Per e-mail verstuurd
De minister van Financiën
E. Heinen
Korte Voorhout 7
2511 CW DEN HAAG

Datum	
Ons kenmerk	24063291
Pagina	1 van 5
Telefoon	AFM
E-mail	AFM
Betreft	Uitvoeringstoets uitvoeringsbesluit digitale operationele weerbaarheid financiële sector (DORA)

Geachte heer Heinen,

Bij brief van 22 mei 2024 heeft u de Autoriteit Financiële Markten (AFM) verzocht om een uitvoeringstoets over het uitvoeringsbesluit verordening Digitale Operationele Weerbaarheid financiële sector (hierna: Uitvoeringsbesluit DORA).

Het Uitvoeringsbesluit DORA strekt tot uitvoering van de verordening digitale operationele weerbaarheid voor de financiële sector (hierna: DORA-verordening).[1] Het Uitvoeringsbesluit en de daarin neergeslagen keuzes zijn in nauw en goed overleg tussen vertegenwoordigers van uw ministerie, De Nederlandsche Bank (DNB) en de AFM tot stand gekomen. Deze brief bevat het resultaat van de uitvoeringstoets; Uit de toets volgt dat de AFM het toezicht op DORA kan uitvoeren in de laagste toezichtintensiteit. Hierin is voorzien in het kostenkader 2025-2028. Daarbij zal de AFM jaarlijks toetsen of de capaciteit nog passend is. Ook zal jaarlijks getoetst worden of en in hoeverre opschaling naar een hogere toezichtintensiteit wenselijk is.

Resultaat uitvoeringstoets
DORA heeft tot doel om op Europees niveau een uniform kader voor digitale operationele weerbaarheid voor de financiële sector tot stand te brengen. DORA omvat naast de eerdergenoemde verordening ook een richtlijn (hierna: DORA-richtlijn).[2] De DORA-verordening en DORA-richtlijn vormen een gezamenlijk het kader ter verbetering van digitale operationele weerbaarheid voor de financiële sector.

De normen uit de DORA-verordening zijn rechtstreeks van toepassing. De AFM zal door middel van het Uitvoeringsbesluit DORA worden aangewezen als de bevoegde toezichthouder om toezicht te houden op de

[1] 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).
[2] 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.

normen uit de verordening. De sanctionering van overtredingen van de normen worden tevens in dit Uitvoeringsbesluit geregeld. Concreet betekent dat de AFM verantwoordelijk is voor het toezicht op de naleving van de normen door onder andere handelsplatformen, beheerders van beleggingsinstellingen, instellingen voor collectieve beleggingen (icbe's), beleggingsondernemingen, adviseurs en bemiddelaars.[3] Zie voor de volledigheid bijlage 1 voor de instellingen waar de AFM toezicht op houdt.

Hieronder zal eerst worden ingegaan op de belangrijkste verplichtingen die de DORA-verordening introduceert voor deze instellingen en waar de AFM door middel van het Uitvoeringsbesluit DORA toezicht op moet gaan houden. Daarna zal ingegaan worden op wat dit betekent voor de uitvoerbaarheid door de AFM en de bekostiging daarvan. Zoals toegezegd in de uitvoeringstoets bij de Implementatiewet DORA van 18 januari 2023 (AFM-23075916), zal daarbij zal ook worden ingegaan op de uitvoerbaarheid door de AFM en de bekostiging van de verplichtingen die voorvloeien uit de DORA-richtlijn.

Inhoud belangrijkste verplichtingen[4]

ICT-risicobeheer
De verordening bevat een algemeen kader waarbinnen financiële ondernemingen verplicht worden om maatregelen te nemen om ICT-risico's te beheersen. 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.

Beheer, classificatie en rapportage van ICT-gerelateerde incidenten
Financiële ondernemingen moeten een beheerproces voor ICT-gerelateerde incidenten inrichten. Als onderdeel hiervan moeten deze ondernemingen incidenten monitoren, vastleggen en classificeren. Ernstige ICT-gerelateerde incidenten moeten bij de AFM worden gemeld. De AFM moet deze incidentrapportages vervolgens in behandeling nemen, vastleggen en doorsturen naar de ESA's.

Testen van digitale operationele weerbaarheid
Financiële ondernemingen dienen periodiek de digitale weerbaarheid te testen op paraatheid, eventuele zwaktes en tekortkomingen. Alle financiële ondernemingen zullen hierbij jaarlijks hun ICT-systemen dienen te testen op een bepaald basisniveau, waarbij 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). De AFM voert

[3] De AFM zal toezicht houden op: met betrekking tot verordening (EU) nr. 600/2014 (MiFIR), beheerders van cruciale benchmarks zoals bedoeld in artikel 20, eerste lid, onderdeel b van verordening (EU) nr. 2016/1011 (benchmarks), verordening (EU) 2020/1503 (crowdfundingdienstverleners voor bedrijven), handelsplatformen, beheerders van beleggingsinstellingen, beheerders van icbe's, datarapporteringdienstverleners als bedoeld in artikel 2, derde lid, eerste alinea van verordening (EU) nr. 600/2014 (MiFIR), beleggingsondernemingen, adviseurs voorzover zij adviseren over verzekeringen, bemiddelaars in verzekeringen, gevolmachtigde agenten of ondergevolmachtigde agenten, en aanbieders van cryptoactivadiensten, als bedoeld in artikel 3, eerste lid, onderdeel 15 van Verordening (EU) nr. 2023/1114 (cryptoactiva);
4 Tweede Kamer, vergaderjaar 2023–2024, 36 482, nr. 3

de integrale begeleiding van deze TLPT-tests uit en verstrekt de onderneming een attest voor de test waaruit blijkt dat aan de kwalitatieve eisen die worden gesteld aan de test, is voldaan.

ICT-risico's bij gebruik van derde partijen
Er worden bepalingen geïntroduceerd ten aanzien van het beheer van ICT-risico's van derde partijen die ICT-diensten aanbieden aan financiële ondernemingen. 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 instelling, 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. 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. De ondernemingen moeten hun contracten met leveranciers van ICT-diensten in een eigen register van informatie bijhouden.

Kritieke derde aanbieders van ICT-diensten
Kritieke derde aanbieders van ICT-diensten worden onderworpen aan een oversightkader op EU-niveau. 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.

Uitvoerbaarheid door de AFM en bekostiging
De AFM zal door middel van het Implementatiebesluit DORA belast worden met het toezicht op de nakoming van de hierboven genoemde verplichtingen. De hierboven genoemde verplichtingen betreffen de belangrijkste verplichtingen die de DORA-verordening introduceert. De DORA-verordening en richtlijn bevatten echter veel meer verplichtingen waar de AFM ook toezicht op moet houden.

De impact van DORA op de AFM en de consequenties voor ons toezicht is substantieel. De huidige beschikbare capaciteit binnen het toezicht en de ondersteunende afdelingen is onvoldoende om adequaat toezicht te houden op de verplichtingen die voortvloeien uit DORA. De benodigde capaciteit in termen van fte's en IT-kosten die hiervoor nodig zijn, is aanzienlijk. Zo zullen de nieuwe verplichtingen gaan gelden voor ongeveer 500 instellingen die onder het toezicht van de AFM vallen. Verder zal voor het overgrote deel van die instellingen het toezicht op IT-aspecten worden uitgebreid van de huidige algemene bedrijfsvoeringsnorm van 3 artikelen naar een wettelijk kader onder DORA van 64 artikelen.

Kosten van toezicht op DORA
De AFM heeft verschillende scenario's uitgewerkt om te bepalen hoe het beste toezicht gehouden kan worden op de nieuwe verplichtingen uit DORA. De scenario's bieden differentiatie in toezichtintensiteit. Er is gekozen voor het scenario met de laagste toezichtintensiteit gegeven de risicotolerantie van de AFM, met de nadrukkelijke mogelijkheid om dit op termijn uit te breiden naar een hogere toezichtintensiteit. Binnen

dit gekozen scenario zal de AFM risicogestuurd toezicht houden, zullen de toezichtactiviteiten gericht zijn op het verbeteren van de compliance en zal de AFM in een periodieke cyclus toezichtactiviteiten uitvoeren bij de financiële instellingen die moeten voldoen aan de verplichtingen uit DORA. Het primaire doel van DORA is het beheersen van systeemrisico en in het verlengde daarvan het consumenten- en beleggersrisico. De gekozen toezichtaanpak legt de nadruk daarom op de meest systeemrelevante instellingen.

Voor het toezicht op andere (niet systeemrelevante) instellingen is ook capaciteit nodig. Binnen het gekozen scenario is beperkte capaciteit beschikbaar voor het toezicht op deze instellingen. De AFM zal zich voor deze instellingen beperken tot activiteiten zoals thematische onderzoeken, marktbrede communicatie-uitingen en de toepassing van instrumenten zoals 'self-assessments'. Hierbij loopt de AFM het risico dat zij IT-risico's in de toezichtspopulatie niet tijdig ziet en oplost. Ten slotte is de AFM verplicht om de rapportageverplichtingen na te komen. Ook hiervoor is capaciteit nodig.

Bij een uitbreiding naar een hoger toezichtintensiteit, zal de AFM het toezicht uitbreiden naar toezichtmogelijkheden op risico's, niet zijnde systeemrisico's. Dit houdt in dat onderzoeken gedaan zullen worden op specifieke thema's en risico's bij instellingen met een middelgrote systeemrelevantie. Op basis van de daaruit gesignaleerde risico's kan de AFM de mate van compliance met DORA van de sector beter in kaart brengen en daar waar nodig verbetertrajecten af te dwingen. Of de AFM wil uitbreiden, hangt af van de situatie die zij aantreft in de sector met betrekking tot DORA compliance. Op dit moment is de informatiepositie van de AFM nog te beperkt om daar een uitspraak over te doen.

Voor het scenario met de laagste toezichtintensiteit is ingeschat dat structureel 17,75 fte's benodigd zal zijn. Daarbij zal de AFM jaarlijks toetsen of de capaciteit nog passend is. Ook zal jaarlijks getoetst worden of en in hoeverre opschaling naar een hogere toezichtintensiteit wenselijk is. In dat geval zal met het ministerie van Financiën in overleg getreden moeten worden.

Kosten ter voorbereiding op DORA
Voordat DORA inwerking treedt is veel voorbereidend werk nodig, zowel vanuit de beleidsfunctie van de AFM, als vanuit experts uit toezicht, de afdeling juridische zaken en IT. De voorbereidingskosten in 2024 zijn van dusdanige omvang, dat dit tot aanpassing van de begroting en het huidige kostenkader heeft geleid (in overleg met het ministerie van Financiën en de Raad van Toezicht van de AFM). Deze voorbereidingskosten lopen tijdens de voorbereiding op van 6,75 FTE in 2023 tot 11,25 FTE in 2024. Vanaf 2025 is structureel 17,75 FTE nodig. De structurele kosten voor het toezicht op DORA zijn verwerkt in het nieuwe kostenkader 2025-2028. De werkzaamheden die worden uitgevoerd tijdens de voorbereiding zien op onder andere het bijdragen aan level 2 wetgeving, het ontwikkelen van toezichtinstrumenten, het opleiden van medewerkers, het werven van medewerkers en het voorbereiden van de sector.

IT-kosten
Ten slotte zijn er IT-investeringen nodig. Voor deze investeringen is EUR 1,2 mln. begroot in 2024. Verder zijn er doorlopende IT-kosten. Deze bedragen vanaf 2025 EUR 0,4 mln. per jaar. Deze kosten zijn voor beheer en onderhoud van de software die nodig is voor het DORA-toezicht en in anticipatie op wijzigingen die nog moeten worden gedaan.

Samenvattend en zoals hierboven toegelicht is, kan geconcludeerd worden dat de AFM het toezicht op DORA (waarbij initieel gekozen is voor het scenario met de laagste toezichtintensiteit), het voorbereidend werk voor DORA en de IT-investeringen alleen kan doen als voorzien wordt in extra budget voor fte's en IT-kosten. In het kostenkader 2025-2028 is hierin voorzien. Verder is het van belang te benadrukken dat bovengenoemde cijfers gebaseerd zijn op schattingen op basis van de situatie zoals die nu is. De praktijk zal moeten uitwijzen of de schattingen voldoende blijken te zijn. Indien u vragen heeft naar aanleiding van de uitvoeringstoets verzoeken wij u contact op te nemen met de AFM.

Hoogachtend,
Autoriteit Financiële Markten