FINNIUS

# Pleidooi voor Proportionaliteit

**9 februari 2023**

5 MINUTEN

U heeft het gezien, de Finnius Vooruitblik is weer uit. Voor ons gevoel werd er, mede gezien de verschillende mails en telefoontjes hierover, niet eerder zo reikhalzend naar uitgekeken. Dat verbaast me niks: ieder jaar spreken wij de hoop en verwachting uit dat het zo ondertussen toch wel wat minder zal worden met de nieuwe toezichtwetgeving. Ieder jaar blijkt het ijdele hoop. De toezichtwetgeving blijft maar verder uitdijen.

Nieuwe loot aan de stam is DORA, kort voor: *Digital Operational Resilience Act*. Een verordening die, heel kort gezegd, gaat over ICT-risicobeheer. Mijn kantoorgenoot Laurens Hillen schreef er eerder al een lezenswaardige blog over. DORA verscheen op 27 december 2022 in het Publicatieblad van de EU. DORA heeft met ingang van 17 januari 2025 rechtstreekse werking binnen de EU. Vanwege een nog te publiceren artikel verdiepte ik me de afgelopen weken in DORA. Ik viel van de ene in de andere verbazing. De mate van diepgang en detail, in combinatie met een abstract definitie-apparaat, maken DORA een wetgevingspakket om met enige angst te verwelkomen.

Ter illustratie: financiële instellen moeten op grond van DORA beschikken over een kader voor ICT-risicobeheer. Artikel 6 lid 2 DORA vereist dat dit kader ten minste moet omvatten (letterlijk overgenomen): ‘strategieën, beleidslijnen, procedures, ICT-protocollen en instrumenten die nodig zijn om alle informatie- en ICT-activa, met inbegrip van computersoftware, hardware, servers naar behoren en toereikend te beschermen, en om alle relevante fysieke elementen en infrastructuur**,** zoals gebouwen en terreinen, datacentra en als gevoelig aangewezen gebieden te beschermen, teneinde te waarborgen dat alle informatie- en ICT-activa toereikend worden beschermd tegen risico’s, waaronder schade, ongeoorloofde toegang en ongeoorloofd gebruik.’ En dit is nog maar één van vele verplichtingen op het gebied van ICT-risicobeheer. Zo’n beetje alles wat je over dit onderwerp zou kunnen verzinnen, wordt door DORA uitgewerkt en voorgeschreven.

DORA is echter niet het enige recente wetgevingspakket dat één specifiek onderwerp zo gedetailleerd uitwerkt. Ik zie diezelfde mate van detail namelijk bijvoorbeeld ook bij nieuwe EBA Richtsnoeren ten aanzien van de Compliance Officer en Remote Customer Onboarding, en net zo goed bij de lagere regelgeving ten aanzien van de SFDR en Taxonomie Verordening. Ook ESMA kan er wat van: denk maar aan de ESMA Richtsnoeren ten aanzien van Cloud Outsourcing en Marketing Communications. Het is nog maar een greep uit recente wet- en regelgeving vanuit Europa.

Dan denk ik zo langzamerhand: je zou maar een fondsbeheerder zijn en vallen binnen het bereik van de AIFMD, MiFID II, PRIIPs, de Wft, het BGfo, de Nrgfo, de Prospectusverordening, de Verordening Marktmisbruik, de Benchmarkverordening, de SFDR, de Taxonomieverordening en straks ook nog DORA… Dan ben ik er vast nog een vergeten en laat ik lagere regelgeving, zoals bijvoorbeeld gedelegeerde verordeningen en de hiervoor genoemde richtsnoeren, buiten beschouwing. Ik geef het je te doen. Groot of klein: dit is hoe dan ook een uitdaging.

Ik bespeur zo langzamerhand ook de nodige metaalmoeheid bij marktpartijen. Natuurlijk is er de wens en instelling om alle nieuwe en bestaande wet- en regelgeving te implementeren en na te leven. Tegelijkertijd is het *zo* veel, in een wereld die toch al bomvol staat van crises, dat het bijna ondoenlijk wordt om alles wat aandacht vraagt, ook de vereiste aandacht te geven. Als we niet oppassen is een volgende stap dan al gauw om een risico-inschatting te maken: aan welk implementatieproject geef ik voorrang? Met dus ook de impliciete acceptatie dat andere trajecten die voorrang niet krijgen… Ik vind dat een onwenselijke ontwikkeling en sta kennelijk ook niet alleen in deze verzuchting, gezien een recente Opinie van Laura van Geest, bestuursvoorzitter van de AFM, in Het Financieele Dagblad.

Alsof deze smeekbede gehoord is door de wijze dames en heren in Brussel, biedt DORA ineens een interessante ontwikkeling. Artikel 4 DORA voorziet namelijk in een nadrukkelijke verankering van het proportionaliteitsbeginsel (in DORA: evenredigheidsbeginsel). De vereisten uit DORA moeten door financiële instellingen worden toegepast, 'rekening houdend met hun omvang, algehele risicoprofiel en de aard, schaal en complexiteit van hun diensten, activiteiten en verrichtingen'. Het zijn elementen die we vaak terugzien waar, veelal ten aanzien van specifieke bepalingen in toezichtwetgeving en dus niet een hele verordening, een beroep op het proportionaliteitsbeginsel is toegestaan. Dat dit principe nu in feite voor heel DORA geldt stemt hoopvol.

Het blijft echter een onzeker spel. Hoe moet je deze elementen uitleggen en concreet toepassen in de praktijk? Wanneer kom je er materieel voor in aanmerking en hoe moet de procedure er formeel uitzien? Hoe weet je nu of een toezichthouder, als op enig moment een thema-onderzoek wordt verricht, dat beroep op proportionaliteit kan volgen, en dus niet handhavend zal optreden ten aanzien van non-compliance met verplichtingen die je op grond van proportionaliteit op een minder stringente wijze naleeft? Er blijft in die gevallen namelijk weinig verdediging over voor de marktpartij: hij heeft nota bene zelf aangegeven dat bepaalde verplichtingen minder stringent worden nageleefd.

DNB publiceerde in 2018 al een rapport over proportioneel en effectief toezicht[1], met name gericht op prudentiële toezichtregels. Een lezenswaardig document, maar DNB geeft, mede gezien de aard van het document, geen concrete handvatten hoe marktpartijen hier in individuele gevallen invulling aan kunnen geven. Voor zover mij bekend is er, een enkele uitzondering daargelaten[2], vanuit de AFM nauwelijks guidance beschikbaar ten aanzien van het proportionaliteitsbeginsel. Die onzekerheid leidt er in de praktijk vaak toe dat marktpartijen dan toch maar een '*better safe than sorry*' aanpak kiezen. Dat is zonde in gevallen waar de wet een proportionele toepassing wel toestaat. De toezichthouder is er ook niet bij gebaat als marktpartijen matig invulling geven aan heel veel regels in plaats van heel goed invulling geven aan minder, maar wel bij het profiel passende regels.

Laten we dan dus, ten aanzien van DORA maar ook in bredere zin, ook écht gebruikmaken van het beginsel van proportionaliteit. Ik snap dat het lastig is dit concreet te maken, maar de

toezichthouders zouden toch wel guidance kunnen geven naar welke criteria ze kijken, wat voor procedures instellingen moeten doorlopen, hoe vaak ze dit beroep moeten herzien, etc.

Laat de AFM en DNB dus nuttige guidance geven en marktpartijen het vertrouwen geven dat daarop in de praktijk, uiteraard mits goed onderbouwd en periodiek herzien, een beroep gedaan kan worden. De markt verdient het en het zou zeer welkom zijn, ook om de moed erin te houden.

Kortom: ik begin het nieuwe toezichtjaar met een pleidooi voor meer proportionaliteit in toezicht.

[1] Zie de link naar het document: https://www.dnb.nl/media/yojpc5a5/dnb-studie-proportioneel-en-effectief-toezicht.pdf.

[2] Zie bijvoorbeeld guidance van de AFM ten aanzien van AIFMD vergunninghouders die van rechtswege een AIFMD vergunning hebben ontvangen: https://www.afm.nl/nl-nl/sector/actueel/2018/jan/verbetering-beheerders-beleggingsinstellingen.

## Specialisten

**Tim de Wit**
T +31 (0)20 767 01 80
T +31 (0)20 820 80 32 (direct)
M +31 (0)6 11 00 45 26
tim.de.wit@finnius.com