Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

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

Nr. 5

VERSLAG

Vastgesteld 16 juni 2021

De vaste commissie voor Economische Zaken en Klimaat, belast met het voorbereidend onderzoek van dit wetsvoorstel, heeft de eer als volgt verslag uit te brengen van haar bevindingen.

Onder het voorbehoud dat de regering op de gestelde vragen en de gemaakte opmerkingen tijdig en genoegzaam zal hebben geantwoord, acht de commissie de openbare beraadslaging over dit wetsvoorstel voldoende voorbereid.

I. ALGEMEEN

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel Uitvoeringswet cyberbeveiligingsverordening. Cyberveiligheid vereist gezien haar grensoverschrijdende karakter, naast een nationale aanpak, ook Europese inspanningen. Deze leden hebben nog enkele vragen over dit wetsvoorstel.

De leden van de D66-fractie hebben met interesse kennisgenomen van de Uitvoeringswet cyberbeveiligingsverordening en onderstrepen het belang van een geharmoniseerde certificatiesystematiek om de cyberbeveiliging in de Europese Unie te vergroten en versterken. Deze leden hebben nog enkele vragen.

De leden van de CDA-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel. Zij hebben hierover verschillende vragen en opmerkingen.

De leden van de SP-fractie hebben kennisgenomen van het wetsvoorstel en hebben hierover nog enkele vragen.

De leden van de GroenLinks-fractie hebben met belangstelling kennisgenomen van het voorliggende wetsvoorstel. De coronacrisis heeft de reeds bestaande trend van snelle digitalisering nog verder aangezet en de voordelen van digitalisering eens te meer duidelijk gemaakt. Aan de

kst-35838-5
ISSN 0921 - 7371
's-Gravenhage 2021

andere kant brengt digitalisering ook kwetsbaarheden met zich mee. Het is van groot belang dat de cyberbeveiliging van digitale producten, diensten en processen goed op orde is.

De leden van de ChristenUnie-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel. Deze leden constateren dat dit wetsvoorstel tot doel heeft cyberbeveiliging op Europees niveau vast te stellen door middel van cyberbeveiligingscertificeringsregelingen. Zij onderschrijven dit doel. Zij hebben hierover nog wel enkele vragen.

1. De hoofdlijnen van de cyberbeveiligingsverordening

a) Reikwijdte

De leden van de VVD-fractie vinden het onduidelijk welke ICT-producten, -diensten en -processen gemoeid zijn met dit wetsvoorstel. Zij vragen de regering meer duidelijkheid te geven over welke producten en diensten dit wetsvoorstel beoogt te certificeren? Wat is hierin het aandeel van slimme apparaten?

De leden van de VVD-fractie vragen hoe het mandaat van het Europees Agentschap voor netwerk- en informatiebeveiliging (Enisa) zich verhoudt tot dat van het Computer Emergency Response Team for the EU Institutions, bodies and agencies (CERT-EU).

De leden van de VVD-fractie lezen in de memorie van toelichting dat de Europese Commissie bevoegd wordt om Europese cyberbeveiligingscertificeringsregelingen voor ICT-producten, -diensten en -processen vast te stellen. Op basis van welke indicatoren gaat de Europese Commissie deze regelingen vaststellen? Hoe zijn deze indicatoren tot stand gekomen?

De leden van de CDA-fractie lezen dat de cyberbeveiligingsverordening lidstaten vrijlaat 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. Zij vragen of de regering voornemens is dit te doen.

De leden van de SP-fractie lezen dat met de verordening de Europese Commissie bevoegd wordt om Europese cyberbeveiligingscertificeringsregelingen voor categorieën van ICT-producten, – diensten en processen vast te stellen. Zij vragen waar de behoefte voor deze soevereiniteitsoverdracht vandaan komt. Immers, de verordening heeft geen betrekking op bevoegdheden van lidstaten betreffende activiteiten inzake openbare beveiliging, defensie, nationale veiligheid en strafrecht aangezien deze thema's onder de nationale competentie van lidstaten vallen. De leden vragen wat de verordening effectief zal betekenen in het bevorderen van cyberveiligheid, of dat zij met name de markt voor cyberveiligheidsproducten zal bevorderen?

De leden van de GroenLinks-fractie lezen in de memorie van toelichting dat de verordening voorziet in de harmonisatie van de vereisten die worden gesteld aan certificaten. Waarom is er niet gekozen voor harmonisatie van de certificaten zelf? Leidt de huidige opzet niet alsnog tot een grote proliferatie aan verschillende certificaten, waardoor eindgebruikers alsnog het overzicht verliezen? Leidt het bovendien niet ertoe dat bedrijven kunnen inzetten op certificatieshopping, waarbij ze certificaten aanvragen bij beoordelingsinstanties in lidstaten die makkelijker zijn in het afgeven van certificaten? Op welke manier wordt dit risico beperkt? Is het niet duidelijker en effectiever om tot een Europees certificaat te komen?

De leden van de GroenLinks-fractie vragen of het cyberbeveiligingscertificeringskader enkel toeziet op certificatieschema's van lidstaten, of ook op schema's die worden beheerd door particuliere organisaties.

De leden van de ChristenUnie-fractie lezen in de memorie van toelichting dat met dit wetsvoorstel wordt gestreefd naar een geharmoniseerd kader voor het ontwikkelen van certificeringsregelingen. Deze leden onderschrijven het belang van het voorkomen van fragmentatie van de Europese digitale interne markt. Toch lezen zij ook in het advies van de Afdeling advisering van de Raad van State dat verplichte certificering op Europees niveau mogelijk pas over enkele jaren wordt verwacht. De regering zal tot die tijd de markt stimuleren om gebruik te maken van de bestaande certificeringstrajecten. Deze leden vragen of er problemen kunnen ontstaan in de transitie van de bestaande nationale certificeringsregelingen naar de nog te verwachten Europese cyberbeveiligingscertificeringsregelingen die pas over enkele jaren verwacht worden. Deze leden vragen de regering hoe deze transitie vormgegeven wordt om het doel van voorkomen van fragmentatie van de Europese digitale interne markt te bewerkstelligen.

b) Nationale cyberbeveiligingscertificeringsautoriteit

De leden van de VVD-fractie stellen vragen over het feit dat binnen deze wet de mogelijkheid bestaat van conformiteitszelfbeoordeling waarbij een fabrikant of aanbieder zelf in plaats van een onafhankelijke instantie, bepaalt of er aan voorschriften van de certificeringsregeling is voldaan. Hoe beoordeelt de regering deze mogelijkheid in het kader van onafhankelijke toetsing en daarmee ook de doelmatigheid van dit wetsvoorstel?

De leden van de VVD-fractie vragen hoe en door welke instantie wordt bepaald welk zekerheidsniveau (basis, substantieel en hoog) geldt voor welk product, dienst of proces. Op basis van welke parameters wordt dit gedaan?

De leden van de VVD-fractie lezen dat de nationale autoriteit de mogelijkheid heeft om sancties op te leggen aan aanbieders en producenten wanneer zij hun verplichtingen niet nakomen. In hoeverre wordt bij het opleggen van deze sancties rekening gehouden met het zekerheidsniveau van de aangeboden producten/diensten/processen?

De leden van de VVD-fractie lezen verder dat de nationale autoriteit het mandaat krijgt om cyberbeveiligingscertificaten met zekerheidsniveau hoog weer in te trekken indien het certificaat niet blijkt te voldoen aan de voorliggende certificeringsregeling. Ligt er een bepaalde overweging ten grondslag aan de mogelijkheid om louter certificaten met zekerheidsniveau hoog in te trekken? Zo ja, welke analyse ligt hieronder? Welke (juridische) mogelijkheden hebben fabrikanten of aanbieders in het geval van intrekking van certificaten nog?

De leden van de CDA-fractie lezen in de memorie van toelichting dat de cyberbeveiligingsverordening stelt dat iedere lidstaat een (of meerdere) nationale cyberbeveiligingscertificeringsautoriteit(en) moet aanwijzen die met toezichthoudende taken wordt belast. Onder andere Cyberveilig Nederland merkt in reactie op het wetsvoorstel op dat de nationale autoriteit over voldoende personele middelen dient te beschikken. Deze leden vragen of dit op tijd gaat lukken, gelet op de schaarste aan ICT-personeel die dikwijls eerder hun weg vinden naar het bedrijfsleven in plaats van naar de overheid. Welke wervingsacties worden op dit terrein ondernomen? Waarom is er niet voor gekozen het Nationaal Cyber Security Centrum als nationale autoriteit aan te wijzen? Onderkent de

regering dat het toezicht op cyberveiligheid nu heel gefragmenteerd is, terwijl er steeds vaker bevoegdheden/taken op dit terrein vanuit Europa geïmplementeerd zullen moeten worden, zonder dat er een echt geschikte toezichthouder is?

c) Europese cyberbeveiligingscertificeringsregelingen

De leden van de VVD-fractie constateren dat Enisa om de vijf jaar elke vastgestelde Europese cyberbeveiligingscertificeringsregeling evalueert. Op basis van welke analyse is deze termijn vastgesteld? Hoe verhoudt deze termijn zich tot de driejarige termijn van de Europese Commissie om bepaalde certificeringsregelingen verplicht te stellen? Ziet de regering ruimte om deze termijnen samen te brengen om verplichting logischer te laten volgen op evaluatie?

De leden van de VVD-fractie constateren tevens dat reeds bestaande nationale certificeringsregelingen voor ICT-producten, -diensten en -processen zal komen te vervallen en zal worden vervangen door Europese cyberbeveiligingscertificeringsregelingen. In hoeverre brengen de Europese regelingen een aanscherping aan op de nationale regeling?

De leden van de CDA-fractie lezen in de memorie van toelichting dat nationale cyberbeveiligingscertificeringsregelingen die hetzelfde onderwerp regelen als een Europese cyberbeveiligingscertificeringsregelingen vanaf een bij de certificeringsregeling vastgestelde datum zullen vervallen. Begrijpen deze leden correct dat op dit moment nog niet kan worden vastgesteld welke nationale cyberbeveiligingscertificeringsregelingen dit zijn?

De leden van de GroenLinks-fractie zijn van mening dat het, om vertrouwen en veiligheid in de digitale economie te borgen, een helder kader voor de certificering van digitale producten, diensten en processen essentieel is. Deze leden juichen dan ook toe dat de cyberbeveiligingsverordening werk maakt van verduidelijking en harmonisatie van dit kader. Zij vragen echter of de huidige opzet, gestoeld op vrijwillige certificering, ver genoeg gaat. Deze leden begrijpen dat een duidelijk kader voor vrijwillige certificering een marktdynamiek in gang kan zetten waarbij steeds meer fabrikanten hun producten vrijwillig laten certificeren. De ervaring leert echter dat er vaak een groep is die zich daar juist aan onttrekt, en wellicht een bewuste keuze maakt voor goedkopere, maar ook onveiligere producten, waar de eindgebruiker, en uiteindelijk de samenleving als geheel, de negatieve gevolgen van dragen. Waarom is er in de verordening niet gekozen voor een meer verplichtend karakter van cyberbeveiligingscertificering? Is de regering bereid om zich hiervoor in te spannen?

De leden van de GroenLinks-fractie vragen waarom de regering er met het wetsvoorstel voor heeft gekozen om geen gebruik te maken van de mogelijkheid onder artikel 56 om certificering verplicht te stellen.

De leden van de GroenLinks-fractie lezen dat bij de uitwerking van specifieke certificeringsregelingen nader ingegaan zal worden op de wijze waarop voorheen onopgemerkte kwetsbaarheden moeten worden aangepakt, door middel van passende regels inzake updates, hacks of patches. Klopt het dat de wijze waarop dat wordt gedaan niet verder wordt ingevuld en dat het daarmee mogelijk blijft dat een certificeringsregeling slechts lichte vereisten stelt op dit gebied? In hoeverre vormt dat een risico? Waarom zijn de minimumvereisten ten aanzien van de omgang met updates, hacks of patches niet opgenomen in de verordening, en in de uitvoeringswet daarvan, zelf?

d) Verstrekking van Europese cyberbeveiligingscertificaten en EU-conformiteitsverklaringen

De leden van de D66-fractie horen graag of verwacht wordt dat een evaluatie om de vijf jaar op vastgestelde Europese cyberbeveiligingscertificeringsregeling, door ENISA, voldoende recht doet aan de snel veranderende sector waar de verordening op toeziet. Deze leden horen graag of de regels bij cyberbeveiligingscertificeringsregeling omtrent het beschikbaar stellen van updates universeel zullen zijn en welke termijnen momenteel hiertoe overwogen worden.

De leden van de CDA-fractie constateren dat de cyberbeveiligingscertificeringsregelingen de basis vormen van de uitgifte van de cyberbeveiligingscertificaten en Europese Unie-conformiteitsverklaringen. Deze uitgifte geschiedt nationaal, door ofwel een conformiteitsbeoordelingsinstantie (zekerheidsniveaus «basis» en «substantieel») ofwel de nationale cyberbeveiligingscertificeringsautoriteit (zekerheidsniveau «hoog»). Kan de regering deze verschillende zekerheidsniveaus met voorbeelden toelichten?

De leden van de SP-fractie vragen in welke mate lidstaten kiezen voor het laten verstrekken van nationale cyberbeveiligingscertificaten voor zekerheidsniveau hoog door de nationale cyberbeveiligingscertificeringsautoriteit dan wel door een conformiteitsbeoordelingsinstantie. Welke gevolgen heeft het gebruik van verschillende regimes voor de wederzijdse erkenning?

De leden van de GroenLinks-fractie lezen dat de verordening ruimte biedt voor conformiteitszelfbeoordelingen door fabrikanten waar het gaat om ICT-producten, -diensten en -processen met een laag risico. Waarom is deze mogelijkheid geboden, zo vragen deze leden? Erkent de regering dat de gevolgen van een cybersecurity incident rond een product met laag risico alsnog serieus kunnen zijn? Wat zijn de risico's van de mogelijkheid tot zelfbeoordeling, en op welke wijze worden die gemitigeerd?

e) Conformiteitsbeoordelingsinstanties

De leden van de CDA-fractie lezen in een bijlage bij de cyberbeveiligingsverordening de vereisten waaraan een conformiteitsbeoordelingsinstantie moet voldoen om te worden geaccrediteerd om Europese cyberbeveiligingscertificaten te kunnen verstrekken. Hoeveel van deze instanties zijn er momenteel in Nederland?

De leden van de SP-fractie vragen welke belangen conformiteitsbeoordelingsinstanties hebben bij het verstrekken van cyberbeveiligingscertificaten.

f) Fabrikanten/aanbieders

De leden van de CDA-fractie lezen in de memorie van toelichting dat fabrikanten of aanbieders van ICT-producten, -diensten of -processen middels de cyberbeveiligingsverordening worden aangespoord om beveiligingsmaatregelen te nemen. De cyberbeveiligingsverordening gaat in eerste instantie uit van certificering op basis van vrijwilligheid, met een eigen keuze voor bedrijven om ervoor te kiezen hun ICT-producten, -diensten en -processen te laten certificeren. Kan de regering ingaan op de keuze voor vrijwillige in plaats van voor verplichtende certificering? Welke criteria liggen hieraan ten grondslag? Wat wordt gedaan wanneer te weinig bedrijven zich certificeren, en op welk moment?

2. Hoofdlijnen van het wetsvoorstel

De leden van de CDA-fractie vragen op welke datum de cyberbeveiligingsverordening moet zijn geïmplementeerd in nationale wetgeving en of de verwachting is dat zowel Nederland als andere lidstaten deze deadline zullen halen.

De leden van de CDA-fractie vragen de regering of zij de overeenkomsten en verschillen met de huidige CE-markering kan schetsen. Deze leden vragen tevens of de regering kan aangeven hoe de cyberbeveiligingscertificering in de Verenigde Staten is georganiseerd. Zijn er parallellen met wat nu in Europa wordt voorgesteld?

a) Nationale cyberbeveiligingscertificeringsautoriteit

De leden van de VVD-fractie achten het positief dat het Agentschap Telecom (AT) wordt aangewezen als nationale autoriteit van deze cyberbeveiligingsverordening gezien de geruime ervaring op het gebied van toezichthoudende werkzaamheden op het digitale domein. Echter, deze leden willen benadrukken dat het beleggen van deze taken bij de Agentschap Telecom een zekere mate van capaciteit vereist en dat andere, huidige taken niet in het geding mogen komen. Hoeveel fulltime equivalent (FTE) gaat de taak van nationale autoriteit naar uw inschatting vereisen? Beschikt het Agentschap Telecom over deze capaciteit?

De leden van de CDA-fractie constateren dat volgens het wetsvoorstel de uitvoering van de taken van de Nationale cyberbeveiligingscertificeringsautoriteit berust bij het Agentschap Telecom. Het AT is in het digitale domein zowel uitvoerder als toezichthouder. Kan de regering de keuze voor het AT als uitvoerder nog eens beargumenteren? Vindt zij dit naast de meest effectieve/efficiënte ook de meeste wenselijke oplossing? Heeft het AT thans voldoende slagkracht om deze extra taken erbij te kunnen nemen? Indien niet, wat heeft het AT nodig om zowel haar nieuwe als bestaande taken optimaal te kunnen doen?

De leden van de GroenLinks-fractie begrijpen de keuze voor het AT als de Nederlandse uitvoerder van de taken die vallen onder de nationale cyberbeveiligingscertificeringsautoriteit. Wat betekent deze uitbreiding van het takenpakket voor de benodigde capaciteit bij het Agentschap Telecom? Ook vragen deze leden op welke wijze de relevante instanties die onder de Minister van Justitie & Veiligheid vallen, zoals het Nationale Cybersecurity Centrum (NCSC), betrokken worden bij de uitvoering van deze taken?

b) Conformiteitsbeoordelingsinstantie en accreditatie

De leden van de CDA-fractie lezen in de memorie van toelichting dat fabrikanten en aanbieders gevestigd in andere lidstaten en derde landen een conformiteitsbeoordeling kunnen laten uitvoeren in Nederland. Geldt dit ook andersom, of zijn er ook (derde) landen waar een conformiteitsbeoordeling voor Nederlandse fabrikanten en aanbieders niet mogelijk is (wederkerigheid)?

De leden van de CDA-fractie constateren dat Nederlandse conformiteitsbeoordelingsinstanties in Nederland geaccrediteerd moeten te zijn. Dienen zij ook uit Nederland afkomstig te zijn, of is het mogelijk dat een buitenlandse organisatie uit bijvoorbeeld China een accreditatie krijgt om in Nederland conformiteitsbeoordelingen te doen?

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

De leden van de VVD-fractie lezen in de memorie van toelichting dat deelname van fabrikanten en aanbieders aan de cyberbeveiligingscertiferingsregelingen vooralsnog vrijwillig is. Dit overwegende, hoe beoordeelt de regering deze mate van vrijwilligheid in het licht van de doelmatigheid van deze wet? Hoe beoordeelt de regering vrijwilligheid bij certificering van producten met een hoog zekerheidsniveau? Deelt de regering de mening dat een verplichtend karakter verstandig kan zijn bij certificering van producten met hoge zekerheidsniveaus in verband met de grote maatschappelijke en economische risico's die verbonden zijn aan deze categorie?

De leden van de CDA-fractie constateren dat de regering met dit wetsvoorstel kiest voor een goedkeuringsmodel, met voorafgaande goedkeuring door de nationale autoriteit, waarbij zowel de markt als de nationale autoriteit actief betrokken zijn bij de conformiteitsbeoordeling. Dit om efficiënt te kunnen inspelen op behoeftes van fabrikanten en leveranciers en wegens hun deskundigheid enerzijds en vanuit kostenoogpunt anderzijds. Zitten hier ook risico's aan, bijvoorbeeld in situaties wanneer de druk op overheidsbudgetten groot is?

De leden van de CDA-fractie constateren dat een certificatietraject voor zekerheidsniveau «hoog» doorgaans een langdurig en kostbaar traject is, waarbij aanzienlijke investeringen van de opdrachtgevers worden gevraagd. Hierom is gekozen voor een goedkeuringsmodel, met een hoge mate van zekerheid en voorspelbaarheid, bedoeld om onnodige kosten te beperken. Wordt de keuze voor dit model door opdrachtgevers en andere stakeholders gesteund?

De leden van de CDA-fractie lezen in de memorie van toelichting de schets van de goedkeuringsprocedure, die zal worden opgedeeld in meerdere stappen. De conformiteitsbeoordelingsinstantie doet melding bij de nationale autoriteit dat een certificeringstraject wordt gestart, legt het onderzoeksplan ter goedkeuring voor aan de nationale autoriteit, legt het onderzoeksrapport en het bijhorende Europese cyberbeveiligingscertificaat dat de conformiteitsbeoordelingsinstantie voornemens is af te geven ter goedkeuring voor aan de nationale autoriteit en geeft het Europese cyberbeveiligingscertificaat af na goedkeuring door de nationale autoriteit.

De leden van de CDA-fractie vragen of met deze procedure/dit model/deze werkwijze geoefend of ervaring opgedaan is. Indien ja, wat waren de uitkomsten daarvan? Waren alle stakeholders hierbij betrokken?

De leden van de CDA-fractie vragen of de regering kan aangeven wat de (maximale) termijnen/doorlooptijden zijn voor eerdergenoemde stappen, zodat een beeld kan worden gevormd van hoe lang een certificeringstraject kan duren. Verwacht de regering dat een lang en kostbaar certificeringstraject opdrachtgevers kan afschrikken om aan vrijwillige certificering mee te doen, waardoor zowel de verordening als het wetsvoorstel hun doel voorbijschieten?

De leden van de CDA-fractie constateren dat de nationale autoriteit ten behoeve van haar besluitvorming advies kan vragen van andere (overheids-)organisaties, zoals de Algemene Inlichtingen- en Veiligheidsdienst (AIVD). Dit advies is echter niet-bindend van aard. Waarom is hiervoor gekozen? Acht de regering het voorstelbaar dat de nationale

autoriteit een advies van de AIVD naast haar neerlegt? In welke situaties? Zou dit geen veiligheidsrisico's met zich meebrengen?

De leden van de CDA-fractie lezen in de memorie van toelichting dat gegevens die de nationale autoriteit in het kader van het goedkeuringsproces en het uitoefenen van een beperkt aantal toezichthoudende taken verkrijgt voor zekerheidsniveau «hoog» uitgezonderd zijn van de toepassing van de Wet openbaarheid van bestuur, ter bescherming van de openbare veiligheid en de concurrentiepositie van bedrijven. Dit lijkt deze leden goed en belangrijk.

De leden van de CDA-fractie lezen verder dat de Wet openbaarheid van bestuur wel van toepassing is op de uitoefening van alle overige toezichthoudende taken met betrekking tot cyberbeveiligingscertificaten met zekerheidsniveau «hoog» (artikelen 58, zevende lid, onderdelen b, c, d, e, f, g en i van de cyberbeveiligingsverordening) op alle toezichthoudende taken inzake cyberbeveiligingscertificaten met zekerheidsniveaus «basis» en «substantieel». Brengt dit nog risico's met zich mee?

De leden van de SP-fractie lezen dat in de memorie van toelichting wordt gesteld dat Nederland goede ervaringen heeft met modellen waarbij de markt wordt ingezet. Kan worden toegelicht welke modellen dit zijn?

3. Regeldruk

De leden van de VVD-fractie lezen met verbazing dat de extra regeldruk voor bedrijven «iets anders ligt» dan voor burgers. Deze leden behoeven meer toelichting van de regering wanneer het gaat om de extra kosten en uren die hiermee gemoeid zijn voor (kleine) ondernemers. Vanzelfsprekend zijn deze leden zich bewust van de noodzaak om strengere eisen te stellen aan de producten/diensten en processen van vitale aanbieders. Deze leden vragen in hoeverre het wenselijk is dat ondernemers in het midden- en kleinbedrijf te maken krijgen met dezelfde regeldruk als grote vitale aanbieders in het geval van eventuele verplichting. Hoe beoordeelt de regering de proportionaliteit van het voorliggende wetsvoorstel in het licht van de verplichtingen die hiervoor worden aangegaan door kleine ondernemers ten opzichte van de grootte en functie van deze bedrijven? Is de regering bereid om meer inzicht te geven in de eventuele extra regeldruk voor bedrijven en specifiek kleine ondernemers?

De leden van de CDA-fractie lezen in de memorie van toelichting dat momenteel nog niet duidelijk is hoeveel Europese cyberbeveiligingscertificeringsregelingen er zullen komen, op welke ICT-producten, -processen, of -diensten deze cyberbeveiligingscertificeringsregelingen betrekking zullen hebben, hoe deze regelingen eruit zullen zien en hoeveel er gebruik van zal worden gemaakt. Deze leden merken op dat het ontbreken van deze informatie het lastig maakt om de volledige (regeldruk)effecten van dit wetsvoorstel te overzien. Wanneer denkt de regering dat hierover meer bekend is?

De leden van de ChristenUnie-fractie vragen wat de nog te verwachten Europese cyberbeveiligingscertificeringsregelingen voor invloed zullen hebben op de regeldruk en kosten voor bedrijven die ICT-producten, -diensten en -processen laten certificeren. Is er een mogelijkheid voor toezicht op of evaluatie van de regeldruk en kosten die de nog te verwachten Europese cyberbeveiligingscertificeringsregelingen mogelijk met zich meebrengen? Is hier bijvoorbeeld een rol voor de nationale cyberbeveiligingscertificeringsautoriteit weggelegd?

a) Aanbieders

De leden van de CDA-fractie lezen in de memorie van toelichting dat er een opwaartse ontwikkeling zichtbaar is van het aantal certificeringen dat in Nederland wordt uitgevoerd. Kan de regering dit kwantificeren?

De leden van de CDA-fractie constateren dat de kosten per certificering sterk kunnen verschillen en zijn afhankelijk van 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. Deze leden vragen of de ontwikkeling van deze kosten zal worden gemonitord.

b) Conformiteitsbeoordelingsinstanties

De leden van de CDA-fractie lezen in de memorie van toelichting dat de totale extra last voor een conformiteitsbeoordelingsinstantie wordt dan bij certificeringen op zekerheidsniveau «hoog» op 270 euro worden geschat. Het is een keuze van de conformiteitsbeoordelingsinstantie om deze kosten aan de aanbieder door te berekenen. Is de verwachting dat veel conformiteitsbeoordelingsinstanties dit zullen doen?

4. Advies en consultatie

4.1. Internetconsultatie

De leden van de D66-fractie horen graag een nadere toelichting waarom er niet voor gekozen wordt om de omgang met updates of hacks vast te leggen in het wetsvoorstel, zoals voorgesteld wordt door zowel de Afdeling advisering van de Raad van State als verschillende inbrengen geleverd bij de internetconsultatie. Waarom zou het wenselijker zijn om dit middels en ministeriële regeling vast te leggen?

De leden van de CDA-fractie merken op dat twee organisaties in hun advies hebben gesteld dat de beslistermijnen van de goedkeuringsprocedure tot onnodige vertraging zullen leiden, met een mogelijk negatieve marktwerking in Nederland tot gevolg. De Algemene wet bestuursrecht (Awb) stelt dat een besluit binnen een redelijke termijn van maximaal acht weken genomen dient te worden. Het uitganspunt van de regering is dat de besluitvormingsprocessen binnen de autoriteit niet tot onnodige vertraging zullen gaan leiden en waar mogelijk gewerkt zal worden met standaardprocedures. Worden de doorlooptijden gemonitord?

4.2. Advies van het Adviescollege Toetsing Regeldruk

De leden van de CDA-fractie merken op dat het Adviescollege Toetsing Regeldruk (ATR) adviseert 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. Dit is nu niet mogelijk, omdat veel relevante informatie nog niet bekend is. Is de regering voornemens in een later stadium alsnog het advies van het ATR op te volgen?

4.3. Uitvoering- en handhaafbaarheidstoets van Agentschap Telecom

De leden van de CDA-fractie merken op dat het AT adviseert om in het wetsvoorstel een grondslag op te nemen voor verplichte certificering op nationaal niveau, op grond waarvan het agentschap adequaat kan ingrijpen op «zich in de praktijk snel en onverwacht manifesterende

cyberrisico's». De regering neemt dit advies niet over, omdat het voorstander is van certificering op Europees niveau. Hoe denkt de regering op andere wijze aan de zorgen van het AT tegemoet te kunnen komen, daar het AT zelf schrijft dat «de bestaande bevoegdheden van het agentschap ontoereikend zijn om bij bepaalde risico's te kunnen ingrijpen»?

De leden van de ChristenUnie-fractie lezen in de memorie van toelichting dat wanneer een cyberbeveiligingscertificaat niet voldoet aan de Europese voorschriften, de cyberbeveiligingscertificeringsautoriteit kan ingrijpen. Als een ICT-product, -dienst of -proces niet voldoet aan de cyberbeveiligingsverordening kan echter niet worden ingegrepen door de nationale cyberbeveiligingscertificeringsautoriteit. Betekent dit dat wanneer een ICT-product, -dienst of -proces zonder certificaat wordt gebruikt er geen toezicht is op correcte cyberbeveiliging van het product, de dienst of het proces?

Deze leden vragen bij wie de verantwoordelijkheid ligt van correcte cyberbeveiligingscertificering van ICT-producten, -diensten of -processen en eventuele gevolgen van incorrecte certificering voor de cyberbeveiliging.

De fungerend voorzitter van de commissie,
Azarkan

De adjunct-griffier van de commissie,
Reinders