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. 6

NOTA NAAR AANLEIDING VAN HET VERSLAG

Ontvangen 15 mei 2024

De regering is de vaste commissie voor Financiën erkentelijk voor de aandacht die zij aan het onderhavige wetsvoorstel heeft geschonken en voor de door haar daarover gestelde vragen. De vragen worden zo veel mogelijk beantwoord in de volgorde van het door de commissie uitgebrachte verslag. Voor zover vragen, vanwege overeenkomst in onderwerp, gezamenlijk beantwoord zijn, is dit vermeld.

1. Inleiding

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-36482-6
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.

2. 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 merken terecht op dat er samenhang is tussen DORA en de prudentiële vereisten voor banken en verzekeraars. Het Capital Requirements Regulation (CRR) / Capital Requirements Directive (CRD) pakket richt zich op de Europese implementatie van Basel III en stelt prudentiële regels voor banken ten behoeve van de financiële stabiliteit. Dit prudentiële bankenpakket voorziet onder meer in een methode voor de berekening van de kapitaalvereisten (het aanhouden van kapitaal) voor operationele risico's en het risicoprofiel van de instelling. Het Solvency II-raamwerk is een risicogebaseerd toezichtraamwerk voor verzekeraars en bevat ook prudentiële vereisten. De eerste pilaar richt zich op kwantificeerbare risico's en bevat vereisten voor het vaststellen van de balans, het eigen vermogen en kapitaalvereisten voor verzekeraars. De tweede pilaar uit het Solvency II raamwerk focust op het risicomanagement en bedrijfsvoering van een verzekeraar. Daarbij dient een verzekeraar ook het operationeel risico adequaat te beheersen. Pilaar 3 focust op de vereisten voor verslaggeving en rapportage. Deze maatregelen zijn dus, simpel gesteld, primair bedoeld om ervoor te zorgen dat banken en verzekeraars voldoende financiële buffers hebben om eventuele verliezen uit operationele problemen op te kunnen vangen.

DORA richt zicht met name op handvatten en vereisten om de weerbaarheid van de belangrijke systemen en processen zelf te versterken. Deze verplichtingen gaan onder andere over de ICT-huishouding van financiële instellingen, de wijze waarop IT-risico's opgepakt moeten worden, het testen van systemen, en het melden van incidenten. DORA richt zich daarmee op andere zaken dan deze twee prudentiële toezichtraamwerken. Tevens is de reikwijdte van DORA breder. Onder DORA vallen bijvoorbeeld ook betaalinstellingen, elektronischgeldinstellingen en pensioenfondsen.

Zowel DORA als Solvency II kennen vereisten rondom het uitbesteden van diensten. Solvency II richt zich specifiek op het uitbestedingsproces voor kritieke en belangrijke uitbestedingen (waaronder beleid, contractering,

monitoring en evaluatie). DORA richt zich op alle ICT-dienstverleners, die opgenomen moeten worden in een nieuw op te stellen informatieregister.

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 het meenemen van de ICT-risico's in de *Supervisory Review and Evaluation Process* (SREP). Dit proces vindt bij banken plaats op grond van artikel 3:18a, eerste lid, van de Wet op het financieel toezicht, die artikel 97 van de richtlijn kapitaalvereisten implementeert. In de SREP werden al de operationele risico's uit artikel 85 van de richtlijn kapitaalvereisten beoordeeld. Onder operationele risico's vielen (impliciet) reeds ICT-risico's en dus werd deze risico's ook al meegenomen in de SREP.[1] De wijzigingen uit DORA maken het meenemen van de ICT-risico's expliciet in de richtlijn, door onder meer te vereisen dat banken ICT-plannen opstellen voor de continuïteit van het bedrijf en respons en herstelplannen, en dat deze plannen opgesteld, beheerd en getest worden volgens de vereisten van artikel 11 van DORA.

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 merken terecht op dat de accountancysector niet onder de reikwijdte van de verordening valt, maar dat dit mogelijkerwijs herzien zal worden met de review van DORA. Nederland heeft zich tijdens de onderhandelingen in de Raad ingezet om de accountancysector onder de reikwijdte te brengen. Hiervoor was echter onvoldoende steun. Ook bij het EP was er geen steun om de accountancysector toe te voegen aan de reikwijdte. De oorzaak hiervoor is gelegen in dat het Ministerie van Financiën in veel andere lidstaten niet beleidsverantwoordelijk is voor de accountancysector. Omdat de Europese verordening zich richt op de financiële sector zagen andere lidstaten geen meerwaarde in de accountancysector hieronder te scharen. Nederland blijft voorstander van het opnemen van de accountancysector in de reikwijdte, omdat ook hier operationale risico's van belang zijn, en zal hier ten tijde van de review aandacht voor vragen.

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?

[1] Zie bijvoorbeeld de EBA richtsnoeren inzake de gemeenschappelijke procedures en methoden voor het proces van toetsing en evaluatie door de toezichthouder (SREP) en stresstests voor toezichtdoeleinden (EBA/GL/2022/03), onderdeel 144.

De leden van GroenLinks-PvdA vragen naar een centrale EU-hub en waarom dit niet in DORA wordt opgericht. De Europese Commissie is nooit verder gegaan dan het voorstel om eerst te kijken naar haalbaarheid en toegevoegde waarde van een dergelijke centrale EU-hub. De verwachting is dat de haalbaarheidsstudie half januari 2025 gereed is. Een centrale EU-hub heeft voordelen, maar brengt ook verantwoordelijkheden en uitvoeringsvraagstukken met zich mee. Het is belangrijk dat binnen de EU-hub veilig informatie gedeeld kan worden en dat er goed gekeken wordt naar wie toegang heeft tot deze gegevens. Bovendien kan het zo zijn dat financiële ondernemingen dan ook mogelijk informatie delen die raken aan de nationale veiligheid. Nationale veiligheid valt expliciet buiten deze verordening, omdat dit ingevolge het Verdrag betreffende de Europese Unie de eigen verantwoordelijkheid is van lidstaten. Om deze redenen is gekozen om de melding die financiële ondernemingen doen nog voor nu nationaal te regelen. Ik vind daarom voor dit moment een haalbaarheidsstudie een werkbaar alternatief welke mogelijkheden biedt voor de toekomst.

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 naar de coördinatie tussen verschillende Europese toezichthouders. DORA betreft sector-overstijgende wetgeving en vereist daarom de samenwerking tussen de drie sectorale Europese toezichthouders (EBA, EIOPA, ESMA), samen de *European Supervisory Authorities* (ESA's), voor de coördinatie van de verschillende gedeeltelijke verantwoordelijkheden. De gedeelde verant-woordelijkheden betreffen onder andere de ontwikkeling van richtsnoeren en technische standaarden, het Oversightkader voor kritieke derde partijen (zoals clouddienstverleners) en het reageren op meldingen van ernstige ICT-incidenten.

De ESA's gaan oversight uitvoeren op kritieke derde aanbieders van ICT-diensten zoals grote clouddienstverleners. Artikel 32 DORA legt de basisbeginselen voor de samenwerking voor het oversightkader. Voor elke kritieke derde dienstverlener wordt één van de ESA's aangewezen als *Lead Overseer* en onder artikel 32(7) DORA worden richtsnoeren opgesteld die de samenwerking tussen de ESA's en nationale bevoegde autoriteiten vormgeven. Daarbij is specifiek gekeken naar een efficiënte manier van samenwerking.

De samenwerking op het gebied van ernstige ICT-gerelateerde incidenten (die gerapporteerd dienen te worden bij de nationale toezichthouder) bestaat uit het beoordelen of een incident van belang is voor andere lidstaten en het centraal verzamelen en rapporteren van de ernstige ICT-gerelateerde incidenten Europees.

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 GroenLinks-PvdA merken terecht op dat er operationele risico's zijn bij cryptoactivadienstverleners. Het veiliger maken van cryptomarkten heeft de aandacht van de regering en het ministerie. Zo wordt gewerkt aan de implementatie van de Europese verordening markten in cryptoactiva (MiCA) die op 30 december 2024 van toepassing wordt. Het gedeelte in MiCA dat gaat over stablecoins[2] wordt al op 30 juni 2024 van toepassing. MiCA brengt cryptoactivadienstverleners en uitgevers van stablecoins onder toezicht. MiCA stelt onder andere regels ten aanzien van consumentenbescherming, het tegengaan van marktmisbruik en prudentiële eisen voor aanbieders van stablecoins en cryptoactivadiensten. Cryptoactivadienstverleners die een vergunning hebben op grond van MiCA vallen dan ook onder het toepassingsgebied van DORA. Dit betekent dat deze dienstverleners ook aan alle vereisten omtrent digitale operationele weerbaarheid moeten voldoen die in DORA vermeld staan. Er is op het gebied van digitale operationele weerbaarheid dus sprake van een gelijk speelveld met traditionele financiële instellingen.

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 GroenLinks-PvdA-fractie vragen naar de additionele toezichtkosten. De Autoriteit Financiële Markten (AFM) en de Nederlandsche Bank (DNB) zullen vanaf de toepassingsdatum van de verordening op 17 januari 2025 toezicht gaan houden. De toezichthouders maken kosten voor dit toezicht en de voorbereiding daarop. Deze kosten worden doorberekend aan de onder toezicht staande instellingen. DNB heeft de voorbereidingskosten tot en met 2024 binnen de eigen begroting opgevangen. Het kostenkader van de AFM is voor 2024 reeds opgehoogd, onder andere in verband met de voorbereidingskosten voor DORA.[3] DNB heeft aangegeven vanaf 2025 structureel ca. 17 fte voor het DORA-toezicht in te zetten. De AFM is van plan om 18 fte in te zetten. Ik ben met de toezichthouders in gesprek over de inhoud van het kostenkader 2025–2028, waarin deze kosten landen, en zal uw Kamer tijdig voorafgaand aan de vaststelling van dit kostenkader informeren. Daarna is het aan de toezichthouders om, binnen de grenzen van het kostenkader, keuzes te maken over de toezichtinzet voor DORA.

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.

Cyberveiligheid is een belangrijk en actueel thema binnen de EU. De leden van de D66-fractie merken terecht op dat er verschillende Europese wetgevingskaders zijn met een eigen set weerbaarheidsmaatregelen. De *Network and Information Security Directive* (NIS2-richtlijn) die de leden aanhalen is gericht op een versterking van de digitale en economische weerbaarheid van Europese lidstaten. Er is hier met name aandacht voor risico's die netwerk- en informatiesystemen bedreigen, zoals cyberbeveiligingsrisico's. In de NIS2-richtlijn is opgenomen dat Verordening (EU) 2022/2554 (DORA) moet worden beschouwd als een sectorspecifieke

[2] Stablecoins zijn een soort cryptoactiva waarvan de uitgever claimt dat deze zijn uitgegeven op basis van een onderliggend reserve van activa. Deze hebben een stabiele monetaire waarde.
[3] Kamerstukken II 2023/24, 32 545, nr. 197.

rechtshandeling van de Unie met betrekking tot de NIS2-richtlijn voor wat financiële entiteiten betreft. Dat betekent dat de weerbaarheidsmaatregelen uit DORA voorgaan op die uit de NIS2-richtlijn, inclusief het toezicht en de zorg- en meldplicht. De reden hiervoor is dat DORA strengere en specifiekere eisen kent dan de NIS2-richtlijn. Het toezicht op de digitale operationele- en cyberweerbaarheid van financiële ondernemingen ligt bij DNB en AFM.

Voorts vragen deze leden van de D66-fractie 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. DORA vereist niet dat aanbieders van ICT-diensten waar financiële ondernemingen gebruik van maken gevestigd moeten zijn in Nederland of in andere EU-lidstaten. Er wordt in DORA ook geen expliciete voorkeur gegeven aan Europese aanbieders van ICT-diensten zoals clouddienstverleners. Wel vallen kritieke derde aanbieders (zoals clouddienstverleners) van ICT-diensten binnen een oversightkader, waarbij er aanvullende regels opgesteld zijn om ook in te kunnen grijpen bij partijen die niet gevestigd zijn in de EU. DORA vereist daarnaast dat financiële ondernemingen een zogenaamde «*multi-vendor* strategie» aanhouden die ervoor moet zorgen dat de afhankelijkheid van een enkele partij verminderd wordt. Strategische autonomie is een belangrijk onderwerp binnen Nederland en Europa waarbinnen de afhankelijkheid van derde landen op bepaalde dienstverlening onderkend wordt. Hoewel het geen expliciet beleid is dat financiële instellingen voorkeur moeten geven aan Europese dienstverleners, wordt er positief gekeken en meegewerkt aan projecten die Europese dienstverleners ondersteunen.

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.

De leden van de CDA-fractie vragen naar de lasten die voortkomen uit DORA voor de verschillende financiële instellingen. DORA betreft op veel onderdelen een stringentere en meer gedetailleerde uitwerking van regels die op dit moment veelal in bestaande sectorale richtlijnen worden gesteld. DORA harmoniseert deze regels door middel van het introduceren van één verordening voor de financiële sector en wijzigt een aantal reeds bestaande Europese richtlijnen. Dit betekent dat veel instellingen tot op zekere hoogte al gewend zijn om aan regels omtrent de operationele weerbaarheid te voldoen.

Zo eist DORA van instellingen dat zij afhankelijkheidsrisico's en concentratierisico's van derde ICT-dienstverleners nauwkeurig in kaart brengen en beheersen. Ook in bestaande wet- en regelgeving wordt reeds verwacht dat een instelling deze uitbestedingsrisico's onder controle heeft. Ook de verplichting van het melden van ernstige ICT-incidenten is een verplichting die bepaalde financiële dienstverleners(zoals banken en betaalinstellingen) al kennen. Wel is het zo dat er bijvoorbeeld voor pensioenfondsen en verzekeraars sprake is van een meer gedetailleerdere uitwerking van de vereisten dan deze twee sub-sectoren tot nu toe gewend zijn. Voor een aantal dienstverleners, zoals ratingbureaus en verzekeringstussenpersonen, bestaan er op dit moment nog helemaal geen wettelijke eisen t.a.v. operationele risico's en geen rapportageverplichtingen.

Voor veel rapportageverplichtingen uit DORA geldt dat deze slechts op verzoek van de toezichthouder aangeleverd dienen te worden en daarmee geen periodieke rapportageverplichting heeft. DNB en de AFM houden risicogestuurd toezicht waardoor dergelijke rapportages vooral opgevraagd zullen worden wanneer daar aanleiding toe is. Daarnaast wordt op een aantal plekken in de verordening ook het proportionaliteits-beginsel toegepast. Zo hoeven midden-, kleine- en micro-ondernemingen aan minder zware regels te voldoen.

3. 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.

De leden van de NSC-fractie vragen naar welke concrete aspecten van de richtlijn hierna nog moeten worden geïmplementeerd. Voor enkele financiële ondernemingen golden al sectorale regels in het kader van ICT-beheer en cyberveiligheid, zoals bijvoorbeeld voor banken vanuit de richtlijn kapitaalvereisten. De implementatie van de DORA-richtlijn zorgt ervoor dat die sectorale regels geharmoniseerd worden. Enkele onderdelen van die sectorale regels zijn middels een algemene maatregel van bestuur geïmplementeerd en dienen nog aangepast te worden. De aanpassingen die nog plaats moeten vinden zien op harmonisering van reeds bestaande regels voor banken, betaalinstellingen, beleggingsondernemingen, icbe's en pensioenfondsen. Dit besluit dient voor 17 januari van kracht te zijn.

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?

De leden van de D66-franctie vragen in hoeverre de financiële instellingen klaar zijn voor de implementatie van DORA. Hoewel de toezichthouders geen totaalbeeld hebben van de status van de implementatie van DORA voor alle financiële instellingen, hebben zij regelmatig contact met de onder toezicht staande instellingen. De toezichthouders hebben het beeld dat de instellingen een flinke inspanning leveren om tijdig aan DORA te kunnen voldoen. Sommige instellingen zijn echt al aan de slag met de implementatie waar andere zich nog aan het inlezen zijn. DNB stelt dat het belangrijk is dat instellingen tijdig beginnen met de DORA implementatie gezien de brede set regels. De toezichthouders zijn in 2023 gestart met externe communicatie over DORA waarbij onder andere is gewezen op het belang om vroegtijdig te starten met implementeren. Communicatie

met de sector gaat onder andere middels nieuwsberichten, het organiseren van seminars en events, contact met brancheverenigingen en meer.[4]

Voorts vragen de leden naar hoe het toezicht vormgegeven gaat worden en wat er gebeurt als de instellingen niet aan de vereisten voldoen. Wanneer DORA per 17 januari 2025 van toepassing wordt, zal in het toezicht op ICT- en operationele risico's gebruik worden gemaakt van de vereisten die in DORA zijn opgenomen. Dit toezicht is risicogebaseerd. Wanneer uit onderzoek blijkt dat een instelling niet voldoet of slechts gedeeltelijk voldoet aan de vereisten dan zal dat kenbaar worden gemaakt aan de instelling en zal gevraagd worden om tijdig verbeteringen door te voeren.

4. 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?

De leden van de BBB-fractie verwijzen naar de memorie van toelichting waarin wordt aangegeven dat DORA naar verwachting zal leiden tot minder cyberincidenten. Het is lastig om een concrete analyse uit te voeren die inzichtelijk maakt hoeveel cyberschade voorkomen kan worden door middel van de implementatie van DORA. Er is destijds door de Europese Commissie, de lidstaten en het Europees Parlement bewust gekozen voor een alomvattend Europees kader op het gebied van digitale operationele weerbaarheid om ICT-risico's in de gehele financiële sector aan te pakken door financiële instellingen beter in staat te stellen om ICT-incidenten te voorkomen en te weerstaan. Dit draagt er ook aan bij dat cyberincidenten zich minder snel verspreiden over de gehele financiële sector. Het effectenbeoordelingsverslag van de Europese Commissie[5] (hierna: het verslag) geeft aan dat het moeilijk is de kosten van operationele incidenten in de financiële sector in te schatten omdat niet alle incidenten worden gemeld en de omvang van de kosten onzeker zijn. Tevens zijn op dit moment zijn niet alle instellingen verplicht om de cyberincidenten, dan wel de schade als gevolg van cyberincidenten, te melden bij de toezichthouder. Als gevolg daarvan is er op dit moment ook nog maar beperkt inzicht in de daadwerkelijke schade als gevolg van cyberincidenten.

---

[4] Zie bijvoorbeeld de websites van AFM (https://www.afm.nl/nl-nl/sector/themas/digitalisering/dora) en de seminars die DNB regelmatig organiseert (https://www.dnb.nl/nieuws-voor-de-sector/oud/toezicht-2023/dora-tijd-om-uit-de-startblokken-te-komen/)

[5] WERKDOCUMENT VAN DE DIENSTEN VAN DE COMMISSIE
SAMENVATTING VAN HET EFFECTBEOORDELINGSVERSLAG
Bij Voorstel voor een VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD betreffende digitale operationele veerkracht voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014 en (EU) nr. 909/2014, Brussel, 24-09-2020

Wel blijkt uit beoordelingen van de sector dat de kosten gerelateerd aan cyberincidenten voor de Europese financiële sector kunnen variëren van 2 tot 27 miljard euro per jaar. DORA zou deze directe kosten en de eventuele bredere gevolgen van grote cyberincidenten voor de financiële stabiliteit beperken. Ook worden de administratieve lasten verminderd door een einde te maken aan overlappende rapportagevereisten. Het verslag stelt dat sommige grootbanken op dit gebied bijvoorbeeld 40 tot 100 miljoen euro per jaar kunnen besparen. Daarnaast introduceert DORA geharmoniseerde testpraktijken die het opsporen van onbekende kwetsbaarheden zal verbeteren. Ook op dit gebied worden de kosten verminderd. Het verslag stelt dat voor de 44 grootste grensoverschrijdende Europese banken de totale verwachte baten van een gemeenschappelijke testaanpak bijvoorbeeld kunnen variëren van 11 tot 88 miljoen euro. De implementatie van DORA brengt tegelijkertijd ook kosten met zich mee voor de financiële instellingen. Deze kosten houden hoofdzakelijk verband met het doen van ICT-investeringen.

Dat gezegd hebbende zijn cyberrisico's uitgegroeid tot één van de belangrijkste aandachtsgebieden in de financiële sector. De AFM constateert een toename in het aantal en de impact van gemelde ICT-gerelateerde incidenten. Het is daarmee belangrijker dan ooit dat financiële instellingen een hoog niveau van operationele weerbaarheid onderhouden.

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 NSC-fractie vragen naar de regeldruk voor Nederlandse bedrijven naar aanleiding van DORA. DORA introduceert een proportioneel stelsel waarbij midden-, kleine- en micro-bedrijven aan minder strenge regels hoeven te voldoen ten opzichte van grote bedrijven. Tevens betreft een groot gedeelte van het DORA-raamwerk het harmoniseren van reeds bestaande ICT-vereisten voor financiële instellingen. Daarnaast zijn sommige financiële entiteiten uit hoofde van het desbetreffende sectorspecifieke Unierecht vrijgesteld of aan een zeer licht regelgevingskader onderworpen.

Dat gezegd hebbende zal het implementeren van DORA voor sommige instellingen een uitdaging zijn. Voor een aantal soorten ondernemingen zal er sprake zijn van een «inhaalslag». Er zijn ondernemingen die tot op heden relatief weinig te maken hebben gehad met regelgeving op het gebied van digitale operationele weerbaarheid. Hoewel er in DORA veel eisen worden gesteld, moeten deze ook worden gezien als een randvoorwaarde om te kunnen opereren in een wereld waarin digitale dreigingen kunnen leiden tot grote schade voor ondernemingen, consumenten, beleggers en de samenleving. Doordat DORA de ruimte laat voor proportionaliteit, is het mogelijk om het toezicht op deze regels risicogebaseerd te benaderen.

In het toezicht is er ook aandacht voor instellingen die een dergelijke inhaalslag moeten maken. AFM en DNB treden in gesprek met de sector om de sector te ondersteunen bij de voorbereiding om tijdig aan DORA te kunnen voldoen.

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 Algemene verordening gegevensbescherming (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 D66-fractie vragen naar het monitoren en rapporteren van ICT-gerelateerde incidenten en hoe wordt toegezien op de AVG. Tevens vragen de leden van de D66-fractie naar hoe de implementatie van deze verordening samenhangt met die van andere Europese verordeningen en hoe wordt voorkomen dat de regeldruk te hoog wordt.

Ten aanzien van het monitoren en rapporteren geldt dat van financiële instellingen wordt verwacht dat zij hun ICT-huishouding monitoren en ernstige ICT-incidenten melden bij de toezichthouder. Voor de ICT-incidentmeldingsplicht is een aantal criteria gedefinieerd, waaronder de financiële schade, de geografische spreiding en dataverlies die gepaard gaan met het ICT-incident. Op het moment dat een ICT-incident voldoet aan meerdere criteria, moet de financiële instelling dit melden bij de AFM of DNB. Het formulier dat hiervoor gebruikt dient te worden is op Unie-niveau vastgesteld op basis van de verordening. De AFM of DNB sturen de ICT-incidentmelding na ontvangst door naar de Europese toezichthouder die grensoverschrijdende coördinatie voert op de ICT-incidenten. Wanneer het een instelling betreft die onder direct toezicht staat van de ECB, wordt de melding naar de ECB gestuurd. Deze ICT-incidentmeldingen worden door de toezichthouders gebruikt voor de invulling van het risicogestuurd toezicht. De formulieren die nu geconsulteerd worden bevatten nauwelijks persoonsgegevens. Wanneer er wel persoonsgegevens verwerkt worden is de AVG van toepassing en wordt hier op passende wijze, conform staand beleid, door de toezichthouders mee omgegaan.

In antwoord op een eerdere vraag van de D66-fractie heb ik reeds de verhouding uitgelegd van de DORA-verordening met de NIS2-richtlijn. Ten aanzien van regeldruk is het zo dat verordeningen rechtstreeks doorwerken in de Nederlandse rechtsorde. Een verordening gaat vergezeld van een impact assessment van de Europese Commissie, waar de gevolgen van de desbetreffende verordening in geschetst worden. De Europese Commissie maakt zich sterk voor het vereenvoudigen van EU-regelgeving door onder andere in te zetten op lastenverlaging. In het jaarlijkse lastenoverzicht van de Europese Commissie is te zien wat zij doet om de regelgeving te vereenvoudigen en de lasten te verlagen.[6]

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

[6] Betere regelgeving: waarom en hoe – Europese Commissie (europa.eu)

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 BBB-fractie halen de passage over de regeldruk in de memorie van toelichting van DORA aan en verzoekt deze entiteiten verder uit te splitsen. Ik wil hierbij benadrukken dat de cijfers, genoemd in de memorie van toelichting, komen uit het effectbeoordelingsverslag van de Europese Commissie en dus betrekking hebben op alle instellingen in de EU die onder DORA gaan vallen, en niet alleen de Nederlandse. De 21.233 Europese entiteiten zijn uitgesplitst naar 5.665 kredietinstellingen, 5.934 beleggingsondernemingen, 2.666 verzekeringsbedrijven, 1.573 IORPs[7], 2.500 beheerders, 350 marktinfrastructuurpartijen (zoals centrale tegenpartijen en handelsplatformen), 45 kredietbeoordelaars en 2.500 betaalinstellingen en elektronischgeldinstellingen. Aanbieders van cryptodiensten, crowdfundingdienstverleners, accountantskantoren en benchmarkbeheerders zijn hierin niet meegenomen. Dit is dus een inschatting voor de gehele EU. Voor het Nederlands landschap geldt dat hier financiële ondernemingen van alle groottes onder vallen.

De verordening heeft impact op veel verschillende bedrijven binnen de financiële sector die gekenmerkt worden door heterogeniteit en niet altijd te vergelijken zijn. Per type financiële ondernemingen zijn de gevolgen daarom lastig in te schatten. De verordening kent proportionaliteit, wat betekent dat niet alle verplichtingen voor alle financiële ondernemingen gelden. Micro, kleine en middelgrote ondernemingen hebben te maken met uitzonderingen onder DORA of een verlicht regime. Daarnaast zijn sommige financiële entiteiten uit hoofde van het desbetreffende sector-specifieke Unierecht vrijgesteld of aan een zeer licht regelgevingskader onderworpen. In het licht van die vrijstellingen zou het niet evenredig zijn de betrokken financiële entiteiten onder het toepassingsgebied van de DORA-verordening te laten vallen, zij zijn dus ook vrijgesteld.[8]

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 afwegings-ruimte 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.

---

[7] Instellingen die vallen onder de Europese richtlijn betreffende de werkzaamheden van en het toezicht op instellingen voor bedrijfspensioenvoorziening ofwel de *Occupational Retirement Provision Directive* (IORP)

[8] Artikel 2, derde lid van Verordening 2022/2554 (verordening digitale operationele weerbaarheid).

De leden van de CDA-fractie vragen naar de meerwaarde van toetsing door het Adviescollege toetsing regeldruk (ATR) en waarom er geen uitwerking wordt gemaakt van technische reguleringsnormen en richtsnoeren. Het is goed om te benoemen dat ATR zelf geen gevolgen van wetgeving (eventueel afkomstig uit de EU) schetst, maar slechts toetst of beleid, waaronder wetgeving, de gevolgen van het te nemen beleid goed in kaart brengt. Omdat een verordening direct doorwerkt in de Nederlandse rechtsorde en in beginsel geen nationale beleidsruimte kent, valt dit buiten de adviestaak van ATR.[9]

De technische reguleringsnormen en richtsnoeren maken geen direct onderdeel uit van de verordening en worden bovendien momenteel op dit moment nog uitgewerkt en vastgesteld, waardoor de regeldruk niet bepaald kan worden.

Vanaf 17 januari 2028 voert de Commissie, na raadpleging van de Europese toezichthouders en het *European Systemic Risk Board*, een evaluatie uit van de DORA-verordening en dient zij bij het Europees Parlement en de Raad een verslag in, al dan niet vergezeld van een wetgevingsvoorstel. In deze evaluatie wordt gekeken naar de effectiviteit van de maatregelen uit DORA en wordt ook rekening gehouden met de praktische ervaring van financiële entiteiten.

Daarnaast hebben de toezichthouders doorlopend contact met de financiële instellingen waarbij regeldruk een belangrijk thema is. Het ministerie heeft op haar beurt regelmatig contact met de toezichthouders waarbij dit soort signalen gedeeld worden en spreekt ook regelmatig met de betrokken brancheorganisaties en individuele instellingen.

Op deze manier houden we en vinger aan de pols bij de instellingen voor wat betreft regeldruk. Dat gezegd hebbende is het weerbaar zijn tegen cyberrisico's belangrijker dan ooit, daarbij wordt het als zeer belangrijk geacht dat de instellingen een hoge mate van weerbaarheid hebben en onderhouden.

De Minister van Financiën,
S.P.R.A. van Weyenberg

[9] Artikel 1:7, eerste lid Algemene Wet Bestuursrecht en aanwijzing 9.16, tweede lid, van de Aanwijzingen voor de regelgeving bepalen dat adviesverplichtingen niet gelden voor één-op-één implementatie van Europese regelgeving.»