Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

22 112 Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie

Nr. 3692 **BRIEF VAN DE MINISTER VAN BUITENLANDSE ZAKEN**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 26 mei 2023

Overeenkomstig de bestaande afspraken ontvangt u hierbij 8 fiches die werden opgesteld door de werkgroep Beoordeling Nieuwe Commissie voorstellen (BNC).

Fiche: Herziening EU farmaceutische wetgeving (Kamerstuk 36 365, nr. 2)

Fiche: Verordening en richtlijnen wijziging Europees crisisraamwerk voor banken (CMDI review) (Kamerstuk 22 112, nr. 3691)

Fiche: Wijziging Verordening Europees kader voor cyberbeveiligingscertificering (Cyber Security Act)

Fiche: Verordeningen aanvullende beschermingscertificaten (ABC's) (Kamerstuk 22 112, nr. 3693)

Fiche: Mededeling Cybersecurity Skills Academie (Kamerstuk 22 112, nr. 3694)

Fiche: Cybersolidariteitsverordening (Kamerstuk 22 112, nr. 3695)

Fiche: Raadsaanbeveling uitbreiding EU-maatregelen resistentie tegen antimicrobiële stoffen (Kamerstuk 22 112, nr. 3696)

Fiche: Raadsaanbevelingen digitaal onderwijs en digitale vaardigheden (Kamerstuk 22 112, nr. 3697)

De Minister van Buitenlandse Zaken,
W.B. Hoekstra

kst-22112-3692
ISSN 0921 - 7371
's-Gravenhage 2023

Fiche: Wijziging Verordening Europees kader voor cyberbeveiligingscertificering (Cyber Security Act)

1. Algemene gegevens

a) *Titel voorstel*
Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services
b) *Datum ontvangst Commissiedocument*
18 april 2023
c) *Nr. Commissiedocument*
COM(2023) 208
d) *EUR-Lex*
https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=COM%3A2023%3A0208%3AFIN
e) *Nr. impact assessment Commissie en Opinie Raad voor Regelgevingstoetsing*
Niet opgesteld
f) *Behandelingstraject Raad*
Raad voor Vervoer, Telecommunicatie en Energie (Telecomraad)
g) *Eerstverantwoordelijk ministerie*
Ministerie van Economische Zaken en Klimaat
h) *Rechtsbasis*
Artikel 114 Verdrag betreffende de Werking van de Europese Unie (VWEU)
i) *Besluitvormingsprocedure Raad*
Gekwalificeerde meerderheid
j) *Rol Europees Parlement*
Medebeslissing

2. Essentie voorstel

a) Inhoud voorstel

Op 18 april 2023 heeft de Europese Commissie (hierna: de Commissie) een pakket gepubliceerd met daarin een tweetal wetgevende voorstellen en een mededeling op het gebied van cybersecurity. Over de voorstellen voor een Cybersolidariteitsverordening[1] en een mededeling over de academie voor cybersecurityvaardigheden[2] wordt uw Kamer gelijktijdig middels aparte BNC-fiches geïnformeerd. In dit BNC-fiche wordt een appreciatie gegeven van het voorstel betreft een wijziging op de Cyberbeveiligingsverordening[3] (*Cybersecurity Act*, hierna: CSA). Met het voorstel wordt het toepassingsgebied van het Europese cyberbeveiligingscertificeringskader verbreed met «beheerde beveiligingsdiensten», op het al reeds bestaande toepassingsgebied van ICT-producten, ICT-diensten en ICT-processen.

[1] COM(2023) 209.
[2] COM(2023) 207.
[3] Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening) (PbEU 2019, L151); Het hoofddoel van de CSA is een geharmoniseerd certificeringsstelsel, teneinde een adequaat niveau van cyberbeveiliging tegen cyberdreigingen binnen de EU te waarborgen. De CSA stelt fabrikanten en dienstverleners in staat om in de hele EU wederzijdse erkende certificaten te gebruiken.

De wijziging ziet op het realiseren van toekomstige vaststelling van Europese cyberbeveiligingscertificeringsregelingen voor beheerde beveiligingsdiensten. Dit zijn specifieke diensten die worden verleend door aanbieders van cyberbeveiligingsdiensten. Het gaat hierbij om respons op incidenten, penetratietests[4] en beveiligingsaudits en -consultancy, om bedrijven en andere organisaties te helpen cyberincidenten te voorkomen, op te sporen, erop te reageren en/of te boven te komen.

Met de voorgestelde wijziging komt de Commissie tegemoet aan de oproep in de Raadsconclusies uit mei 2022[5] om de cyberweerbaarheid van de EU te versterken. Het doel van het voorstel is om de kwaliteit van geleverde beheerde beveiligingsdiensten te verbeteren en hun vergelijkbaarheid te vergroten door Europese cyberbeveiliging certificeringschema's op te stellen.

De Commissie stelt een definitie van beheerde beveiligingsdiensten voor, waarbij aangesloten wordt bij de definitie van aanbieders van beheerde beveiligingsdiensten onder de herziene Europese richtlijn inzake beveiliging van netwerk- en informatiesysteem[6] (NIB-2-richtlijn).

Daarnaast voegt de Commissie doelstellingen toe voor beheerde beveiligingsdiensten waarin organisatorische componenten zijn opgenomen die medebepalend zijn voor certificering. Overige wijzigingen zijn van technische aard en zijn bedoeld om bestaande relevante bepalingen, die momenteel gelden voor ICT-producten, -diensten en -processen, ook voor beheerde beveiligingsdiensten te laten gelden.

De wijziging in de CSA creëert de bevoegdheid voor de Commissie om certificeringsregelingen voor beheerde beveiligingsdiensten vast te stellen en heeft feitelijk pas effect als dergelijke certificeringsregelingen zijn vastgesteld in een later stadium.

De Commissie stelt dat EU-certificering een doeltreffend middel is om vertrouwen op te bouwen in de kwaliteit van die diensten en zo de opkomst van een betrouwbare Europese cyberbeveiligingsdienstensector te vergemakkelijken en bijdraagt aan het voorkomen van versnippering van de interne markt. Er zijn namelijk diverse lidstaten die zijn begonnen met de adaptatie van nationale certificeringsregelingen. De wijziging beoogt de werking van de interne markt te verbeteren en fragmentatie te voorkomen.

De voorgestelde Cybersolidariteitsverordening voorziet in een procedure voor het selecteren van aanbieders om een cyberbeveiligingsreserve op EU-niveau te vormen[7], waarbij onder meer rekening moet worden gehouden met het feit of die aanbieders een Europese of nationale cyberbeveiligingscertificering hebben verkregen. Toekomstige certificeringsregelingen voor beheerde beveiligingsdiensten zullen dus een

---

[4] Een penetratietest of pentest is een toets van een of meer computersystemen op kwetsbaarheden, waarbij deze kwetsbaarheden ook werkelijk gebruikt worden om in deze systemen in te breken.

[5] EU 9364/22; Council conclusions on the development of the European Union's cyber posture.

[6] Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (PbEU 2022, L333).

[7] Deze reserve moet bestaan uit betrouwbare aanbieders die diensten voor de respons op incidenten leveren en waarmee vooraf een contract wordt gesloten zodat zij op verzoek van lidstaten, instellingen, organen en agentschappen van de Unie meteen kunnen ingrijpen bij een significant of grootschalig cyberbeveiligings-incident.

belangrijke rol spelen bij de uitvoering van de Cybersolidariteitsverordening.

b) Impact assessment Commissie

Er is geen impact assessment opgesteld.

3. Nederlandse positie ten aanzien van het voorstel

a) Essentie Nederlands beleid op dit terrein

Het Rijksbrede beleid voor cybersecurity is vastgelegd in de Nederlandse Cybersecurity Strategie[8] (NLCS). Het doel van de NLCS is om Nederland digitaal veilig te maken door de digitale weerbaarheid te verhogen en dreigingen tegen te gaan. Het kabinet zet in op het versterken en transformeren van het digitale ecosysteem waarbij één organisatie of één individu niet langer de zwakste schakel kan zijn. Dat vergt een systeemtransformatie die in de vier pijlers van de NLCS wordt uitgelicht. De pijlers zijn I) Digitale weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties; II) Veilige en innovatieve digitale producten en diensten, III) Tegengaan van digitale dreigingen van staten en criminelen, en IV) Cybersecurity-arbeidsmarkt, onderwijs, en de digitale weerbaarheid van burgers. Dit vergt de inzet van een uitgebalanceerd samenspel aan instrumenten: van intensievere publiek-private samenwerking tot nieuwe (Europese) wetgeving, met als doel een ecosysteem te creëren waarbij burgers, organisaties en (kleine) bedrijven in beginsel veilige producten en diensten kunnen afnemen. Eén van de doelstellingen uit pijler II van de NLCS is het veiliger maken van ICT-producten en diensten. Het ontwikkelen en implementeren van Europese cybersecuritycertificering onder de CSA is één van de maatregelen onder deze doelstelling.

In het kader van de Europese digitale ééngemaakte markt, de competitieve wereldeconomie, het streven naar een gelijk speelveld en veilige ICT-producten en -diensten zet het kabinet waar mogelijk in op het ontwikkelen van Europese wet- en regelgeving. Gezien het inherent grensoverschrijdende karakter van cybersecurity en digitale dreigingen staat Europese en internationale samenwerking in de Nederlandse aanpak centraal.

Gegeven het feit dat hackers steeds vaker geavanceerde methoden gebruiken om toegang te krijgen tot netwerken en gegevens en groeiende vraag vanuit de markt om hier iets tegen te doen, heeft Nederland in 2021 in samenwerking met verzekeraars, politie, VNO-NCW en MKB-Nederland met CCV als beheerder een nationaal certificeringsregeling voor penetratietesten geïntroduceerd. Dit Europees voorstel dat het toepassingsgebied van de CSA verbreedt met beheerde beveiligingsdiensten biedt voor Nederland een kans om de Nederlandse certificering penetratietesten op Europees niveau in te brengen als een volwaardig en volwassen cyberbeveiligingscertificeringsregeling dat als input kan dienen voor Europees stelsel.

b) Beoordeling + inzet ten aanzien van dit voorstel

Het kabinet staat positief tegenover het voorstel, maar heeft ook een aandachtspunt. Het voorstel sluit aan bij de kabinetsinzet op het gebied van de digitale interne markt en het bevorderen van de in de hele EU wederzijds erkende certificaten.

---

[8] Kamerstuk 26 643, nr. 925.

Het is de verwachting van het kabinet dat het voorstel kan bijdragen aan het versterken van het vertrouwen van burgers en bedrijven in de veiligheid van producten en de kwaliteit van aangeboden diensten omdat de schaalvergroting die optreedt door ontwikkeling van Europees geharmoniseerde certificeringsschema's certificering op EU-niveau efficiënter en goedkoper kan maken. Een dergelijke samenhangende EU-brede benadering van certificering moet daarbij geen uitsluitende werking hebben voor niet-EU-aanbieders. Het voorstel zal ook bijdragen aan een gelijk speelveld en het concurrentievermogen van (Nederlandse) cybersecuritybedrijven in de EU.

In het voorstel wordt niet helder gedefinieerd waarom een nieuwe categorie beheerde beveiligingsdiensten wordt ingesteld, terwijl het ook onder een bestaande categorie ICT-diensten conform de huidige CSA kan vallen. Het kabinet is van oordeel dat genoemde diensten zoals penetratietesten en *incident response* die als beheerde beveiligingsdiensten worden aangemerkt, onder de bestaande categorie ICT-services kunnen vallen. Het kabinet zal daarom inzetten op verduidelijking en onderbouwing van deze nieuwe categorie. Daarnaast is het kabinet kritisch omdat een niet goed afgebakende additionele categorie «beheerde beveiligingsdiensten» tot gevolg heeft dat er onnodig veel diensten verplicht zouden kunnen worden zonder dat daarbij een zorgvuldige afweging wordt gemaakt.

De voorgestelde wijzigingen zijn beperkt tot wat strikt noodzakelijk is om de reikwijdte van de verordening te verbreden met enkel beheerde beveiligingsdiensten. Het voorstel wijzigt verder niets aan de werking van de CSA en blijft consistent met de Algemene verordening gegevensbescherming[9] (AVG). De wijziging verandert niets aan het vrijwillige karakter van de certificeringsregelingen. Het is echter niet ondenkbaar dat het vrijwillige karakter van de CSA dan wel de wijziging van de CSA via bijvoorbeeld de NIB-2-richtlijn of andere Europese regelgeving van tijdelijke aard is. Bovendien is niet uit te sluiten dat in dit kader ook andere aanpassingen aan de CSA nodig blijken zijn dan die door de Commissie zijn voorgesteld.

In het voorstel wordt aangegeven dat de nieuwe definitie van beheerde beveiligingsdiensten aansluit bij de definitie van de NIB-2 richtlijn waarin wordt gesproken over de aanbieder van beheerde beveiligingsdiensten. Alhoewel de Commissie meent dat de definitie in lijn is met de NIB-2 richtlijn, is niet duidelijk welke diensten onder de beheerde beveiligingsdiensten zullen vallen.

Het is niet uitgesloten dat het Nederlands en Europees bedrijfsleven geconfronteerd wordt met meer verplichte certificeringsregelingen zonder zorgvuldige afweging met als gevolg daarvan toenemende administratieve lasten en kosten. Ook hier zal het kabinet om nadere toelichting vragen. Het kabinet zet er op in om de regeldruk/administratieve lasten te beperken tot waar dat noodzakelijk is om het doel van de gewijzigde verordening te bereiken.

c) Eerste inschatting van krachtenveld

Naar verwachting zullen de meeste lidstaten positief tegenover het voorstel staan voor het versterken van de cyberbeveiliging in de EU door Europese certificering voor «beheerde beveiligingsdiensten».

---

[9] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119).

De positie van het Europees Parlement (hierna: EP) op het voorstel is nog niet bekend. In het algemeen is het EP voorstander van een Europees geharmoniseerd certificeringsstelsel. Het voorstel wordt behandeld in het *Committee on Industry Reseach and Energy* (ITRE). De rapporteur is Josianne Cutajar (Malta Labour Party).

4. Beoordeling bevoegdheid, subsidiariteit en proportionaliteit

a) Bevoegdheid

Het oordeel van het kabinet is positief. Het voorstel is gebaseerd op artikel 114 VWEU. Dit artikel geeft de EU de bevoegdheid om maatregelen vast te stellen inzake de onderlinge aanpassing van de wettelijke en bestuursrechtelijke bepalingen van de lidstaten die de instelling en de werking van de interne markt betreft. Op het terrein van de interne markt is sprake van een gedeelde bevoegdheid tussen de EU en de lidstaten (artikel 4, tweede lid, onder a, VWEU). Het kabinet kan zich vinden in deze rechtsgrondslag.

b) Subsidiariteit

Het oordeel van het kabinet is positief. Het voorstel heeft tot doel om de goedkeuring van Europese regelingen voor cyberbeveiligingscertificering voor beheerde beveiligingsdiensten mogelijk te maken en versnippering van de interne markt te voorkomen. Zo beoogt het uiteindelijk de cyberveiligheid/cyberweerbaarheid binnen de EU te vergroten. Gezien het inherent grensoverschrijdende karakter van cyberbeveiliging en cyberdreiging kan dit onvoldoende door de lidstaten op centraal, regionaal of lokaal niveau worden verwezenlijkt, daarom is een EU-aanpak nodig. Bovendien worden deze diensten, waarop de voorgestelde wijziging gericht is, aangeboden door aanbieders die in de hele Unie actief zijn, evenals hun grootste potentiële klanten. Door geharmoniseerde certificeringseisen wordt het gelijk speelveld op het terrein van cyberveiligheidsdienstverlening verbeterd en worden belemmeringen op de interne markt weggenomen. Bovendien kan een wijziging van bestaande EU-regelgeving enkel op EU-niveau plaatsvinden. Om die redenen is optreden op het niveau van de EU gerechtvaardigd.

c) Proportionaliteit

Het oordeel van het kabinet is positief. Het voorstel heeft tot doel om de goedkeuring van Europese regelingen voor cyberbeveiligingscertificering voor beheerde beveiligingsdiensten mogelijk te maken en versnippering van de interne markt te voorkomen. Zo beoogt het uiteindelijk de cyberveiligheid/cyberweerbaarheid binnen de EU te vergroten.

Het voorgestelde optreden is geschikt om deze doelstelling te bereiken, omdat het ervoor zorgt dat een certificeringsregeling kan worden opgesteld die in alle lidstaten wordt erkend. Het (mogelijk maken van het) opstellen van een certificeringsregeling die in alle lidstaten wordt erkent, bevordert het gelijk speelveld en voorkomt wildgroei aan nationale certificeringsstelsels. Geharmoniseerde en in alle lidstaten geldige certificering biedt duidelijkheid over de te treffen beveiligingsmaatregelen en investeringen die daarmee gepaard gaan, op die manier kan het dus het gebruik van certificering vergroten. Het gebruik van certificering waarborgt de veiligheid van producten en de kwaliteit van aangeboden diensten. Hierdoor vergroot het uiteindelijk ook de cyberveiligheid/cyberweerbaarheid binnen de EU.

Ook gaat het voorgestelde optreden niet verder dan noodzakelijk gezien het feit dat de wijziging alleen betrekking heeft op de additionele categorie en verder geen andere wijzigingen aanbrengt op de CSA.

Het kabinet heeft echter een aandachtspunt voor wat betreft de afbakening van de ICT-diensten versus beheerde beveiligingsdiensten. In het voorstel wordt niet duidelijk afgebakend welke diensten in de nieuwe categorie zullen vallen. Afhankelijk van de uitwerking bestaat het risico dat er een grotere groep diensten onder de nieuwe categorie zal vallen dan nodig om de gestelde doelstelling van het voorstel te bereiken. Het kabinet zal daarom inzetten om een duidelijke afbakening van de diensten die in de nieuwe categorie zullen vallen.

5. Financiële consequenties, gevolgen voor regeldruk, concurrentiekracht en geopolitieke aspecten

a) Consequenties EU-begroting

Er zijn geen consequenties voor de EU-begroting. Het kabinet is van mening dat de eventuele EU-middelen gevonden dienen te worden binnen de in de Raad afgesproken financiële kaders van de EU-begroting 2021–2027 en dat deze moeten passen bij een prudente ontwikkeling van de jaarbegroting.

b) Financiële consequenties (incl. personele) voor rijksoverheid en/of medeoverheden

De Rijksinspectie Digitale Infrastructuur (hierna: RDI) is op basis van de Uitvoeringswet cyberbeveiligingsverordening conform de CSA reeds aangewezen en ingericht als de nationale cybersecuritycertificeringsautoriteit (NCCA) in Nederland. Met betrekking tot dit voorstel wordt gekeken hoe op efficiënte wijze de bestaande kennis en expertise binnen de rijksoverheid kan worden ingezet. Voor medeoverheden zijn geen financiële consequenties voorzien. Eventuele budgettaire gevolgen worden ingepast op de begroting van het beleidsverantwoordelijke departement, conform de regels van de budgetdiscipline.

c) Financiële consequenties en gevolgen voor regeldruk voor bedrijfsleven en burger

Gegeven het feit dat dit voorstel een zeer beperkte en gerichte wijziging betreft en de certificering vrijwillig is, leidt de wijziging van de verordening mogelijk tot extra regeldruk danwel administratieve lasten voor het bedrijfsleven. Een cybersecuritybedrijf kan zelf de afweging maken of het certificaat van toegevoegde waarde is en tot certificatie over gaan. Certificering onder de CSA is vrijwillig. Het certificeren van een beheerde beveiligingsdienst zal wel enige kosten met zich meebrengen voor het bedrijfsleven indien bedrijven hiervoor kiezen.

Voor burgers zijn geen directe gevolgen voorzien.

d) Gevolgen voor concurrentiekracht en geopolitieke aspecten

Vanwege het EU-brede karakter worden zowel binnen als buiten de EU positieve consequenties verwacht voor de Europese concurrentiekracht, gezien de verwachte bijdrage van de wijziging aan de kwaliteit van zowel leverende organisaties, de geleverde diensten als daarmee de beveiliging van Europese ondernemingen. Het gelijk speelveld van de digitale interne markt zal voor aanbieders van beheerde beveiligingsdiensten worden bevorderd.

6. Implicaties juridisch

a) Consequenties voor nationale en decentrale regelgeving en/of sanctionering beleid (inclusief toepassing van de lex silencio positivo)

De verordening is rechtstreeks toepasselijk in de lidstaten. Op nationaal niveau zal de Uitvoeringswet moeten worden aangepast conform de definitieve wijziging.

b) Gedelegeerde en/of uitvoeringshandelingen, incl. NL-beoordeling daarvan

Het voorstel bevat, in aanvulling op de al bestaande uitvoeringsbevoegdheid ter vaststelling van certificeringsregelen voor ICT producten, ICT diensten en ICT processen, een nieuwe bevoegdheid voor de Commissie om ook uitvoeringshandelingen te nemen ter vaststelling van certificeringsregelingen voor de beheerde beveiligingsdiensten Omdat het hier een beperkte wijziging van een bestaande uitvoeringsbevoegdheid betreft, wordt deze bevoegdheid niet verder beoordeeld in dit BNC-fiche.

c) Voorgestelde implementatietermijn (bij richtlijnen), dan wel voorgestelde datum inwerkingtreding (bij verordeningen en besluiten) met commentaar t.a.v. haalbaarheid

De verordening treedt zoals gebruikelijk in werking op de twintigste dag na de dag van publicatie in het Publicatieblad van de Europese Unie. De voorgestelde inwerkingtredingsdatum is niet haalbaar omdat de uitvoering van deze verordening een wijziging van de Uitvoeringswet cyberbeveiligingsverordening vergt. Daarvoor is doorgaans minstens anderhalf jaar nodig.

d) Wenselijkheid evaluatie-/horizonbepaling

Het voorgestelde amendement wijzigt niets aan de bestaande evaluatiebepaling van de CSA. De huidige verordening bepaalt dat de Commissie de verordening elke vijf jaar evalueert waarbij de eerste plaatsvindt op 28 juni 2024. Het opnemen van een evaluatie-/horizonbepaling is daarmee niet nodig op basis van dit amendement.

e) Constitutionele toets

Niet van toepassing

7. Implicaties voor uitvoering en/of handhaving

Het toezicht valt onder de toegekende taken onder de huidige CSA toe aan de RDI. Dit betekent een taakverzwaring voor RDI, ondanks dat er naar verwachting synergiën mogelijk zullen zijn met de huidige taken van RDI. RDI kan voortbouwen op de opgebouwde capaciteit en expertise voor toezicht. Naast het toezicht, beoordeelt RDI ook de cyberbeveiligingscertificaten met zekerheidsniveau hoog en keurt die goed.

Dit betekent dat investeringen nodig zullen zijn in de capaciteit en expertise bij RDI om passend toezicht en beoordeling in te kunnen richten.

8. Implicaties voor ontwikkelingslanden

Er zijn geen specifieke gevolgen voor ontwikkelingslanden voorzien ten opzichte van de verwachte gevolgen voor derde landen in het algemeen.