# DORA: veiligheid door veerkracht?

**Op 16 januari 2023 is DORA in werking getreden. Financiële ondernemingen moeten vanaf 17 januari 2025 DORA-proof zijn. De vraag is of daarmee niet te veel van de sector wordt gevergd.**

DORA (Digital Operational Resilience Act) is een Europees wetgevingspakket dat als doel heeft om binnen de financiële sector de digitale operationele weerbaarheid te bevorderen. Het pakket moet ervoor zorgen dat de financiële sector in de EU bij ernstige operationele verstoringen veerkrachtig blijft functioneren. DORA bestaat op dit moment uit een richtlijn en een verordening. In 2024 zullen daar nog gedelegeerde regels van vooral technische aard aan worden toegevoegd. De regeling is van toepassing op nagenoeg alle soorten financiële ondernemingen, op een aantal kleinere financiële ondernemingen na, zoals AIFMD light-beheerders en bepaalde kleinere verzekeraars. DORA is ook van belang voor de inrichting van ICT-arrangementen met ICT-dienstverleners, die ook rechtstreeks onder DORA komen te vallen. Als zij cruciale diensten verlenen, komen zij bovendien onder toezicht te staan van de relevante financiële toezichthouder.

DORA voorziet voor de gehele EU in uniforme vereisten voor de beveiliging van netwerk- en informatiesystemen van de door de regeling bestreken ondernemingen, zodat deze bestand zijn tegen alle soorten ICT-gerelateerde verstoringen en dreigingen. Het pakket bevat regels op het punt van ICT-risicobeheer, ICT-incidentmanagement, het testen van operationele weerbaarheid, risicobeheer bij gebruikmaking van externe ICT-dienstverleners, rechtstreeks toezicht op cruciale ICT-dienstverleners, en samenwerking en toezicht door de verschillende toezichthouders. Dat deze regelgeving hoognodig is, staat buiten kijf. Financiële ondernemingen worden bijna dagelijks geconfronteerd met (pogingen tot) hacks en cyberaanvallen. DORA zal zeker bijdragen aan het mitigeren van deze risico's.

De financiële sector heeft twee jaar de tijd om DORA in de bedrijfsvoering te implementeren. Als het aan de AFM ligt – zoals bleek uit de column van Laura van Geest van 14 april 2023 in het FD – zou het bij voorkeur nog sneller moeten. De vraag is of daarmee niet te veel van de sector wordt gevergd. In de eerste plaats zullen de betrokken financiële ondernemingen in kaart moeten brengen wat DORA precies voor hen betekent. Het gaat daarbij om het analyseren van complexe regels. Vervolgens zullen zij hun interne ICT-huishouding moeten doorlichten en deze waar nodig anders moeten inrichten. Daarnaast zullen de met ICT-dienstverleners aangegane overeenkomsten kritisch moeten worden bekeken en eventueel moeten worden aangepast. Dat geldt ook als deze overeenkomsten recentelijk nog zijn geamendeerd om ze in overeenstemming te brengen met de richtsnoeren van de toezichthouders op het punt van uitbesteding.

Ook de in het vooruitzicht gestelde toevoeging aan DORA in 2024 van gedelegeerde regels van technische aard maakt een tijdige invoering er niet gemakkelijker op. Zolang die regels niet bekend zijn, is volledige implementatie immers niet mogelijk. En dan is er sinds 27 december 2022 ook nog de tweede Europese richtlijn inzake de beveiliging van netwerk- en informatiesystemen, de NIS2-richtlijn. Deze richtlijn moet op 17 oktober 2024 geïmplementeerd zijn in het nationale recht. De NIS2-richtlijn voorziet voor verschillende kritieke sectoren in risicobeheersingsverplichtingen op het gebied van cyberbeveiliging. Zij is ook van toepassing op banken, handelsplatformen en CCPs. Weliswaar prevaleert DORA als sectorspecifieke regeling boven de NIS2-richtlijn, maar de wetgever moet nog wel zorgen voor de noodzakelijke afstemming.

DORA-proof worden vóór 17 januari 2025 lijkt geen eenvoudige opgave en is in ieder geval een uitdaging. ■

Door **Prof. Mr. W.A.K. Rank**, Advocaat bij NautaDutilh te Amsterdam en Hoogleraar Financieel Recht aan de Universiteit Leiden