Wet tot uitvoering van Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 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 (Uitvoeringswet verordening cyberweerbaarheid)
VOORSTEL VAN WET

(CONCEPT 25 februari 2025)

Wij Willem-Alexander, bij de gratie Gods, Koning der Nederlanden, Prins van Oranje-Nassau, enz. enz. enz.

Allen, die deze zullen zien of horen lezen, saluut! doen te weten:

Alzo Wij in overweging genomen hebben, dat het noodzakelijk is regels te stellen ter uitvoering van Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 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);

Zo is het, dat Wij, de Afdeling advisering van de Raad van State gehoord, en met gemeen overleg der Staten-Generaal, hebben goedgevonden en verstaan, gelijk Wij goedvinden en verstaan bij deze:

HOOFDSTUK 1 ALGEMENE BEPALINGEN

Artikel 1.1 Begripsbepalingen

In deze wet en de daarop berustende bepalingen wordt verstaan onder:

- *CSIRT:* Computer security incident response team;
- *Onze Minister*: Onze Minister van Economische Zaken;
- *Raad voor Accreditatie*: Stichting Raad voor Accreditatie als bedoeld in artikel 2, eerste lid, van de Wet aanwijzing nationale accreditatie-instantie;
- *Verordening cyberweerbaarheid:* Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 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.

HOOFDSTUK 2 AANWIJZINGEN

Artikel 2.1 Aanwijzing Onze Minister als aanmeldende autoriteit

1. Onze Minister is de aanmeldende autoriteit, bedoeld in artikel 36, eerste lid, van de Verordening cyberweerbaarheid, en is bevoegd om de taken uit te voeren en de bevoegdheden uit te oefenen die bij of krachtens de Verordening cyberweerbaarheid zijn toegekend aan de aanmeldende autoriteit, met inachtneming van het tweede lid.
2. De Raad voor Accreditatie voert de taken en oefent de bevoegdheden, bedoeld in het eerste lid, uit voor zover het gaat over de beoordeling en monitoring van conformiteitsbeoordelingsinstanties.

Artikel 2.2 Aanwijzing Onze Minister als markttoezichtautoriteit

Onze Minister is de markttoezichtautoriteit, bedoeld in artikel 52, tweede lid, van de Verordening cyberweerbaarheid, en is bevoegd om de taken uit te voeren en de bevoegdheden uit te oefenen die bij of krachtens de Verordening cyberweerbaarheid zijn toegekend aan de markttoezichtautoriteit.

Artikel 2.3 Bevoegdheid als coördinator aangewezen CSIRT

Het krachtens artikel 17, eerste lid, van de Cyberbeveiligingswet als coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden aangewezen CSIRT is het als coördinator

aangewezen CSIRT, bedoeld in artikel 3, onder 51, van de Verordening cyberweerbaarheid, en is bevoegd om de taken uit te voeren en de bevoegdheden uit te oefenen die bij of krachtens de Verordening cyberweerbaarheid zijn toegekend aan het als coördinator aangewezen CSIRT.

HOOFDSTUK 3 TOEZICHT EN SANCTIONERING

Artikel 3.1 Toezicht

Met het toezicht op de naleving van de Verordening cyberweerbaarheid zijn belast de bij besluit van Onze Minister aangewezen ambtenaren.

Artikel 3.2 Sanctionering

1. Onze Minister is bevoegd tot oplegging van een bestuurlijke boete van ten hoogste het bedrag, genoemd in artikel 64, tweede lid, van de Verordening cyberweerbaarheid, ter handhaving van de in dat lid genoemde verplichtingen.
2. Onze Minister is bevoegd tot oplegging van een bestuurlijke boete van ten hoogste het bedrag, genoemd in artikel 64, derde lid, van de Verordening cyberweerbaarheid, ter handhaving van de in dat lid genoemde bepalingen.
3. Onze Minister is bevoegd tot oplegging van een bestuurlijke boete van ten hoogste het bedrag, genoemd in artikel 64, vierde lid, van de Verordening cyberweerbaarheid, ter handhaving van dat lid.
4. Onze Minister is bevoegd tot oplegging van een last onder bestuursdwang ter handhaving van de in artikel 64, tweede lid, van de Verordening cyberweerbaarheid, genoemde verplichtingen.
5. Onze Minister is bevoegd tot oplegging van een last onder bestuursdwang ter handhaving van de in artikel 64, derde lid, van de Verordening cyberweerbaarheid, genoemde bepalingen.
6. Onze Minister is bevoegd tot oplegging van een last onder bestuursdwang ter handhaving van artikel 64, vierde lid, van de Verordening cyberweerbaarheid.

HOOFDSTUK 4. NADERE REGELS

Artikel 4.1 Nadere regels uitvoering Verordening cyberweerbaarheid

Onze Minister kan bij ministeriële regeling regels stellen voor zover dat nodig is voor een goede uitvoering van de Verordening cyberweerbaarheid en de op grond van de Verordening cyberweerbaarheid vastgestelde uitvoeringshandelingen en gedelegeerde handelingen.

HOOFDSTUK 5. WIJZIGING ANDERE WETGEVING

Artikel 5.1 Wijziging Algemene wet bestuursrecht

Bijlage 2 bij de Algemene wet bestuursrecht wordt als volgt gewijzigd:

1. In artikel 7 worden in de alfabetische volgorde ingevoegd:
- Uitvoeringswet verordening cyberweerbaarheid
- Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 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.

2. In artikel 11 worden in de alfabetische volgorde ingevoegd:
- Uitvoeringswet verordening cyberweerbaarheid
- Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 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.

HOOFDSTUK 6. SLOTBEPALINGEN

Artikel 6.1 Inwerkingtreding

Deze wet treedt in werking op een bij koninklijk besluit te bepalen tijdstip, dat voor de verschillende artikelen of onderdelen daarvan verschillend kan worden vastgesteld.

Artikel 6.2 Citeertitel
Deze wet wordt aangehaald als: Uitvoeringswet verordening cyberweerbaarheid.

Lasten en bevelen dat deze in het Staatsblad zal worden geplaatst en dat alle ministeries, autoriteiten, colleges en ambtenaren die zulks aangaat, aan de nauwkeurige uitvoering de hand zullen houden.

Gegeven

De Minister van Economische Zaken,
D.S. Beljaarts

Wet tot uitvoering van Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 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 (Uitvoeringswet verordening cyberweerbaarheid)

MEMORIE VAN TOELICHTING

(CONCEPT 25 februari 2025)

I. ALGEMEEN

1. Inleiding

Dit wetsvoorstel strekt tot uitvoering van verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 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 (hierna: de Verordening cyberweerbaarheid of Cyber Resilience Act, CRA). De Verordening cyberweerbaarheid is op 10 december 2024 in werking getreden.

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

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

2. De hoofdlijnen van de Verordening cyberweerbaarheid

De tweeledige hoofddoelstelling van de Verordening cyberweerbaarheid is: (1) het creëren van horizontale robuuste cybersecurity voorwaarden voor alle producten met digitale elementen waar fabrikanten, leveranciers en importeurs van dergelijke producten aan moeten voldoen vóór plaatsing op de interne markt en tijdens de productlevenscyclus, en (2) het zorgen voor transparantie over de mate van cybersecurity van dergelijke producten ten behoeve van de keuze van gebruikers (consumenten en organisaties). Dit moet leiden tot een veiligere Europese digitale interne markt en samenleving waar onveilige producten van de markt kunnen worden geweerd en gehaald. De EU is wereldwijd de eerste partij die met dergelijke wetgeving komt en kan hiermee mondiaal de standaard zetten voor de productie van digitaal veilige producten. Wanneer derde landen, waar een groot deel van de productie van digitale producten plaatsvindt, deze standaard overnemen, draagt de verordening bij aan een wereldwijd veiligere waardenketen.

De CRA regelt dat producten met digitale elementen aan cybersecurityvereisten moeten voldoen voordat ze mogen worden aangeboden op de interne markt. Fabrikanten moeten daarnaast zorgen dat gedurende de gehele levensduur van het product veiligheidsupdates worden aangeboden om kwetsbaarheden in het product aan te pakken. Ook bevat de CRA een meldplicht voor incidenten en actief misbruikte kwetsbaarheden.

Het kabinet heeft namens Nederland actief gepleit voor en bijgedragen aan deze Europese horizontale cybersecurityproducteisen. In 2022 is de Nederlandse Cybersecuritystrategie (NLCS) gepubliceerd. Bij de totstandkoming van dit beleid zijn de aanbevelingen van de Onderzoeksraad voor Veiligheid in haar rapport 'Kwetsbaar door software: lessen naar aanleiding van beveiligingslekken door software van Citrix' uit 2021 meegenomen. Dat geldt ook voor aanbevelingen uit de evaluatie van de Roadmap Digitaal Veilige Hard- en Software. Uit beide rapporten komt de behoefte naar voren aan een verschuiving van de verantwoordelijkheid voor digitaal veilige producten en diensten van de gebruikers (consument, bedrijven en andere organisaties) naar de leverancier of fabrikant. In de NLCS is dan ook als doel gesteld om op Europees niveau een wettelijke zorgplicht voor cybersecurity voor fabrikanten en leveranciers van digitale producten overeen te komen, die fabrikanten en leveranciers gedurende de gehele

levenscyclus verantwoordelijk maakt voor de cybersecurity van hun product. Met de CRA zoals deze is vastgesteld wordt deze kabinetsdoelstelling ingevuld.

a) Reikwijdte

De verordening legt cybersecurityvereisten vast voor 'producten met digitale elementen' waarvan het beoogde doel of het redelijkerwijs voorzienbaar gebruik een directe of indirecte logische of fysieke verbinding met een eindapparaat of netwerk omvat. Onder 'product met digitale elementen' wordt verstaan een software- of hardwareproduct en geïntegreerde 'oplossingen voor gegevensverwerking op afstand', met inbegrip van software- of hardwarecomponenten die afzonderlijk in de handel worden gebracht. De verordening is daarmee van toepassing op een hele brede variëteit aan producten. Er vallen consumentenproducten onder zoals smartphones, laptops, slimme televisies en slimme deurbellen, routers, smart watches, passwordmanagers, browsers en apps. Maar ook producten voor zakelijk gebruik zoals VPN- en boekhoudsoftware en producten voor industriële toepassing (OT) zoals besturingssystemen voor sluizen en fabrieken zijn producten met digitale elementen die onder de CRA vallen, evenals microprocessoren en microcontrollers, firewalls, virusscanners en systemen voor inbraakdetectie en -preventie. Doordat ook los in de handel gebrachte componenten worden beschouwd als product met digitale elementen heeft de verordening betrekking op de hele toeleveringsketen van producten met digitale elementen. Uitgezonderd zijn medische (in-vitro) apparaten, motorvoertuigen, producten gerelateerd aan de burgerluchtvaart, reserve-onderdelen die identiek zijn aan de componenten die zij beogen te vervangen, en producten die exclusief zijn ontwikkeld voor de nationale veiligheid of defensiedoeleinden of om gerubriceerde informatie te verwerken. Ook software-as-a-service en niet-commerciële digitale producten (waaronder sommige open source-software) vallen buiten de reikwijdte van de CRA.

De verordening is alleen van toepassing op marktdeelnemers met betrekking tot de producten met digitale elementen die zij 'op de markt aanbieden', en dus in het kader van een handelsactiviteit (commercieel) worden geleverd voor distributie of gebruik op de markt van de Unie.[1] De marktdeelnemers waarop de verplichtingen betrekking hebben, zijn in de eerste plaats de fabrikanten die de producten (laten) ontwerpen, ontwikkelen en vervaardigen en onder hun naam of merk in de handel brengen. Daarnaast zijn er afgeleide verplichtingen voor importeurs die producten onder naam of merk van een buiten de EU gevestigde partij in de handel brengen, en de distributeurs die deze producten op de markt aanbieden. Elk type marktdeelnemer heeft hierbij eigen verantwoordelijkheden. Zo mag een importeur uitsluitend een product met digitale elementen in de handel brengen indien de fabrikant van buiten de EU zich aan de verplichtingen voor fabrikanten in de CRA houdt. De importeur heeft de zorgplicht om na te gaan of de fabrikant aan deze eisen heeft voldaan en ook zal blijven voldoen nadat het product in de handel is gebracht.

b) Verplichtingen voor fabrikanten, importeurs en distributeurs

Het stelsel van verplichtingen dat de CRA oplegt aan de fabrikanten, importeurs en distributeurs kan in twee categorieën worden onderverdeeld: een set aan ex-ante verplichtingen waaraan aanbieders van producten met digitale elementen moeten voldoen vóórdat deze producten in de handel mogen worden gebracht, en een set aan ex-post verplichtingen die gelden nádat de producten in de handel zijn gebracht.

Zo moeten fabrikanten en importeurs onder het ex-ante gedeelte van de verordening ervoor zorgen dat hun producten met digitale elementen zijn ontworpen, ontwikkeld en geproduceerd overeenkomstig de essentiële cyberbeveiligingsvereisten in bijlage I van de CRA voordat deze op de interne markt in de handel worden gebracht. Ten eerste wordt vereist dat producten met digitale elementen zodanig worden ontworpen, ontwikkeld en geproduceerd dat zij een passend cyberbeveiligingsniveau waarborgen op basis van de risico's. Daarnaast moet het product afhankelijk van de beoordeling van de cyberbeveiligingsrisico's die de fabrikant dient uit te voeren, voldoen aan de in bijlage I opgenomen cybersecurityvereisten. Hieronder vallen bijvoorbeeld de

[1] De omstandigheden die relevant zijn om te bepalen wanneer sprake is van een 'handelsactiviteit', onder meer in verband met opensourcesoftware en door overheidsinstanties geleverde producten, worden nader toegelicht in overweging 15 tot en met 20 van de verordening.

vereisten dat het product op de markt moet worden aangeboden zonder bekende uitbuitbare kwetsbaarheden, en met een *secure-by-default*-configuratie. De fabrikant moet aantonen dat het product met digitale elementen aan deze essentiële vereisten voldoet, alvorens het op de interne markt mag worden gebracht. Hiervoor zijn verschillende conformiteitsbeoordelingsprocedures beschreven. De hoofdregel is dat de fabrikant kan kiezen voor zelfbeoordeling (de procedure voor interne controle), voor een beoordeling door een aangemelde conformiteitsbeoordelingsinstantie of met een Europees cyberbeveiligingscertificaat (indien beschikbaar). Voor producten met digitale elementen die vallen onder de categorieën van producten die in bijlage III en bijlage IV van de verordening als 'belangrijke' of 'kritieke' producten zijn aangemerkt, zijn de conformiteitsbeoordelingsprocedures meer gericht op onafhankelijke beoordeling door conformiteitsbeoordelingsinstanties. Voor belangrijke producten in klasse I geldt dat zelfbeoordeling alleen is toegestaan als daarbij een geharmoniseerde norm wordt toegepast (een Europese norm die de essentiële eisen vertaalt in technische maatregelen die moeten worden toegepast om aan de eisen te voldoen, en die als zodanig is goedgekeurd door de Europese Commissie door deze te citeren in het Publicatieblad van de EU). Indien een dergelijke geharmoniseerde norm niet beschikbaar is moet de fabrikant het product laten beoordelen door een aangemelde conformiteitsbeoordelingsinstantie, of de conformiteit aantonen met een Europees beveiligingscertificaat op ten minste het assuranceniveau "substantieel". Voor belangrijke producten in klasse II en voor kritieke producten, zoals opgenomen in bijlage IV van de verordening, is zelfbeoordeling in geen geval toegestaan. De Europese Commissie is bevoegd om via gedelegeerde handeling productcategorieën op de lijst van belangrijke en kritieke producten van bijlage III en IV te schrappen of toe te voegen.

Voor de ex-post verplichtingen geldt dat de fabrikant er gedurende de redelijk te verwachten gebruiksduur van het product (de zogeheten ondersteuningsperiode) voor moet zorgen dat kwetsbaarheden van het product met digitale elementen, en componenten daarvan, doeltreffend worden aangepakt. Dit moet gebeuren in overeenstemming met de essentiële eisen daarvoor in deel II van bijlage I bij de CRA, waarin bijvoorbeeld staat voorgeschreven dat veiligheidsupdates onverwijld en kosteloos[2] moeten worden verstrekt. Ook staat hierin onder meer voorgeschreven dat de fabrikant een softwarestuklijst (software bill of materials, of SBOM) moet opstellen, dat de beveiliging regelmatig moet worden getest en geëvalueerd, dat de fabrikant een beleid inzake gecoördineerde openbaarmaking van kwetsbaarheden moet hanteren, en dat er een contactadres moet zijn zodat derden kwetsbaarheden die in diens product worden ontdekt, kunnen melden. De duur van de ondersteuningsperiode moet door de fabrikant worden bepaald in overeenstemming met de voorschriften in artikel 13, achtste lid, van de CRA, waarbij met name van belang is dat deze de verwachte gebruiksduur van het product weerspiegelt. De einddatum van de ondersteuningsperiode moet op het moment van aankoop duidelijk vermeld staan, en de onderbouwing van de gekozen ondersteuningsperiode wordt opgenomen in de technische documentatie.

Wanneer de fabrikant kennisneemt van een actief uitgebuite kwetsbaarheid in het product, of zich een ernstig incident heeft voorgedaan dat een impact kan hebben op de veiligheid van het product, moet de fabrikant dit melden bij het krachtens artikel 12 van de NIS2-richtlijn[3] als coördinator[4] aangewezen Computer security incident response team (CSIRT) en bij het Agentschap van de Europese Unie voor cyberbeveiliging (ENISA). Een eerste zogenaamde 'vroegtijdige waarschuwing' moet worden gedaan zonder onnodige vertraging en in elk geval binnen 24 uur nadat de fabrikant er kennis van heeft gekregen. Dit moet zonder onnodige vertraging en in elk geval binnen 72 uur worden opgevolgd door een zogenaamde 'kwetsbaarheidsmelding' dan wel 'incidentmelding' waarin algemene informatie wordt verstrekt voor zover beschikbaar over onder meer de aard van de kwetsbaarheid/het incident, een eerste beoordeling en welke corrigerende of risicobeperkende maatregelen zijn genomen door de fabrikant, en welke maatregelen kunnen worden genomen door gebruikers. Uiterlijk 14 dagen nadat een corrigerende of risicobeperkende maatregel beschikbaar is

[2] Tenzij anders overeengekomen tussen een fabrikant en een zakelijke gebruiker met betrekking tot een product met digitale elementen dat op maat voor de gebruiker is ontworpen, mogen geen kosten in rekening worden gebracht voor veiligheidsupdates.
[3] Richtlijn (EU) 2022/2055, hierna: NIS2-richtlijn.
[4] Dit betreft telkens en dus ook in Nederland het CSIRT dat krachtens artikel 12 van de NIS2-richtlijn is aangewezen als coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden.

moet een eindverslag worden ingediend, bij een incident is dat binnen een maand na de incidentmelding.

Verder moeten fabrikanten voordat zij het product met digitale elementen in de handel brengen technische documentatie opstellen ten behoeve van de toezichthouder, met daarin de beoordeling van de cyberbeveiligingsrisico's die verbonden zijn aan het product en alle relevante gegevens die aantonen dat het product voldoet aan de eisen in bijlage I van de CRA. Deze documentatie zal gedurende de gehele ondersteuningsperiode van het product actueel moeten worden gehouden. Ook moet de fabrikant informatie en instructies voor de gebruiker bijvoegen bij het product.

Voor importeurs en distributeurs van producten met digitale elementen gelden afgeleide verplichtingen om erop toe te zien dat de fabrikant aan de verplichtingen heeft voldaan.

3. Hoofdlijnen van het wetsvoorstel

Dit wetsvoorstel strekt tot uitvoering van de verplichtingen voor de lidstaat die in de verordening zijn vastgelegd en waarvoor een wettelijke regeling nodig is. Zo verplicht de verordening onder meer om een aanmeldende autoriteit aan te wijzen die verantwoordelijk is voor de procedure om conformiteitsbeoordelingsinstanties te beoordelen, aan te wijzen, aan te melden en te monitoren. Daarnaast moeten op grond van de verordening effectief toezicht en handhaving worden belegd bij een markttoezichtautoriteit, die de bevoegdheid moet krijgen om bij overtreding bestuurlijke boetes met de in de verordening voorgeschreven maximumomvang op te leggen. Ook moet een beroepsprocedure voor de besluiten van de markttoezichthouder worden ingericht. Tot slot moet de instantie worden aangewezen die belast zal zijn met de uitoefening van de taken en bevoegdheden die in de verordening zijn toebedeeld aan het als coördinator aangewezen CSIRT, en zal daartoe een meldpunt moeten worden ingericht bij dat CSIRT voor (onder meer) de meldplicht bij actief uitgebuite kwetsbaarheden en ernstige incidenten die gevolgen hebben voor de beveiliging van het product met digitale elementen. Hoe deze verplichtingen met dit wetsvoorstel worden ingevuld wordt hieronder nader toegelicht.

a) Aanwijzing van de aanmeldende autoriteit

In het wetsvoorstel wordt de minister van Economische Zaken aangewezen als aanmeldende autoriteit. De bijbehorende taken en bevoegdheden zullen in de praktijk worden uitgevoerd door de Rijksinspectie Digitale Infrastructuur (RDI). De aanwijzing heeft tot gevolg dat de RDI de taken en bevoegdheden krijgt die in de verordening aan de aanmeldende autoriteit zijn toegekend. Dit betekent dat een conformiteitsbeoordelingsinstantie om aangemeld te kunnen worden (hetgeen een vereiste is om conformiteitsbeoordelingen op grond van de CRA te kunnen uitvoeren), hiertoe een aanvraag zal moeten doen bij de RDI. Conform de op grond van artikel 36, tweede lid, van de verordening geboden mogelijkheid daartoe, bepaalt het wetsvoorstel dat de beoordeling en monitoring van conformiteitsbeoordelingsinstanties wordt uitgevoerd door de Raad voor Accreditatie. De conformiteitsbeoordelingsinstantie toont middels de accreditatie aan dat deze voldoet aan de eisen op het gebied van kwaliteit en onafhankelijkheid die in artikel 39 van de verordening worden gesteld. De Raad voor Accreditatie controleert of de instantie aan de eisen voldoet, en zal dit ook jaarlijks herhalen om te monitoren of de conformiteitsbeoordelingsinstantie aan de eisen blijft voldoen. De conformiteitsbeoordelingsinstantie draagt zoals gebruikelijk zelf de kosten voor accreditatie.

Indien een conformiteitsbeoordelingsinstantie aan de eisen van artikel 39 van de CRA voldoet, meldt RDI deze aan bij de Europese Commissie en wordt de conformiteitsbeoordelingsinstantie als aangemelde instantie opgenomen in het NANDO-informatiesysteem van aangemelde instanties. Hierbij wordt uitvoerig beschreven voor welke conformiteitsbeoordelingsactiviteiten en -modules, en voor welke producten met digitale elementen de aangemelde instantie bevoegd en bekwaam is.

De RDI is al bekend met de taken en bevoegdheden van een aanmeldende autoriteit op grond van de Radioapparatuurrichtlijn (geïmplementeerd in de Telecommunicatiewet) en vergelijkbare taken als nationale cyberbeveiligingscertificeringsautoriteit, bedoeld in artikel 58, eerste lid, van de cyberbeveiligingsverordening en heeft aldus de juiste expertise en capaciteit om deze taak ook voor de CRA op zich te nemen.

b) Inrichting toezicht en handhaving en bestuurlijke boetebevoegdheden

Op grond van artikel 52 van de verordening moeten lidstaten een of meer markttoezichtautoriteiten aanwijzen en van voldoende middelen voorzien om de doeltreffende uitvoering van de verordening te waarborgen. Het wetsvoorstel regelt in artikel 2.2 dat in Nederland het toezicht op en de handhaving van de regels in de CRA worden belegd bij de minister van Economische Zaken, die deze taken belegt bij markttoezichthouder RDI. De RDI is reeds markttoezichthouder op de cybersecurityeisen die op grond van de Radioapparatuurrichtlijn[5] aan draadloos verbonden apparaten zijn gesteld en heeft aldus de juiste expertise en capaciteit om deze taken op zich te nemen.

Naast de bevoegdheden die titel 5.2 van de Algemene wet bestuursrecht toekent aan de in dit wetsvoorstel met het toezicht belaste personen om hun taak als toezichthouder te kunnen vervullen, beschikt de RDI over de bevoegdheden die de verordening aan de nationale markttoezichtautoriteit toekent. Wanneer dat nodig is kan RDI als aangewezen markttoezichtautoriteit bijvoorbeeld een met redenen omkleed verzoek doen waarop op grond van artikel 53 van de verordening toegang moet worden verleend tot de gegevens die zij nodig hebben om te beoordelen of de fabrikant zich aan de eisen van de verordening ten aanzien van ontwerp, ontwikkeling, productie en kwetsbaarhedenrespons heeft gehouden. Ook bepaalt de verordening in artikel 54 dat de RDI, wanneer er voldoende reden is om aan te nemen dat een product met digitale elementen een significant cybersecurityrisico inhoudt, een evaluatie uitvoert of een product met digitale elementen voldoet aan alle vereisten van de verordening. Als de toezichthouder daarbij vaststelt dat niet aan de vereisten van de CRA wordt voldaan, gelast de toezichthouder de fabrikant, importeur of distributeur alle passende corrigerende maatregelen te nemen om het product binnen de gestelde termijn in overeenstemming te brengen met de vereisten, uit de handel te nemen of terug te roepen. Als de corrigerende maatregelen niet binnen de gestelde termijn worden genomen, neemt de RDI alle passende voorlopige maatregelen om te verbieden of beperken dat het product op de Nederlandse markt wordt aangeboden, of om het product in Nederland uit de handel te laten nemen of terug te laten roepen.

Waar de RDI oordeelt dat een aanbieder van producten met digitale elementen de regels niet naleeft en de gevolgen hiervan niet beperkt zijn tot zijn grondgebied, zal de RDI de Europese Commissie en de andere lidstaten informeren over de evaluatie en maatregelen die het jegens de aanbieder heeft genomen. De Europese Commissie kan markttoezichthouders verzoeken een onderzoek te verrichten als het voldoende redenen heeft om aan te nemen dat een product niet aan de voorwaarden voldoet. In uitzonderlijke omstandigheden waarbij 1) een product een aanzienlijk cyberbeveiligingsrisico heeft, 2) het niet aan de voorwaarden voldoet en 3) de markttoezichthouder geen doeltreffende maatregelen heeft genomen, mag de Europese Commissie op basis van een evaluatie, ondersteund door analyse van ENISA, in overleg met de betrokken lidstaten en fabrikant(en) tot onmiddellijke interventie overgaan en middels een uitvoeringshandeling maatregelen nemen op EU-niveau, waaronder het terugroepen van het product van de interne markt. Verder kunnen markttoezichthouders zelf, of op verzoek van de Europese Commissie of ENISA, met andere relevante toezichthouders een gezamenlijk onderzoek verrichten naar producten die een cybersecurityrisico vormen. Ten slotte kunnen onder de coördinatie van de Europese Commissie gelijktijdige nalevingscontroles worden gehouden door de markttoezichthouders (zogenaamde "*sweeps*"). Voor de uniforme toepassing van de CRA wordt de ADCO opgericht, waarin vertegenwoordigers van de aangewezen markttoezichtautoriteiten, waaronder RDI, deelnemen. De ADCO zal voor categorieën producten met digitale elementen statistieken publiceren over gemiddelde ondersteuningsperioden en richtsnoeren met indicatieve ondersteuningsperioden.

De RDI werkt als markttoezichtautoriteit op grond van artikel 52 samen met de cyberbeveiligingscertificeringsautoriteiten (in Nederland is dat de RDI zelf) en – in het kader van het toezicht op de meldplicht) met ENISA en het Nationaal Cyber Security Centrum (NCSC), en wisselt regelmatig informatie uit met deze partijen. Hetzelfde geldt voor de samenwerking en informatie-uitwisseling met de Autoriteit Persoonsgegevens en met andere markttoezichtautoriteiten die op basis van andere harmonisatiewetgeving zijn aangewezen. Ook brengt de RDI jaarlijks verslag uit aan de Europese Commissie over de resultaten van hun activiteiten en – zodra er informatie wordt verkregen die potentieel van belang kan zijn voor de

[5] De cybersecurityeisen uit de Radioapparatuurrichtlijn gaan over in de eisen van de CRA.

toepassing van het mededingingsrecht – aan de Autoriteit Consument en Markt. De aanwijzing als markttoezichtautoriteit in artikel 2.2 van dit wetsvoorstel brengt met zich mee dat de RDI bevoegd is tot deze informatie-uitwisseling.

Lidstaten moeten op grond van artikel 64 van de verordening een sanctieregime vastleggen voor inbreuken op de verordening. Het wetsvoorstel voorziet hierin, door in artikel 3.1 de Minister van Economische Zaken (in de praktijk de RDI) de bevoegdheid te verlenen een last onder dwangsom of een bestuurlijke boete, met de maxima die in artikel 64 van de verordening worden voorgeschreven op te leggen. Op grond van artikel 64, tiende lid, zijn micro-ondernemingen of kleine ondernemingen uitgezonderd van deze boetebepaling waar het gaat om het niet naleven van de meldplicht op grond van artikel 14, tweede lid, onder a, en vierde lid, onder a, om 'zonder onnodige vertraging en in elk geval binnen 24 uur nadat de fabrikant er kennis van heeft gekregen' een vroegtijdige waarschuwing in te dienen van een actief uitgebuite kwetsbaarheid of een ernstig incident dat gevolgen heeft voor de beveiliging van het product met digitale elementen. Ook kunnen op grond van artikel 64, tiende lid, geen boetes worden opgelegd voor inbreuk op de verordening door opensourcesoftwarestewards.

c) Aanwijzing van het als coördinator aangewezen CSIRT voor het meldpunt bij actief uitgebuite kwetsbaarheden en ernstige incidenten

In het wetsvoorstel wordt het krachtens artikel 17 van de Cyberbeveiligingswet als 'coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden' aangewezen CSIRT tevens belast met de uitoefening van de taken en bevoegdheden die in de verordening zijn toebedeeld aan het als coördinator aangewezen CSIRT. Naar verwachting zal het NCSC, onderdeel van het ministerie van Justitie en Veiligheid, in de praktijk de aan de coördinator toebedeelde taken gaan uitvoeren en zal daar aldus ook het meldloket worden ingericht waar de meldingen op grond van de CRA kunnen worden ontvangen. In dat geval zal zo veel als mogelijk worden aangesloten op de inrichting van het loket voor meldingen op grond van de Cyberbeveiligingswet. Op grond van artikel 14 van de CRA geldt een meldplicht voor fabrikanten bij actief uitgebuite kwetsbaarheden en bij ernstige incidenten die gevolgen hebben voor de beveiliging van het product met digitale elementen. De meldingen op grond van artikel 14 moeten gelijktijdig worden ontvangen door ENISA en door het als coördinator aangewezen CSIRT. Daarnaast voorziet de CRA in artikel 15 in de mogelijkheid om vrijwillige meldingen te doen bij de als coördinator aangewezen CSIRT.

d) Rechtsbescherming

Op basis van artikel 48 CRA moet een lidstaat voorzien in een beroepsprocedure tegen besluiten van aangemelde instanties. Dit volgt in het Nederlandse wettelijke stelsel al uit de Algemene wet bestuursrecht. In het wetsvoorstel wordt wel opgenomen dat tegen besluiten die zijn genomen op grond van de CRA of deze wet beroep in eerste aanleg moet worden ingesteld bij de rechtbank Rotterdam. Ook is in het wetsvoorstel opgenomen dat hoger beroep tegen uitspraken over zulke besluiten moet worden ingesteld bij het College van Beroep voor het bedrijfsleven. Hier zit van oudsher de juridisch-technische expertise om dergelijke besluiten te beoordelen.

4. Verhouding tot overig EU-recht

Het wetsvoorstel strekt tot uitvoering van de CRA. De CRA is een Europese verordening die deel uitmaakt van het Europese stelsel van productregelgeving, het zogeheten Nieuw Regelgevend Kader. Binnen dit kader worden in diverse richtlijnen en verordeningen essentiële eisen gesteld waar producten aan moeten voldoen om op de Europese Unie op de markt te mogen worden aangeboden. De CRA sluit hierbij aan door gebruik te maken van de gebruikelijke terminologie, standaardisatie, conformiteitsbeoordeling, accreditatie en het stelsel van markttoezicht.

De CRA heeft mede tot doel het NIS2-entiteiten makkelijker te maken om te voldoen aan de op grond van de NIS2-richtlijn (Richtlijn (EU) 2022/2555) gestelde vereisten voor de toeleveringsketen, door ervoor te zorgen dat de producten met digitale elementen die zij voor de verlening van hun diensten gebruiken, op veilige wijze worden ontwikkeld en dat zij toegang hebben tot tijdige beveiligingsupdates voor deze producten.

De CRA sluit daarnaast aan op de Cyberbeveiligingsverordening (Verordening (EU) 2019/881) door het mogelijk te maken om bij de conformiteitsbeoordeling gebruik te maken van een passend Europees cyberbeveiligingscertificaat voor zover het cyberbeveiligingscertificaat of de

conformiteitsverklaring of delen daarvan die vereisten dekken. De Europese Commissie krijgt in de CRA de bevoegdheid om bij gedelegeerde handeling te kunnen bepalen dat kritieke producten alleen met een Europees cyberbeveiligingscertificaat kunnen aantonen dat zij aan de eisen van de CRA voldoen, mits hiervoor een passend schema beschikbaar is en wordt voldaan aan de overige voorwaarden in artikel 8 van de verordening.

De CRA bevat horizontale productregelgeving die geldt voor een zeer brede groep producten (producten met digitale elementen). Wanneer sectorspecifieke Europese regelgeving gelijke of strengere cybersecurityeisen stelt, zijn deze producten uitgesloten van de CRA (de lex specialis gaat dan voor). Dit is het geval voor medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek (Verordening (EU) 2017/745 en Verordening (EU) 2017/746), en voor voertuigen en luchtvaartproducten (Verordening (EU) 2019/2144 en Verordening (EU) 2018/1139). Indien na publicatie van de CRA nieuwe sectorspecifieke cybersecurityeisen worden vastgesteld, kunnen deze bij gedelegeerde handeling worden uitgezonderd van de CRA.

De CRA bevat tot slot nog een specifieke bepaling (artikel 12) die de verhouding tot de Verordening artificële intelligentie (AI Verordening (EU) 2024/1689) beschrijft ten aanzien van AI-systemen met een hoog risico.

5. Regeldruk

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

De CRA en de voorgestelde uitvoeringswet leiden niet tot extra regeldruk voor burgers. Ook bedrijven die uitsluitend producten met digitale elementen afnemen (of in ieder geval niet als fabrikant, importeur of distributeur worden aangemerkt) leidt deze wetgeving ook niet tot extra regeldruk.

De keuze in de uitvoeringswet om accreditatie voor te schrijven bij de beoordeling en monitoring van conformiteitsbeoordelingsinstanties die wensen te worden aangemeld door de aanmeldende autoriteit kan tot extra regeldruk voor deze conformiteitsbeoordelingsinstanties leiden, al is accreditatie voor deze bedrijven een zeer gebruikelijke manier om de vereiste onafhankelijkheid en deskundigheid aan te tonen. De conformiteitsbeoordelingsinstanties dragen de kosten voor accreditatie door de Raad voor Accreditatie.

Fabrikanten die producten met digitale elementen op de markt aanbieden en importeurs en distributeurs van deze producten, krijgen op grond van de CRA te maken met verplichtingen die voor een deel als regeldruk worden aangemerkt. Deze regeldrukeffecten vloeien echter niet voort uit de uitvoeringswet, maar rechtstreeks uit de verordening.

6. Advies en consultatie

6.61 Internetconsultatie

[...]

6.2 Advies van het Adviescollege Toetsing Regeldruk

[...]

6.3 Advies van de Raad voor de rechtspraak

[...]

6.4 Uitvoering- en handhaafbaarheidstoets Rijksinspectie Digitale Infrastructuur en Nationaal Cyber Security Centrum

[...]

7. Inwerkingtreding

Artikel 71, tweede lid, van de CRA voorziet in een gefaseerde inwerkingtreding. De meldplicht voor fabrikanten in artikel 14 van de verordening is van toepassing met ingang van 11 september 2026.

De artikelen 35 tot en met 51, die betrekking hebben op de aanmelding van conformiteitsbeoordelingsinstanties, is van toepassing met ingang van 11 juni 2026. De rest van de verordening is van toepassing met ingang van 11 december 2027.

Bij deze data zal in het koninklijk besluit waarmee de verschillende onderdelen van dit wetsvoorstel in werking treden (afhankelijk van de doorlooptijd van de wetgevingsprocedure voor dit wetsvoorstel) zo veel als mogelijk worden aangesloten.

II. ARTIKELSGEWIJZE TOELICHTING

Artikel 3.1 Toezicht

Artikel 3.1 beoogt de bij besluit van de Minister van Economische Zaken aangewezen ambtenaren van de RDI te belasten met het toezicht op de naleving van de verordening. Met deze aanwijzing zijn deze ambtenaren toezichthouder als bedoeld in titel 5.2 van de Algemene wet bestuursrecht, en komen aan hen de in die titel beschreven bevoegdheden toe ten behoeve van de vervulling van die taak. Op grond van artikel 5:20 van de Algemene wet bestuursrecht is eenieder verplicht aan de toezichthouder alle medewerking te verlenen die deze redelijkerwijs kan vorderen bij de uitoefening van zijn bevoegdheden, en is de Minister van Economische Zaken bevoegd tot oplegging van een last onder bestuursdwang om deze medewerkingsverplichting te handhaven.

Artikel 3.2 Sanctionering

Op basis van artikel 64 van de CRA moeten lidstaten sancties vaststellen voor inbreuken op de verordening. Dit is uitgewerkt in het voorgestelde artikel 3.2 van dit wetsvoorstel. In het voorgestelde artikel 3.2, eerste, tweede en derde lid, wordt aangesloten bij het bepaalde in artikel 64, tweede, derde en vierde lid, van de CRA.

In het voorgestelde artikel 3.2, vierde, vijfde en zesde lid, is op basis van artikel 64, negende lid, CRA ervoor gekozen om de markttoezichtautoriteit ook bevoegd te maken tot het opleggen van een last onder bestuursdwang ter handhaving van artikel 64, tweede, derde en vierde lid, van de CRA.

Er is geen gebruik gemaakt van de mogelijkheid die artikel 64, zevende lid, van de CRA biedt om administratieve geldboeten uit te sluiten voor overheidsinstanties en overheidsorganen. In het (niet gebruikelijke) geval dat een overheidsinstantie of overheidsorgaan een product met digitale elementen op de markt aanbiedt, en aldus als fabrikant moet worden beschouwd, valt deze onverkort onder het sanctieregime op basis van artikel 3.2 van de Uitvoeringswet verordening cyberweerbaarheid.

De in artikel 3.2, eerste, tweede en derde lid, Uitvoeringswet verordening cyberweerbaarheid opgenomen administratieve boetes zijn blijkens artikel 64, tiende lid, van de CRA in een enkel, daarin bepaald geval, niet van toepassing op micro-ondernemingen of kleine ondernemingen en in het geheel niet op opensourcesoftwarestewards. De uitsluiting van artikel 64, tiende lid, van de CRA geldt onverkort voor de in artikel 3.2, vierde, vijfde en zesde lid, Uitvoeringswet verordening cyberweerbaarheid beoogde herstelsancties.

Artikel 4.1 Nadere regels ter uitvoering

Voorgesteld wordt om de Minister van Economische Zaken de bevoegdheid te verlenen om, voor het geval het voor een goede uitvoering van de verordening en de op basis daarvan vastgestelde gedelegeerde handelingen en uitvoeringshandelingen, nodig blijkt om in aanvulling op hetgeen in dit wetsvoorstel is geregeld, nationaal nadere regels te stellen, daar bij ministeriële regeling uitvoering aan te kunnen geven. Het zal daarbij gaan om - nu nog niet voorziene - zaken uit de genoemde Europese regelgeving die, behoudens op ondergeschikte punten, geen ruimte laten voor het maken van keuzen van beleidsinhoudelijke aard, maar die voor een goede uitvoering ervan nog wel in Nederlandse wetgeving moeten worden verwerkt.

Artikel 5.1 Wijziging Algemene wet bestuursrecht

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

III. Transponeringstabel Cyber Resilience Act

Bepaling Cyber Resilience Act	Bepaling in wetsvoorstel of bestaande regeling; toelichting indien niet geïmplementeerd of naar zijn aard geen implementatie behoeft	Omschrijving beleidsruimte	Toelichting op de keuze(n) bij de invulling van de beleidsruimte
Hoofdstuk I (Algemene bepalingen)			
Artikel 1 (Onderwerp)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 2 (Toepassingsgebied)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 3 (Definities)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 4 (Vrij verkeer)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 5 (Aankoop of gebruik van producten met digitale elementen)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 6 (Vereisten voor producten met digitale elementen)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 7 (Belangrijke producten met digitale elementen)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 8 (Kritieke producten met digitale elementen)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 9 (Raadpleging van belanghebbenden)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 10 (Verbetering van vaardigheden in een cyberveerkrachtige digitale omgeving)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 11 (Algemene productveiligheid)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 12 (AI-systemen met een hoog risico)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Hoofdstuk II (Verplichtingen van marktdeelnemers en bepalingen in verband met vrije en opensourcesoftware)			
Artikel 13 (Verplichtingen van fabrikanten)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 14 (Rapportageverplichtingen van fabrikanten)	Artikel 2.3 van dit wetsvoorstel	Geen	
Artikel 15 (Vrijwillige melding)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 16 (Oprichting van een centraal meldingsplatform)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 17 (Andere bepalingen in verband met melding)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 18 (Gemachtigde vertegenwoordigers)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 19 (Verplichtingen van importeurs)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	

Artikel 20 (Verplichtingen van distributeurs)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 21 (Gevallen waarin de verplichtingen van fabrikanten van toepassing zijn op importeurs en distributeurs)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 22 (Andere gevallen waarin de verplichtingen van fabrikanten van toepassing zijn)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 23 (Identificatie van marktdeelnemers)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 24 (Verplichtingen van opensourcesoftwarestewards)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 25 (Beveiligingsattestatie van vrije en opensourcesoftware)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 26 (Richtsnoeren)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Hoofdstuk III (Conformiteit van het product met digitale elementen)			
Artikel 27 (Vermoeden van conformiteit)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 28 (EU-conformiteitsverklaring)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 29 (Algemene beginselen van de CE-markering)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 30 (Regels en voorwaarden voor het aanbrengen van de CE-markering)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 31 (Technische documentatie)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 32 (Conformiteitsbeoordelingsprocedures voor producten met digitale elementen)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 33 (Steunmaatregelen voor micro-ondernemingen en kleine en middelgrote ondernemingen, met inbegrip van start-ups)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 34 (Overeenkomsten inzake wederzijdse erkenning)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Hoofdstuk IV (Aanmelding van conformiteitsbeoordelingsinstanties)			
Artikel 35 (Aanmelding)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 36 (Aanmeldende autoriteiten)	Lid 1: artikel 2.1, eerste lid, van dit wetsvoorstel Lid 2: artikel 2.1, tweede lid, van dit wetsvoorstel Overige leden: Behoeft naar de aard van deze bepaling geen implementatie	Keuze aanwijzen aanmeldende autoriteit en gebruik maken van de mogelijkheid om de	Zie § 3.a van deze MvT

		beoordeling en monitoring te laten uitvoeren door de nationale accreditatie-instantie	
Artikel 37 (Vereisten met betrekking tot aanmeldende autoriteiten)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 38 (Informatieverplichting voor aanmeldende autoriteiten)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 39 (Eisen met betrekking tot aangemelde instanties)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 40 (Vermoeden van conformiteit van aangemelde instanties)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 41 (Dochterondernemingen van en uitbesteding door aangemelde instanties)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 42 (Verzoek om aanmelding)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 43 (Aanmeldingsprocedure)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 44 (Identificatienummers en lijsten van aangemelde instanties)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 45 (Wijzigingen in de aanmelding)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 46 (Betwisting van de bekwaamheid van aangemelde instanties)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 47 (Operationele verplichtingen van aangemelde instanties)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 48 (Beroep tegen besluiten van aangemelde instanties)	Artikel 5.1 van dit wetsvoorstel	Voorzien in een beroepsprocedure	Zie § 3.d van deze MvT
Artikel 49 (Informatieplicht voor aangemelde instanties)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 50 (Uitwisseling van ervaringen)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 51 (Coördinatie van aangemelde instanties)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Hoofdstuk V (Markttoezicht en handhaving)			
Artikel 52 (Markttoezicht op en controle van producten met digitale elementen op de markt van de Unie)	Lid 2: Artikel 2.2 van dit wetsvoorstel Overige leden: Behoeft naar de aard van deze bepaling geen implementatie	Keuze markttoezicht autoriteit	Zie § 3.b van deze MvT
Artikel 53	Behoeft naar de aard van deze bepaling geen implementatie	Geen	

(Toegang tot gegevens en documentatie)			
Artikel 54 (Procedure op nationaal niveau voor producten met digitale elementen die een significant cyberbeveiligingsrisico inhouden)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 55 (Vrijwaringsprocedure van de Unie)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 56 (Procedure op het niveau van de Unie voor producten met digitale elementen die een significant cyberbeveiligingsrisico inhouden)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 57 (Conforme producten met digitale elementen die een significant cyberbeveiligingsrisico inhouden)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 58 (Formele non-conformiteit)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 59 (Gezamenlijke activiteiten van markttoezichtautoriteiten)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 60 (Bezemacties)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Hoofdstuk VI (Bevoegdheidsdelegatie en comitéprocedure)			
Artikel 61 (Uitoefening van de bevoegdheidsdelegatie)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 62 (Comitéprocedure)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Hoofdstuk VII (Vertrouwelijkheid en sancties)			
Artikel 63 (Vertrouwelijkheid)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 64 (Sancties)	Lid 1 – 4: Artikel 3.2, eerste, tweede en derde lid, van dit wetsvoorstel Lid 7: artikel 3.2 van dit wetsvoorstel Lid 9: artikel 3.2, vierde, vijfde en zesde lid, van dit wetsvoorstel Overige leden: Behoeft naar de aard van deze bepaling geen implementatie	Ten aanzien van de in lid 7 geboden mogelijkheid wordt beoogd dat geldboeten ook kunnen worden opgelegd aan overheidsinstanties en overheidsorganen	Zie § 3.b van deze MvT
Artikel 65 (Representatieve vorderingen)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Hoofdstuk VIII (Overgangs- en slotbepalingen)			
Artikel 66 (Wijziging van Verordening (EU) 2019/1020)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 67 (Wijziging van Richtlijn (EU) 2020/1828)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	

Artikel 68 (Wijziging van Verordening (EU) nr. 168/2013)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 69 (Overgangsbepalingen)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 70 (Evaluatie en toetsing)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
Artikel 71 (Inwerkingtreding en toepassing)	Artikel 6.1 van dit wetsvoorstel	Geen	Zie § 6 van deze MvT

De Minister van Economische Zaken,
D.S. Beljaarts