Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

36 482 Wijziging van de Wet op het financieel toezicht ter implementatie van Richtlijn (EU) 2022/2556 betreffende een kader voor digitale operationele weerbaarheid van de financiële sector (Implementatiewet digitale operationele weerbaarheid)

Nr. 5

VERSLAG

Vastgesteld 28 februari 2024

De vaste commissie voor Financiën, belast met het voorbereidend onderzoek van bovenstaand wetsvoorstel, heeft de eer als volgt verslag uit te brengen van haar bevindingen.

Onder het voorbehoud dat de regering op de gestelde vragen tijdig en genoegzaam zal hebben geantwoord, acht de commissie de openbare beraadslaging over dit wetsvoorstel voldoende voorbereid.

ALGEMEEN

De leden van de GroenLinks-PvdA-fractie hebben kennisgenomen van het wetsvoorstel en verwelkomen het wetsvoorstel. Zij hebben hierover een aantal vragen.

De leden van de NSC-fractie hebben kennisgenomen van de Wijziging van de Wet op het financieel toezicht ter implementatie van Richtlijn (EU) 2022/2556 betreffende een kader voor digitale operationele weerbaarheid van de financiële sector. Daarbij hebben deze leden een aantal vragen en opmerkingen.

De leden van de D66-fractie hebben met interesse kennisgenomen van het wetsvoorstel tot implementatie van de richtlijn digitale weerbaarheid. Deze leden vinden het positief dat de risicobeheersing van ICT-systemen wordt verbeterd en dat de weerbaarheid van de financiële sector voor IT-dreigingen wordt vergroot. Zo is het van groot belang dat bijvoorbeeld het betalingsverkeer in Nederland goed en veilig kan plaatsvinden.

De leden van de BBB-fractie hebben met belangstelling kennisgenomen van de Implementatiewet digitale operationele weerbaarheid. Deze leden zijn van mening dat de financiële sector weerbaar moet zijn tegen bedreigingen en (cyber)aanvallen. Daartoe begrijpen de leden de noodzaak om een verordening en richtlijn zoals die voorliggen vorm te geven. Wel willen zij benadrukken dat er geen sprake mag zijn van disproportionele regeldruk en dat het harmoniseren van kaders niet mag

kst-36482-5
ISSN 0921 - 7371
's-Gravenhage 2024

leiden tot inefficiëntie omdat er geen rekening wordt gehouden met de eigenschappen van specifieke groepen bedrijven in specifieke lidstaten.

De leden van de CDA-fractie hebben kennisgenomen van de Implementatiewet digitale operationele weerbaarheid. Zij merken op dat het om implementatie van een verordening gaat, waar eerder op EU-niveau door Nederland mee is ingestemd. Bij implementatie blijft er daarom weinig beleidsruimte over.

De leden van de ChristenUnie-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel hetgeen beoogt de Wet op het financieel toezicht te wijzigen ter implementatie van Richtlijn (EU) 2022/2556 betreffende een kader voor digitale operationele weerbaarheid van de financiële sector (Implementatiewet digitale operationele weerbaarheid). Deze leden hebben in deze fase van de behandeling geen behoefte aan een nadere toelichting.

3. Inhoud verordening

De leden van de GroenLinks-PvdA-fractie vragen naar de samenhang tussen de Digital Operational Resilience Act (DORA) en het recent overeengekomen CRR/CRD-pakket voor banken en de Solvency-richtlijn voor verzekeraars. Daar zitten al de vereisten in dat operationele risico's adequaat beheerst moeten worden. Op welke manier vloeien er vanuit DORA additionele verplichtingen voor banken en verzekeraars voort?

De leden van de GroenLinks-PvdA-fractie vernemen dat door implementatie van het DORA-pakket ICT-risico's expliciet worden opgenomen in de Single Review and Evaluation Proces (SREP). In hoeverre was hier, zo vragen deze leden, noodzaak toe omdat het SREP al naar operationele risico's kijkt? Is hier sprake van dubbeling of was de SREP hier tot nu toe onvoldoende expliciet over?

De leden van de GroenLinks-PvdA-fractie vragen naar de reikwijdte van het wetsvoorstel. Deze ziet, zo zij begrijpen, niet op de accountancysector (hier is alleen een review clause op). Zal de Nederlandse regering zich er ten tijde van de review voor inspannen dat de reikwijdte van DORA ook uitgebreid moet worden naar accountancy-organisaties?

De leden van de GroenLinks-PvdA-fractie vragen wat de appreciatie is van de regering van het feit dat in het DORA-akkoord geen grondslag ter oprichting van een centrale EU-hub zit waarin alle omvangrijke ICT-incidenten gemeld kunnen worden. Hier zal de Commissie nu enkel een haalbaarheidsstudie naar doen. Is de regering het met deze leden eens dat een dergelijke hub het delen van kennis en best practices ten goede kan komen? Is de regering het bovendien met deze leden eens dat zo'n hub de meldprocedure voor financiële instellingen kan vereenvoudigen? Is de regering daarom bereid zich in de toekomst in te zetten voor een dergelijke hub?

De leden van de GroenLinks-PvdA-fractie vragen naar de coördinatie tussen de verschillende Europese toezichthouders. Hoe gaan zijn in de praktijk soepel vorm geven aan deze gedeeltelijke verantwoordelijkheid? Hoe wordt voorkomen dat het gemeenschappelijke toezichtnetwerk een bureaucratische kluwen wordt maar effectief toezicht bevordert?

De leden van de GroenLinks-PvdA-fractie vragen of de regering kan schetsen of aanbieders van cryptodiensten ook onder DORA vallen en zo niet, op welke manier Markets in Crypto-Assets Regulation (MiCA) dezelfde operationele vereisten stelt aan crypto-aanbieders als DORA aan

meer traditionele financiële instellingen. Deze leden benadrukken immers dat hier sprake moet zijn van een gelijk speelveld en wijzen er bovendien op dat operationele risico's bij crypto-aanbieders in de praktijk hoog blijken te zijn.

De leden van de GroenLinks-PvdA-fractie vragen of nader gespecificeerd kan worden wat de additionele toezichtkosten zijn als gevolg van de implementatie van het wetsvoorstel en hoe deze onder verschillende toezichthouders verdeeld zijn.

De leden van de D66-fractie willen weten hoe de weerbaarheidsmaatregelen zich verhouden tot de maatregelen die in het kader van de NIS2-richtlijn inzake cyberbeveiliging moeten worden genomen. In hoeverre zijn deze geüniformeerd? Voorts vragen deze leden in hoeverre het expliciet beleid is dat de voorkeur wordt gegeven aan aanbieders van ICT-diensten (zoals clouddiensten) van Europese bodem, zodat dit geen risico's meebrengt voor de strategische autonomie.

De leden van de CDA-fractie merken op dat de verordening, hoewel in het belang van goede digitale weerbaarheid, toch een behoorlijk aantal eisen en rapportageverplichtingen oplegt. Deze leden vragen de regering in hoeverre de in de verordening en richtlijn gestelde eisen een aanvullende last opleggen aan Nederlandse financiële instellingen, beleggingsondernemingen en marktexploitanten in de gereglementeerde markt, bovenop de nu van toepassing zijnde sectorale richtlijnen.

4. Wijze van implementatie en inhoud wetsvoorstel

De leden van de NSC-fractie lezen dat met dit wetsvoorstel de richtlijn deels wordt geïmplementeerd. Deze leden vragen welke concrete aspecten van de richtlijn hierna nog moeten worden geïmplementeerd en op welke termijn wordt verwacht dat dit plaats zal vinden.

Financiële instellingen hebben de afgelopen periode al aanpassingen moeten doen om te voldoen aan de verordening, begrijpen de leden van de D66-fractie. Kan de regering aangeven in hoeverre de financiële instellingen reeds klaar zijn voor de implementatie, zo vragen deze leden. Is er verschil tussen financiële entiteiten in het implementeren van DORA? Hoe worden financiële instellingen geholpen om tijdig klaar te zijn voor de implementatie en is daarin bijvoorbeeld een rol voor de AFM of DNB weggelegd? Deze leden vragen hoe het toezicht op de implementatie en de uitvoering van de verordening wordt vormgegeven, vragen de leden. Wat gebeurt er als financiële instellingen niet tijdig klaar zijn met het implementeren van de verordening of niet voldoen aan de risico-eisen uit de verordening?

5. Gevolgen

De leden van de BBB-fractie lezen dat de regering op pagina 6 van de memorie van toelichting het volgende schrijft naar aanleiding van de effectbeoordeling van de verordening door de Europese Commissie: «ook vermeldenswaardig, aldus de effectbeoordeling, is dat het verstevigen van de digitale operationele weerbaarheid van de financiële sector naar verwachting zal leiden tot een afname van cyberincidenten. Dit komt de continuïteit van de onderneming ten goede en leidt in den brede tot verbeterde financiële stabiliteit en vertrouwen in de financiële sector. Financiële ondernemingen zullen op termijn om die reden naar verwachting minder kosten hoeven te maken voor het mitigeren en herstellen van dit soort incidenten.» Is er een concrete analyse

beschikbaar van hoeveel cyberschade zou kunnen worden voorkomen door gebruik van deze richtlijn c.q. verordening?

Regeldruk

De leden van de NSC-fractie lezen dat de regeldruk voor de implementatie van de richtlijn proportioneel is. Hierbij is logischerwijs geen rekening gehouden met de regeldruk die ontstaat naar aanleiding van de verordening, aangezien de verordening rechtstreeks doorwerkt in de Nederlandse rechtsorde. Toch kan deze gezamenlijke toename van regeldruk voor bepaalde bedrijven wel degelijk buitenproportioneel zijn. Zeker voor ondernemers zonder eerdere vergelijkbare sectorale regelingen. De leden vragen hoe de regering deze gezamenlijke toename van regeldruk inschat voor de bedrijven en hoe de regering deze bedrijven daarin kan bijstaan.

De leden van de D66-fractie begrijpen ook dat financiële instellingen moeten monitoren en rapporteren over ICT-gerelateerde incidenten. Kan de regering aangeven hoe dit precies in z'n werk gaat en wat er met deze informatie wordt gedaan? Hoe wordt er bijvoorbeeld op toegezien dat de AVG hier goed gehandhaafd wordt, ook als het gaat om het delen van deze gegevens, vragen de leden. En kan de regering aangeven hoe de implementatie van deze verordening samenhangt met die van andere Europese verordeningen en hoe wordt voorkomen dat de regeldruk voor instellingen te hoog wordt?

De leden van de BBB-fractie lezen dat de regering op pagina 6 van de memorie van toelichting verder over de regeldrukkosten schrijft: «de effectbeoordeling beschrijft dat van alle bestaande instellingen die onder de verordening gaan vallen, zijn de 21.233 entiteiten, de verwachting is dat 2.100 een additionele investering dienen te doen van 5% van het bestaande ICT-budget om aan de minimumvereisten van de verordening te voldoen.» Kan de regering deze groep bedrijven uitsplitsen? Gaat het om het midden- en kleinbedrijf (mkb) of grotere instellingen? En in welke aantallen? Kan de regering aangeven hoeveel bedrijven gemiddeld extra moeten investeren als percentage van de omzet? Gaat het hierbij om extra regels of enkel om harmonisatie? Wat is de impact op het gebied van regeldruk voor bedrijven?

De leden van de CDA-fractie vragen of het volgens de regering meerwaarde kan bieden om het Adviescollege toetsing regeldruk (ATR) naar de gevolgen van de verordening en richtlijn voor de Nederlandse markt te laten kijken, met name om inzicht te krijgen in wat er precies op de betrokken partijen afkomt en wat daarvan de administratieve lasten en kosten zijn. Deze leden vragen of volgens de regering de impactanalyse van de Europese Commissie voldoende specifieke informatie geeft. Ook vragen deze leden waarom geen nadere analyse van de regeldruk wordt gemaakt voor de uitwerking van technische reguleringsnormen en richtsnoeren, zoals in de consultatieronde ook is gevraagd. Ook daar zijn deze leden van mening dat los van het argument dat er geen afwegingsruimte is, het belangrijk is om inzicht te hebben in de regeldruk en -last die dit met zich meebrengt. Deze leden vinden het belangrijk om de vinger aan de pols te kunnen houden wanneer de regeldruk te ver oploopt, gezien de enorme regeldruk waar financiële instellingen nu al aan moeten voldoen in het kader van antiwitwaswetgeving.

De fungerend voorzitter van de commissie,
Tielen

De adjunct-griffier van de commissie,
Meijerink