Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken

> Retouradres Postbus 450 9700 AL Groningen

Ministerie van Economische Zaken
DG Economie en Digitalisering
Directie Digitale Economie
[redacted]
Postbus 20401
2500 EK Den Haag

Emmasingel 1
9726 AH Groningen
Postbus 450
9700 AL Groningen
T (088) 041 60 00
F (050) 587 74 00
www.rdi.nl
info@rdi.nl

Ons kenmerk
RDI-EZK-00196231

Bijlagen
-

Datum 31 maart 2025
Betreft Resultaat UHT Uitvoeringswet verordening cyberweerbaarheid

[redacted],

Uw directie heeft de Rijksinspectie Digitale Infrastructuur (hierna: de RDI) gevraagd een uitvoerbaarheids- en handhaafbaarheidstoets uit te voeren op de Verordening cyberweerbaarheid (hierna: de Verordening) en de Uitvoeringswet verordening cyberweerbaarheid (hierna: de Uitvoeringswet).

Conclusie toets
De RDI acht bovengenoemde Uitvoeringswet uitvoerbaar, handhaafbaar en fraudebestendig, mits de onderstaande aandachtspunten in acht wordt genomen.

De RDI heeft in haar uitvoerbaarheids- en handhaafbaarheidstoets een aantal aandachtspunten vastgesteld. Hieronder volgt een toelichting op de aandachtspunten.

Aandachtspunten Uitvoeringswet
Bevoegdheidsverdeling Raad voor Accreditatie (hierna: RvA) en RDI
In artikel 2.1 van de Uitvoeringswet is de bevoegdheidsverdeling tussen de RvA en de RDI uitgewerkt. De RDI is aangewezen als aanmeldende autoriteit in de zin van artikel 36 lid 1 Verordening en de RvA wordt belast met beoordeling en monitoring van de conformiteitsbeoordelingsinstanties in de zin van artikel 36 lid 2 van de Verordening.

Voor de RDI ontbreekt de bevoegdheid om (op basis van eigen bevindingen) te handhaven op conformiteitsbeoordelingsinstanties die niet aan de eisen van de Verordening voldoen. Door de bevoegdheid om conformiteitsbeoordelings-instanties te monitoren bij de RvA te beleggen, heeft de RDI geen zelfstandige bevoegdheid om toezicht te houden op de conformiteitsbeoordelingsinstanties. De RDI is daarin volledig afhankelijk van de actieve monitoring door de RvA. Hiermee lijkt de rol van de RDI, wat betreft de conformiteitsbeoordelingsinstanties, beperkt tot een uitvoerende rol als aanmeldende instantie.

Voor de uitvoerbaarheid en handhaafbaarheid van deze wet en verordening is de RDI van mening dat zij ook de bevoegdheid moet hebben om op te treden tegen

conformiteitsbeoordelingsinstanties die niet aan de eisen uit Verordening voldoen. De RDI moet in staat zijn om op basis van eigen onderzoek de aanwijzing en aanmelding van conformiteitbeoordelingsinstanties te beperken, schorsen of in te trekken. Daarmee wordt de meer systeemgerichte monitoring van de RvA gecompleteerd met het dossiergerichte toezicht door RDI. Het optreden tegen niet goed functionerende conformiteitbeoordelingsinstanties kan bij ministeriële regeling verder uitgewerkt worden op basis van artikel 4.1 Uitvoeringswet.

Integraliteit van wet- en regelgeving
De RDI vraagt, net als in de toets op de uitvoerbaarheid en handhaafbaarheid van de Cyberbeveiligingswet, aandacht voor de integraliteit van de wet- en regelgeving.

Zo worden diverse fabrikanten onder de Verordening ook geconfronteerd met eisen uit de Cyberbeveiligingswet, die ook een zorg- en meldplicht oplegt aan entiteiten uit de vervaardigingsindustrie en digitale dienstverlening (cloud).[1] Voor deze entiteiten geldt dat ze bij het op de Europese markt aanbieden van producten onder de Verordening incidenten en kwetsbaarheden in producten moeten melden. Ook worden er eisen gesteld aan risicobeheersing, kwetsbaarhedenbeheersing en assetbeheersing in relatie tot producten. Voor de Verordening geldt dat ook ondersteunende interne informatie- en netwerksystemen tot het product gerekend worden, mits deze benodigd zijn voor het functioneren van de essentiële onderdelen van het product (de zogeheten oplossingen voor gegevensverwerking op afstand). In de praktijk levert dit overlap op, waar ook weer verschillen tussen zitten: meerdere meldplichten met diverse termijnen, aanleidingen en een wisselend detailniveau, potentieel bij verschillende meldpunten.

Daarnaast geldt dat producten met digitale elementen onder de Verordening die ook een hoog-risico AI-systeem onder de AI-Verordening zijn, aan de cybersecurity-eisen uit beide verordeningen moeten voldoen.[2] In artikel 52 lid 14 van de Verordening is opgenomen dat de markttoezichthouder op de AI-Verordening in dit geval ook de markttoezichthouder is die belast is met toezicht op de Verordening.

Graag wijst de RDI u erop met deze integraliteit rekening te houden bij het opstellen van nadere wet- en regelgeving, in het bijzonder de uitvoeringswet van de AI-Verordening. De RDI wordt daarbij ook graag betrokken om eventuele knelpunten die er ontstaan tijdig te kunnen adresseren.

Aandachtspunt Verordening
Naast de Uitvoeringswet is de Verordening ook op verzoek meegenomen in de uitvoerbaar- en handhaafbaarheidstoets. Ondanks dat de Verordening is vastgesteld en alleen kan worden aangepast door de Europese Commissie is er

[1] De Cyberbeveilingswet als Nederlandse implementatiewet van de Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn).
[2] Verordening (EU) 2024/1689 van het Europees Parlement en de Raad van 13 juni 2024 tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie en tot wijziging van de Verordeningen (EG) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 en (EU) 2019/2144, en de Richtlijnen 2014/90/EU, (EU) 2016/797 en (EU) 2020/1828 (verordening artificiële intelligentie).

ook ten aanzien van de Verordening een punt dat RDI graag onder de aandacht brengt.

Geharmoniseerde normen

In de Verordening worden eisen gesteld waaraan producten met digitale elementen moeten voldoen. Deze volgen uit bijlage I van de Verordening. Fabrikanten moeten een conformiteitsbeoordeling uitvoeren waarmee zij verklaren dat hun product voldoet aan de cyberbeveiligingsvereisten uit de Verordening. Uit de Verordening blijkt dat fabrikanten dat kunnen doen door gebruik te maken van geharmoniseerde normen. Bij het gebruik van de geharmoniseerde normen, of delen daarvan, volgt uit artikel 27 van de Verordening dat er een vermoeden van conformiteit met de essentiële eisen ontstaat. Voor de ontwikkeling van deze normen heeft de Europese Commissie een standaardisatieverzoek verstrekt aan CEN/CENELEC en ETSI voor de ontwikkeling van minstens veertig geharmoniseerde normen met een deadline in oktober 2026.

Vanuit de ervaring van RDI als toezichthouder op Europese productregelgeving, blijkt dat het gebruik van deze normen vaak wordt toegepast door fabrikanten in combinatie met een module A (zelfbeoordeling) conformiteitbeoordeling. De normen worden veel gebruikt, omdat het gebruik van geharmoniseerde normen het vermoeden van conformiteit oplevert, en daarmee houvast biedt voor fabrikanten en aangemelde instanties. Zeker voor het midden- en kleinbedrijf is de tijdige beschikbaarheid van normen belangrijk. Verder zal het ontbreken van geharmoniseerde normen bij de RvA ook een probleem vormen bij het beoordelen van de competenties van conformiteitbeoordelingsinstanties in het kader van accreditatie.

Daarnaast is de toepassing van volledig geciteerde geharmoniseerde normen voorwaardelijk voor alle producten die in bijlage III, deel 1 zijn opgenomen om deze conformiteitbeoordelingsmethode toe te passen. Op het moment dat deze geharmoniseerde normen niet beschikbaar zijn, of niet volledig toegepast zijn of kunnen worden moet uitgeweken worden naar aan conformiteitbeoordeling door een aangemelde instantie. De ontwikkeling van deze normen geniet daarom prioriteit binnen Europa. In de situatie dat deze normen toch niet tijdig beschikbaar zijn, is het niet aannemelijk dat er genoeg capaciteit bij aangemelde instanties beschikbaar is. Dit komt omdat conformiteitbeoordeling complex is en het opschalen naar de benodigde capaciteit en expertise voor een aangemelde instantie geen gezonde commerciële propositie is, in de wetenschap dat een deel van de klandizie wegvalt zodra deze normen alsnog beschikbaar komen.

De RDI draagt al vanaf het eerste moment actief bij aan de ontwikkeling van deze geharmoniseerde normen. Hoewel de ontwikkeling van normen de verantwoordelijkheid is van CEN/CENELEC, ETSI en de Europese Commissie, leunt het proces significant op de beschikbaarheid van experts. Door een actieve bijdrage te leveren kan RDI vooraf richting geven aan de wijze waarop fabrikanten en aangemelde instanties de essentiële eisen interpreteren en toepassen op hun product. Ook draagt het RDI bij aan het wegnemen van onzekerheid door in een vroeg stadium binnen de standaardisatie uitleg te geven aan de complexe definities uit de Verordening.

Gelet op het belang van geharmoniseerde normen en de bijbehorende risico’s voor de cyberveiligheid van producten en het toezicht op de Verordening als deze

niet tijdig beschikbaar zijn, is het van cruciaal belang dat het standaardisatieverzoek correct en tijdig wordt afgerond. De RDI kan hier gezien haar eerdere ervaring en expertise op het gebied van geharmoniseerde normen een significante bijdrage in leveren.

Slotopmerking
Zoals eerder in deze brief is benadrukt, vraagt cyberwetgeving vanuit Europa veel van Nederland als lidstaat, de Nederlandse marktpartijen en van de RDI als toezichthouder. Het cyberveilig houden van onze maatschappij is een grote, maar gezien de geopolitieke ontwikkelingen, noodzakelijke uitdaging. Het vraagt van ons als overheid een gezamenlijke aanpak vanuit deze maatschappelijke opgave. Alleen met een integrale en brede blik op het gehele stelsel van Europese wetgeving kan deze opgave opgepakt worden. Een goede en nauwe samenwerking tussen beleid en toezicht is dus van groot belang om deze klus te klaren. De RDI kijkt ernaar uit om de bestaande samenwerking met de beleidskern voort te zetten en Nederland veilig verbonden te houden.

Ik ga ervan uit u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,

mr. A.T.A.J. van Dijk
Inspecteur-generaal
Rijksinspectie Digitale Infrastructuur