EUROPESE UNIE

HET EUROPEES PARLEMENT **DE RAAD**

Brussel, 20 november 2024
(OR. en)

2023/0108(COD) **PE-CONS 93/24**

CYBER 207
JAI 1083
TELECOM 217
DATAPROTECT 246
MI 632
IND 327
CODEC 1587

WETGEVINGSBESLUITEN EN ANDERE INSTRUMENTEN

Betreft:	VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD tot wijziging van Verordening (EU) 2019/881 wat betreft beheerde beveiligingsdiensten

VERORDENING (EU) 2024/…
VAN HET EUROPEES PARLEMENT EN DE RAAD

van …

tot wijziging van Verordening (EU) 2019/881 wat betreft beheerde beveiligingsdiensten

(Voor de EER relevante tekst)

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 114,

Gezien het voorstel van de Europese Commissie,

Na toezending van het ontwerp van wetgevingshandeling aan de nationale parlementen,

Gezien het advies van het Europees Economisch en Sociaal Comité[1],

Na raadpleging van het Comité van de Regio's,

Handelend volgens de gewone wetgevingsprocedure[2],

---

1 PB C 349 van 29.9.2023, blz. 167.

2 Standpunt van het Europees Parlement van 24 april 2024 (nog niet in het Publicatieblad bekendgemaakt) en besluit van de Raad van ....

Overwegende hetgeen volgt:

(1) Verordening (EU) 2019/881 van het Europees Parlement en de Raad[3] voorziet in een kader voor de vaststelling van Europese cyberbeveiligingscertificeringsregelingen teneinde een toereikend cyberbeveiligingsniveau van ICT (informatie- en communicatietechnologie)-producten, -diensten en -processen in de Unie te waarborgen, alsook om versnippering van de interne markt wat betreft cyberbeveiligingscertificeringsregelingen in de Unie te vermijden.

[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) (PB L 151 van 7.6.2019, blz. 15).

(2) Om ervoor te zorgen dat de Unie bestand is tegen cyberaanvallen en om kwetsbaarheden in de interne markt te voorkomen, is deze verordening bedoeld als aanvulling op het horizontale regelgevingskader tot vaststelling van uitgebreide cyberbeveiligingsvereisten voor producten met digitale elementen overeenkomstig Verordening (EU) 2024/… van het Europees Parlement en de Raad[4+], door beveiligingsdoelstellingen te bepalen voor beheerde beveiligingsdiensten alsook voor de toepassing en de betrouwbaarheid van die diensten.

---

4 Verordening (EU) 2024/… van het Europees Parlement en de Raad van … betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordeningen (EU) nr. 168/2013 en (EU) 2019/1020 en Richtlijn (EU) 2020/1828 (Verordening cyberweerbaarheid) (PB L, …, ELI: …).

\+ PB: gelieve in de tekst het nummer van de verordening in document PE-CONS 100/23 (2022/0272(COD)) in te voegen, en in de overeenkomstige voetnoot het nummer, de datum, de publicatiegegevens en de ELI-referentie daarvan.

(3) Beheerde beveiligingsdiensten worden verleend door aanbieders van beheerde beveiligingsdiensten zoals gedefinieerd in artikel 6, punt 40), van Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad[5]. De definitie van beheerde beveiligingsdiensten in deze verordening moet daarom stroken met die van aanbieders van beheerde beveiligingsdiensten in Richtlijn (EU) 2022/2555. Die diensten bestaan uit het uitvoeren van of het verlenen van bijstand voor activiteiten die verband houden met de beheersing van het cyberbeveiligingsrisico van hun klanten en zijn steeds belangrijker geworden bij de preventie en beperking van incidenten. De aanbieders van die diensten worden dan ook beschouwd als essentiële of belangrijke entiteiten die behoren tot een zeer kritieke sector overeenkomstig Richtlijn (EU) 2022/2555. Zoals aangegeven in overweging 86 van die richtlijn spelen dat aanbieders van beheerde beveiligingsdiensten op het gebied van bijvoorbeeld incidentrespons, penetratietesten, beveiligingsaudits en consultancy een bijzonder belangrijke rol in het bijstaan van entiteiten bij hun inspanningen om incidenten te voorkomen, op te sporen, erop te reageren en ervan te herstellen. Aanbieders van beheerde beveiligingsdiensten zijn echter ook zelf het doelwit van cyberaanvallen geweest en vormen een bijzonder risico vanwege hun nauwe integratie in de activiteiten van hun klanten. Het is daarom belangrijk dat essentiële en belangrijke entiteiten in de zin van Richtlijn (EU) 2022/2555 nog meer zorgvuldigheid betrachten bij de selectie van aanbieders van beheerde beveiligingsdiensten.

---

[5] Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gemeenschappelijk 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 (NIS 2-richtlijn) (PB L 333 van 27.12.2022, blz. 80).

(4) De definitie van beheerde beveiligingsdiensten in het kader van deze verordening omvat een niet-uitputtende lijst van beheerde beveiligingsdiensten die in aanmerking kunnen komen voor Europese cyberbeveiligingscertificeringsregelingen, zoals incidentenbehandeling, penetratietests, beveiligingsaudits, en adviesdiensten in verband met technische ondersteuning. Beheerde beveiligingsdiensten kunnen cyberbeveiligingsdiensten omvatten die de paraatheid voor, de preventie, opsporing, analyse en beperking van, de respons op en het herstel van incidenten ondersteunen. Het verstrekken van inlichtingen over cyberdreigingen en risicobeoordelingen in verband met technische ondersteuning kunnen ook worden aangemerkt als beheerde beveiligingsdiensten. Voor verschillende beheerde beveiligingsdiensten kunnen aparte Europese cyberbeveiligingscertificeringsregelingen bestaan. De overeenkomstig dergelijke regelingen afgegeven Europese cyberbeveiligingscertificaten moeten betrekking hebben op specifieke beheerde beveiligingsdiensten van een specifieke aanbieder van die diensten.

(5) Aanbieders van beheerde beveiligingsdiensten kunnen ook een belangrijke rol spelen met betrekking tot acties van de Unie ter ondersteuning van de respons en het initiële herstel in geval van significante en grootschalige cyberbeveiligingsincidenten, waarbij zij vertrouwen op diensten van betrouwbare particuliere aanbieders en op het testen van kritieke entiteiten op mogelijke kwetsbaarheden op basis van op Unieniveau gecoördineerde beveiligingsrisicobeoordelingen. De certificering van beheerde beveiligingsdiensten kan een rol spelen bij de selectie van betrouwbare aanbieders van beheerde beveiligingsdiensten zoals gedefinieerd in Verordening (EU) …/… van het Europees Parlement en de Raad[6+].

(6) De certificering van beheerde beveiligingsdiensten is niet alleen relevant bij de selectie voor de EU-cyberbeveiligingsreserve die is ingesteld bij Verordening (EU) …/…[++], maar is ook een essentiële kwaliteitsindicator voor particuliere en publieke entiteiten die van plan zijn dergelijke diensten aan te kopen. Gezien het kritieke karakter van beheerde beveiligingsdiensten en de gevoeligheid van de gegevens die worden verwerkt, kan certificering potentiële klanten belangrijke aanwijzingen en zekerheid bieden over de betrouwbaarheid van die diensten. Europese cyberbeveiligingscertificeringsregelingen voor beheerde beveiligingsdiensten dienen ertoe bij te dragen versnippering van de interne markt te voorkomen. Deze verordening heeft derhalve tot doel de werking van de interne markt te verbeteren.

---

6 Verordening (EU) .../... van het Europees Parlement en de Raad van ... tot vaststelling van maatregelen ter versterking van de solidariteit en de capaciteit in de Unie om cyberdreigingen en -incidenten op te sporen, zich erop voor te bereiden en erop te reageren en tot wijziging van Verordening (EU) 2021/694 (verordening cybersolidariteit) (PB L, ..., ELI: ...).

\+ PB: gelieve in de tekst het nummer van de verordening in document PE-CONS 94/24 (2023/0109(COD)) in te voegen, en in de overeenkomstige voetnoot het nummer, de datum, de publicatiegegevens en de ELI-referentie daarvan.

++ PB: gelieve in de tekst het nummer van de verordening in document PE-CONS 94/24 (2023/0109(COD)) in te voegen.

(7) Europese cyberbeveiligingscertificeringsregelingen voor beheerde beveiligingsdiensten moeten het gebruik van deze diensten stimuleren en de concurrentie tussen aanbieders van beheerde beveiligingsdiensten bevorderen. Onverminderd de doelstelling om een toereikend en passend niveau van relevante technische kennis en beroepsintegriteit van dergelijke aanbieders te waarborgen, moeten dergelijke certificeringsregelingen daarom de markttoegang en het aanbieden van beheerde beveiligingsdiensten vergemakkelijken door, voor zover mogelijk, de potentiële regelgevings-, administratieve en financiële lasten voor aanbieders, met name kleine en middelgrote ondernemingen, met inbegrip van micro-ondernemingen, te vereenvoudigen wanneer zij beheerde beveiligingsdiensten aanbieden. Daarnaast moeten Europese cyberbeveiligingscertificeringsregelingen, om het gebruik van beheerde beveiligingsdiensten aan te moedigen en de vraag ernaar te stimuleren, een bijdrage leveren aan de toegankelijkheid van deze diensten, met name voor kleinere actoren, zoals kleine en middelgrote ondernemingen, met inbegrip van micro-ondernemingen, alsook lokale en regionale overheden die over een beperkte capaciteit en beperkte middelen beschikken maar die gevoeliger zijn voor inbreuken op de cyberbeveiliging die financiële, juridische en operationele gevolgen kunnen hebben en kunnen leiden tot reputatieschade.

(8) Het is belangrijk kleine en middelgrote ondernemingen, met inbegrip van micro-ondernemingen, te ondersteunen bij de uitvoering van deze verordening en bij de aanwerving van personeel met de gespecialiseerde vaardigheden en deskundigheid op het gebied van cyberbeveiliging die nodig zijn om beheerde beveiligingsdiensten te verlenen overeenkomstig de in deze verordening vastgestelde vereisten. In het programma Digitaal Europa, opgericht bij Verordening (EU) 2021/694 van het Europees Parlement en de Raad[7] en andere relevante programma's van de Unie is bepaald dat de Commissie financiële en technische ondersteuning moet bieden die die ondernemingen in staat stelt bij te dragen aan de groei van de economie van de Unie en aan de versterking van het gemeenschappelijke niveau van cyberbeveiliging in de Unie, onder meer door de financiële steun uit het programma Digitaal Europa en andere relevante programma's van de Unie te stroomlijnen en door kleine en middelgrote ondernemingen, met inbegrip van micro-ondernemingen, te ondersteunen.

(9) De Europese cyberbeveiligingscertificeringsregelingen voor beheerde beveiligingsdiensten van de Unie moeten bijdragen aan de beschikbaarheid van beveiligde en hoogwaardige diensten waarmee een veilige digitale transitie wordt gewaarborgd, en aan de verwezenlijking van de streefcijfers in het kader van het beleidsprogramma voor het digitale decennium tot 2030, ingesteld bij Besluit (EU) 2022/2481 van het Europees Parlement en de Raad[8], met name de doelstelling om ervoor te zorgen dat ten minste 75 % van de ondernemingen in de Unie gebruikmaakt van cloudcomputingdiensten, big data of artificiële intelligentie, de doelstelling om ervoor te zorgen dat meer dan 90 % van kleine en middelgrote ondernemingen, met inbegrip van micro-ondernemingen, ten minste een basisniveau van digitale intensiteit haalt en de doelstelling om ervoor te zorgen dat belangrijke overheidsdiensten toegankelijk zijn.

---

7 Verordening (EU) 2021/694 van het Europees Parlement en de Raad van 29 april 2021 tot oprichting van het programma Digitaal Europa en tot intrekking van Besluit (EU) 2015/2240 (PB L 166 van 11.5.2021, blz. 1).

8 Besluit (EU) 2022/2481 van het Europees Parlement en de Raad van 14 december 2022 tot vaststelling van het beleidsprogramma voor het digitale decennium tot 2030 (PB L 323 van 19.12.2022, bl. 4).

(10) Naast de uitrol van ICT-producten, -diensten of -processen bieden aanbieders van beheerde beveiligingsdiensten vaak aanvullende diensten aan die afhankelijk zijn van de competenties, deskundigheid en ervaring van het personeel van de aanbieders van dergelijke diensten. Een zeer hoog niveau van die competenties, deskundigheid en ervaring, alsook passende interne procedures moeten deel uitmaken van de beveiligingsdoelstellingen om te waarborgen dat de verleende beheerde beveiligingsdiensten van zeer hoge kwaliteit zijn. Om ervoor te zorgen dat alle aspecten van beheerde beveiligingsdiensten onder specifieke Europese cyberbeveiligingscertificeringsregelingen kunnen vallen, moet Verordening (EU) 2019/881 worden gewijzigd. Er moet rekening worden gehouden met de resultaten en aanbevelingen van de evaluatie en toetsing waarin Verordening (EU) 2019/881 voorziet.

(11) Met het oog op de bevordering van de groei van een betrouwbare interne markt en de totstandbrenging van partnerschappen met gelijkgestemde derde landen moet het certificeringsproces dat wordt vastgesteld binnen het bij Verordening (EU) 2019/881 vastgestelde kader voor Europese cyberbeveiligingscertificeringsregelingen worden uitgevoerd op een wijze die internationale erkenning en afstemming op internationale normen vergemakkelijkt.

(12) De Unie heeft te kampen met een tekort aan geschoolde professionals en een snel evoluerend dreigingslandschap, wat ook wordt erkend in de mededeling van de Commissie van 18 april 2023 met als titel “Wegwerken van het tekort aan cyberbeveiligingsprofessionals om het concurrentievermogen, de groei en de veerkracht van Europa te versterken (“De academie voor cyberbeveiligingsvaardigheden”)”. De leermiddelen en formele opleidingsvormen zijn gevarieerd en kennis kan op verschillende manieren worden verworven: door middel van formeel leren, bijvoorbeeld aan universiteiten of via cursussen, of door middel van informeel leren, bijvoorbeeld via opleiding op de werkplek of werkervaring op het betreffende gebied. Om de totstandbrenging van hoogwaardige beheerde beveiligingsdiensten te stimuleren en meer inzicht te verkrijgen in de samenstelling van de beroepsbevolking van de Unie die werkzaam is in de cyberbeveiliging, is het dan ook belangrijk dat de samenwerking tussen de lidstaten, de Commissie, het Agentschap van de Europese Unie voor cyberbeveiliging, opgericht bij Verordening (EU) 2019/881 (“Enisa”) en de verschillende belanghebbenden, waaronder de particuliere sector en de academische wereld, wordt versterkt en dat er publiek-private partnerschappen worden opgezet, initiatieven op het gebied van onderzoek en innovatie worden ondersteund en wordt gewerkt aan de ontwikkeling en wederzijdse erkenning van gemeenschappelijke normen en de certificering van cyberbeveiligingsvaardigheden, onder meer via het Europees kader voor cyberbeveiligingsvaardigheden. Een dergelijke samenwerking zou tevens de mobiliteit van cyberbeveiligingsprofessionals in de Unie ten goede komen en bijdragen aan de integratie van kennis en scholing op het gebied van cyberbeveiliging in onderwijsprogramma´s, waarbij de toegang van jongeren, waaronder mensen die in achtergestelde regio´s wonen, zoals eilanden en dunbevolkte, plattelands- en afgelegen gebieden, tot leerlingplaatsen en stages gewaarborgd moet worden. Het is belangrijk dat dergelijke samenwerking erop gericht is meer vrouwen en meisjes op dit gebied aan te trekken en bijdraagt aan het dichten van de genderkloof op het vlak van wetenschap, technologie, engineering en wiskunde, en dat de particuliere sector opleidingen op de werkplek tracht aan te bieden die gericht zijn op de meest gevraagde vaardigheden, waarbij overheidsdiensten en start-ups, alsook kleine en middelgrote ondernemingen, met inbegrip van micro-ondernemingen worden betrokken. Het is ook belangrijk dat aanbieders en de lidstaten samenwerken en bijdragen aan de verzameling van gegevens over de situatie en de ontwikkelingen op de cyberbeveiligingsarbeidsmarkt.

(13) Enisa speelt een belangrijke rol bij de voorbereiding van potentiële Europese cyberbeveiligingscertificeringsregelingen. Bij de opstelling van het ontwerp van algemene begroting van de Unie moet de Commissie volgens de procedure van artikel 29 van Verordening (EU) 2019/881 beoordelen welke begrotingsmiddelen de personeelsformatie van Enisa daarvoor nodig heeft.

(14) Deze verordening voorziet in gerichte wijzigingen van Verordening (EU) 2019/881 om het mogelijk te maken om Europese cyberbeveiligingscertificeringsregelingen voor beheerde beveiligingsdiensten vast te stellen. Daarbij wordt ook een aantal bepalingen van die verordening gespecificeerd en verduidelijkt met betrekking tot de voorbereiding en werking van alle Europese cyberbeveiligingscertificeringsregelingen, teneinde de transparantie en openheid ervan te waarborgen. Laatstgenoemde wijzigingen, die beperkt zijn tot de specificatie of verduidelijking van Verordening (EU) 2019/881, met name de wijzigingen betreffende de informatie die Enisa moet verstrekken bij toezending van de potentiële regeling, de voor elke potentiële regeling opgerichte ad-hocwerkgroepen, en informatie en raadpleging met betrekking tot Europese cyberbeveiligingscertificeringsregelingen, mogen op geen enkele wijze vooruitlopen op de krachtens artikel 67 van die verordening vereiste bredere evaluatie en toetsing, met name de evaluatie van de gevolgen, de doeltreffendheid en de efficiëntie van de titel van die verordening met betrekking tot het cyberbeveiligingscertificeringskader. De evaluatie en toetsing van die titel moeten gebaseerd zijn op een brede raadpleging van belanghebbenden en een volledige en grondige analyse van de betrokken procedures.

(15) Daar de doelstelling van deze verordening, namelijk het mogelijk maken om Europese cyberbeveiligingscertificeringsregelingen voor beheerde beveiligingsdiensten vast te stellen, niet voldoende door de lidstaten kan worden verwezenlijkt, maar vanwege de omvang en de gevolgen ervan beter door de Unie kan worden verwezenlijkt, kan de Unie, overeenkomstig het in artikel 5 van het Verdrag betreffende de Europese Unie neergelegde subsidiariteitsbeginsel, maatregelen nemen. Overeenkomstig het in hetzelfde artikel neergelegde evenredigheidsbeginsel gaat deze verordening niet verder dan nodig is om die doelstelling te verwezenlijken.

(16) Overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad[9] is de Europese Toezichthouder voor gegevensbescherming geraadpleegd, en op 10 januari 2024 heeft hij een advies uitgebracht,

HEBBEN DE VOLGENDE VERORDENING VASTGESTELD:

[9] Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG (PB L 295 van 21.11.2018, blz. 39).

Artikel 1

Wijzigingen van Verordening (EU) 2019/881

Verordening (EU) 2019/881 wordt als volgt gewijzigd:

1) in artikel 1, lid 1, eerste alinea, wordt punt b) vervangen door:

"b) een kader voor de vaststelling van Europese cyberbeveiligingscertificeringsregelingen teneinde een toereikend cyberbeveiligingsniveau van ICT-producten, -diensten en -processen en beheerde beveiligingsdiensten in de Unie te waarborgen, alsmede om versnippering van de interne markt wat betreft cyberbeveiligingscertificeringsregelingen in de Unie te vermijden.";

2) artikel 2 wordt als volgt gewijzigd:

a) de punten 9, 10 en 11 worden vervangen door:

"9) "Europese cyberbeveiligingscertificeringsregeling": een uitvoerige reeks voorschriften, technische vereisten, normen en procedures die op Unieniveau zijn vastgesteld en die van toepassing zijn op de certificering of conformiteitsbeoordeling van specifieke ICT-producten, -diensten en -processen of beheerde beveiligingsdiensten;

10) “nationale cyberbeveiligingscertificeringsregeling”: een uitvoerige reeks voorschriften, technische vereisten, normen en procedures die door een nationale overheidsinstantie zijn ontwikkeld en vastgesteld en die van toepassing zijn op de certificering of conformiteitsbeoordeling van ICT-producten, -diensten en -processen of beheerde beveiligingsdiensten die binnen het toepassingsgebied van de specifieke regeling vallen;

11) “Europees cyberbeveiligingscertificaat”: een door een bevoegde instantie afgegeven document waarin wordt bevestigd dat is geëvalueerd of een bepaald ICT-product, een bepaalde ICT-dienst, een bepaald ICT-proces of een bepaalde beheerde beveiligingsdienst voldoet aan de specifieke, in een Europese cyberbeveiligingscertificeringsregeling vastgestelde beveiligingsvoorschriften;”;

b) het volgende punt wordt ingevoegd:

“14 bis) “beheerde beveiligingsdienst”: een aan een derde verleende dienst die bestaat uit het uitvoeren van of het verlenen van bijstand voor activiteiten die verband houden met de beheersing van cyberbeveiligingsrisico’s, zoals incidentenbehandeling, penetratietesten, beveiligingsaudits en adviesdiensten, met inbegrip van deskundig advies in verband met technische ondersteuning;”;

c) de punten 20, 21 en 22 worden vervangen door:

"20) "technische specificatie": een document waarin de technische vereisten of conformiteitsbeoordelingsprocedures zijn voorgeschreven waaraan een ICT-product, ICT-dienst, ICT-proces of beheerde beveiligingsdienst moet voldoen;

21) "zekerheidsniveau": een basis voor vertrouwen dat een ICT-product, -dienst of -proces of een beheerde beveiligingsdienst aan de beveiligingsvoorschriften van een specifieke Europese cyberbeveiligingscertificeringsregeling voldoet, die aangeeft op welk niveau het betrokken ICT-product, de betrokken ICT-dienst, het betrokken ICT-proces of de betrokken beheerde beveiligingsdienst is geëvalueerd maar als zodanig geen maatstaf is voor de beveiliging van het betrokken ICT-product, de betrokken ICT-dienst, het betrokken ICT-proces of de betrokken beheerde beveiligingsdienst;

22) "conformiteitszelfbeoordeling": een maatregel die wordt uitgevoerd door een fabrikant of aanbieder van ICT-producten, -diensten of -processen of beheerde beveiligingsdiensten die evalueert of de ICT-producten, -diensten of -processen of beheerde beveiligingsdiensten voldoen aan de in een specifieke Europese cyberbeveiligingscertificeringsregeling opgenomen voorschriften.";

3) in artikel 4 wordt lid 6 vervangen door:

"6. Enisa bevordert het gebruik van Europese cyberbeveiligingscertificering om versnippering van de interne markt te vermijden. Enisa draagt bij tot het tot stand brengen en handhaven van een Europees cyberbeveiligingscertificeringskader overeenkomstig titel III van deze verordening, met het oog op een transparantere cyberbeveiliging van ICT-producten, -diensten en -processen en beheerde beveiligingsdiensten, waardoor het vertrouwen in de digitale interne markt en haar concurrentievermogen wordt versterkt.";

4) artikel 8 wordt als volgt gewijzigd:

a) lid 1 wordt als volgt gewijzigd:

i) de aanhef wordt vervangen door:

"1. Enisa ondersteunt en bevordert de ontwikkeling en uitvoering van het Uniebeleid inzake de cyberbeveiligingscertificering van ICT-producten, -diensten en -processen en beheerde beveiligingsdiensten, zoals vastgesteld in titel III van deze verordening, door:";

ii) punt b) wordt vervangen door:

"b) potentiële Europese cyberbeveiligingscertificeringsregelingen (potentiële regelingen) voor ICT-producten, -diensten en -processen en beheerde beveiligingsdiensten voor te bereiden overeenkomstig artikel 49;";

b) lid 3 wordt vervangen door:

"3. Enisa stelt richtsnoeren op en maakt die bekend, en ontwikkelt goede praktijken, wat betreft de cyberbeveiligingsvoorschriften voor ICT-producten, -diensten en -processen en beheerde beveiligingsdiensten, in samenwerking met de nationale cyberbeveiligingscertificeringsautoriteiten en de sector in een formeel, gestructureerd en transparant proces.";

c) lid 5 wordt vervangen door:

"5. Enisa vergemakkelijkt de opstelling en toepassing van Europese en internationale normen voor risicobeheersing en voor de beveiliging van ICT-producten, -diensten en -processen en beheerde beveiligingsdiensten.";

5) artikel 46 wordt vervangen door:

"*Artikel 46*

Europees cyberbeveiligingscertificeringskader

1. Het Europees cyberbeveiligingscertificeringskader wordt ingesteld teneinde de omstandigheden voor de werking van de interne markt te verbeteren, en wel middels een verhoging van het cyberbeveiligingsniveau in de Unie en het mogelijk maken van een geharmoniseerde aanpak op Unieniveau van Europese cyberbeveiligingscertificeringsregelingen, met als doel de totstandbrenging van een digitale eengemaakte markt voor ICT-producten, -diensten en -processen en beheerde beveiligingsdiensten.

2. Het Europees cyberbeveiligingscertificeringskader voorziet in een mechanisme voor de instelling van Europese cyberbeveiligingscertificeringsregelingen en om te waarborgen dat ICT-producten, -diensten en -processen die door middel van dergelijke regelingen zijn geëvalueerd, aan gespecificeerde beveiligingsvoorschriften voldoen met als doel de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of de functies of diensten die via die producten, diensten en processen worden aangeboden of toegankelijk zijn, te beschermen gedurende hun gehele levenscyclus. Voorts waarborgt het dat beheerde beveiligingsdiensten die door middel van dergelijke regelingen zijn geëvalueerd, aan gespecificeerde beveiligingsvoorschriften voldoen met als doel de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens die in verband met de verlening van die diensten worden opgevraagd, verwerkt, opgeslagen of verzonden, te beschermen, en dat die diensten permanent met de vereiste bekwaamheid, deskundigheid en ervaring worden verleend door personeel met een voldoende en passend niveau van relevante technische kennis en professionele integriteit.";

6) artikel 47 wordt als volgt gewijzigd:

a) lid 2 wordt vervangen door:

"2. Het voortschrijdend werkprogramma van de Unie omvat met name een lijst van ICT-producten, -diensten en -processen, alsook beheerde beveiligingsdiensten, of categorieën daarvan, die kunnen worden opgenomen in het toepassingsgebied van een Europese cyberbeveiligingscertificeringsregeling.";

b) lid 3 wordt als volgt gewijzigd:

i) de inleidende tekst wordt vervangen door:

"3. De opname in het voortschrijdend werkprogramma van de Unie van specifieke ICT-producten, -diensten en -processen of beheerde beveiligingsdiensten, of categorieën daarvan, geschiedt op een of meer van de volgende gronden:"

ii) punt a) wordt vervangen door:

"a) de beschikbaarheid en ontwikkeling van nationale cyberbeveiligingscertificeringsregelingen voor een specifieke categorie ICT-producten, -diensten of -processen of beheerde beveiligingsdiensten en met name ten aanzien van het risico op versnippering;";

iii) het volgende punt wordt ingevoegd:

"c bis) technologische ontwikkelingen en de beschikbaarheid en ontwikkeling van internationale cyberbeveiligingscertificeringsregelingen en internationale normen en door de industrie gebruikte normen;";

7) artikel 49 wordt als volgt gewijzigd:

a) de leden 1 tot en met 4 worden vervangen door:

"1. Naar aanleiding van een verzoek van de Commissie overeenkomstig artikel 48 bereidt Enisa een potentiële regeling voor die voldoet aan de in de artikelen 51, 51 bis, 52 en 54 bepaalde toepasselijke voorschriften.

2. Naar aanleiding van een verzoek van de EGC overeenkomstig artikel 48, lid 2, kan Enisa een potentiële regeling opstellen die voldoet aan de in de artikelen 51, 51 bis, 52 en 54 bepaalde toepasselijke eisen. Indien Enisa een dergelijk verzoek afwijst, motiveert het zijn afwijzing. Een besluit tot afwijzing van een dergelijk verzoek wordt genomen door de raad van bestuur.

3. Bij de opstelling van een potentiële regeling, raadpleegt Enisa tijdig door middel van een formele, open, transparante en inclusieve raadplegingsprocedure alle betrokken partijen. Bij de toezending van de potentiële regeling aan de Commissie overeenkomstig lid 6, verstrekt Enisa informatie over de wijze waarop het aan dit lid heeft voldaan.

4. Voor elke potentiële regeling stelt Enisa overeenkomstig artikel 20, lid 4, een ad-hocwerkgroep in, met het doel Enisa van specifiek advies en expertise te voorzien. Die ad-hocwerkgroepen omvatten, in voorkomend geval en onverminderd de in artikel 20, lid 4, vastgestelde procedures en keuzevrijheid, deskundigen van de overheidsdiensten van de lidstaten, de instellingen, organen en instanties van de Unie en de particuliere sector.";

b) lid 7 wordt vervangen door:

"7. Op basis van de door Enisa opgestelde potentiële regeling kan de Commissie uitvoeringshandelingen vaststellen om te voorzien in een Europese cyberbeveiligingscertificeringsregeling voor ICT-producten, -diensten en -processen en beheerde beveiligingsdiensten die voldoen aan de in de artikelen 51, 51 bis, 52 en 54 bepaalde relevante voorschriften. Die uitvoeringshandelingen worden vastgesteld overeenkomstig de in artikel 66, lid 2, bedoelde onderzoeksprocedure.";

8) het volgende artikel wordt ingevoegd:

"*Artikel 49 bis*

Informatie en raadpleging over Europese cyberbeveiligingscertificeringsregelingen

1. De Commissie maakt de informatie over haar in artikel 48 bedoelde verzoek aan Enisa om een potentiële regeling op te stellen of een bestaande Europese cyberbeveiligingscertificeringsregeling te herzien, openbaar.

2. Tijdens de opstelling van een potentiële regeling door Enisa overeenkomstig artikel 49 kunnen het Europees Parlement, de Raad, of beide, de Commissie in haar hoedanigheid van voorzitter van de EGC, en Enisa verzoeken om driemaandelijks relevante informatie over een ontwerp van potentiële regeling te verstrekken. Op verzoek van het Europees Parlement of de Raad kan Enisa, in overleg met de Commissie, en onverminderd artikel 27, relevante delen van een ontwerp van potentiële regeling ter beschikking stellen van het Europees Parlement en de Raad op een wijze die past bij het vereiste vertrouwelijkheidsniveau, en in voorkomend geval op beperkte wijze.

3. Om de dialoog tussen de instellingen van de Unie te versterken en bij te dragen tot een formeel, open, transparant en inclusief raadplegingsproces, kunnen het Europees Parlement, de Raad, of beide, de Commissie en Enisa verzoeken kwesties te bespreken met betrekking tot de werking van Europese cyberbeveiligingscertificeringsregelingen voor ICT-producten, -diensten en -processen of beheerde beveiligingsdiensten.

4. De Commissie houdt bij de evaluatie van deze verordening overeenkomstig artikel 67 in voorkomend geval rekening met elementen die voortvloeien uit de standpunten van het Europees Parlement en van de Raad over de in lid 3 van dit artikel bedoelde aangelegenheden.”;

9) artikel 51 wordt als volgt gewijzigd:

a) de titel wordt vervangen door:

“*Beveiligingsdoelstellingen van Europese cyberbeveiligingscertificeringsregelingen voor ICT-producten, -diensten en -processen*”

b) de inleidende zin wordt vervangen door:

“De opzet van een Europese cyberbeveiligingscertificeringsregeling voor ICT-producten, -diensten of -processen is van dien aard dat, voor zover van toepassing, ten minste de volgende beveiligingsdoelstellingen worden verwezenlijkt:”;

10) het volgende artikel wordt ingevoegd:

"*Artikel 51 bis*
Beveiligingsdoelstellingen van Europese cyberbeveiligingscertificeringsregelingen voor beheerde beveiligingsdiensten

De opzet van een Europese cyberbeveiligingscertificeringsregeling voor beheerde beveiligingsdiensten is van dien aard dat, voor zover van toepassing, ten minste de volgende beveiligingsdoelstellingen worden verwezenlijkt:

a) dat de beheerde beveiligingsdiensten worden verleend met de vereiste bekwaamheid, deskundigheid en ervaring, en dat het personeel dat belast is met het verlenen van die diensten beschikt over een voldoende en passend niveau van technische kennis en bekwaamheid op het specifieke gebied, over voldoende en passende ervaring en over de hoogste mate van professionele integriteit;

b) dat de aanbieder over passende interne procedures beschikt om te waarborgen dat de beheerde beveiligingsdiensten te allen tijde op een voldoende en passend kwaliteitsniveau worden verleend;

c) dat gegevens die in verband met de verlening van beheerde beveiligingsdiensten zijn opgevraagd, opgeslagen, verzonden of anderszins zijn verwerkt, worden beschermd tegen onopzettelijk(e) of ongeoorloofd(e) toegang, opslag, openbaarmaking, vernietiging, andere verwerking, verlies of wijziging of onbeschikbaarheid;

d) dat in geval van een fysiek of technisch incident de beschikbaarheid van en de toegang tot gegevens, diensten en functies tijdig worden hersteld;

e) dat bevoegde personen, programma's of machines uitsluitend toegang kunnen hebben tot de gegevens, diensten of functies waarvoor hun recht van toegang geldt;

f) dat een register wordt bijgehouden en beschikbaar is om na te gaan, op welk tijdstip en door wie gegevens, diensten of functies zijn ingezien, zijn gebruikt of anderszins zijn verwerkt;

g) dat de ICT-producten, -diensten en -processen die bij de verlening van de beheerde beveiligingsdiensten worden ingezet, qua ontwerp en standaard veilig zijn en, in voorkomend geval, voorzien zijn van de recentste beveiligingsupdates en geen bekende kwetsbaarheden bevatten.";

11) artikel 52 wordt als volgt gewijzigd:

a) lid 1 wordt vervangen door:

"1. In een Europese cyberbeveiligingscertificeringsregeling kunnen voor ICT-producten, -diensten en -processen en beheerde beveiligingsdiensten een of meer van de volgende zekerheidsniveaus worden gespecificeerd: "basis", "substantieel" of "hoog". Het zekerheidsniveau staat in verhouding tot het niveau van risico dat verbonden is aan het beoogde gebruik van een ICT-product, -dienst of -proces of beheerde beveiligingsdienst, wat betreft de waarschijnlijkheid en de gevolgen van een incident.";

b) lid 3 wordt vervangen door:

"3. In de betrokken Europese cyberbeveiligingscertificeringsregeling worden de overeenkomstige beveiligingsvoorschriften voor elk zekerheidsniveau bepaald, waaronder de overeenkomstige beveiligingsfuncties en de overeenkomstige grondigheid en diepgang van de evaluatie waaraan dat ICT-product, die ICT-dienst, dat ICT-proces of die beheerde beveiligingsdienst wordt onderworpen.";

c) de leden 5, 6 en 7 worden vervangen door:

"5. Een Europees cyberbeveiligingscertificaat of EU-conformiteitsverklaring voor het zekerheidsniveau "basis" biedt de zekerheid dat de ICT-producten, -diensten of -processen of beheerde beveiligingsdiensten waarvoor dat certificaat of die EU-conformiteitsverklaring is afgegeven, voldoen aan de overeenkomstige beveiligingsvoorschriften, waaronder beveiligingsfuncties, en dat zij geëvalueerd zijn op het niveau dat bedoeld is om de bekende basisrisico's van cyberincidenten en -aanvallen tot een minimum te beperken. De te ondernemen evaluatiewerkzaamheden behelzen ten minste een toetsing van technische documenten. Indien een dergelijke toetsing niet geschikt is, worden vervangende gelijkwaardige evaluatiewerkzaamheden ondernomen.

6. Een Europees cyberbeveiligingscertificaat voor het zekerheidsniveau "substantieel" biedt de zekerheid dat de ICT-producten, -diensten of -processen of beheerde beveiligingsdiensten waarvoor dat certificaat is afgegeven, voldoen aan de overeenkomstige beveiligingsvoorschriften, waaronder beveiligingsfuncties, en dat zij geëvalueerd zijn op een niveau dat bedoeld is om de bekende cyberbeveiligingsrisico's, en het risico op cyberincidenten en -aanvallen door actoren met beperkte vaardigheden en middelen, tot een minimum te beperken. De te ondernemen evaluatiewerkzaamheden behelzen ten minste het volgende: verifiëren dat er geen algemeen bekende kwetsbaarheden zijn, en testen of bij de ICT-producten, -diensten of -processen of beheerde beveiligingsdiensten de benodigde beveiligingsfuncties correct worden toegepast. Indien dergelijke evaluatiewerkzaamheden niet geschikt zijn, worden vervangende gelijkwaardige evaluatiewerkzaamheden ondernomen.

7. Een Europees cyberbeveiligingscertificaat voor het zekerheidsniveau “hoog” biedt de zekerheid dat de ICT-producten, -diensten of -processen of beheerde beveiligingsdiensten waarvoor dat certificaat is afgegeven, voldoen aan de overeenkomstige beveiligingsvoorschriften, waaronder beveiligingsfuncties, en dat zij geëvalueerd zijn op een niveau dat bedoeld is om het risico van geavanceerde cyberaanvallen door actoren met aanzienlijke vaardigheden en middelen, tot een minimum te beperken. De te ondernemen evaluatiewerkzaamheden behelzen ten minste het volgende: verifiëren dat er geen algemeen bekende kwetsbaarheden zijn; testen of bij de ICT-producten, -diensten of -processen of beheerde beveiligingsdiensten de benodigde beveiligingsfuncties volgens de huidige stand van de techniek correct worden toegepast; en testen van hun weerbaarheid tegen deskundige aanvallers door middel van penetratietests. Indien dergelijke evaluatiewerkzaamheden niet geschikt zijn, worden vervangende gelijkwaardige evaluatiewerkzaamheden ondernomen.”;

12) in artikel 53 worden de leden 1, 2 en 3 vervangen door:

“1. In een Europese cyberbeveiligingscertificeringsregeling mag worden bepaald dat een conformiteitszelfbeoordeling uitsluitend onder de verantwoordelijkheid van de fabrikant of aanbieder van ICT-producten, -diensten of -processen of beheerde beveiligingsdiensten wordt uitgevoerd. Conformiteitszelfbeoordelingen worden uitsluitend toegestaan voor ICT-producten, -diensten en -processen of beheerde beveiligingsdiensten met een laag risico dat overeenkomt met het zekerheidsniveau “basis”.

2. De fabrikant of aanbieder van ICT-producten, -diensten of -processen of beheerde beveiligingsdiensten kan een EU-conformiteitsverklaring afgeven waarin wordt verklaard dat is aangetoond dat aan de voorschriften van de regeling is voldaan. Door een dergelijke verklaring op te stellen, aanvaardt de fabrikant of aanbieder van ICT-producten, -diensten of -processen of beheerde beveiligingsdiensten verantwoordelijkheid voor de conformiteit van het ICT-product, de ICT-dienst, het ICT-proces of de beheerde beveiligingsdienst met de in die regeling bepaalde voorschriften.

3. De fabrikant of aanbieder van ICT-producten, -diensten of -processen of beheerde beveiligingsdiensten stelt de EU-conformiteitsverklaring, de technische documenten en alle andere relevante informatie over de conformiteit van de ICT-producten, ICT-diensten, ICT-processen of beheerde beveiligingsdiensten met de regeling ter beschikking van de overeenkomstig artikel 58 aangewezen nationale cyberbeveiligingscertificeringsautoriteit gedurende de termijn die is vastgesteld in de betrokken Europese cyberbeveiligingscertificeringsregeling. Aan de nationale cyberbeveiligingscertificeringsautoriteit en aan Enisa wordt een kopie van de EU-conformiteitsverklaring voorgelegd.”;

13) in artikel 54 wordt lid 1 als volgt gewijzigd:

a) punt a) wordt vervangen door:

“a) het onderwerp en het toepassingsgebied van de certificeringsregeling, met inbegrip van het type of de categorieën ICT-producten, -diensten of -processen of beheerde beveiligingsdiensten die eronder vallen;”;

b) punt g) wordt vervangen door:

"g) de specifieke evaluatiecriteria en -methoden, met inbegrip van soorten evaluaties, die worden gebruikt om aan te tonen dat de in de artikelen 51 en 51 bis genoemde toepasselijke beveiligingsdoelstellingen worden verwezenlijkt;";

c) punt j) wordt vervangen door:

"j) de regels voor het toezicht op de conformiteit van ICT-producten, -diensten of -processen of beheerde beveiligingsdiensten met de vereisten van de Europese cyberbeveiligingscertificaten of de EU-conformiteitsverklaringen, met inbegrip van mechanismen om aan te tonen dat de vermelde cyberbeveiligingsvoorschriften nog altijd worden nageleefd;";

d) punt l) wordt vervangen door:

"l) regels over de gevolgen voor ICT-producten, -diensten of -processen of beheerde beveiligingsdiensten die zijn gecertificeerd of waarvoor een EU-conformiteitsverklaring is afgegeven, maar die niet voldoen aan de voorschriften van de regeling;";

e) punt o) wordt vervangen door:

"o) een overzicht van nationale of internationale cyberbeveiligingscertificeringsregelingen die betrekking hebben op hetzelfde type of dezelfde categorieën ICT-producten, -diensten of -processen of beheerde beveiligingsdiensten, beveiligingsvoorschriften, evaluatiecriteria en -methoden en zekerheidsniveaus;";

f) punt q) wordt vervangen door:

"q) de beschikbaarheidstermijn van de EU-conformiteitsverklaring, de technische documentatie en alle andere relevante informatie die door de fabrikant of aanbieder van ICT-producten, -diensten of -processen of beheerde beveiligingsdiensten ter beschikking moet worden gesteld;";

14) artikel 56 wordt als volgt gewijzigd:

a) lid 1 wordt vervangen door:

"1. ICT-producten, -diensten en -processen en beheerde beveiligingsdiensten die zijn gecertificeerd uit hoofde van een overeenkomstig artikel 49 vastgestelde Europese cyberbeveiligingscertificeringsregeling worden geacht te voldoen aan de voorschriften van een dergelijke regeling.";

b) lid 3 wordt als volgt gewijzigd:

i) de eerste alinea wordt vervangen door:

"De 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 om te zorgen voor een passend niveau van cyberbeveiliging van ICT-producten, -diensten en -processen en, vanaf … [de datum van inwerkingtreding van deze verordening], beheerde beveiligingsdiensten in de Unie en om de werking van de interne markt te verbeteren. De eerste zulke beoordeling vindt uiterlijk op 31 december 2023 plaats en daaropvolgende beoordelingen vinden ten minste om de twee jaar daarna plaats. Op basis van de resultaten van die beoordelingen stelt de Commissie een lijst op van de onder een bestaande certificeringsregeling vallende ICT-producten, -diensten en -processen en beheerde beveiligingsdiensten die door een verplichte certificeringsregeling moeten worden gedekt.";

ii) de derde alinea wordt als volgt gewijzigd:

– punt a) wordt vervangen door:

“a) rekening houden met de gevolgen die de maatregelen hebben voor de fabrikanten of aanbieders van zulke ICT-producten, -diensten of -processen of beheerde beveiligingsdiensten en voor de gebruikers in termen van de kosten van die maatregelen, evenals de maatschappelijke of economische voordelen die voortvloeien uit de verwachte betere beveiliging voor de beoogde ICT-producten, -diensten of -processen of beheerde beveiligingsdiensten;”;

– punt d) wordt vervangen door:

“d) rekening houden met eventuele uitvoeringstermijnen, overgangsmaatregelen en overgangstermijnen, in het bijzonder betreffende de mogelijke gevolgen van de maatregelen voor de fabrikanten of aanbieders van ICT-producten, -diensten of -processen of beheerde beveiligingsdiensten, met inbegrip van de specifieke belangen en behoeften van kleine en middelgrote ondernemingen, met inbegrip van micro-ondernemingen;”;

c) de leden 7 en 8 worden vervangen door:

"7. De natuurlijke of rechtspersoon die zijn ICT-producten, -diensten of -processen of beheerde beveiligingsdiensten aan de certificering onderwerpt, stelt aan de overeenkomstig artikel 58 aangewezen nationale cyberbeveiligingscertificeringsautoriteit, indien deze autoriteit de instantie is die het Europees cyberbeveiligingscertificaat afgeeft, of aan de in artikel 60 bedoelde conformiteitsbeoordelingsinstantie alle informatie ter beschikking die nodig is voor de uitvoering van de certificering.

8. De houder van een Europees cyberbeveiligingscertificaat stelt de autoriteit of de instantie bedoeld in lid 7 in kennis van kwetsbaarheden of onregelmatigheden in verband met de beveiliging van een gecertificeerde ICT-product, -dienst of -proces of beheerde beveiligingsdienst die achteraf zijn vastgesteld en die gevolgen kunnen hebben voor de naleving van de met de certificering verband houdende voorschriften. Die autoriteit of de instantie stuurt die informatie onverwijld door naar de betrokken nationale cyberbeveiligingscertificeringsautoriteit.";

15) in artikel 57 worden de leden 1 en 2 vervangen door:

"1. Onverminderd lid 3 van dit artikel hebben nationale cyberbeveiligingscertificeringsregelingen en de daaraan verbonden procedures voor de ICT-producten, -diensten en -processen en beheerde beveiligingsdiensten die onder een Europese cyberbeveiligingscertificeringsregeling vallen, niet langer gevolgen vanaf de datum die wordt bepaald in de op grond van artikel 49, lid 7, vastgestelde uitvoeringshandeling. Nationale cyberbeveiligingscertificeringsregelingen en de daaraan verbonden procedures voor ICT-producten, -diensten en -processen en beheerde beveiligingsdiensten die niet onder een Europese cyberbeveiligingscertificeringsregeling vallen, blijven bestaan.

2. De lidstaten voeren geen nieuwe nationale cyberbeveiligingscertificeringsregelingen in voor ICT-producten, -diensten en -processen en beheerde beveiligingsdiensten die reeds onder een van kracht zijnde Europese cyberbeveiligingscertificeringsregeling vallen.";

16) artikel 58 wordt als volgt gewijzigd:

a) lid 7 wordt als volgt gewijzigd:

i) de punten a) en b) worden vervangen door:

"a) zien toe op en handhaven op grond van artikel 54, lid 1, punt j), in Europese cyberbeveiligingscertificeringsregelingen opgenomen regels voor toezicht op de conformiteit van ICT-producten, -diensten en -processen en beheerde beveiligingsdiensten met de voorschriften van de Europese cyberbeveiligingscertificaten die zijn afgegeven op hun respectieve grondgebieden, in samenwerking met andere betrokken markttoezichtautoriteiten;

b) monitoren de naleving door en handhaven de verplichtingen van de fabrikanten of aanbieders van ICT-producten, -diensten of -processen of beheerde beveiligingsdiensten die gevestigd zijn op hun respectieve grondgebieden en conformiteitszelfbeoordelingen verrichten, en zien met name toe op de naleving en handhaving van de in artikel 53, leden 2 en 3, en in de overeenkomstige Europese cyberbeveiligingscertificeringsregeling bepaalde verplichtingen;";

ii) punt h) wordt vervangen door:

"h) werken samen met andere nationale cyberbeveiligingscertificeringautoriteiten of andere overheidsinstanties, onder meer door informatie uit te wisselen over de mogelijke niet-conformiteit van ICT-producten, -diensten of -processen of beheerde beveiligingsdiensten met de voorschriften van deze verordening of met de voorschriften van specifieke Europese cyberbeveiligingscertificeringsregelingen; en";

b) lid 9 wordt vervangen door:

"9. Nationale cyberbeveiligingscertificeringsautoriteiten werken samen met elkaar en met de Commissie en wisselen met name informatie, ervaringen en goede praktijken uit op het vlak van cyberbeveiligingscertificering en technische vraagstukken met betrekking tot de cyberbeveiliging van ICT-producten, -diensten en -processen en beheerde beveiligingsdiensten.";

17) in artikel 59, lid 3, worden de punten b) en c) vervangen door:

"b) de procedures voor het toezicht op en de handhaving van de regels voor het toezicht op de conformiteit van ICT-producten, -diensten en -processen en beheerde beveiligingsdiensten met Europese cyberbeveiligingscertificaten op grond van artikel 58, lid 7, punt a);

c) de procedures voor de monitoring en handhaving van de verplichtingen van fabrikanten en aanbieders van ICT-producten, -diensten of -processen of beheerde beveiligingsdiensten op grond van artikel 58, lid 7, punt b);";

18) in artikel 67 worden de leden 2 en 3 vervangen door:

"2. Bij de evaluatie wordt ook gekeken naar de gevolgen, de doeltreffendheid en de efficiëntie van de bepalingen van titel III van deze verordening, met inbegrip van de procedures die leiden tot de vaststelling van Europese cyberbeveiligingscertificeringsregelingen en de empirische grondslagen daarvan, met betrekking tot de doelstellingen om een adequaat cyberbeveiligingsniveau van ICT-producten, -diensten en -processen en beheerde beveiligingsdiensten in de Unie te waarborgen en de werking van de interne markt te verbeteren.

3. Bij de evaluatie wordt beoordeeld of er voor cyberbeveiliging essentiële voorschriften voor toegang tot de interne markt nodig zijn om te voorkomen dat ICT-producten, -diensten en -processen en beheerde beveiligingsdiensten die niet aan de basisvoorschriften inzake cyberbeveiliging voldoen, de interne markt binnenkomen.";

19) de bijlage wordt gewijzigd overeenkomstig de bijlage bij deze verordening.

Artikel 2

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te …,

Voor het Europees Parlement	*Voor de Raad*
De voorzitter	*De voorzitter*

BIJLAGE

De bijlage bij Verordening (EU) 2019/881 wordt als volgt gewijzigd:

1) de punten 2 tot en met 5 worden vervangen door:

"2. Een conformiteitsbeoordelingsinstantie is een derde instantie die onafhankelijk is van de door haar beoordeelde organisatie of ICT-producten, -diensten en -processen of beheerde beveiligingsdiensten.

3. Een instantie die behoort tot een branche- of beroepsorganisatie die ondernemingen vertegenwoordigt die betrokken zijn bij het ontwerpen, vervaardigen, leveren, monteren, gebruiken of onderhouden van de door haar beoordeelde ICT-producten, -diensten en -processen of beheerde beveiligingsdiensten, kan als conformiteitsbeoordelingsinstantie worden beschouwd op voorwaarde dat haar onafhankelijkheid en de afwezigheid van belangenconflicten zijn aangetoond.

4. De conformiteitsbeoordelingsinstanties, hun hoogste leidinggevenden en personen die de conformiteitsbeoordelingstaken verrichten, mogen niet de ontwerper, fabrikant, leverancier, installateur, koper, eigenaar, gebruiker of onderhouder zijn van het ICT-product, de ICT-dienst, het ICT-proces of de beheerde beveiligingsdienst die of dat wordt beoordeeld, noch de gemachtigde van één van die partijen. Dat verbod belet echter niet dat de beoordeelde ICT-producten voor activiteiten van de conformiteitsbeoordelingsinstantie of voor persoonlijke doeleinden worden gebruikt.

5. De conformiteitsbeoordelingsinstanties, hun hoogste leidinggevenden en personen die de conformiteitsbeoordelingstaken verrichten, zijn noch rechtstreeks noch als vertegenwoordiger van de betrokken partijen betrokken bij het ontwerpen, vervaardigen of bouwen, verstrekken, op de markt brengen, installeren, gebruiken of onderhouden van de ICT-producten, -diensten of -processen of beheerde beveiligingsdiensten die worden beoordeeld. De conformiteitsbeoordelingsinstanties, hun hoogste leidinggevenden en personen die de conformiteitsbeoordelingstaken verrichten, voeren geen activiteiten uit die hun onafhankelijk oordeel of hun integriteit met betrekking tot hun conformiteitsbeoordelingswerkzaamheden in het gedrang kunnen brengen. Dat verbod geldt met name voor adviesdiensten.";

2) punt 10 wordt als volgt gewijzigd:

a) de inleidende tekst wordt vervangen door:

"10. Een conformiteitsbeoordelingsinstantie beschikt te allen tijde, voor elke conformiteitsbeoordelingsprocedure en voor elke soort, categorie of subcategorie ICT-producten, -diensten of -processen of beheerde beveiligingsdiensten over:";

b) punt c) wordt vervangen door:

"c) procedures voor de uitoefening van haar werkzaamheden, die naar behoren rekening houden met de omvang van een onderneming, de sector waarin deze actief is, de structuur ervan, de relatieve complexiteit van de technologie van het ICT-product, de ICT-dienst, het ICT-proces of de beheerde beveiligingsdienst in kwestie en het massa- of seriële karakter van het productieproces.";

3) de punten 19 en 20 worden vervangen door:

"19. Conformiteitsbeoordelingsinstanties voldoen aan de eisen van de toepasselijke geharmoniseerde norm zoals gedefinieerd in artikel 2, punt 9), van Verordening (EG) nr. 765/2008 voor de accreditatie van conformiteitsbeoordelingsinstanties die ICT-producten, -diensten of -processen of beheerde beveiligingsdiensten certificeren.

20. Conformiteitsbeoordelingsinstanties zorgen ervoor dat testlaboratoria die worden gebruikt voor conformiteitsbeoordelingen voldoen aan de eisen van de toepasselijke geharmoniseerde norm zoals gedefinieerd in artikel 2, punt 9), van Verordening (EG) nr. 765/2008 voor de accreditatie van laboratoria die tests uitvoeren.".

Er is een verklaring met betrekking tot deze verordening opgesteld, die te vinden is in [PB te voorzien: PB C XXX, XX.XX.2024, blz. XX] en op de volgende link: [PB: gelieve de link naar de verklaring in te voegen].