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. 3

MEMORIE VAN TOELICHTING

ALGEMEEN

§ 1. Inleiding

Dit wetsvoorstel voorziet in de aanpassingen van de Wet op het financieel toezicht (Wft) die noodzakelijk zijn ter implementatie van Richtlijn (EU) 2022/2556 van het Europees Parlement en de Raad tot wijziging van de Richtlijnen 2009/65/EG, 2009/138/EG, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 en (EU) 2016/2341 wat betreft digitale operationele weerbaarheid voor de financiële sector (PbEU 2022, L 333) (hierna: de richtlijn). Bij deze toelichting is een transponeringstabel behorende bij de implementatie van de richtlijn opgenomen.

Naast deze richtlijn is er ook een verordening, Verordening (EU) 2022/2554 van het Europees Parlement en de Raad betreffende digitale operationele weerbaarheid voor de financiële sector en amendering van verordeningen (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 en (EU) No 909/2014 (PbEU 2022, L 333) (hierna: de verordening). De richtlijn en de verordening vormen een gezamenlijk kader ter verbetering van de digitale operationele weerbaarheid voor de financiële sector. De verordening is van toepassing vanaf 17 januari 2025 en de richtlijn dient op diezelfde datum geïmplementeerd te zijn in nationale wet- en regelgeving. Deze verordening staan in het Engels bekend als de *Digital Operational Resilience Act* en wordt afgekort tot DORA.

In paragraaf 2 wordt de aanleiding en totstandkoming van zowel de richtlijn als de verordening besproken. In paragraaf 3 wordt de inhoud van de verordening besproken, deze hangt samen met de richtlijn en verdient daarom inhoudelijke bespreking. In paragraaf 4 wordt de wijze van implementatie en de inhoud van het wetsvoorstel besproken. In paragraaf 5 komen de regeldrukkosten, uitvoering en financiële gevolgen van het wetsvoorstel aan de orde. De consultatie van het wetsvoorstel en de reactie daarop zal besproken worden in paragraaf 6. Daarna zullen de wijzigingen van deze implementatiewet artikelsgewijs worden besproken.

kst-36482-3
ISSN 0921 - 7371
's-Gravenhage 2023

§ 2. Aanleiding en totstandkoming richtlijn en verordening

De toegenomen digitalisering van de financiële sector brengt kansen met zich mee, maar ook risico's. Financiële ondernemingen worden steeds meer afhankelijk van informatie- en communicatietechnologie (ICT), ook voor kritische interne processen. Verstoringen van deze ICT-processen kunnen leiden tot problemen in de continuïteit van de bedrijfsvoering van financiële ondernemingen, wat weer kan leiden tot risico's van consumentenbescherming en voor financiële stabiliteit. Daarom is op EU-niveau een uniform kader voor digitale operationele weerbaarheid voor de financiële sector tot stand gekomen.

Na de financiële crisis zijn veel wijzigingen in het regelgevend kader voor de financiële sector aangebracht, voornamelijk om prudentiële risico's van financiële ondernemingen te verkleinen en de consumentenbescherming te verhogen. Sindsdien heeft zich een bredere ontwikkeling van digitalisering van financiële dienstverlening voltrokken, wat tot gevolg heeft dat financiële ondernemingen steeds meer cyber- en ICT-risico's lopen. In de afgelopen jaren zijn digitale ketens langer geworden, is de connectiviteit tussen ondernemingen en derde partijen (zoals clouddienstverleners) toegenomen en zijn er nieuwe digitale kwetsbaarheden bij financiële ondernemingen bijgekomen die kwaadwillenden kunnen misbruiken. ICT-verstoringen bij financiële ondernemingen kunnen tot grote problemen leiden, niet alleen voor de financiële onderneming zelf, maar ook voor de financiële stabiliteit en consumentenbescherming in den brede en kan daarmee ook maatschappelijke gevolgen hebben. Het uitvallen van één partij vanwege een ICT-risicogerelateerd incident kan een effect hebben op andere partijen in de keten, wat kan leiden tot systeemrisico's.

Hoewel er reeds Unieregels op sectoraal niveau bestaan die zien op ICT, en operationele en cyberrisico's, gelden deze maar voor een klein aantal typen dienstenaanbieders, zoals banken en betaalinstellingen. Voor overige financiële dienstverleners hebben sommige lidstaten zelf regelgevende kaders opgesteld. De normen zijn vaak algemeen en in veel gevallen zijn er helemaal geen regels. Het wettelijk kader voor financiële ondernemingen op dit terrein is daardoor zeer versnipperd. Dit maakt effectief toezicht houden moeilijk en leidt tot inconsistenties in wet- en regelgeving tussen lidstaten, een imperfecte interne markt en onnodige kosten voor de sector. Om bovenstaande redenen is deze verordening en richtlijn opgesteld om in de Unie te komen tot een eenvormig wetgevend kader ten aanzien van digitale operationele weerbaarheid van de financiële sector.

§ 3. Inhoud verordening

In deze paragraaf wordt kort de inhoud van de verordening besproken. De verordening kent drie hoofddoelen. Ten eerste worden de reeds bestaande, maar versnipperde sectorale Unieregels ten aanzien van cyberweerbaarheid van de financiële sector geharmoniseerd middels een richtlijn, zodat ze in lijn zijn met de verordening, hierover wordt verder gesproken in paragraaf 4. Ten tweede creëert de verordening een regelgevend kader voor financiële ondernemingen waarvoor nog geen weerbaarheidseisen bestonden. Ten derde bevat de verordening regels om de risico's van uitbesteding van kritieke ICT-processen van financiële ondernemingen aan derde aanbieders van ICT-diensten (zoals clouddienstverleners) beter te mitigeren en om de versnippering van de regels daaromtrent tegen te gaan.

In de verordening is gekozen voor een risicogebaseerde aanpak. Financiële diensten kunnen sterk van elkaar verschillen, en ook binnen dezelfde diensten zijn er verschillen in grootte van instellingen en bedrijfsmodellen. De verordening houdt daarom rekening met onder andere de omvang en het algehele risicoprofiel en de aard van de financiële onderneming, alsook de complexiteit van diensten, activiteiten en verrichtingen.

De verordening bevat allereerst een algemeen kader waarbinnen financiële ondernemingen verplicht worden om maatregelen te nemen om ICT-risico's te beheersen (artikelen 5 tot en met 16). Zo dient de financiële onderneming onder andere kaders op te stellen om ICT-risico's te beheersen, ervoor te zorgen dat zij adequate ICT-systemen gebruikt en deze goed te onderhouden, beschermings- en preventiemaatregelen te nemen waar nodig en continuïteitsplannen op te stellen en deze regelmatig te actualiseren. Voor een aantal ondernemingen, die een relatief laag risico vormen voor het financiële stelsel, is er vanuit het oogpunt van proportionaliteit een vereenvoudigd kader voor ICT-risicobeheer opgesteld.

Vervolgens worden financiële ondernemingen verplicht om ernstige ICT-gerelateerde incidenten te melden bij de bevoegde autoriteit, en hiervoor systemen op te zetten waarmee incidenten gemonitord, vastgelegd en geclassificeerd worden (artikelen 17 tot en met 23).

Financiële ondernemingen dienen daarnaast periodiek de digitale weerbaarheid te testen op paraatheid, eventuele zwaktes en tekortkomingen (artikelen 24 tot en met 27). Alle financiële ondernemingen zullen hierbij jaarlijks hun ICT-systemen dienen te testen op een bepaald basisniveau, waarbij significante instellingen, die worden aangewezen door de bevoegde autoriteiten, ook minimaal eens per drie jaar geavanceerde ethische hacktesten op basis van actuele dreigingsinformatie zullen ondergaan, zogenaamde «Threat Led Penetration Testing» (TLPT).

Vervolgens worden er bepalingen geïntroduceerd ten aanzien van het beheer van ICT-risico's van derde partijen die ICT-diensten aanbieden aan financiële ondernemingen (artikelen 28 tot en met 30). Financiële ondernemingen die gebruik maken van de diensten van bepaalde derde partijen (bijv. clouddienstverleners) zullen onder andere het functioneren van deze diensten, en de eventuele bijkomende risico's die deze diensten kunnen vormen voor de kernprocessen van de financiële onderneming, in kaart moeten brengen en blijven monitoren. Om deze monitoring effectief uit te kunnen voeren dienen bepaalde aspecten van de dienstverlening en de relatie tussen dienstverlener en financiële onderneming vastgelegd te worden in contractuele afspraken. Deze bevatten bijvoorbeeld afspraken over de locaties waar persoonlijke data wordt verwerkt en exit-strategieën als de financiële onderneming wil overstappen van aanbieder. Naast gestandaardiseerde contractclausules zullen ook vrijwillige clausules worden ontwikkeld, specifiek voor clouddienstverleners. Financiële ondernemingen dienen daarnaast te voorkomen dat er concentratierisico's ontstaan door een te grote afhankelijkheid van bepaalde dienstverleners voor het uitvoeren van kritische processen.

Verder worden kritieke derde aanbieders van ICT-diensten onderworpen aan een *oversight*kader op Unieniveau (artikelen 31 tot en met 44). ICT-aanbieders worden op EU-niveau kritiek geacht op basis van (een combinatie van) de aard, omvang, en het belang van hun diensten, klanten, en marktaandeel, alsmede de mate waarin hun dienstverlening te vervangen is en de grensoverschrijdendheid daarvan. Het gaat hierbij om veelal zeer grote technologiebedrijven die een groot gedeelte van de

financiële sector op EU-niveau bedienen, waarbij er risico's zijn dat een verstoring bij deze dienstverleners tot problemen kan leiden voor meerdere financiële ondernemingen in de EU, en daarmee de financiële stabiliteit in het algemeen. De Europese Toezichthoudende Autoriteiten (ETA's) krijgen gezamenlijk een mandaat, dit zijn de Europese Bankenautoriteit (EBA), de Europese autoriteit voor verzekeringen en bedrijfspensioenen (EIOPA) en de Europese autoriteit voor effecten en markten (ESMA). Binnen dit gezamenlijke mandaat kunnen de ETA's onder andere audits uit te voeren bij, en bindende aanbevelingen doen aan de kritieke derde aanbieder van ICT-diensten. De nationale bevoegde autoriteit kan, indien de kritieke derde aanbieder van ICT-diensten de aanbevelingen niet opvolgt, vervolgmaatregelen nemen richting de financiële onderneming, waarbij in uiterst geval geëist kan worden dat de financiële onderneming de dienstverlening moet beëindigen. Tenslotte bevat de verordening een wettelijk kader voor financiële ondernemingen om onderling informatie over cyberbedreigingen te delen (artikel 45).

§ 4. Wijze van implementatie en inhoud wetsvoorstel

Zoals eerder genoemd is er een richtlijn en een verordening. Een verordening werkt rechtstreeks door in de Nederlandse rechtsorde. Wel moet voorzien worden in uitvoering en handhaving van de verordening. Dat gebeurt met een wijziging van het Besluit uitvoering EU-verordeningen financiële markten zoals dat gebruikelijk is.

Met dit wetsvoorstel wordt de richtlijn deels geïmplementeerd. Ook op besluitniveau dienen nog enkele wijzigingen doorgevoerd te worden om de richtlijn volledig te implementeren. De richtlijn is bedoeld om eventuele eerder, in sectorale richtlijnen, geïntroduceerde eisen aan de ICT-huishouding van financiële ondernemingen te harmoniseren. In veel sectorale richtlijnen zijn reeds eisen gesteld ten aanzien van risicobeheer, interne procedures en respons- en herstelplannen. De richtlijn bewerkstelligt dat deze, bestaande, sectorale richtlijnen nu in lijn met de verordening worden gebracht. Deze sectorale richtlijnen zijn geïmplementeerd in de Wft en onderliggende regelgeving. Wijzigingen die in de Wft dienen te worden doorgevoerd, betreffen wijzigingen ten aanzien van de richtlijn kapitaalvereisten[1], de richtlijn herstel en afwikkeling van banken en beleggingsondernemingen[2], de richtlijn markten voor financiële instrumenten 2014[3] en de richtlijn betaaldiensten[4]. De wijzigingen die worden doorgevoerd in de Wft zijn erop gericht dat duidelijk is dat voor de ondernemingen waar reeds ICT-eisen voor bestonden, deze zich nu aan de eisen moeten houden gesteld in de verordening, waarin één uniform kader is vastgesteld. Voor enkele richtlijnen zijn ook wijzigingen op besluitniveau nodig. Enkele richtlijnen behoeven geen wijziging van

---

[1] Richtlijn 2013/36/EU van het Europees Parlement en de Raad van 26 juni 2103 betreffende toegang tot het bedrijf van kredietinstellingen en het prudentieel toezicht op kredietinstellingen, tot wijziging van Richtlijn 2002/87/EG en tot intrekking van de Richtlijnen 2006/48/EG en 2006/49 EG (PbEU 2013, L 176).

[2] Richtlijn nr. 2014/59/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende de totstandbrenging van een kader voor het herstel en de afwikkeling van kredietinstellingen en beleggingsondernemingen en tot wijziging van Richtlijn 82/891/EEG van de Raad en de Richtlijnen 2001/24/EG, 2002/47/EG, 2004/25/EG, 2005/56/EG, 2007/36/EG, 2011/35/EU, 2012/30/EU en 2013/36/EU en Verordeningen (EU) nr. 1093/2010 en (EU) nr. 648/2012, van het Europees Parlement en de Raad (PbEU 2014, L 173).

[3] Richtlijn nr. 2014/65/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende markten voor financiële instrumenten en tot wijziging van richtlijn 2002/92/EG en richtlijn 2011/61/EU (herschikking) (PbEU 2014, L 173).

[4] Richtlijn 2015/2366 EU van het Europees Parlement en de Raad van 25 november 2015 betreffende betaaldiensten in de interne markt, houdende wijziging van de Richtlijnen 2002/65/EG, 2009/110/EG en 2013/36/EU en Verordening (EU) nr. 1093/2010 en houdende intrekking van Richtlijn 2007/64/EG (PbEU 2015, L 337).

Nederlandse wet- en regelgeving, omdat in de Wft en onderliggende besluiten al voldoende ruimte is gecreëerd om aan de verplichtingen uit de verordening te kunnen voldoen, of omdat er middels een dynamische verwijzing in de Nederlandse tekst al naar de richtlijn zelf wordt verwezen. Dit betreft de richtlijn instellingen voor collectieve belegging in effecten[5], richtlijn solvabiliteit II[6], richtlijn beheerders van alternatieve beleggingsinstellingen[7] en de richtlijn instellingen voor bedrijfspensioenvoorziening[8].

De wijzigingen die deze richtlijn voornamelijk doorvoert in sectorale richtlijnen zien op wijziging van bestaande regels omtrent ICT-huishouding. Daarnaast dienen risico's, die geïdentificeerd worden tijdens tests van digitale operationele weerbaarheid bij banken, meegenomen te worden in reeds bestaande evaluaties. Ook dient de afwikkelingsautoriteit van banken en beleggingsondernemingen in het reeds op te stellen afwikkelingsplan de eisen van de verordening te betrekken ten aanzien van netwerk- en informatiesystemen. Beleggingsondernemingen dienen daarnaast aan de verordening te voldoen ten aanzien van het ICT-risicobeheer van handelssystemen die zich bezighouden met algoritmische handel, interne procedures ten aanzien van storingen van handelssystemen aan de verordening vereisten te laten voldoen. Ook dienen marktexploitanten ervoor te zorgen dat de door hen geëxploiteerde gereglementeerde markt voldoet aan de eisen van de verordening. De gereglementeerde markt dient daarnaast ook operationele weerbaarheid op te bouwen, hetzelfde geldt voor respons- en herstelplannen en het testen van algoritmes.

§ 5. Gevolgen

Regeldruk

In deze paragraaf wordt ingegaan op de regeldrukeffecten als gevolg van de implementatie van de richtlijn. De regeldrukeffecten als gevolg van de verordening worden hier niet meegenomen omdat de verordening rechtstreeks werkt en dus niet in Nederlandse wetgeving wordt geïmplementeerd. Voor de regeldrukeffecten van de verordening zij verwezen naar de effectbeoordeling van de Europese Commissie.[9] Zoals uit de effectbeoordeling naar voren komt zijn de eisen die voortvloeien uit de verordening in algemene zin proportioneel voor de instellingen gezien onder andere hun aard, omvang, complexiteit en risicoprofiel. Vermeldenswaardig is nog dat voor ondernemingen waarvoor nog geen sectorale regels op dit gebied bestaan de verordening wel regeldrukkosten met zich brengt maar dat deze ondernemingen veelal reeds op eigen initiatief maatregelen hebben getroffen om ICT-risico's te verminderen die overeenkomen met de nieuwe eisen, zoals de Europese Commissie benoemt in de effectbeoordeling.

---

[5] Richtlijn 2009/65/EG van het Europees Parlement en de Raad van de Europese Unie van 13 juli 2009 tot coördinatie van de wettelijke en bestuursrechtelijke bepalingen betreffende bepaalde instellingen voor collectieve belegging in effecten (icbe's) (PbEU 2009, L 302).

[6] richtlijn 2009/138/EG van het Europees Parlement en de Raad van 25 november 2009 betreffende de toegang tot en uitoefening van het verzekerings- en het herverzekeringsbedrijf (Solvabiliteit II) (herschikking) (PbEU 2009, L 335).

[7] Richtlijn nr. 2011/61/EU van het Europees Parlement en de Raad van de Europese Unie van 8 juni 2011 inzake beheerders van alternatieve beleggingsinstellingen en tot wijziging van de Richtlijnen 2003/41/EG en 2009/65/EG en van de Verordeningen (EG) Nr. 1060/2009 en (EU) Nr. 1095/2010 (PbEU 2011, L 174).

[8] Richtlijn 2016/2341/EU van het Europees Parlement en de Raad van 14 december 2016 betreffende de werkzaamheden van en het toezicht op instellingen voor bedrijfspensioenvoorziening (IBPV's) (PbEU 2016, L 354).

[9] Europese Commissie, COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT SWD(2020)0203 final.

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.

De richtlijn beperkt zich, kort gezegd, tot regeldruk voor ICT-risicobeheer voor de financiële ondernemingen die reeds sectorale regelgeving kenden. Deze ondernemingen dienen op basis van de sectorale richtlijnen genoemd in de vorige pararaaf enkele wijzigingen door te voeren. Deze eisen zijn opgenomen in de verordening, en worden dus niet beschreven in de richtlijn.

Kort gezegd worden voornamelijk de reeds gestelde sectorale eisen verder uitgewerkt. Instellingen dienden op basis van bovengenoemde sectorale richtlijnen te voldoen aan niet-gelijke vereisten inzake risicobeheer van de ICT-huishouding, waaronder het opstellen van nood- en continuïteitplannen. De effectbeoordeling beschrijft dat van alle bestaande instellingen die onder de verordening gaan vallen, zijnde 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. De terugkerende kosten zijn naar verwachting veel lager, omdat veel financiële ondernemingen reeds de investeringen in ICT en cyber security hebben verhoogd. Dat is ook gelijk het aandachtspunt. Sommige instellingen hebben reeds veel maatregelen getroffen en investeringen gedaan in hun ICT-risicobeheer. Het verschilt daarom van geval tot geval wat de daadwerkelijke investering moet zijn, de 5% is dus een gemiddelde.

Naast het bovenstaande zijn nog drie zaken noemenswaardig. In de richtlijn betaaldiensten zijn specifieke regels opgenomen met het oog op het verkrijgen van een machtiging tot het verrichten van betalingsdiensten. Deze machtigingsregels moeten worden gewijzigd om ze in overeenstemming te brengen met de verordening. Om de administratieve lasten te verminderen en complexe en overlappende rapportagevereisten te vermijden mogen daarnaast de in die richtlijn vervatte regels voor incidentenmelding niet langer van toepassing zijn op betalingsdienstaanbieders die onder die richtlijn en tevens onder de verordening vallen, zodat die betalingsdienstaanbieders kunnen profiteren van één volledig geharmoniseerd mechanisme voor de melding van alle betalingsgerelateerde operationele of beveiligingsincidenten, ongeacht of dergelijke incidenten ICT-gerelateerd zijn.

De wijzigingen in de richtlijn markten voor financiële instrumenten 2014 bewerkstelligen dat de gereglementeerd markt adequaat dient te zijn toegerust om risico's waaraan deze wordt blootgesteld, te beheren overeenkomstig de verordening. Dit geldt ook voor het testen van algoritmes. De verwachting is dat dit leidt tot een gemiddelde verhoging van 5% van de reeds bestaande kosten die in dit kader worden gemaakt.

Tenslotte dient opgemerkt te worden dat de tot nu toe bestaande sectorale regelgeving algemeen geformuleerd is, maar dat de richtsnoeren die door de ETA's uitgevaardigd zijn, specifiekere eisen bevatten waar instellingen zich reeds aan dienen te houden. Dit geldt ook voor de verordening, ook hier zal een deel van de regeldruk bepaald worden door technische reguleringsnormen en richtsnoeren, welke pas later vastgesteld zullen worden. Daarin zal wel zo veel mogelijk ingezet worden op de proportio-

naliteit die ook de verordening kent. Dat zal voor kleine instellingen een positief effect hebben.

Het adviescollege toetsing regeldruk (ATR) heeft aangegeven dat de richtlijn voor deze implementatiewet geen afwegingsruimte kent. Deze valt daarmee onder de uitzonderingen die zijn afgesproken met de Minister van EZK.[10]
Het wetsvoorstel hoeft daarmee niet aan het adviescollege te worden voorgelegd.

Uitvoering en handhaafbaarheid

De Autoriteit Financiële Markten (AFM) en de Nederlandsche Bank (DNB) hebben een uitvoeringstoets verricht op deze implementatiewet[11]. Beide constateren dat de richtlijn enkele bestaande sectorale richtlijnen wijzigt en daarmee de eisen die daarin worden gesteld in lijn brengt met de eisen uit de verordening. Hieruit volgen wel lasten, maar die zijn op basis van de verordening, waarin de inhoudelijke eisen zijn opgenomen. AFM en DNB zullen bij de uitvoeringstoets bij het implementatiebesluit toelichten wat de benodigde capaciteit zal zijn voor alle verplichtingen die voortvloeien uit de verordening en richtlijn. In het implementatiebesluit wordt namelijk de uitvoering en handhaving van de verordening geregeld in het Besluit uitvoering EU-verordeningen financiële markten.

Financiële gevolgen

Het wetsvoorstel heeft geen gevolgen voor de Rijksbegroting. De enige kosten voor de overheid betreffen toezichtkosten. In de financiële sector worden alle toezichtkosten gedragen door de ondertoezichtstaande ondernemingen zelf. Bij algemene maatregel van bestuur worden de toezichthouders aangewezen en in dat kader wordt inzicht gegeven in de kosten die dit meebrengt voor de toezichthouders.

Data Protection Impact Assessment

De richtlijn biedt voor financiële instellingen geen grondslag voor het verwerken van persoonsgegevens. De verordening biedt wel voor de ETA's en de bevoegde autoriteiten grondslagen wanneer het verwerken van persoonsgegevens nodig is het voor vervullen van de verplichtingen uit de verordening. Deze verwerking dient in lijn te zijn met de Algemene Verordening Gegevensbescherming. De verordening heeft bovendien onder andere als doel dat er meer ICT-veiligheid komt, wat de kans op datalekken (van onder andere persoonsgegevens) verkleint.

§ 6. Consultatie

Een concept van het wetsvoorstel en de memorie van toelichting is openbaar geconsulteerd op www.internetconsultatie.nl van 23 mei 2023 tot en met 26 juni 2023.

Er is naar aanleiding hiervan een consultatiereactie ontvangen van Adfiz (de branchevereniging voor onafhankelijke financieel adviseurs. In deze reactie wordt gevraagd om de aanvullende regelgeving (zoals richtsnoeren en technische reguleringsnormen) te laten toetsen door het Adviescollege Toetsing Regeldruk (ATR). De uitwerking van aanvullende

[10] 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.
[11] Tevens ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer

regelgeving wordt gedaan door de ETA's en de Europese Commissie. De nationale wetgever heeft geen rol in deze nadere uitwerking, die om deze reden dan ook niet door ATR getoetst kan worden.

Transponeringstabel behorende bij Richtlijn (EU) 2022/2556 van het Europees Parlement en de Raad van 14 december 2022 tot wijziging van de Richtlijnen 2009/65/EG, 2009/138/EG, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 en (EU) 2016/2341 wat betreft digitale operationele weerbaarheid voor de financiële sector (PbEU 2022, L 333/153).

Bepaling EU-regeling	**Bepaling in implementatieregeling of bestaande regeling** *(Toelichting indien niet geïmplementeerd of naar zijn aard geen implementatie behoeft)*	**Omschrijving beleids-ruimte**	**Toelichting op de keuze(n) bij de invulling van de beleids-ruimte**
Artikel 1, eerste lid	Wordt geïmplementeerd in artikel 29a van het Besluit gedragstoezicht financiële ondernemingen Wft (BGfo)	Geen	
Artikel 1, tweede lid	Behoeft geen implementatie, bepaling gericht tot de Europese Commissie	Geen	
Artikel 2, eerste lid	Implementatie door middel van bestaande regelgeving in artikel 3:17, tweede lid, aanhef en onderdeel a en c, Wft juncto artikel 26.2 Besluit prudentiële regels Wft (Bpr)	Geen	
Artikel 2, tweede lid	Behoeft geen implementatie, bepaling gericht tot de Europese Commissie.	Geen	
Artikel 3	Is al geïmplementeerd d.m.v. dynamische verwijzing in artikel 29a BGfo	Geen	
Artikel 4, eerste lid	Is al geïmplementeerd d.m.v. bestaand recht in 1:74 Wft	Geen	
Artikel 4, tweede lid	Wordt geïmplementeerd in artikel 20, vierde lid, Bpr	Geen	
Artikel 4, derde lid	Is al geïmplementeerd d.m.v. dynamische verwijzing in artikel 23a, aanhef en onderdeel a, Bpr	Geen	
Artikel 4, vierde lid	3:18a, eerste lid, Wft	Geen	
Artikel 5, eerste lid, onderdeel a en b	3A:9, vierde lid, Wft	Geen	
Artikel 5, tweede lid	Behoeft geen implementatie, want bijlage zonder implementatie	Geen	
Artikel 6, eerste lid, onderdeel a en b	Wordt geïmplementeerd in artikel 29a BGfo	Geen	
Artikel 6, tweede lid, onderdeel a	4:91n, tweede lid, Wft	Geen	
Artikel 6, tweede lid, onderdeel b	Behoeft geen implementatie, bepaling gericht tot de ETA's.	Geen	
Artikel 6, derde lid, onderdeel a en b	5:30, eerste lid, Wft.	Geen	
Artikel 6, vierde lid, onderdeel a, eerste alinea	5:30a, eerste lid, Wft, vernummering in het Besluit gereglementeerde markten Wft en artikel 10 van het Besluit bestuurlijke boetes financiële sector (Bbbfs)	Geen	
Artikel 6, vierde lid, onderdeel b	5:30a, tweede lid, onderdeel b, Wft, artikel 4b van het Besluit gereglementeerde markten Wft en artikel 10 Bbbfs	Geen	
Artikel 6, vierde lid, onderdeel c	Behoeft geen implementatie, bepaling gericht tot de Europese Commissie	Geen	
Artikel 7, eerste lid	1:5a, tweede lid, onderdeel j, Wft	Geen	

Bepaling EU-regeling	Bepaling in implementatieregeling of bestaande regeling *(Toelichting indien niet geïmplementeerd of naar zijn aard geen implementatie behoeft)*	Omschrijving beleids-ruimte	Toelichting op de keuze(n) bij de invulling van de beleids-ruimte
Artikel 7, tweede lid, onderdeel a, eerste sub	Wordt geïmplementeerd in artikel 26bb Bpr	Geen	
Artikel 7, tweede lid, onderdeel a, tweede sub	Wordt geïmplementeerd in artikel 26c Bpr en artikel 3a, eerste lid, onderdeel t van het Besluit Markttoegang financiële ondernemingen (Bmfo)	Geen	
Artikel 7, tweede lid, onderdeel a, derde sub	Wordt geïmplementeerd in artikel 26d Bpr en artikel 3a, eerste lid, onderdeel v Bmfo	Geen	
Artikel 7, tweede lid, onderdeel b	Wordt geïmplementeerd in artikel 26c, tweede lid onder a Bpr en artikel 3a, onderdeel x Bmfo	Geen	
Artikel 7, derde lid	Deze tekst staat reeds in de richtlijn betaaldiensten en behoeft niet opnieuw te worden geïmplementeerd.	Geen	
Artikel 7, vierde lid	Wordt geïmplementeerd in artikel 26f Bpr	Geen	
Artikel 7, vijfde lid	Wordt geïmplementeerd in artikel 26g Bpr	Geen	
Artikel 7, zesde lid	Behoeft geen implementatie, bepaling gericht tot EBA	Geen	
Artikel 8	Wordt geïmplementeerd in artikel 18 van het Besluit financieel toetsingskader pensioenfondsen	Geen	

ARTIKELSGEWIJS

Artikel I

A

Omdat er verwezen wordt in de Wft naar de verordening wordt ten behoeve van de leesbaarheid een definitie in artikel 1:1 Wft ingevoegd.

B

Artikel 1:5a, tweede lid, Wft bevat bepalingen over wat niet verstaan wordt als het verlenen van betaaldiensten. Ingevolge artikel 7, eerste lid, van de richtlijn wordt artikel 3, onder j, van de richtlijn betaaldiensten gewijzigd. Hiervoor wordt artikel 1:5a, tweede lid, onderdeel j, van de Wft gewijzigd. De wijziging voorziet erin dat over informatie- en communicatietechnologie (ICT) en communicatienetwerken wordt gesproken. Hiermee wordt de terminologie in dit artikel in overeenstemming gebracht met de richtlijn.

C

Ingevolge artikel 4, onderdeel 4, van de richtlijn wordt aan artikel 97, eerste lid, van de richtlijn kapitaalvereisten[12] een onderdeel toegevoegd. Dit onderdeel behelst een aanvulling op de bestaande opsomming van risico's die in dit eerste lid worden genoemd. Met die aanvulling wordt geborgd dat de risico's die zijn geïdentificeerd tijdens tests van digitale operationele weerbaarheid overeenkomstig hoofdstuk IV van de verordening worden meegenomen in de evaluatie bedoeld in de aanhef van het eerste lid van artikel 97 van de richtlijn kapitaalvereisten. De Nederlandse implementatie[13] van deze bepaling uit de richtlijn kapitaalvereisten hanteert een vergelijkbare opsomming van risico's in artikel 3:18a, eerste lid, van de Wft. Daarom wordt in artikel 3:18a Wft dit risico toegevoegd aan de al bestaande opsomming van risico's.

D

Artikel 3A:9, vierde lid, Wft verwijst naar artikel 8, vijfde tot en met twaalfde lid, van de verordening gemeenschappelijk afwikkelingsmechanisme[14] en verklaart die van overeenkomstige toepassing op het vaststellen van een afwikkelingsplan door DNB. De verordening past de verordening gemeenschappelijk afwikkelingsmechanisme niet aan, waardoor verwijzing in Nederlandse wetgeving naar de relevante bepaling ontbreekt. Om dit te ondervangen wordt artikel 3A:9, vierde lid, Wft aangepast waarbij er een verwijzing wordt opgenomen naar artikel 10, zevende lid, van de richtlijn herstel en afwikkeling van banken en beleggingsondernemingen, welke bepaling wel gewijzigd is door de richtlijn.

E

In artikel 4:91n, tweede lid, Wft, waarmee artikel 17, eerste lid, richtlijn markten voor financiële instrumenten 2014 is geïmplementeerd, zijn voorschriften opgenomen waaraan beleggingsondernemingen die zich met algoritmische handel bezighouden moeten voldoen, zoals voorgeschreven in de richtlijn markten voor financiële instrumenten 2014. De in dit onderdeel opgenomen wijzigingen van artikel 4:91n, tweede lid, Wft strekken tot implementatie van de in artikel 6, tweede lid, onderdeel a, van de richtlijn digitale operationele weerbaarheid opgenomen wijzigingen van artikel 17, eerste lid, van de richtlijn markten voor financiële instrumenten 2014.

In artikel 4:91n, tweede lid, aanhef, Wft wordt een verwijzing naar artikel 17, eerste lid, van de richtlijn markten voor financiële instrumenten 2014 opgenomen. Die wijziging bewerkstelligt dat de in artikel 4:91n, tweede lid, aanhef, Wft bedoelde interne procedures, die – kort samengevat – tot doel hebben de ordelijke werking van de handelssystemen van de beleggingsonderneming te waarborgen, de met in achtneming van de ingevolge artikel 17, eerste lid, van de richtlijn markten voor financiële instrumenten 2014 gestelde regels in aanmerking moeten nemen. Tot die

---

[12] Richtlijn 2013/36/EU van het Europees Parlement en de Raad van 26 juni 2013 betreffende toegang tot het bedrijf van kredietinstellingen en het prudentieel toezicht op kredietinstellingen, tot wijziging van Richtlijn 2002/87/EG en tot intrekking van de Richtlijnen 2006/48/EG en 2006/49/EG (PbEU 2013, L 176).

[13] Stb 2020, 509.

[14] Verordening (EU) nr. 806/2014 van het Europees Parlement en de Raad van 15 juli 2014 tot vaststelling van eenvormige regels en een eenvormige procedure voor de afwikkeling van kredietinstellingen en bepaalde beleggingsondernemingen in het kader van een gemeenschappelijk afwikkelingsmechanisme en een gemeenschappelijk afwikkelingsfonds en tot wijziging van Verordening (EU) nr. 1093/2010 (PbEU 2014, L 225).

regels behoren de in hoofdstuk II van de verordening opgenomen vereisten ten aanzien van ICT-risicobeheer waaraan de handelssystemen van beleggingsondernemingen die zich met algoritmische handel bezighouden op grond van artikel 17, eerste lid, eerste alinea, van de richtlijn markten voor financiële instrumenten 2014 moeten voldoen.

Verder wordt aan artikel 4:91n, tweede lid, Wft een (nieuw) onderdeel c toegevoegd. Hiermee wordt de derde alinea van artikel 17, eerste lid, richtlijn markten voor financiële instrumenten 2014 verwerkt. Artikel 4:91n, tweede lid, onderdeel c, Wft bepaalt dat een beleggingsonderneming die zich met algoritmische handel bezighoudt dient te beschikken over interne procedures om met storingen van haar handelssystemen verband houdende risico's te ondervangen zodat de bedrijfscontinuïteit van de beleggingsonderneming is gewaarborgd. Van die interne procedures dienen overeenkomstig artikel 11 van verordening opgestelde beleidslijnen en plannen ten aanzien van ICT-bedrijfscontinuïteit en ICT-respons- en herstelplannen deel uit te maken. Voorts bepaalt artikel 4:91n, tweede lid, onderdeel c, Wft dat een beleggingsonderneming haar handelssystemen volledig test en op adequate wijze controleert.

F

In artikel 5:27, eerste lid, onderdeel c Wft wordt verwezen naar artikel 5:30 Wft. In verband met verlettering in artikel 5:30 Wft is de verwijzing daarnaar in dit artikel aangepast.

G

Op grond van artikel 5:30, eerste lid, Wft moet een marktexploitant ervoor zorgen dat de (door hem geëxploiteerde) gereglementeerde markt voldoet aan de in dat artikel opgenomen voorschriften. Zo bepaalt artikel 5:30, eerste lid, Wft dat de gereglementeerde markt adequaat dient te zijn toegerust om de risico's waaraan dat handelsplatform is blootgesteld te kunnen beheren.

De wijzigingen van artikel 5:30, eerste lid, Wft strekken tot implementatie van de in artikel 6, derde lid, onderdelen a en b, van de richtlijn. Hierin worden aanpassingen gedaan in artikel 47, eerste lid, onderdelen b en c, van de richtlijn markten voor financiële instrumenten 2014. Laatstbedoelde onderdelen zijn verwerkt in artikel 5:30, eerste lid, onderdelen b en c, Wft. Aan dat voorschrift wordt toegevoegd dat dit beheer ook ziet op ICT-risico's op de ingevolge artikel 11 van de verordening gestelde regels. Tot die regels behoren de in hoofdstuk II van de verordening opgenomen voorschriften inzake ICT-risicobeheer.

Artikel 6, derde lid, onderdeel b, van de richtlijn schrapt artikel 47, eerste lid, onderdeel c, van de richtlijn markten voor financiële instrumenten 2014. In verband hiermee vervalt artikel 5:30, eerste lid, onderdeel c, Wft – waarin artikel 47, eerste lid, onderdeel c, van de richtlijn markten voor financiële instrumenten 2014 is verwerkt – en worden enige onderdelen van dat artikel verletterd.

Voor de goede orde wordt nog opgemerkt dat de in artikel 5:30, eerste lid, Wft bedoelde marktexploitant beschikt over een vergunning als bedoeld in artikel 5:26, eerste lid, Wft voor het in Nederland exploiteren of beheren van een gereglementeerde markt.

H

De in dit onderdeel opgenomen wijziging van artikel 5:30a, eerste lid, Wft strekt tot implementatie van de in artikel 6, vierde lid, onderdelen a en b, van de richtlijn opgenomen wijzigingen van het eerste respectievelijk zesde lid van artikel 48 van de richtlijn markten voor financiële instrumenten 2014. In de eerste plaats wordt de aanhef van artikel 5:30a, eerste lid, Wft gewijzigd. Die wijziging verwerkt artikel 6, vierde lid, onderdeel a, eerste alinea, van de hiervoor bedoelde richtlijn. Artikel 5:30a, eerste lid, aanhef, bepaalt dat een marktexploitant die beschikt over een vergunning als bedoeld in artikel 5:26, eerste lid, Wft en die een gereglementeerde markt exploiteert ervoor dient te zorgen dat de gereglementeerde markt operationele weerbaarheid opbouwt in overeenstemming met de in hoofdstuk II van de verordening opgenomen vereisten. Die vereisten hebben betrekking op het doeltreffende en prudent beheer van ICT gerelateerde risico's.

Verder wordt artikel 5:30a, eerste lid, onderdeel b, Wft gewijzigd. Die wijziging verwerkt artikel 6, vierde lid, onderdeel a, tweede alinea, van de richtlijn. In 5:30a, eerste lid, onderdeel b, wordt een nieuwe zinsnede opgenomen. Op grond van die zinsnede maken van de in dat onderdeel bedoelde regels deel uit beleidslijnen en plannen inzake ICT-bedrijfscontinuïteit en respons- en herstelplannen voor ICT die in overeenstemming zijn met de ingevolge artikel 11 van de verordening gestelde regels. Dat artikel regelt onder meer dat de hiervoor bedoelde respons- en herstelplannen in overeenstemming dienen te zijn met de voorschriften inzake respons en herstel bij elk type ICT-gerelateerde incident.

In het nieuwe tweede lid van artikel 5:30a Wft zijn de aanhef en de onderdelen c, d en f van het huidige artikel 5:30a, eerste lid, Wft vrijwel ongewijzigd overgenomen. De enige aanpassing is dat in artikel 5:30a, tweede lid, onderdeel b, Wft nader wordt gespecifieerd dat de in dat onderdeel bedoelde testomgevingen (voor het testen van algoritmen) moeten voldoen aan de in de hoofdstukken II (ICT-risicobeheer) en IV (Testen van digitale operationele weerbaarheid) van de verordening neergelegde voorschriften. Deze wijziging van artikel 5:30a, tweede lid, onderdeel b, Wft verwerkt de in artikel 6, vierde lid, onderdeel b, van de richtlijn opgenomen wijziging van het huidige artikel 48, zesde lid, van de richtlijn markten voor financiële instrumenten 2014.

In artikel 5:30a, zesde lid, (nieuw) Wft worden enige verwijzingen aangepast. Die aanpassingen houden verband met de introductie van een nieuw tweede lid in artikel 5:30a Wft waardoor enige andere leden van dat artikel dienden te worden vernummerd.

I

In de bijlagen behorende bij de artikelen 1:79 en 1:80 Wft wordt verwezen naar artikel 5:30a Wft. In verband met de vernummering van artikel 5:30a Wft is de verwijzing daarnaar in de bijlagen behorende bij de artikelen 1:79 en 1:80 aangepast.

De Minister van Financiën,
S.A.M. Kaag