Raad van de
Europese Unie

Brussel, 21 april 2023
(OR. en)

8511/23

Interinstitutioneel dossier:
2023/0108(COD)

CYBER 91
JAI 469
TELECOM 107
DATAPROTECT 109
MI 312
IND 180
CODEC 661

VOORSTEL

van:	de secretaris-generaal van de Europese Commissie, ondertekend door mevrouw Martine DEPREZ, directeur
ingekomen:	19 april 2023
aan:	mevrouw Thérèse BLANCHET, secretaris-generaal van de Raad van de Europese Unie
nr. Comdoc.:	COM(2023) 208 final
Betreft:	Voorstel voor een VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD tot wijziging van Verordening (EU) 2019/881 wat betreft beheerde beveiligingsdiensten

Hierbij gaat voor de delegaties document COM(2023) 208 final.

Bijlage: COM(2023) 208 final

EUROPESE
COMMISSIE

Straatsburg, 18.4.2023
COM(2023) 208 final

2023/0108 (COD)

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

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

(Voor de EER relevante tekst)

TOELICHTING

1. ACHTERGROND VAN HET VOORSTEL

• Motivering en doel van het voorstel

Deze toelichting vergezelt het voorstel voor een verordening van het Europees Parlement en de Raad tot wijziging van Verordening (EU) 2019/881[1] wat betreft beheerde beveiligingsdiensten.

De voorgestelde gerichte wijziging is bedoeld om door middel van uitvoeringshandelingen van de Commissie de vaststelling mogelijk te maken van Europese cyberbeveiligingscertificeringsregelingen voor "beheerde beveiligingsdiensten", naast informatie- en communicatietechnologieproducten (ICT-producten), ICT-diensten en ICT-processen, die reeds onder de cyberbeveiligingsverordening vallen. Beheerde beveiligingsdiensten spelen een steeds belangrijkere rol bij het voorkomen en beperken van cyberbeveiligingsincidenten.

In zijn conclusies van 23 mei 2022[2] over de ontwikkeling van de cyberstrategie van de Europese Unie heeft de Raad de Unie en haar lidstaten opgeroepen meer inspanningen te leveren om het algemene niveau van cyberbeveiliging te verhogen, bijvoorbeeld door de opkomst van betrouwbare aanbieders van cyberbeveiligingsdiensten te vergemakkelijken, en heeft hij benadrukt dat het stimuleren van de ontwikkeling van dergelijke aanbieders een prioriteit moet zijn voor het industriebeleid van de Unie op het gebied van cyberbeveiliging. De Raad heeft de Commissie ook verzocht opties voor te stellen om de opkomst van een betrouwbare cyberbeveiligingsdienstensector te stimuleren. De certificering van beheerde beveiligingsdiensten is een doeltreffend middel om vertrouwen in de kwaliteit van die diensten op te bouwen en aldus de opkomst van een betrouwbare Europese cyberbeveiligingsdienstensector te bevorderen.

In de gezamenlijke mededeling "Het EU-beleid op het gebied van cyberdefensie" die de Commissie en de hoge vertegenwoordiger op 10 november 2022 hebben aangenomen[3], werd aangekondigd dat de Commissie de ontwikkeling van cyberbeveiligingscertificeringsregelingen op EU-niveau voor de cyberbeveiligingssector en particuliere bedrijven zou onderzoeken. Aanbieders van beheerde beveiligingsdiensten zullen ook een belangrijke rol spelen in de EU-cyberbeveiligingsreserve, waarvan de geleidelijke totstandbrenging wordt ondersteund door de verordening cybersolidariteit, die tegelijk met deze verordening wordt voorgesteld. De EU-cyberbeveiligingsreserve moet worden gebruikt ter ondersteuning van responsacties en acties gericht op onmiddellijk herstel in geval van significante en grootschalige cyberbeveiligingsincidenten. De relevante cyberbeveiligingsdiensten van "betrouwbare aanbieders" als bedoeld in de verordening cybersolidariteit komen overeen met "beheerde beveiligingsdiensten" in dit voorstel.

Sommige lidstaten zijn al begonnen met de vaststelling van certificeringsregelingen voor beheerde beveiligingsdiensten. Er is dan ook een toenemend risico op versnippering van de interne markt voor beheerde beveiligingsdiensten als gevolg van inconsistenties tussen cyberbeveiligingscertificeringsregelingen in de Unie. Dit voorstel maakt het mogelijk

---

1 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 151/15 van 7.6.2019.

2 9364/22.

3 JOIN(2022) 49 final.

Europese cyberbeveiligingscertificeringsregelingen voor die diensten op te zetten om een dergelijke versnippering te voorkomen.

- **Verenigbaarheid met bestaande bepalingen op het beleidsterrein**

Dit voorstel is in overeenstemming met de cyberbeveiligingsverordening, die erdoor wordt gewijzigd. Het bouwt voort op de bepalingen van die verordening en past deze aan zodat ook beheerde beveiligingsdiensten daaronder vallen. De voorgestelde wijzigingen zijn beperkt tot het strikt noodzakelijke en veranderen niets aan de kenmerken of de werking van de cyberbeveiligingsverordening.

Dit voorstel is ook in overeenstemming met 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 (NIS 2-richtlijn)[4]. De aanbieders van beheerde beveiligingsdiensten worden beschouwd als essentiële of belangrijke entiteiten die behoren tot een zeer kritieke sector overeenkomstig Richtlijn (EU) 2022/2555. In overweging 86 van die richtlijn staat dat aanbieders van beheerde beveiligingsdiensten op het gebied van bijvoorbeeld incidentrespons, penetratietesten, beveiligingsaudits en consultancy een bijzonder belangrijke rol spelen 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. Essentiële en belangrijke entiteiten in de zin van Richtlijn (EU) 2022/2555 moeten daarom nog meer zorgvuldigheid betrachten bij de selectie van een aanbieder van beheerde beveiligingsdiensten.

Met dit voorstel wordt beoogd de kwaliteit van beheerde beveiligingsdiensten te verbeteren en de vergelijkbaarheid ervan te vergroten. Daardoor kunnen essentiële en belangrijke entiteiten bij de selectie van een aanbieder van beheerde beveiligingsdiensten de grotere zorgvuldigheid betrachten die krachtens Richtlijn (EU) 2022/2555 vereist is. Bovendien is de definitie van "beheerde beveiligingsdiensten" in dit voorstel afgeleid van en lijkt zij sterk op de definitie van "aanbieders van beheerde beveiligingsdiensten" in Richtlijn (EU) 2022/2555. Om deze redenen is het voorstel zeer complementair met de NIS 2-richtlijn.

Ten slotte vormt dit voorstel een aanvulling op de voorgestelde verordening cybersolidariteit. De voorgestelde verordening cybersolidariteit voorziet in een procedure voor de selectie van aanbieders om een EU-cyberbeveiligingsreserve te vormen, waarbij onder meer rekening moet worden gehouden met de vraag of die aanbieders een Europese of nationale cyberbeveiligingscertificering hebben verkregen. Toekomstige certificeringsregelingen voor beheerde beveiligingsdiensten zullen dus een belangrijke rol spelen bij de uitvoering van de verordening cybersolidariteit.

- **Verenigbaarheid met andere beleidsterreinen van de Unie**

Dit voorstel doet geen afbreuk aan de verenigbaarheid van de cyberbeveiligingsverordening met Verordening (EU) 2016/679 (de algemene verordening gegevensbescherming, "AVG")[5] en de bepalingen daarvan over de vaststelling van certificeringsmechanismen en gegevensbeschermingszegels en -merktekens om aan te tonen dat verwerkingsactiviteiten door verwerkingsverantwoordelijken en verwerkers aan deze verordening voldoen. De cyberbeveiligingsverordening doet geen afbreuk aan de certificering van

[4] PB L 333/810 van 27.12.2022.
[5] PB L 119/1 van 4.5.2016.

gegevensverwerkingen overeenkomstig de algemene verordening gegevensbescherming, ook niet als dergelijke verwerkingen in producten en diensten zijn geïntegreerd.

Voorts doet dit voorstel geen afbreuk aan de verenigbaarheid van de cyberbeveiligingsverordening met Verordening (EG) nr. 765/2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht[6], met name wat betreft het kader voor nationale accreditatie- en conformiteitsbeoordelingsinstanties, en nationale autoriteiten voor certificeringstoezicht.

2. RECHTSGRONDSLAG, SUBSIDIARITEIT EN EVENREDIGHEID

• Rechtsgrondslag

Dit voorstel wijzigt de cyberbeveiligingsverordening, die gebaseerd is op artikel 114 van het Verdrag betreffende de werking van de Europese Unie (VWEU). Zoals in het geval van de cyberbeveiligingsverordening beoogt dit voorstel versnippering van de interne markt te voorkomen, namelijk door het mogelijk te maken Europese cyberbeveiligingscertificeringsregelingen voor beheerde beveiligingsdiensten vast te stellen. De lidstaten zijn begonnen met de vaststelling van nationale certificeringsregelingen voor beheerde beveiligingsdiensten. Er bestaat dus een concreet risico op versnippering van de interne markt voor deze diensten, dat met dit voorstel moet worden aangepakt. Daarom is artikel 114 VWEU de relevante rechtsgrondslag voor dit initiatief.

• Subsidiariteit (bij niet-exclusieve bevoegdheid)

De doelstelling om de vaststelling van Europese cyberbeveiligingscertificeringsregelingen voor beheerde beveiligingsdiensten mogelijk te maken en versnippering van de interne markt te voorkomen, kan niet op nationaal niveau worden verwezenlijkt, maar alleen op het niveau van de Unie. Bovendien worden beheerde beveiligingsdiensten, waarop de voorgestelde wijziging gericht is, aangeboden door aanbieders die in de hele Unie actief zijn, net zoals hun grootste potentiële klanten. Actie op het niveau van de Unie is derhalve noodzakelijk en doeltreffender dan actie op nationaal niveau.

• Evenredigheid

Het voorstel is een gerichte wijziging van de cyberbeveiligingsverordening. Het is beperkt tot wat strikt noodzakelijk is om de doelstelling ervan te verwezenlijken, namelijk het mogelijk maken om Europese cyberbeveiligingscertificeringsregelingen vast te stellen voor beheerde beveiligingsdiensten, naast ICT-producten, -diensten en -processen. Met de voorgestelde wijzigingen wordt met name het toepassingsgebied van het Europees cyberbeveiligingscertificeringskader aangepast zodat ook “beheerde beveiligingsdiensten” daaronder vallen, wordt een definitie van die diensten geïntroduceerd in overeenstemming met de NIS 2-richtlijn en worden de beveiligingsdoelstellingen van de Europese cyberbeveiligingscertificering aangepast aan “beheerde beveiligingsdiensten”. De overige wijzigingen zijn van technische aard en zijn bedoeld om ervoor te zorgen dat de desbetreffende artikelen ook van toepassing zijn op “beheerde beveiligingsdiensten”. Het voorgestelde initiatief is dus evenredig met de doelstelling.

• Keuze van het instrument

Aangezien het voorstel een wijziging van Verordening (EU) 2019/881 inhoudt, is een verordening het passende rechtsinstrument.

---

[6] PB L 218/30 van 13.8.2008.

3. EVALUATIE, RAADPLEGING VAN BELANGHEBBENDEN EN EFFECTBEOORDELING

- **Evaluatie van bestaande wetgeving en controle van de resultaatgerichtheid ervan**

Niet van toepassing.

- **Raadpleging van belanghebbenden**

Er is gericht overleg gepleegd met de lidstaten en Enisa. In dit overleg hebben de lidstaten hun huidige activiteiten en standpunten met betrekking tot de certificering van beheerde beveiligingsdiensten beschreven. Enisa heeft zijn standpunten en bevindingen uit besprekingen met de lidstaten en belanghebbenden toegelicht. De van de lidstaten en Enisa ontvangen opmerkingen en informatie zijn in dit voorstel verwerkt.

- **Bijeenbrengen en gebruik van expertise**

Niet van toepassing.

- **Effectbeoordeling**

Er is verzocht om ontheffing van de noodzaak van een effectbeoordeling, aangezien het voorstel een zeer beperkte en gerichte wijziging van de cyberbeveiligingsverordening betreft. Het zou de Commissie machtigen om door middel van uitvoeringshandelingen certificeringsregelingen vast te stellen voor "beheerde beveiligingsdiensten", naast ICT-producten, -diensten en -processen, die reeds onder de verordening vallen. De wijziging zou echter pas effect hebben wanneer dergelijke certificeringsregelingen in een later stadium worden vastgesteld. Bovendien zou de wijziging het vrijwillige karakter van de certificeringsregelingen niet veranderen.

- **Resultaatgerichtheid en vereenvoudiging**

Niet van toepassing.

- **Grondrechten**

Het voorstel heeft geen voorzienbare gevolgen voor de bescherming van de grondrechten.

4. GEVOLGEN VOOR DE BEGROTING

Geen.

5. OVERIGE ELEMENTEN

- **Uitvoeringsplanning en regelingen betreffende controle, evaluatie en rapportage**

De bij het voorstel te wijzigen bepalingen zullen worden geëvalueerd in het kader van de periodieke evaluatie van de cyberbeveiligingsverordening die de Commissie overeenkomstig artikel 67 daarvan zal uitvoeren. Bij die evaluatie wordt ook gekeken naar de gevolgen, de doeltreffendheid en de efficiëntie van de bepalingen inzake het cyberbeveiligingscertificeringskader met betrekking tot de doelstellingen om een toereikend cyberbeveiligingsniveau van ICT-producten, -diensten en -processen in de Unie te waarborgen en de werking van de interne markt te verbeteren. Het voorstel bevat een wijziging die ervoor zorgt dat de evaluatie ook betrekking heeft op beheerde beveiligingsdiensten. De Commissie zendt ook een verslag over de evaluatie en haar conclusies toe aan het Europees Parlement, de Raad en de raad van bestuur van Enisa en maakt de bevindingen van het verslag openbaar.

- **Artikelsgewijze toelichting**

Het voorstel bevat twee artikelen. Terwijl artikel 1 de wijzigingen van Verordening (EU) 2019/881 bevat, heeft artikel 2 betrekking op de inwerkingtreding. Artikel 1 bevat gerichte wijzigingen om het toepassingsgebied van het Europees cyberbeveiligingscertificeringskader in de cyberbeveiligingsverordening te wijzigen zodat ook “beheerde beveiligingsdiensten” daaronder vallen (artikelen 1 en 46 van de cyberbeveiligingsverordening). Er wordt een definitie van die diensten geïntroduceerd, die zeer nauw aansluit bij de definitie van “aanbieders van beheerde beveiligingsdiensten” in de NIS 2-richtlijn (artikel 2 van de cyberbeveiligingsverordening). Ook wordt een nieuw artikel 51 bis toegevoegd over de beveiligingsdoelstellingen van de Europese cyberbeveiligingscertificering, aangepast aan “beheerde beveiligingsdiensten”. Ten slotte bevat het voorstel een aantal technische wijzigingen om ervoor te zorgen dat de desbetreffende artikelen ook van toepassing zijn op “beheerde beveiligingsdiensten”.

2023/0108 (COD)

Voorstel voor een

VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD

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,

Gezien het advies van het Comité van de Regio's;

Handelend volgens de gewone wetgevingsprocedure,

Overwegende hetgeen volgt:

(1) Verordening (EU) 2019/881 van het Europees Parlement en de Raad[7] voorziet in een kader voor de vaststelling van Europese cyberbeveiligingscertificeringsregelingen teneinde een toereikend cyberbeveiligingsniveau van ICT-producten, -diensten en -processen in de Unie te waarborgen, alsmede om versnippering van de interne markt wat betreft cyberbeveiligingscertificeringsregelingen in de Unie te vermijden.

(2) Beheerde beveiligingsdiensten, d.w.z. diensten die bestaan uit het uitvoeren van of het verlenen van bijstand bij activiteiten die verband houden met de beheersing van het cyberbeveiligingsrisico van hun klanten, zijn steeds belangrijker geworden bij de preventie en beperking van cyberbeveiligingsincidenten. 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 van het Europees Parlement en de Raad[8]. In overweging 86 van die richtlijn staat dat aanbieders van beheerde beveiligingsdiensten op het gebied van bijvoorbeeld incidentrespons, penetratietesten, beveiligingsaudits en consultancy een bijzonder belangrijke rol spelen 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

[7] 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).

[8] 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).

geweest en vormen een bijzonder risico vanwege hun nauwe integratie in de activiteiten van hun klanten. Essentiële en belangrijke entiteiten in de zin van Richtlijn (EU) 2022/2555 moeten daarom nog meer zorgvuldigheid betrachten bij de selectie van een aanbieder van beheerde beveiligingsdiensten.

(3) Aanbieders van beheerde beveiligingsdiensten spelen ook een belangrijke rol in de EU-cyberbeveiligingsreserve, waarvan de geleidelijke totstandbrenging wordt ondersteund door Verordening (EU) …/…. [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] De EU-cyberbeveiligingsreserve moet worden gebruikt ter ondersteuning van responsacties en acties gericht op onmiddellijk herstel in geval van significante en grootschalige cyberbeveiligingsincidenten. Verordening (EU) .../... [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] voorziet in een selectieprocedure voor de aanbieders die de EU-cyberbeveiligingsreserve vormen, waarbij onder meer rekening moet worden gehouden met de vraag of de betrokken aanbieder een Europese of nationale cyberbeveiligingscertificering heeft verkregen. De relevante diensten die worden verleend door "betrouwbare aanbieders" overeenkomstig Verordening (EU) ..../..... [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], komen overeen met "beheerde beveiligingsdiensten" overeenkomstig deze verordening.

(4) Certificering van beheerde beveiligingsdiensten is niet alleen relevant bij de selectie voor de EU-cyberbeveiligingsreserve, 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 in het kader daarvan worden verwerkt, kan certificering potentiële klanten belangrijke aanwijzingen en zekerheid bieden over de betrouwbaarheid van deze diensten. Europese certificeringsregelingen voor beheerde beveiligingsdiensten dragen ertoe bij versnippering van de interne markt te voorkomen. Deze verordening heeft derhalve tot doel de werking van de interne markt te verbeteren.

(5) Naast de uitrol van ICT-producten, -diensten of -processen bieden aanbieders van beheerde beveiligingsdiensten vaak aanvullende diensten die afhankelijk zijn van de competenties, deskundigheid en ervaring van hun personeel. Een zeer hoog niveau van deze competenties, deskundigheid en ervaring, alsmede 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 een beheerde beveiligingsdienst onder een certificeringsregeling kunnen vallen, moet Verordening (EU) 2019/881 worden gewijzigd.

De Europese Toezichthouder voor gegevensbescherming is geraadpleegd overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725 van het Europees Parlement en de Raad en heeft op [DD/MM/JJJJ] advies uitgebracht.

HEBBEN DE VOLGENDE VERORDENING VASTGESTELD:

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 en beheerde beveiligingsdiensten die onder 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 dienst die bestaat uit het uitvoeren van of het verlenen van bijstand voor activiteiten die verband houden met de beheersing van cyberbeveiligingsrisico's, met inbegrip van incidentrespons, penetratietesten, beveiligingsaudits en consultancy";

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

"(20) "technische specificaties": 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 vervangen door:

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

a) de ontwikkelingen op het vlak van normalisatie in aanverwante gebieden voortdurend te blijven volgen en op grond van artikel 54, lid 1, punt c), passende technische specificaties aan te bevelen voor gebruik bij de ontwikkeling van Europese cyberbeveiligingscertificeringsregelingen indien geen normen beschikbaar zijn;

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

c) vastgestelde Europese cyberbeveiligingscertificeringsregelingen overeenkomstig artikel 49, lid 8, te evalueren;

d) op grond van artikel 59, lid 4, deel te nemen aan collegiale toetsingen;

e) op grond van artikel 62, lid 5, de Commissie bij te staan bij het verzorgen van het secretariaat van de EGC.";

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) In artikel 46 worden de leden 1 en 2 vervangen door:

"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. Het waarborgt 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 zeer hoog niveau van relevante technische kennis en professionele integriteit.";

(6) In artikel 47 worden de leden 2 en 3 vervangen door:

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

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

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;

b) relevant recht en beleid ter zake van de Unie of de lidstaten;

c) de marktvraag;

d) ontwikkelingen in het cyberdreigingslandschap;

e) verzoek om opstelling van een specifieke potentiële regeling door de EGC.";

(7) In artikel 49 wordt lid 7 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, 52 en 54 bepaalde voorschriften. Deze uitvoeringshandelingen worden vastgesteld volgens de in artikel 66, lid 2, bedoelde onderzoeksprocedure.";

(8) 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:"

(9) 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) ervoor zorgen 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 zeer hoog niveau van technische kennis en bekwaamheid op het specifieke gebied, over voldoende en passende ervaring en over de hoogste mate van professionele integriteit;

b) ervoor zorgen dat de aanbieder over passende interne procedures beschikt om te waarborgen dat de beheerde beveiligingsdiensten te allen tijde op een zeer hoog kwaliteitsniveau worden verleend;

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

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

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

f) registreren, en het mogelijk maken na te gaan, op welk tijdstip en door wie gegevens, diensten of functies zijn ingezien, zijn gebruikt of anderszins zijn verwerkt;

g) ervoor zorgen dat de ICT-producten, -diensten en -processen [en de hardware] die bij de verlening van de beheerde beveiligingsdiensten worden ingezet, standaard en qua ontwerp veilig zijn, geen bekende kwetsbaarheden bevatten en voorzien zijn van de recentste beveiligingsupdates;";

(10) 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 en -processen en 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 en -processen en 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 en -processen en 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 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.";

(11) 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 en 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 of beheerde beveiligingsdiensten met de regeling ter beschikking van de in artikel 58 bedoelde 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.";

(12) 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 en beheerde beveiligingsdiensten die eronder vallen;";

b) punt j) wordt vervangen door:

"j) de regels voor het toezicht op de conformiteit van ICT-producten, -diensten en -processen en 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;";

c) punt l) wordt vervangen door:

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

d) 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 en -processen en beheerde beveiligingsdiensten, beveiligingsvoorschriften, evaluatiecriteria en -methoden en zekerheidsniveaus;";

e) 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;";

(13) 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 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:

a bis) 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;";

b ter) 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 kleine en middelgrote 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 in artikel 58 bedoelde nationale cyberbeveiligingscertificeringsautoriteit, indien deze autoriteit 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 instantie of het orgaan bedoeld in lid 7 in kennis van kwetsbaarheden of onregelmatigheden in verband met de beveiliging van gecertificeerde ICT-producten, -diensten of -processen of beheerde beveiligingsdiensten die achteraf zijn vastgesteld en die gevolgen kunnen hebben voor de naleving van de met de certificering verband houdende voorschriften. Die instantie of dat orgaan stuurt die informatie onverwijld door naar de betrokken nationale cyberbeveiligingscertificeringsautoriteit."

(14) 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 onder een van kracht zijnde Europese cyberbeveiligingscertificeringsregeling vallen.";

(15) 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 en -processen en 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.";

(16) 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);";

(17) 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 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 markt van de Unie binnenkomen.".

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 Straatsburg,

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