zorgen dat conformiteitsbeoordelingsinstanties, houders van Europese cyberbeveiligingscertificaten en afgevers van EU-conformiteitsverklaringen de cyberbeveiligingsverordening of een Europese cyberbeveiligingscertificeringsregeling naleven.

Artikel 11

Op grond van artikel 58, achtste lid, onderdeel e, van de cyberbeveiligingsverordening, is een nationale cyberbeveiligingscertificeringsautoriteit bevoegd om Europese cyberbeveiligingscertificaten voor zekerheidsniveau hoog in te trekken die niet aan de cyberbeveiligingsverordening of een Europese cyberbeveiligingscertificeringsregeling voldoen. 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 ziet niet op gevallen 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).
Met dit artikel wordt uitvoering gegeven aan artikel 58, achtste lid, onderdeel e, van de cyberbeveiligingsverordening door Onze Minister van Economische Zaken en Klimaat bevoegd te maken voor de intrekking van de op grond van artikel 5, derde lid, door de Minister afgegeven goedkeuring indien het certificaat niet voldoen aan de cyberbeveiligingsverordening of de een Europese cyberbeveiligingscertificeringsregeling. Het betreft een discretionaire bevoegdheid om de mogelijkheid te hebben om gebreken van ondergeschikt belang te (laten) corrigeren, zonder dat het certificaat dient te worden ingetrokken.

Artikel 12

Met dit artikel wordt uitvoering gegeven aan artikel 58, achtste lid, onderdeel f, van de cyberbeveiligingsverordening.

Artikel 13

Met dit artikel wordt uitvoering gegeven aan artikel 65 van de cyberbeveiligingsverordening en ook een boetemogelijkheid opgenomen voor overtreding van de medewerkingsplicht van artikel 5:20 van de Algemene wet bestuursrecht.

Het tweede lid bepaalt dat de boete ten hoogste € 900.000 per overtreding bedraagt. Als doelstelling geldt dat de hoogte van de boete evenredig is aan de ernst van de gepleegde overtreding en voldoende afschrikwekkend is voor zowel de overtreder (specifieke preventie) als andere potentiële overtreders (generieke preventie). De hoogte van de boete wordt, voor zover van toepassing, in ieder geval afgestemd op de ernst van de overtreding, de mate waarin deze aan de overtreder kan worden verweten, en de omstandigheden waaronder de overtreding is gepleegd. Het wettelijk boetemaximum van € 900.000 geldt op dit moment voor overtredingen van de Wet handhaving consumentenbescherming en de Telecommunicatiewet (waaronder ook essentiële eisen voor radioapparaten), welke kunnen worden gezien als aangrenzende rechtsgebieden, die net als de cyberbeveiligingsverordening betrekking hebben op de bescherming van de consumentenbelangen, en veiligheid van producten, diensten, en processen. Om eenheid in de hoogte van geldboetes te waarborgen is in dit wetsvoorstel gekozen voor een absoluut boetemaximum van € 900.000.

Artikel 14

Onze Minister van Economische Zaken en Klimaat wordt in het wetsvoorstel aangewezen als nationale autoriteit en is daarmee verantwoordelijk voor het vervullen van in de cyberbeveiligingsverordening aan die autoriteit toegekende taken. In het eerste lid wordt voorgesteld om ten aanzien van de werkzaamheden of diensten die de Minister ter uitvoering van de cyberbeveiligingsverordening verricht de mogelijkheid bieden om een vergoedingsregeling in leven te kunnen roepen. In aanvulling hierop wordt in het tweede lid voorgesteld om kosten van het toezicht op de naleving van deze wet en gerelateerde lagere regelgeving en de verordening te kunnen doorberekenen. Beide bepalingen zijn facultatief. Vooralsnog worden deze bepalingen niet geeffectueerd om daadwerkelijk kosten door te berekenen. Het facultatieve karakter maakt het echter mogelijk om na een evaluatie hier wel toe over te gaan.

Het voorgestelde artikel 14 biedt een algemeen kader om bij of krachtens algemene maatregel van bestuur regels te stellen over de vergoeding die is verschuldigd door degene ten behoeve van wie werkzaamheden of diensten zijn verricht. In lijn met het rapport Maat Houden dient de vergoeding verband te houden met de desbetreffende werkzaamheden of diensten.[5] Voor de uitvoering van het onderhavige wetsvoorstel is doorberekening van toelatings- en handhavingskosten van aanmerkelijk belang. Een belangrijk argument hiervoor is dat mag worden verwacht dat een bedrijf een zeker belang of voordeel zal hebben bij de door de overheid te verrichten toelatings- of handhavingsactiviteiten.

[5] Staatscourant 2014, 16734.

Het rapport Maat Houden maakt een onderscheid tussen het doorberekenen van kosten op het vlak van toelatingsactiviteiten en toezicht op de niet-naleving. Het goedkeuren van een certificaat kan ook als toelatingsactiviteit beschouwd worden. Voor toelatingskosten geldt dat deze bij particulieren in rekening kunnen worden gebracht, omdat er sprake is van een individueel toerekenbaar voordeel. Ook in het voorgestelde eerste lid van artikel 14 wordt hiervan uitgegaan.
Het tweede lid heeft betrekking op het doorberekenen van de kosten van het toezicht op naleving. In het algemeen wordt gesteld dat dergelijke kosten niet doorberekend kunnen worden. Echter, op grond van het profijtbeginsel kan er sprake zijn van een uitzondering hierop waardoor handhavingsactiviteiten toch doorberekend kunnen worden. Er is onder meer sprake van profijt wanneer de handhavingsactiviteiten leidt tot een groter vertrouwen in de producten, processen en diensten van de ondertoezichtgestelden. Dit vertrouwen leidt ertoe dat de producten, processen en diensten ook daadwerkelijk worden afgenomen. Hiervan profiteert een beperkt aantal partijen.
Daarnaast leiden de handhavingsactiviteiten ook tot een onderling sterker vertrouwen onder de ondertoezichtgestelden: de aanbieders, fabrikanten en conformiteitsbeoordelingsinstanties. Er is immers sprake van een vrijwillig certificeringsstelsel, aanbieders en fabrikanten kunnen producten, diensten of processen vrijwillig laten certificeren. De toepassing van handhavingsactiviteiten leiden ertoe dat er meer vertrouwen ontstaat in het stelsel.

Indien er sprake is van toepassing van het profijtbeginsel, en er op basis van een voldoende zorgvuldige onderbouwing wordt besloten tot (gedeeltelijke) doorberekening van kosten dan worden hierbij de uitgangspunten uit het rapport Maat Houden gehanteerd.

Via lagere regelgeving dient de mogelijkheid om kosten door te berekenen verder uitgewerkt te worden. Zoals opgemerkt zal er vooralsnog geen lagere regelgeving op dit terrein ontwikkeld worden. Er zal vooralsnog dan ook geen sprake zijn van doorberekening. Op dit moment is er ook geen aanleiding of noodzaak om dit te doen. Deze bepaling geeft echter een optie om alsnog hiertoe over te gaan indien het nodig blijkt om kosten door te berekenen (bijvoorbeeld na evaluatie).

Artikel 16

In artikel 7 van bijlage 2 bij de Algemene wet bestuursrecht wordt de rechtbank Rotterdam aangewezen als bevoegde rechtbank voor beroep in eerste instantie. In artikel 11 van die bijlage wordt het College van Beroep voor het bedrijfsleven aangewezen als hoger beroepsinstantie. De reden om één bevoegde rechtbank aan te wijzen, is dat er specifieke kennis is vereist voor de toepassing van de bepalingen uit dit wetsvoorstel en de cyberbeveiligingsverordening. Naar verwachting zal het aantal (hoger) beroepen op grond van deze wetgeving te beperkt zijn om bij elke rechtbank in Nederland voldoende specialisatie te verkrijgen en te behouden, en eenheid in de gerechtelijke uitspraken te waarborgen. Er is voor de rechtbank Rotterdam gekozen, omdat deze rechtbank reeds op verschillende terreinen van het economisch publiekrecht als de bevoegde bestuursrechter is aangewezen. Daarbij kan bijvoorbeeld worden gedacht aan de bevoegdheid in het kader van de Wet handhaving consumentenbescherming, de Telecommunicatiewet, en de Wet beveiliging netwerk- en informatiesystemen. In lijn met deze reeds bestaande bevoegdheid is de rechtbank Rotterdam een voor de hand liggende keuze. Tegen een uitspraak van de rechtbank Rotterdam staat om diezelfde reden hoger beroep open bij het College van Beroep voor het bedrijfsleven.

Artikel 18

Gelet op toepasselijkheid van de Cyberbeveiligingsverordening vanaf 28 juni 2021 voor de artikelen waar uitvoering aan wordt gegeven door middel van de onderhavige wet, kan het beleid inzake vaste verandermomenten niet worden gevolgd, zowel ten aanzien van het moment van inwerkingtreding als het moment van publicatie.

III. IMPLEMENTATIETABEL

Verordening 2019/881/EU	Bepaling in implementatieregeling of bestaande regeling	Omschrijving beleidsruimte	Toelichting op de keuze(n) bij de invulling van de beleidsruimte
Artikel 1 (Onderwerp en toepassingsgebied)	Behoeft naar zijn aard geen uitvoering, betreft het onderwerp en het toepassingsgebied van de verordening	Geen	–
Artikel 2 (Definities)	Artikel 1	Geen	–
Artikel 3 (Mandaat)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 4 (Doelstellingen)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 5 (Ontwikkeling en uitvoering van Uniebeleid en -recht)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 6 (Capaciteitsopbouw)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 7 (Operationele samenwerking op Unieniveau)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 8 (Markt, cyberbeveiligingscertificering en normalisatie)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 9 (Kennis en informatie)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 10 (Bewustmaking en voorlichting)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 11 (Onderzoek en innovatie)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 12 (Internationale samenwerking)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 13 (Structuur van Enisa)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 14 (Samenstelling van de raad van bestuur), eerste lid	Behoeft naar zijn aard geen uitvoering, betreft feitelijke handelingen	Geen	–
Artikel 14 (Samenstelling van de raad van bestuur), tweede, derde en vierde lid	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 15 (Taken van de raad van bestuur)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 16 (Voorzitter van de raad van bestuur)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 17 (Vergaderingen van de raad van bestuur)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 18 (Stemregels in de raad van bestuur)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–

Verordening 2019/881/EU	Bepaling in implementatieregeling of bestaande regeling	Omschrijving beleidsruimte	Toelichting op de keuze(n) bij de invulling van de beleidsruimte
Artikel 19 (Dagelijks bestuur)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 20 (Taken van de uitvoerend directeur)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 21 (Enisa-adviesgroep)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 22 (Groep van belanghebbenden bij cyberbeveiligingscertificering)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 23 (Netwerk van nationale verbindingsfunctionarissen), eerste lid, eerste en derde volzin, tweede, derde, vierde en vijfde lid	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 23 (Netwerk van nationale verbindingsfunctionarissen), eerste lid, tweede volzin	Behoeft naar zijn aard geen uitvoering, betreft feitelijke handelingen. Het aanstellen van de verbindingsfunctionaris in de zin van artikel 23, eerste lid, CSA is in Nederland belegd bij het Nationaal Cyber Security Centrum (NCSC), onderdeel van het Ministerie van Justitie en Veiligheid.	Geen	–
Artikel 24 (Enig programmeringsdocument)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 25 (Belangenverklaring)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 26 (Transparantie)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 27 (Vertrouwelijkheid)	Behoeft naar zijn aard geen uitvoering, betreft een EU-procedure	Geen	–
Artikel 28 (Toegang tot documenten)	Behoeft naar zijn aard geen uitvoering, betreft een EU-procedure	Geen	–
Artikel 29 (Vaststelling van de begroting van Enisa)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 30 (Structuur van de begroting van Enisa)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 31 (Uitvoering van de begroting van Enisa)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 32 (Financiële regels)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 33 (Fraudebestrijding)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 34 (Algemene bepalingen)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 35 (Voorrechten en immuniteit)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 36 (Uitvoerend directeur)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 37 (Gedetacheerde nationale deskundigen en andere personeelsleden)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–

Verordening 2019/881/EU	Bepaling in implementatieregeling of bestaande regeling	Omschrijving beleidsruimte	Toelichting op de keuze(n) bij de invulling van de beleidsruimte
Artikel 38 (Juridische status van Enisa)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 39 (Aansprakelijkheid van Enisa)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 40 (Talenregeling), eerste lid, eerste volzin, en tweede lid	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 40 (Talenregeling), eerste lid, tweede volzin	Behoeft naar zijn aard geen uitvoering, betreft feitelijke handelingen	Geen	–
Artikel 41 (Bescherming van persoonsgegevens)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 42 (Samenwerking met derde landen en internationale organisaties)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 43 (Beveiligingsvoorschriften voor de bescherming van gevoelige niet-gerubriceerde informatie en gerubriceerde informatie)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 44 (Zetelovereenkomst en voorwaarden voor de werking)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 45 (Administratief toezicht)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 46 (Europees cyberbeveiligingscertificeringskader)	Behoeft naar zijn aard geen uitvoering, rechtstreekse werking volstaat	Geen	–
Artikel 47 (Het voortschrijdend werkprogramma van de Unie voor Europese cyberbeveiligingscertificering)	Behoeft naar zijn aard geen uitvoering, de bepaling richt zich tot de Europese Commissie	Geen	–
Artikel 48 (Verzoek om een Europese cyberbeveiligingscertificeringsregeling)	Behoeft naar zijn aard geen uitvoering, de bepaling richt zich tot de Europese Commissie	Geen	–
Artikel 49 (Opstelling, vaststelling en herziening van een Europese cyberbeveiligingscertificeringsregeling), eerste tot en met zesde lid, achtste lid, eerste volzin	Behoeft naar zijn aard geen uitvoering, de bepaling richt zich tot Enisa	Geen	–
Artikel 49 (Opstelling, vaststelling en herziening van een Europese cyberbeveiligingscertificeringsregeling), zevende lid en achtste lid, tweede volzin	Behoeft naar zijn aard geen uitvoering, de bepaling richt zich tot de Europese Commissie Mbt lid 7: aan Europese cyberbeveiligingscertificeringsregeling vastgesteld op grond van dit lid wordt uitvoering gegeven via ministeriële regelingen vastgesteld op grond van artikel 7 van de wet	Geen	–
Artikel 50 (Website over Europese cyberbeveiligingscertificeringsregelingen)	Behoeft naar zijn aard geen uitvoering, de bepaling richt zich tot Enisa	Geen	–
Artikel 51 (Beveiligingsdoelstellingen van Europese cyberbeveiligingscertificeringsregelingen)	Behoeft naar zijn aard geen uitvoering, rechtstreekse werking volstaat	Geen	–
Artikel 52 (Zekerheidsniveaus van Europese cyberbeveiligingscertificeringsregelingen),	Behoeft naar zijn aard geen uitvoering, rechtstreekse werking volstaat	Geen	–

Verordening 2019/881/EU	Bepaling in implementatieregeling of bestaande regeling	Omschrijving beleidsruimte	Toelichting op de keuze(n) bij de invulling van de beleidsruimte
Artikel 53 (Conformiteitszelfbeoordeling), eerste, tweede en derde lid	Behoeft naar zijn aard geen uitvoering, rechtstreekse werking volstaat	Geen	–
Artikel 53 (Conformiteitszelfbeoordeling), vierde lid	Van de mogelijkheid om een EU-conformiteitsverklaring verplicht te stellen wordt geen gebruik gemaakt	Mogelijkheid om een EU-conformiteitsverklaring verplicht te stellen	Aan het bedrijfsleven wordt de ruimte geboden om binnen de kaders van de verordening en de daaruit voortvloeiende cyberbeveiligingsregelingen te kiezen voor een EU-conformiteitsverklaring dan wel een certificaat.
Artikel 53 (Conformiteitszelfbeoordeling), vijfde lid	Behoeft naar zijn aard geen uitvoering, betreft feitelijke handelingen	Geen	–
Artikel 54 (Elementen van Europese cyberbeveiligingscertificeringsregelingen), eerste, tweede en derde lid	Behoeft naar zijn aard geen uitvoering, rechtstreekse werking volstaat	Geen	–
Artikel 54 (Elementen van Europese cyberbeveiligingscertificeringsregelingen), vierde lid	Van de mogelijkheid om in nationaal recht te bepalen dat een Europese cyberbeveiligingscertificeringsregeling kan worden gebruikt om het vermoeden van conformiteit met de wettelijke voorschriften vast te stellen wordt geen gebruik gemaakt	Mogelijkheid om in nationaal recht te bepalen dat een Europese cyberbeveiligingscertificeringsregeling kan worden gebruikt om het vermoeden van conformiteit met de wettelijke voorschriften vast te stellen	Het streven is dat de cyberbeveiligingscertificeringregelingen via Europese regelgeving verplicht worden gesteld om fragmentatie tussen de lidstaten te voorkomen. Indien cyberbeveiligingscertificeringsregelingen via Europese regelgeving verplicht worden gesteld komt dit de digitale interne markt ten goede.
Artikel 55 (Aanvullende cyberbeveiligingsinformatie voor gecertificeerde ICT-producten, -diensten en -processen)	Behoeft naar zijn aard geen uitvoering, rechtstreekse werking volstaat	Geen	–
Artikel 56 (Cyberbeveiligingscertificering), eerste, vierde, vijfde, zevende, achtste en negende lid	Behoeft naar zijn aard geen uitvoering, rechtstreekse werking volstaat	Geen	–
Artikel 56 (Cyberbeveiligingscertificering), tweede lid	Van de mogelijkheid om de cyberbeveiligingscertificering verplicht te stellen wordt geen gebruik gemaakt	Mogelijkheid om de cyberbeveiligingscertificering verplicht te stellen	Het streven is dat de cyberbeveiligingscertificeringregelingen via Europese regelgeving verplicht worden gesteld om fragmentatie tussen de lidstaten te voorkomen. Indien cyberbeveiligingscertificeringsregelingen via Europese regelgeving verplicht worden gesteld komt dit de digitale interne markt ten goede.
Artikel 56 (Cyberbeveiligingscertificering), derde lid	Behoeft naar zijn aard geen uitvoering, de bepaling richt zich tot de Europese Commissie	Geen	–

Verordening 2019/881/EU	Bepaling in implementatieregeling of bestaande regeling	Omschrijving beleidsruimte	Toelichting op de keuze(n) bij de invulling van de beleidsruimte
Artikel 56 (Cyberbeveiligingscertificering), zesde lid	Artikelen 3 t/m 6	De lidstaat dient een keuze te maken voor een model voor de afgifte van een Europees cyberbeveiligingscertificaat met zekerheidsniveau hoog. De lidstaat kiest voor a) afgegeven door een nationale cyberbeveiligingscertificeringsautoriteit, of, (b) door een conformiteitsbeoordelingsinstantie nadat de nationale cyberbeveiligingscertificeringsautoriteit elk door de conformiteitsbeoordelingsinstantie afgegeven individueel Europees cyberbeveiligingscertificaat heeft goedgekeurd, of (c) door een conformiteitsbeoordelingsinstantie op basis van een algemene delegatie.	Zie hoofdstuk I, punt 3, paragraaf c
Artikel 56 (Cyberbeveiligingscertificering), tiende lid	Behoeft naar zijn aard geen uitvoering, betreft feitelijke handelingen. Waarborging naleving op basis van Wet Naleving Europese regelgeving publieke entiteiten	Geen	–
Artikel 57 (Nationale cyberbeveiligingscertificeringsregelingen en -certificaten), eerste, tweede en vierde lid	Behoeft naar zijn aard geen uitvoering, betreft feitelijke handelingen. Waarborging naleving op basis van Wet Naleving Europese regelgeving publieke entiteiten	Geen	–
Artikel 57 (Nationale cyberbeveiligingscertificeringsregelingen en -certificaten), derde lid	Behoeft naar zijn aard geen uitvoering, rechtstreekse werking volstaat	Geen	–
Artikel 58 (Nationale cyberbeveiligingscertificeringsautoriteiten), eerste lid	Artikel 2	Iedere lidstaat wijst één of meer nationale cyberbeveiligingscertificeringsautoriteiten op zijn grondgebied aan, of wijst, in onderlinge overeenstemming met een andere lidstaat, één of meer in die andere lidstaat gevestigde nationale cyberbeveiligingscertificeringsautoriteiten aan die verantwoordelijk zijn voor de toezichthoudende taken in de aanwijzende lidstaat.	Vanuit het oogpunt van effectiviteit en efficiëntie wordt er één nationale autoriteit aangewezen op het eigen grondgebied. Hiermee ontstaat er ook geen afhankelijkheid ten aanzien van een autoriteit in een andere lidstaat. De taken worden ondergebracht bij een bestaande organisatie die geruime ervaring heeft met zowel uitvoerende als, afdoende daarvan gescheiden, toezichthoudende werkzaamheden binnen het digitale domein. Zie ook hoofdstuk I, punt 3, paragraaf a
Artikel 58 (Nationale cyberbeveiligingscertificeringsautoriteiten), tweede, derde, vierde, vijfde, zesde en negende lid	Behoeft naar zijn aard geen uitvoering, betreft feitelijke handelingen. Waarborging naleving op basis van Wet Naleving Europese regelgeving publieke entiteiten.	Geen	–
Artikel 58 (Nationale cyberbeveiligingscertificeringsautoriteiten), zevende lid, achtste lid, onder a en b	Behoeft naar zijn aard geen uitvoering, rechtstreekse werking volstaat	Geen	–

Verordening 2019/881/EU	Bepaling in implementatieregeling of bestaande regeling	Omschrijving beleidsruimte	Toelichting op de keuze(n) bij de invulling van de beleidsruimte
Artikel 58, (Nationale cyberbeveiligingscertificeringsautoriteiten), achtste lid, onder c	Artikel 10	Geen	–
Artikel 58, (Nationale cyberbeveiligingscertificeringsautoriteiten), achtste lid, onder d	Artikel 5:15, Algemene wet bestuursrecht		–
Artikel 58, (Nationale cyberbeveiligingscertificeringsautoriteiten), achtste lid, onder e	Artikel 11	Geen	–
Artikel 58, (Nationale cyberbeveiligingscertificeringsautoriteiten), achtste lid, onder f	Artikelen 12 en 13	Geen	–
Artikel 59 (Collegiale toetsing), eerste, tweede, derde, vierde en zesde lid	Behoeft naar zijn aard geen uitvoering, betreft feitelijke handelingen	Geen	–
Artikel 59 (Collegiale toetsing), vijfde lid	Behoeft naar zijn aard geen uitvoering, betreft regelgevende bevoegdheden voor de Europese Commissie	Geen	–
Artikel 60 (Conformiteitsbeoordelingsinstanties)	Behoeft naar zijn aard geen uitvoering, rechtstreekse werking volstaat	Geen	–
Artikel 61 (Aanmelding), eerste lid en vierde lid, eerste volzin	Behoeft naar zijn aard geen uitvoering, betreft feitelijke handelingen. Waarborging naleving op basis van Wet Naleving Europese regelgeving publieke entiteiten.	Geen	–
Artikel 61 (Aanmelding), tweede, derde lid en vierde lid, tweede volzin	Behoeft naar zijn aard geen uitvoering, de bepaling richt zich tot de Europese Commissie	Geen	–
Artikel 61 (Aanmelding), vijfde lid	Behoeft naar zijn aard geen uitvoering, betreft regelgevende bevoegdheden voor de Europese Commissie	Geen	–
Artikel 62 (Europese Groep voor cyberbeveiligingscertificering)	Behoeft naar zijn aard geen uitvoering, betreft interne EU-aangelegenheden	Geen	–
Artikel 63 (Recht om een klacht in te dienen)	Behoeft naar zijn aard geen uitvoering, rechtstreekse werking volstaat	Geen	–
Artikel 64 (Recht op een doeltreffende voorziening in rechte)	Behoeft naar zijn aard geen uitvoering, rechtstreekse werking volstaat	Geen	–
Artikel 65 (Sancties), eerste en tweede volzin	Artikel 13	Geen	
Artikel 65 (Sancties), derde volzin	Behoeft naar zijn aard geen uitvoering, betreft feitelijke handelingen	Geen	–
Artikel 66 (Comitéprocedure)	Behoeft naar zijn aard geen uitvoering, betreft regelgevende bevoegdheden van de Europese Commissie	Geen	–
Artikel 67 (Evaluatie en toetsing)	Behoeft naar zijn aard geen uitvoering, de bepaling richt zich tot de Europese Commissie	Geen	–
Artikel 68 (Intrekking en opvolging), eerste en tweede lid	Behoeft naar zijn aard geen uitvoering, betreft de intrekking van Verordening (EU) nr. 526/2013	Geen	–

Verordening 2019/881/EU	Bepaling in implementatieregeling of bestaande regeling	Omschrijving beleidsruimte	Toelichting op de keuze(n) bij de invulling van de beleidsruimte
Artikel 68 (Intrekking en opvolging), derde, vierde, vijfde en zesde lid	Behoeft naar zijn aard geen uitvoering, de bepaling richt zich tot Enisa	Geen	–
Artikel 69 (Inwerkingtreding)	Behoeft naar zijn aard geen uitvoering, betreft de inwerkingtreding en toepassing van de verordening	Geen	–
Bijlage	Behoeft naar zijn aard geen uitvoering, rechtstreekse werking volstaat	Geen	–

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