Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2025–2026

36 875 Uitvoering van Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 betreffende horizontale cyberbeveiligingsvereisten voorproducten met digitale elementen en tot wijziging van Verordeningen (EU) nr. 168/2013 en (EU) 2019/1020 en Richtlijn (EU) 2020/1828 (Uitvoeringswet verordening cyberweerbaarheid)

Nr. 3

MEMORIE VAN TOELICHTING

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

kst-36875-3
ISSN 0921 - 7371
's-Gravenhage 2025

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 daarvan 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 van de CRA opgenomen cybersecurityvereisten. Hieronder vallen bijvoorbeeld de 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»

[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.

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

---

[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.

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 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.

De CRA voorziet ook in manieren om bedrijven te ondersteunen bij het naleven van de verplichtingen. Zo zullen lidstaten waar nodig zorgen voor bewustwordingsactiviteiten en trainingen, een speciaal ingericht communicatiekanaal en ondersteuning van test- en conformiteitsbeoordelingsactiviteiten. Daarbij staan de behoeftes van kleine en microbedrijven centraal. Lidstaten kunnen ook een testomgeving voor regelgeving opzetten («regulatory sandbox»), waarin voorafgaand aan het op de markt brengen van een product gekeken kan worden naar ontwikkeling, ontwerp, validering en het testen, met het oog op een goede naleving van de regels. Daarnaast brengt de Europese Commissie richtsnoeren uit die bedrijven meer duidelijkheid zullen geven over naleving van de CRA. Ook wordt er onder het Digital Europe-programma subsidie beschikbaar gesteld voor ondersteuning bij naleving van de wet, vooral voor het MKB en microbedrijven. Kleinere en micro-ondernemingen kunnen bij de conformiteitsbeoordeling de vereiste documentatie in vereenvoudigde vorm verstrekken. Het hiervoor benodigde formulier zal door de Europese Commissie worden vastgelegd in uitvoeringshandelingen. Ook moet bij het vaststellen van de vergoedingen voor conformiteitsbeoordelingsprocedures rekening gehouden worden met de belangen van het MKB en micro-ondernemingen.

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 artikel 2.1, eerste lid, van 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 (hierna: Awb) toekent aan de in dit wetsvoorstel met het toezicht belaste personen om hun taak als toezichthouder te kunnen vervullen, beschikt de

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

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 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 bestuursdwang of een bestuurlijke boete op te leggen. Een bestuursorgaan dat bevoegd is een last onder bestuursdwang op te leggen, kan in plaats daarvan aan de overtreder een last onder dwangsom opleggen, dit reeds op basis van artikel 5:32 van de Awb. Voor de bestuurlijke boete uit artikel 3.7, eerste tot en met derde lid, gelden de maxima die in artikel 64 van de verordening worden voorgeschreven. 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.

Naast de bevoegdheden op grond van de CRA zelf, moeten lidstaten de bevoegdheden op grond van artikel 14, vierde lid, van de Markttoezichtverordening[6] verlenen aan de markttoezichtautoriteit. Een deel van deze bevoegdheden overlapt met taken en bevoegdheden die op grond van de CRA al aan de marktoezichtautoriteit worden toegekend, of worden in de Awb al aan de toezichthouder verleend, zoals het vorderen van gegevens door de toezichthouder. Op grond van de Markttoezichtverordening moeten daarnaast nog enkele aanvullende bevoegdheden worden verleend aan de markttoezichthouder. Het wetsvoorstel voorziet hierin in de artikelen 3.2 tot en met 3.7, waarin is aangesloten bij de daarvoor gekozen formuleringen in de Wet uitvoering markttoezichtverordening (die de daartoe benodigde wijzigingen aanbracht in de destijds al onder deze verordening vallende kaders, zoals de Metrologiewet en de Telecommunicatiewet.)

Het gaat hierbij ten eerste om de bevoegdheid om onaangekondigd inspecties ter plaatse te verrichten: op grond van artikel 5:15 van de Awb is er al de bevoegdheid voor de toezichthouder om elke plaats te betreden, maar woningen zijn van deze bevoegdheid uitgesloten. Het wetsvoorstel breidt – ter uitvoering van de verplichting uit de Markttoezichtverordening – deze bevoegdheid ten aanzien van het toezicht op de CRA uit naar woningen, met de nodige waarborgen in het proces: hiervoor is een voorafgaande machtiging vereist van de rechtercommissaris die de proportionaliteit en subsidiariteit van de verzochte binnentreding van de woning vooraf toetst. Een tweede bevoegdheid die op grond van de Markttoezichtverordening moet worden verleend is om een «mystery shopper» in te zetten bij het verkrijgen van producten met digitale elementen waar toezicht op wordt gehouden. Ten derde moet de toezichthouder een zelfstandige last kunnen opleggen als er geen andere doeltreffende middelen beschikbaar zijn om een door een product met digitale elementen gevormd ernstig risico weg te nemen. Deze

[6] Verordening (EU) 2019/1020 van het Europees Parlement en de Raad van 20 juni 2019 betreffende markttoezicht en conformiteit van producten en tot wijziging van Richtlijn 2004/42/EG en de Verordeningen (EG) nr. 765/2008 en (EU) nr. 305/2011 (PbEU 2019, L169).

zelfstandige last kan inhouden dat degene die daartoe in staat is inhoud moet verwijderen van een online interface (zoals een website, platform of app), of de toegang daartoe moet beperken, dan wel een waarschuwing voor eindgebruikers te plaatsen. Als dat niet binnen de daarvoor gestelde termijn gebeurt, kan aan de aanbieder van de website, platform of app worden opgelegd dat deze alle maatregelen treft die redelijkerwijs kunnen worden gevergd om de toegang ertoe te beperken. Deze zelfstandige lasten kunnen niet leiden tot het blokkeren of filteren van internetverkeer. Ook voor het kunnen opleggen van een zelfstandige last is een voorafgaande machtiging van de rechter-commissaris vereist. Tot slot wordt geregeld dat toezichthoudende ambtenaren gebruik kunnen maken van bepaalde bevoegdheden wanneer zij ingaan op een verzoek om bijstand van een markttoezichtautoriteit uit een andere EU-lidstaat.

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 Awb. 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.

Onderdeel van dat stelsel van markttoezicht zijn bepaalde verplichtingen op basis van de Markttoezichtverordening, die leiden tot de voorgestelde onderzoeks- en handhavingsbevoegdheden, zoals beschreven in paragraaf 3 b en de artikelsgewijze toelichting bij de artikelen 3.2 tot en met 3.7.

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 specifieke bepalingen die de verhouding tot de Verordening artificiële intelligentie (AI Verordening (EU) 2024/1689) beschrijven ten aanzien van AI-systemen met een hoog risico. Artikel 12, tweede lid, CRA verwijst naar de AI Verordening ten behoeve van de conformiteitsbeoordelingsprocedure en artikel 52, veertiende lid, CRA verwijst naar de AI Verordening in het kader van het toezicht.

Bij de uitvoering van de CRA in Nederland wordt zo veel mogelijk aangesloten bij de uitvoering en implementatie van de NIS2-richtlijn en de Cyberbeveiligingsverordening. Zo wordt het meldloket voor actief misbruikte kwetsbaarheden en incidenten ondergebracht bij het meldloket voor meldingen op grond van de NIS-implementatie (Cyberbeveiligingswet). Dit is voor beide wetten het als coördinator aangewezen CSIRT, in Nederland het NCSC. Ook wordt met de keuze voor RDI als toezichthouder en aanmeldende autoriteit aangesloten bij de taken, bevoegdheden en expertise op grond van de radioapparatenrichtlijn, de Cyberbeveiligingsverordening, de NIS2-richtlijn en de AI-verordening. De CRA bevat verder voorschriften voor de nationale markttoezichthouder (artikel 52, zevende lid) om bij samenloop met de regels op grond van de Algemene verordening gegevensbescherming samen te werken met de toezichthouder (in Nederland de Autoriteit Persoonsgegevens). Zie over deze samenwerking ook paragraaf 3 b van deze toelichting.

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 van deze memorie van toelichting is de transponeringstabel opgenomen.

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

In het geval van wettelijk voorgeschreven conformiteitsbeoordelingen zoals op grond van de CRA is het kabinetsbeleid[7] dat de conformiteitsbeoordelingsinstanties op basis van accreditatie worden aangewezen. De kosten voor accreditatie zijn voor rekening van de conformiteitsbeoordelingsinstantie zelf. 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 in theorie tot extra regeldruk voor deze conformiteitsbeoordelingsinstanties leiden. Ook zonder deze keuze zullen conformiteitsbeoordelingsinstanties, om aangemeld te kunnen worden, moeten aantonen dat zij voldoen aan de eisen op het gebied van competentie, onafhankelijkheid en consistente bedrijfsvoering die in artikel 39 van de verordening worden gesteld. Accreditatie is voor deze bedrijven veruit de gebruikelijkste manier om dit aan te tonen. Het is moeilijk te kwantificeren wat een theoretische alternatieve manier om aan te tonen dat de instantie hieraan voldoet zou kosten en of dit bedrag hoger of lager zou liggen dan de voorgeschreven route van accreditatie. Naar schatting zal het in Nederland gaan om circa drie bedrijven, die ieder naar schatting gemiddeld 120 uur zullen besteden van het doen van de aanvraag voor accreditatie, naar schatting gemiddeld 72 uur voor het reageren op vragen of het ontvangen van de Raad voor Accreditatie in het kader van de beoordeling, en na verkrijging van de accreditatie naar schatting gemiddeld acht uur zullen besteden aan het indienen van een verzoek om aanmelding bij RDI. Dit komt op een totaal van 200 uur tegen een standaardtarief van € 54[8] per bedrijf (€ 10.800) x drie bedrijven is in totaal naar schatting € 32.400. De monitoring kost naar schatting 120 uur per jaar per bedrijf, wat tegen het standaardtarief neerkomt op € 6.480 per jaar. Wanneer er niet voor gekozen zou worden om de beoordeling en monitoring door de Raad voor Accreditatie te laten uitvoeren zou van hetzelfde geschatte aantal uren en dezelfde tarieven worden uitgegaan. Daarbij wordt opgemerkt dat de kosten die de conformiteitsbeoordelingsinstantie moeten maken om aangemeld te kunnen worden, kunnen worden gecompenseerd door de inkomsten die zij zullen genereren met het uitvoeren van conformiteitsbeoordelingen op grond van de CRA. De verwachting is dat de vraag naar deze diensten flink zal toenemen als gevolg van de CRA.

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. Er is geen exacte informatie beschikbaar over het aantal fabrikanten, importeurs en

---

[7] Kamerstuk 29304, nr. 6 | Overheid.nl > Officiële bekendmakingen

[8] Handboek Meting Regeldrukkosten, standaard intern uurtarief voor hoogopgeleide medewerkers.

distributeurs dat aan de verplichtingen van de CRA moeten voldoen omdat dit niet op deze manier wordt geregistreerd. Op basis van beschikbare algemenere cijfers van het Centraal Bureau voor de Statistiek wordt geschat dat in Nederland rond de 52.000 fabrikanten en 12.000 importeurs en distributeurs aan de regels van de CRA moeten voldoen.[9]Voor softwareontwikkelaars en hardwarefabrikanten zal de CRA directe nalevingskosten voor nieuwe beveiligingsvereisten, documentatie- en rapportageverplichtingen met zich meebrengen die volgens de Impact Assessment van de Europese Commissie leiden tot geaggregeerde kosten die voor de gehele EU oplopen tot € 29 miljard, voor een geschatte marktwaarde van producten met digitale elementen van maximaal € 1.485 miljard aan omzet. Deze kosten splitsen zich per fabrikant uit in de volgende bedragen:

- Aanpassingen in de ontwikkeling en productie om aan de essentiële eisen te voldoen worden geschat op gemiddeld € 42.700 aan additionele productontwikkelingskosten voor een gemiddeld product met digitale elementen (waarbij de gemiddelde totale ontwikkelingskosten € 140.000 bedragen).
- Het doorlopen van de verplichte conformiteitsbeoordelingsprocedure:
  - bij zelfbeoordeling: € 18.400 (het gros van de producten met digitale elementen),
  - bij beoordeling door een conformiteitsbeoordelingsinstantie: € 25.000 (voorgeschreven bij belangrijke producten in klasse I tenzij er gebruik wordt gemaakt van een geharmoniseerde norm, belangrijke producten klasse II en kritieke producten).
- Administratieve kosten voor verplichte informatieverschaffing richting eindgebruikers en toezichthouders (technische documentatie, EU-conformiteitsverklaring, CE-markering, gebruikersinstructies, einddatum ondersteuningsperiode) en de meldplicht: gemiddeld
- € 12.600 per product (9% additionele kosten op het gemiddelde totaal van € 140.000 per product met digitale elementen).

De kosten voor fabrikanten kunnen worden verrekend in de prijs die aan de afnemer in rekening wordt gebracht. Consumenten, zakelijke gebruikers en overheden die deze producten met digitale elementen gebruiken zullen dus te maken kunnen krijgen met hogere prijzen. Dit moet worden afgewogen tegen de baten van gebruikers van verhoogde transparantie, dat producten met digitale elementen die zij afnemen standaard veiliger zijn en hun fundamentele rechten zoals privacy en bescherming van hun data ook beter zijn geborgd. Naar verwachting zullen de risico's op cybersecurityincidenten en cybercrime aanzienlijk afnemen als gevolg van de CRA. Voor de hele EU wordt geschat dat de CRA kan leiden tot een kostenverlaging van incidenten die bedrijven treffen met ongeveer € 180 tot 290 miljard per jaar.

[9] Er zijn geen precieze cijfers bekend van het aantal bedrijven dat producten met digitale elementen produceren, importeren en distribueren. Bedrijven kunnen bovendien meerdere rollen vervullen. Ook kan het zijn dat fabrikanten, importeurs en distributeurs niet aan de verplichtingen van de CRA hoeven te voldoen door het soort product met digitale elementen dat wordt geproduceerd, geïmporteerd of gedistribueerd wanneer het product door de CRA wordt uitgesloten. Dit kan bijvoorbeeld het geval zijn wanneer het product met digitale elementen gereguleerd wordt door andere sectorspecifieke regelgeving. In de StatLine databank van het Centraal Bureau voor de Statistiek zijn de volgende SBI-codes (Standaard Bedrijfsindeling) geraadpleegd. De voorlopige cijfers van het eerste kwartaal van 2025 zijn voor de berekening gebruikt. Voor fabrikanten: 26, 27, 28, 2612, 262, 2630, 264, 268, 271, 2720, 2731, 582, 6201 en voor distributeurs: 465, 4741, 4742, 4754, 47912.

6. Advies en consultatie

6.1 Internetconsultatie

Een ontwerp van het wetsvoorstel is op internetconsultatie gepubliceerd, in de periode van 7 maart 2025 tot en met 6 april 2025. Hierop zijn vijf reacties ingediend.

Een respondent geeft aan dat de Verordening cyberweerbaarheid en de Uitvoeringswet verordening cyberweerbaarheid ook voor Bonaire, Sint Eustatius en Saba van toepassing zouden moeten zijn. Hoewel de BES-eilanden staatkundig deel uitmaken van Nederland, worden ze EU-rechtelijk gerekend onder de landen en gebieden overzee. Voor landen en gebieden overzee is het EU-recht slechts van toepassing voor zover dat uitdrukkelijk is geregeld. Dat is bij de Verordening cyberweerbaarheid niet het geval. De Uitvoeringswet verordening cyberweerbaarheid kan deze territoriale werkingssfeer niet vergroten. Desondanks kunnen gebruikers van producten met digitale elementen positieve effecten ondervinden van producten die met het oog op de wetgeving van de interne markt worden geproduceerd en mede worden aangeboden op de BES-eilanden.

Een respondent (een ICT/cybersecurity-aanbieder) stelt voor een centraal register aan te leggen waarin alle fabrikanten die digitale producten aan de Europese markt leveren hun producten moeten registreren, waarbij de SBOM wordt genoemd als manier om dit eventueel nationaal te regelen. In de CRA is niet gekozen voor een dergelijke registratie, en in de uitvoeringswet wordt geen nationale kop toegevoegd aan de uitvoering van deze Europese verordening. Een aanvullende registratieplicht wordt door het kabinet bovendien niet wenselijk geacht. Wat er in de SBOM moet worden opgenomen wordt op Europees niveau geregeld, hiervan wordt nationaal niet afgeweken. Een van de doelen van deze wetgeving is immers het creëren van een gelijk speelveld voor fabrikanten in de interne markt.

Deze respondent vraagt daarnaast wat te doen als de distributeur de fabrikant vraagt haar CE-keurmerk te delen, maar de fabrikant weigert, of er dan producten moeten worden teruggehaald, wie in dat geval opdraait voor de kosten en wat als een eindklant weigert het product te retourneren. En wat te doen met de bestaande *«installed base»*? Benadrukt wordt dat de verplichtingen[10] alleen van toepassing zijn op producten met digitale elementen die na 11 december 2027 in de handel zullen worden gebracht, producten die voor die tijd in omloop zijn hoeven dus niet te worden teruggehaald. Een distributeur dienst vanaf 11 december 2027 voorafgaand aan het op de markt aanbieden van een product controleren of er een CE-markering is aangebracht. Is dat niet het geval omdat de fabrikant dit weigert, dan zal de distributeur het product niet op de markt aan mogen bieden (artikel 20, tweede lid, onderdeel a, van de CRA).

De respondent vraagt verder of het gaat om het bestaande CE-markering, dat is inderdaad het geval. De CE-markering staat voor conformiteit met alle Europese productregelgeving, waar de CRA deel van uitmaakt. Wel bestaat er een bevoegdheid voor de Europese Commissie om in een uitvoeringshandeling technische specificaties vast te stellen voor etiketten, pictogrammen of andere merktekens, die kunnen worden geplaatst naast de CE-markering, die specifiek gaan over de cybersecurity

[10] Met uitzondering van de meldplicht bij actief uitgebuite kwetsbaarheden en ernstige incidenten: die is ook van toepassing op producten met digitale elementen die al eerder in de handel zijn gebracht.

van het product en de gehanteerde ondersteuningsperiode. Het is nog niet bekend of een dergelijke uitvoeringshandeling zal worden opgesteld.

Een respondent (een cybersecurity-aanbieder) vraagt of zakelijke digitale diensten waarbij ten behoeve van deze dienst een hard/software-component wordt geplaatst onder de CRA valt. De CRA is alleen van toepassing op het op de markt aanbieden van producten met digitale elementen en bijbehorende oplossingen voor gegevensverwerking op afstand. Of het als onderdeel van deze dienstverlening aanbieden van een product als op de markt aanbieden van dat product kwalificeert hangt af van de omstandigheden van het geval. De Europese Commissie zal richtsnoeren opstellen voor de toepassing van de CRA, waarbij het kabinet aandacht vraagt voor de toepassing van de CRA in geval van maatwerkoplossingen.

Deze respondent vraagt verder waar de CE-markering geregeld is, omdat dit niet in de uitvoeringswet en de memorie van toelichting wordt behandeld. De CRA is een verordening en heeft daarmee rechtstreekse werking en wordt niet omgezet in nationale wetgeving. De uitvoeringswet regelt uitsluitend die zaken die nog nodig zijn voor een juiste uitvoering in Nederland. De memorie van toelichting geeft dan ook geen volledige beschrijving van alles dat in de CRA is geregeld: daarvoor wordt verwezen wordt naar de CRA zelf, m.b.t. de CE-markering naar artikel 13, 29 en 30 van de CRA.

Deze respondent maakt daarnaast opmerkingen over de bewoording van de artikelen 3.1 en 3.7 die echter voor een correcte juridische werking van hetgeen wordt voorgesteld bewust zo gekozen is. In de toelichting wordt vervolgens aandacht besteed aan het in begrijpelijke taal voor een bredere doelgroep uitleggen wat er in de artikeltekst wordt voorgesteld. Deze respondent vraagt tot slot of er op grond van artikel 4.1 nadere regels kunnen worden gesteld over hetgeen in artikel 7, vierde lid, van de verordening (uitvoeringshandeling met de technische beschrijving van de categorieën belangrijke en kritieke producten), dit zou inderdaad een voorbeeld kunnen zijn van een uitvoeringshandeling als genoemd in artikel 4.1.

Een respondent (ontwikkelaar van opensource internetsoftware) maakt van de gelegenheid gebruik om haar waardering uit te spreken voor de Nederlandse inzet voor een passende aanpak van vrije en open source software in de CRA. De respondent noemt het resultaat in de CRA van grote waarde zowel voor ontwikkelaars van vrij en open source software als voor de gehele markt. Vrije en open source software vormt volgens de respondent immers het fundament van vrijwel alle moderne software- en digitale dienstontwikkeling. In het bijzonder het vereiste voor fabrikanten om code of documentatie voor verholpen kwetsbaarheden in een opensourcecomponenten te delen met de persoon of entiteit die de component vervaardigt of onderhoudt heeft volgens respondent de potentie kwetsbaarheden in de gehele digitale toeleveringsketen te verminderen. Een passende aanpak voor opensourcesoftware is inderdaad een van de speerpunten geweest van het kabinet tijdens de onderhandelingen over de CRA.

Een respondent (belangenorganisatie voor cybersecuritybedrijven) spreekt uit zeer positief te staan tegenover de CRA gezien het gegeven dat veel hard- en software kwetsbaarheden bevat die organisaties kunnen raken in hun cybersecurity, terwijl de dreigingen alleen maar toenemen. De belangenorganisatie is dan ook groot voorstander van tijdige melding en mitigatie van kwetsbaarheden. De respondent vraagt om waarborgen in de CRA op te nemen ten aanzien van de toegang van veiligheids- en

inlichtingendiensten tot de informatie die gedeeld moet worden over actief uitgebuite kwetsbaarheden. De tekst van de CRA ligt al vast en kan niet meer worden gewijzigd. Daarnaast zijn de bevoegdheden van veiligheids- en inlichtingendiensten bij uitstek een nationale bevoegdheid die niet in Europese wetgeving wordt geregeld. In Nederland worden de bevoegdheden van deze diensten en de daarbij behorende waarborgen geregeld in o.a. de Wet op de inlichtingen- en veiligheidsdiensten 2017.

6.2 Advies van het Adviescollege toetsing regeldruk

Het Adviescollege toetsing regeldruk heeft op 9 april 2025 advies uitgebracht op een eerder concept van het wetsvoorstel. Het college constateert dat in de toelichting nut en noodzaak van de verordening, en daarmee van het regelen van het toezicht met de uitvoeringswet, helder zijn aangetoond. Het college ziet geen minder belastend alternatief (dan de voorgeschreven accreditatie) om te borgen dat conformiteitsbeoordelingsinstanties voldoen aan de eisen op het gebied van kwaliteit en onafhankelijkheid. Wel adviseert het college in de toelichting de regeldruk van de accreditatie conform de Rijksbrede methodiek in kaart te brengen. Ook adviseert het college in de toelichting de regeldruk aan te vullen middels een schatting van het aantal bedrijven dat aan de verplichtingen van de verordening moet voldoen. Deze adviezen zijn opgevolgd in de regeldrukparagraaf.

Daarnaast adviseert het college in de toelichting aandacht te besteden aan de wijze waarop het MKB en grote bedrijven ondersteund zullen worden bij het naleven van de verplichtingen. Hierop is de toelichting in paragraaf 2 aangevuld.

Het college oordeelt dat het voorstel kan worden ingediend/vastgesteld nadat met de adviespunten rekening is gehouden.

6.3 Advies van de Raad voor de rechtspraak

De Raad voor de rechtspraak heeft op 18 juni 2025 advies uitgebracht. De Raad voor de rechtspraak heeft geen zwaarwegende bezwaren tegen het wetsvoorstel, maar geeft in overweging om het wetsvoorstel te verduidelijken ten aanzien van de samenloop met Europese regelgeving. Hierop is paragraaf 4 van de toelichting aangevuld.

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

De RDI heeft op 31 maart 2025 de uitkomst van de uitvoerbaarheids- en handhaafbaarheidstoets toegezonden. De RDI acht het wetsvoorstel uitvoerbaar, handhaafbaar en fraudebestendig. Wel wijst zij erop dat de formulering van artikel 2, tweede lid, in de voor deze toets toegezonden eerdere versie van het wetsvoorstel ertoe zou leiden dat de RDI zelf geen bevoegdheid zou hebben om te handhaven op conformiteitsbeoordelingsinstanties die niet aan de eisen van de CRA voldoen. Naar aanleiding van deze opmerking is de formulering van artikel 2, tweede lid, gewijzigd, zodat beter tot uitdrukking wordt gebracht dat accreditatie weliswaar een voorgeschreven onderdeel van de beoordeling en monitoring is, maar dat dit niet afdoet aan de bevoegdheden van RDI om de bepalingen ten aanzien van conformiteitsbeoordelingsinstanties zelfstandig (in voorkomend geval ook op basis van eigen bevindingen) te handhaven. Daarnaast vraagt de RDI er bij de opstelling van nadere wet- en regelgeving rekening te houden met de integraliteit van deze regelgeving met andere (Europese) regelgeving, bijvoorbeeld ten aanzien van de implementatie van de NIS2-richtlijn en de uitvoering van de AI-verordening.

Ook wijst de RDI op het belang van de tijdige totstandkoming van geharmoniseerde normen voor een goede werking van de CRA en de bijdrage die expertise vanuit RDI hier aan kan leveren. Het kabinet onderschrijft het belang van normalisatie en volgt en ondersteunt dit proces waar mogelijk, onder meer door het subsidiëren van de kosten voor het voeren van het secretariaat voor de werkgroep bij CEN/CENELEC die hier aan werkt en de betrokkenheid van RDI-experts bij dit proces.

Op 8 april 2025 heeft het NCSC naar aanleiding van het verzoek om een uitvoeringstoets de resultaten van een quick scan hiertoe toegezonden. Het NCSC concludeert dat de voor het NCSC voorziene rol en taken op grond van de CRA uitvoerbaar zijn als aan een aantal randvoorwaarden wordt voldaan. Als randvoorwaarden noemt het NCSC onder meer de uitbreiding van de meldfunctionaliteit voor de NIS2-richtlijn (Cyberbeveiligingswet) waarmee deze tevens bruikbaar wordt als meldloket voor de CRA. Ook wijst het NCSC erop dat zij voor de aansluiting op het Europese centraal meldingsplatform afhankelijk is van de architectuur en technische, operationele en organisatorische maatregelen die ENISA zal opstellen met betrekking tot de oprichting, onderhoud en veilige werking van het centrale meldingsplatform. Als tijdig aan de nodige randvoorwaarden wordt voldaan geeft het NCSC aan vanaf 11 september 2026, de inwerkingtredingsdatum van de meldplicht op grond van de CRA, een elektronisch meldloket voor de CRA in bedrijf te kunnen hebben. Voor een goede inschatting van de structurele kosten bij het NCSC kan op termijn een herijking nodig zijn zodra meer bekend is over de inrichting van het meldloket en de daadwerkelijk benodigde aantallen FTE voor het beoordelen van meldingen en helpdeskondersteuning. Tot slot wijst het NCSC erop dat het nog nodig zal zijn beleid te formuleren in het kader van de uitvoering van de CRA, bijvoorbeeld ten aanzien van de afweging wanneer bewustmaking van het publiek «noodzakelijk» is om een ernstig incident met gevolgen voor de beveiliging van het product met digitale elementen te voorkomen of beperken omdat dit beoordelingsruimte laat aan het NCSC.

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 Awb, 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 Awb 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.

Artikelen 3.2 tot en met 3.6: Uitvoering artikel 14, vierde lid, Markttoezichtverordening

Bij de formulering van de voorgestelde artikelen 3.2 tot en met 3.6 ter uitvoering van de Markttoezichtverordening en bij de artikelsgewijze toelichting op deze artikelen is met het oog op uniforme wetgeving aangesloten bij de Wet uitvoering markttoezichtverordening en de bijbehorende memorie van toelichting. Voor de leesbaarheid zijn de desbetreffende passages aangepast op onderhavig wetsvoorstel en waar relevant opgenomen in deze artikelsgewijze toelichting.

Artikel 3.2 Markttoezichtverordening

De Markttoezichtverordening noemt onderzoeks- en handhavingsbevoegdheden waarover elke bevoegde autoriteit ten minste dient te beschikken (artikel 14, vierde lid). Onderhavig artikel bevat drie bijzondere maatregelen, te weten die in artikel 14, vierde lid, onderdelen f, g en h, van de Markttoezichtverordening. Het gaat bij deze bepalingen om een verplichte uitvoering van de betreffende bevoegdheden in nationale wetgeving.

Het gaat daarbij allereerst om de bevoegdheid van markttoezichtautoriteiten om op eigen initiatief onderzoeken in te stellen om gevallen van non-conformiteit vast te stellen en te beëindigen (artikel 14, vierde lid, onderdeel f, van de Markttoezichtverordening). Ten tweede gaat het om de bevoegdheid voor de toezichthouder om marktdeelnemers te gelasten passende maatregelen te nemen om een geval van non-conformiteit te beëindigen of het risico weg te nemen (artikel 14, vierde lid, onderdeel g, van de Markttoezichtverordening). Ten slotte ziet deze bepaling op de bevoegdheid voor de toezichthouder om passende corrigerende maatregelen te nemen, met inbegrip van de bevoegdheid om het op de markt aanbieden van een product te verbieden of te beperken of te gelasten dat het product uit de handel genomen of teruggeroepen wordt, indien een marktdeelnemer verzuimt passende maatregelen te nemen of indien de non-conformiteit of het risico blijft bestaan (artikel 14, vierde lid, onderdeel h, van de Markttoezichtverordening).

Artikel 3.3 Betreden woning zonder toestemming van de bewoner

Marktdeelnemers kunnen activiteiten ook vanuit een woning ondernemen, in het bijzonder in het geval van producten met digitale elementen. In dat geval kan het nodig zijn dat de marktoezichtautoriteit voor de opsporing van non-conformiteit en het vergaren van bewijsmateriaal de woning betreedt. Artikel 14, vierde lid, onderdeel e, van de Markttoezichtverordening, bepaalt dat de markttoezichtautoriteit over de bevoegdheid moet beschikken om gebouwen, terreinen en vervoermiddelen te betreden die de marktdeelnemer bij zijn handels-, ondernemings-, ambachtelijke of beroepsactiviteiten gebruikt, om non-conformiteit op te sporen en bewijsmateriaal te verkrijgen.

Artikel 5:15 van de Awb bepaalt dat de ambtenaren die aangewezen zijn door een markttoezichtautoriteit bevoegd zijn om «elke plaats te betreden met uitzondering van een woning zonder toestemming van de bewoner». De vereiste bevoegdheid uit de Markttoezichtverordening is ruimer, nu daarin de woning niet wordt uitgezonderd. Om die reden is deze bevoegdheid opgenomen in het wetsvoorstel. Hierbij is aangesloten bij de wijze waarop deze bevoegdheid is uitgevoerd in andere nationale

wetgeving, zoals artikel 15.7a van de Telecommunicatiewet, waarin uitvoering wordt gegeven aan EU-harmonisatiewetgeving ten aanzien waarvan de Markttoezichtverordening van toepassing is.

Op de bevoegdheid tot het binnentreden van een woning zijn de artikelen van de Algemene wet op het binnentreden (Awbi) van toepassing en vullen de voorgestelde bevoegdheid verder aan, behalve voor zover zij zijn uitgezonderd in de voorgestelde artikelen.

De volgende bepalingen zijn in het bijzonder relevant. Artikel 4 van de Awbi regelt dat de vereiste machtiging uitsluitend kan worden gegeven aan degene die bij of krachtens de wet bevoegd is verklaard om zonder toestemming van de bewoners in een woning binnen te treden. In artikel 8 van de Awbi wordt geregeld dat degene die de machtiging heeft gegeven, degene die bevoegd is binnen te treden kan vergezellen. In artikel 9 van de Awbi is bepaald dat degene die bevoegd is om de woning te betreden zonder toestemming van de bewoner, bevoegd is zich de toegang tot of de doorgang in de woning verschaffen, voor zover het doel van het binnentreden dit redelijkerwijs vereist en dat hij daartoe zo nodig de hulp van de sterke arm kan inroepen. In artikel 10 van de Awbi is geregeld dat degene die zonder toestemming van de bewoner in een woning is binnengetreden, een schriftelijk verslag opmaakt omtrent het binnentreden.

Artikelen 2 en 3 van de Awbi worden niet van toepassing verklaard. Artikel 2 van de Awbi vereist een schriftelijke machtiging bij binnentreden in een woning zonder toestemming en artikel 3 van de Awbi geeft de bevoegdheid tot het geven van een machtiging tot binnentreden in een woning voor andere doeleinden dan strafvordering, aan de burgemeester van de gemeente waar de woning in gelegen is. Deze bepalingen worden inhoudelijk vervangen door het tweede lid van de voorgestelde bepaling, waarin bij het uitoefenen van de bevoegdheid een voorafgaande machtiging wordt vereist van de rechter-commissaris.

Zoals ook is toegelicht in de memorie van toelichting bij het voorstel voor de Wet uitvoering markttoezichtverordening, wordt onderkend dat de toepassing van deze door de Markttoezichtverordening voorgeschreven bevoegdheid leidt tot een beperking van het huisrecht (artikel 12 van de Grondwet en artikel 8 van het Europees Verdrag tot bescherming van de Rechten van de Mens). Artikel 12, eerste lid, van de Grondwet bepaalt dat het binnentreden in een woning zonder toestemming van de bewoner alleen is geoorloofd in gevallen bij of krachtens wet bepaald, door hen die daartoe bij of krachtens wet zijn aangewezen.

Het huisrecht kan op grond van artikel 8, tweede lid, van het Europees Verdrag tot bescherming van de Rechten van de Mens worden beperkt indien dit bij wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen. De in het wetsvoorstel opgenomen bevoegdheid voldoet, tezamen met de vereisten van de Markttoezichtverordening, aan de vereisten van het Europees Verdrag tot bescherming van de Rechten van de Mens voor het stellen van een beperking. Het wetsvoorstel voorziet in een wettelijke regeling van de bevoegdheid en bevat waarborgen die maken dat de toepassing van deze bevoegdheid alleen plaatsvindt met het oog op het gerechtvaardigde belang van verbetering van markttoezicht op producten met digitale elementen om te waarborgen dat enkel

producten met digitale elementen worden aangeboden die een passend cyberbeveiligingsniveau waarborgen op basis van de risico's.

Artikel 3.4 Fictieve identiteit en hoedanigheid

Op basis van artikel 14, vierde lid, onderdeel j, van de Marktoezichtverordening moet de markttoezichtautoriteit de bevoegdheid hebben om onder valse identiteit productmonsters te verkrijgen.

Voor effectief toezicht kan het nodig zijn dat een markttoezichtautoriteit zonder zich als zodanig bekend te maken, deelneemt aan het handelsverkeer om te onderzoeken of een marktdeelnemer zich houdt aan de productregelgeving. De digitalisering van de handel brengt met zich mee dat veel aankopen niet langer alleen fysiek, maar ook online plaatsvinden. Bij aankopen via webpagina's doet zich vaak de situatie voor dat een toezichthouder contactgegevens moet verstrekken. Indien de toezichthouder in dergelijke situaties als zodanig persoonlijk bekend is, is effectief toezicht niet mogelijk. Artikel 14, vierde lid, onderdeel j, van de Markttoezichtverordening schrijft daarom voor dat de bevoegde autoriteit de bevoegdheid heeft om te opereren onder een fictieve identiteit. De Markttoezichtverordening spreekt van het «verkrijgen van productmonsters», waaronder ook te verstaan valt de handelingen gerelateerd aan het verkrijgen van dergelijke monsters. Hiermee zijn bedoeld handelingen met het oog op het sluiten van een overeenkomst of handelingen ter uitvoering van de overeenkomst. Hierbij kan gedacht worden aan het kopen van een product met digitale elementen in een fysieke winkel of het doen van een aankoop via een online verkoopkanaal.

Om te bewerkstelligen dat de Nederlandse markttoezichtautoriteit kan handelen met een fictieve identiteit als ware hij een eindgebruiker, voorziet dit wetsvoorstel in een uitzondering op de identificatieplicht van artikel 5:12, tweede lid, van de Awb. Als de toezichthouder door de marktdeelnemer wordt gevraagd zijn legitimatiebewijs te tonen, hoeft hij niet zijn legitimatiebewijs als toezichthouder te laten zien. Ook in die situatie kan de toezichthouder tegenover een marktdeelnemer blijven handelen als ware hij een eindgebruiker. De uitzondering op de legitimatieplicht van artikel 5:12, tweede lid, van de Awb geldt alleen tijdens de inzet van de bevoegdheid bedoeld in artikel 14, vierde lid, onderdeel j, van de Markttoezichtverordening. Als de toezichthouder na afloop van de inzet, of bij inzet van een andere bevoegdheid, wordt gevraagd om zijn legitimatiebewijs, dient hij dit wel te tonen.

De bevindingen van de toezichthouder bij het verkrijgen van toegang met een fictieve identiteit zijn onderdeel van zijn onderzoek en kunnen worden gebruikt als onderbouwing van het besluit tot oplegging van een bestuurlijke herstelsanctie of een bestuurlijke boete. Dat betekent dat het uitoefenen van toezicht onder een fictieve identiteit ingrijpende gevolgen kan hebben voor een marktdeelnemer.

Opgemerkt wordt dat de voorgestelde bevoegdheid zich onderscheidt van onderzoek in het kader van toezicht naar informatie die reeds openbaar is. Daarvoor is geen aanvullende wettelijke grondslag nodig. Ook moet deze bevoegdheid worden onderscheiden van anoniem toezicht. Anoniem toezicht is in de praktijk gebruikelijk en behoeft geen expliciete wettelijke basis. Het College van Beroep voor het bedrijfsleven heeft in zijn uitspraak van 8 juli 2015 geoordeeld dat vanwege de doeltreffendheid van het onderzoek naar de naleving van de wet het in beginsel toelaatbaar is dat

de toezichthouders anoniem toezicht uitoefenen.[11] De artikelen 5:13 en 5:15 van de Awb bieden daar ruimte voor.

Bij aankopen met een fictieve identiteit, waarbij de toezichthouder valse gegevens verstrekt aan een marktdeelnemer, is een wettelijke grondslag op zijn plaats omdat de marktdeelnemer hierdoor informatie kan verstrekken die hij niet zou hebben verstrekt als hij had geweten dat de persoon tegenover hem een toezichthouder is. Met het oog op een eerlijk proces mag een toezichthouder een marktdeelnemer niet tot andere overtredingen brengen dan waarop diens opzet was gericht en zijn praktijk is ingericht.

Uitgangspunt is dat het gebruik van een fictieve identiteit nodig en proportioneel moet zijn, zowel ten aanzien van de zwaarte van de overtreding als van de mogelijkheden om alternatieve toezichtsbevoegdheden in te zetten. Bovendien wordt het wenselijk geacht om de wijze waarop deze vorm van toezicht wordt uitgeoefend met nadere waarborgen te omkleden in het belang van degene op wie het onderzoek betrekking heeft. De handelwijze van de toezichthouder dient achteraf toetsbaar te zijn voor de rechter, wanneer deze moet oordelen over een besluit tot het opleggen van een bestuurlijke herstelsanctie of een bestuurlijke boete die is gebaseerd, of mede is gebaseerd, op bewijs dat door middel van deze methode is verkregen. Dat wordt bewerkstelligd door de plicht voor een toezichthouder tot het opstellen van een verslag waarin hij meldt wat hem is gebleken en wat er verder tijdens het onderzoek is voorgevallen.

Artikel 3.5 Zelfstandige last

Eindgebruikers maken vaak gebruik van het internet voor de aankoop van producten of het afnemen van diensten. Toezicht op deze digitale handel brengt bepaalde uitdagingen met zich mee voor markttoezichthouders. Het voorgestelde artikel biedt enkele bevoegdheden rondom *online interfaces*. Het gaat daarbij bijvoorbeeld om websites, platforms en apps.

Het voorgestelde eerste lid biedt de grondslag voor de markttoezichtautoriteit om een zelfstandige last op te leggen, in de vorm van het gelasten van de verwijdering van inhoud in verband met producten met digitale elementen van een online interface dan wel het vereisen van een waarschuwing voor eindgebruikers wanneer zij zich toegang verschaffen tot een online interface (artikel 14, vierde lid, onderdeel k, onder i, van de Markttoezichtverordening), of – als aan deze verzoeken niet wordt voldaan – het verplichten van de beperking van toegang tot de online interface (artikel 14, vierde lid, onderdeel k, onder ii, van de Markttoezichtverordening).

Op grond van het voorgestelde tweede lid is het verboden in strijd te handelen met een zelfstandige last als bedoeld in het eerste lid van het artikel. Bij overtreding van dit verbod is de markttoezichtautoriteit op grond van artikel 3.7, achtste lid, bevoegd tot het opleggen van een last onder bestuursdwang. Een last onder bestuursdwang kan ook gelijktijdig met de zelfstandige last worden opgelegd, als de omstandigheden van het geval daar aanleiding toe geven.

In het derde lid wordt bepaald dat geen zelfstandige last opgelegd kan worden die zou leiden tot het blokkeren of filteren van internetverkeer. Het is niet toegestaan om een ondernemer te verplichten om DNS- of IP-blokkades uit te voeren. Bij inzet van de bevoegdheid is van belang wat

[11] ECLI:NL:CBB:2015:191.

de gevolgen van de zelfstandige last voor het internetverkeer zijn. De inzet van de bevoegdheid mag er niet toe leiden dat dienstverleners van de informatiemaatschappij die fungeren als tussenpersoon in de positie gebracht worden dat zij het internetverkeer moeten filteren. Het is immers niet hun taak om op eigen initiatief een inschatting te maken van de onrechtmatigheid van door hen doorgegeven uitingen.

Vanwege de mogelijke beperking van grondrechten en het bijzondere belang van rechtsbescherming daarbij, wordt voorgesteld om de inzet van de bevoegdheid afhankelijk te stellen van een voorafgaande machtiging van de rechter-commissaris. Het voorgestelde vereiste van een rechterlijke machtiging draagt bij aan de rechtseenheid waar het gaat om de inzet van deze bevoegdheid in verschillende rechtsgebieden. Tevens draagt dit bij aan de uniformiteit van wetgeving.

Artikel 14, vierde lid, onderdeel k, van de Markttoezichtverordening verplicht de lidstaat om de markttoezichtautoriteit de bevoegdheid te geven tot het opleggen van een last tot verwijdering, eis tot het geven van een waarschuwing of verplichting tot het beperken van toegang. Deze maatregelen worden genomen overeenkomstig de beginselen die zijn neergelegd in de Richtlijn inzake elektronische handel (Richtlijn 2000/31/EG, overweging 41 bij de Markttoezichtverordening). In Nederland wordt deze eis, last of verplichting, zonder dat aan het niet vervullen van deze eis, last of verplichting een consequentie is verbonden, een zelfstandige last genoemd in de zin van artikel 5:2, tweede lid, Awb. Een zelfstandige last is geen bestuurlijke sanctie, maar is wel een besluit in de zin van de Awb, omdat het een wettelijke grondslag kent, met een daarop gericht rechtsgevolg. Na oplegging van de voorgestelde zelfstandige last staat daarom voor belanghebbenden bezwaar en beroep open op grond van de Awb. De machtiging van de rechter-commissaris kan in deze procedure betrokken worden. Dit neemt niet weg dat de proportionaliteit en noodzakelijkheid van de zelfstandige last gronden voor bezwaar en beroep kunnen zijn, die de bestuursrechter zelfstandig en integraal kan toetsen.

Artikel 3.6 Bijstand verlenen aan marktoezichtautoriteiten andere lidstaten

Markttoezichtautoriteiten zijn verplicht om in het kader van wederzijdse bijstand (artikel 22 van de Markttoezichtverordening) en verzoeken om handhavingsmaatregelen (artikel 23 van de Markttoezichtverordening) taken voor een andere markttoezichtautoriteit te verrichten. Het voorgestelde artikel voorziet erin dat de toezichthoudende ambtenaren van de bevoegdheden van titel 5.2 van de Awb gebruik kunnen maken ingeval van een verzoek om bijstand van een markttoezichtautoriteit uit een andere EU-lidstaat.

Artikel 3.7 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 3.7 van dit wetsvoorstel. In het voorgestelde artikel 3.7, 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 3.7, 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.

Met het voorgestelde artikel 3.7, zevende en achtste lid, wordt een mogelijkheid gecreëerd om een last onder bestuursdwang op te leggen aan degene die een zelfstandige last niet naleeft. Dit is in lijn met andere wetgeving ter uitvoering van de Markttoezichtverordening. De last onder bestuursdwang is een herstelsanctie in de zin van artikel 5:2 van de Awb. Krachtens artikel 5:32 van de Awb kan in plaats daarvan tevens een last onder dwangsom worden opgelegd. Met de last onder bestuursdwang kan de markttoezichtautoriteit marktdeelnemers dwingen om hun verplichtingen onder de verordening na te komen. De last onder dwangsom geeft ook invulling aan de bevoegdheden in artikel 14, vierde lid, van de Markttoezichtverordening, die lidstaten aan hun markttoezichtautoriteiten moeten toebedelen. 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 3.7 van de Uitvoeringswet verordening cyberweerbaarheid.

De in artikel 3.7, 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 3.7, 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 Awb 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; werkt rechtstreeks richting lidstaten	Geen	
Artikel 5 (Aankoop of gebruik van producten met digitale elementen)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks richting lidstaten	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; lid 3 en 4 werkt rechtstreeks richting de Europese Commissie	Geen	
Artikel 8 (Kritieke producten met digitale elementen)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks richting de Europese Commissie	Geen	
Artikel 9 (Raadpleging van belanghebbenden)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks richting de Europese Commissie	Geen	
Artikel 10 (Verbetering van vaardigheden in een cyberveerkrachtige digitale omgeving)	Behoeft naar de aard van deze bepaling geen implementatie; feitelijke invulling door bewustwordingsactiviteiten en trainingen	Bevorderen vaardigheden en samenwerking	Zie § 2.b van deze MvT
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	

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 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	

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
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; werkt rechtstreeks richting de Europese Commissie	Geen	
Hoofdstuk III (Conformiteit van het product met digitale elementen)			
Artikel 27 (Vermoeden van conformiteit)	Behoeft naar de aard van deze bepaling geen implementatie; werkt gedeeltelijk rechtstreeks richting de Europese Commissie	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; feitelijke invulling door bewustwordingsactiviteiten, trainingen en regulatory sandboxes	Waar passend ondernemen bepaalde acties	Zie § 2.b van deze MvT
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; werkt rechtstreeks richting lidstaten	Geen	

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
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 beoordeling en monitoring te laten uitvoeren door de nationale accreditatie-instantie	Zie § 3.a van deze MvT
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; werkt rechtstreeks richting lidstaten en de Europese Commissie	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; werkt rechtstreeks richting de Europese Commissie	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; werkt rechtstreeks richting lidstaten en de Europese Commissie	Geen	

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
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; werkt rechtstreeks richting de Europese Commissie	Geen	
Artikel 51 (Coördinatie van aangemelde instanties)	Behoeft naar de aard van deze bepaling geen implementatie; werkt rechtstreeks richting de Europese Commissie en lidstaten	Geen	
Hoofdstuk V (Markttoezicht en handhaving)			
Artikel 52 (Markttoezicht op en controle van producten met digitale elementen op de markt van de Unie)	Lid 1: Implementatie van artikel 14, vierde lid, Markttoezichtverordening in de artikelen 3.2 tot en met 3.7. Lid 2: Artikel 2.2 van dit wetsvoorstel Overige leden: behoeft naar de aard van deze bepaling geen implementatie	Keuze markttoezichtautoriteit	Zie § 3.b en 4 van deze MvT en de artikelsgewijze toelichting bij de artikelen 3.2 tot en met 3.7.
Artikel 53 (Toegang tot gegevens en documentatie)	Behoeft naar de aard van deze bepaling geen implementatie	Geen	
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; werkt rechtstreeks richting de Europese Commissie en lidstaten	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; werkt rechtstreeks richting de Europese Commissie en lidstaten	Geen	

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
Artikel 57 (Conforme producten met digitale elementen die een significant cyberbeveiligingsrisico inhouden)	Behoeft naar de aard van deze bepaling geen implementatie; werkt gedeeltelijk rechtstreeks richting de Europese Commissie en lidstaten	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; werkt rechtstreeks richting de Europese Commissie	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 3.7, eerste, tweede en derde lid, van dit wetsvoorstel Lid 7: artikel 3.7 van dit wetsvoorstel Lid 9: artikel 3.7, 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	

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
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; werkt rechtstreeks richting de Europese Commissie	Geen	
Artikel 71 (Inwerkingtreding en toepassing)	Artikel 6.2 van dit wetsvoorstel	Geen	Zie § 6 van deze MvT

De Minister van Economische Zaken,
V.P.G. Karremans