159. DORA: van theorie naar praktijk

MR. L.B.G. HILLEN EN MR. M.H. KOK

DORA, DORA, klik op DORA. Zo luidt niet alleen het begin van de pakkende titelsong van het bekende kinderprogramma, maar ook het dringende advies van toezichthouders AFM en DNB[1] aan alle financiële ondernemingen die per 17 januari 2025 aan deze belangrijke nieuwe Europese verordening moeten gaan voldoen. Dit artikel beoogt financiële ondernemingen te voorzien van een stoomcursus DORA, inclusief praktische aanbevelingen voor de voorbereiding op de nieuwe regels voor digitale operationele weerbaarheid.

1. Introductie

De inwerkingtreding van de Europese *Digital Operational Resilience Act* (DORA)[2] komt steeds dichterbij. Deze verordening richt zich op het stroomlijnen en verbeteren van het ICT-risicobeheer van financiële ondernemingen en het creëren van een uniform kader voor digitale operationele weerbaarheid binnen de Europese financiële sector.[3] Na de introductie van het wetsvoorstel van de Europese Commissie in 2020 is op 27 december 2022 de finale tekst gepubliceerd, de zogenoemde Level 1 regelgeving. DORA Level 1 is al zeer uitgebreid, maar er komt nog meer op de financiële sector af. De Europese toezichthouders ESMA, EBA en EIOPA (ESA's)[4] hebben van de Europese wetgever de taak gekregen om door middel van zogeheten 'technische reguleringsnormen' (*Regulatory Technical Standards*, RTS) en 'technische uitvoeringsnormen' (*Implementing Technical Standards*, ITS) verschillende verplichtingen uit DORA nader uit te werken. Dit wordt ook wel Level 2 regelgeving genoemd. Tot slot zullen de ESA's op deelonderwerpen richtsnoeren en andere vormen van aanvullende *guidance* publiceren. Dit zijn zogeheten Level 3 teksten.

De opbouw van dit artikel is als volgt. Eerst zullen wij in vogelvlucht stilstaan bij de kern van DORA (par. 2) en welke ondernemingen binnen de reikwijdte van deze verordening zullen vallen (par. 3). Daarna zullen we ingaan op wat er verwacht wordt van binnen de reikwijdte vallende financiële ondernemingen (par. 4) en wat dit betekent voor ICT-dienstverleners van financiële ondernemingen (par. 5). We sluiten af met vijf praktische tips voor de voorbereiding op de inwerkingtreding van DORA (par. 6).

2. DORA in vogelvlucht

First things first: wat houdt DORA in de kern in? Er kan op meerdere manieren naar deze verordening worden gekeken. Redenerend vanuit processen zou DORA kunnen worden samengevat als een gedetailleerd raamwerk voor vier verschillende ICT-gerelateerde processen, namelijk (i) het ICT-risicobeheer, bestaande uit allerlei sub-processen, (ii) de omgang met ICT-gerelateerde incidenten, (iii) het doorlopend testen van de eigen ICT-weerbaarheid en (iv) het risicomanagement ten aanzien van ingeschakelde ICT-dienstverleners.

1 Zie het nieuwsbericht van de AFM, '*AFM vraagt aandacht voor de voorbereiding op DORA*' (20 juli 2023) te raadplegen via www.afm.nl, en het nieuwsbericht van DNB, '*DORA; tijd om uit de startblokken te komen*' (31 oktober 2023), te raadplegen via www.dnb.nl.

2 Verordening (EU) nr. 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011.

3 Inmiddels is al de nodige literatuur en guidance verschenen over DORA. Zie o.a. A. Carrier, 'Digital operational resilience for the financial services sector: overview of the proposed European Regime', *FRP* 2021/1050, afl. 7-8, p. 32-37; de DORA special van het *Tijdschrift voor Financieel Recht* (2023, nr. 5); S. Uiterwijk & J.V. Willems, 'DORA – een Europees kader voor de beheersing van ICT-risico's binnen de financiële sector', *Bb* 2023/10, afl. 4, p. 35-39; K. Christianen, 'DORA: meer veiligheid door wisselwerking tussen toezichtrecht en civiel recht', *MvV* 2023, afl. 6, p. 197-207; M.J. van Loopik, I.P. Palm-Steyerberg e.a., *The Twin Transition: Digital & Sustainable Finance. Preadvies voor de Vereniging voor Financieel Recht 2022* (Serie Van der Heijden Instituut nr. 179), Deventer: Wolters Kluwer 2022, hoofdstuk 2 (*DORA: beheersing van ICT-risico's en Europees toezicht op BigTech ondernemingen*); DNB, '*Voorbereiding op DORA: vergroten van de digitale weerbaarheid*' (27 maart 2024), te raadplegen via www.dnb.nl; en de reeks AFM publicaties over DORA (gedateerd 20 juli 2023, 1 december 2023 en 7 maart 2024), te raadplegen via www.afm.nl.

4 Voluit: de *European Securities and Markets Authority* (ESMA), de *European Banking Authority* (EBA) en de *European Insurance and Occupational Pensions Authority* (EIOPA).

Daarnaast kan DORA ook worden geduid door een onderscheid te maken tussen enerzijds regels voor de interne bedrijfsvoering van de financiële onderneming en anderzijds regels voor externe relaties. Als het gaat om de interne bedrijfsvoering bevat DORA bijvoorbeeld eisen met betrekking tot de vereiste ICT-kennis in het bestuur, het verankeren van de *three lines of defense* (of vergelijkbaar model) tegen ICT-risico's met bijbehorende rapportagelijnen en het beschikken over een ICT-strategie. Bij externe relaties doelen wij allereerst op de relaties tussen de financiële onderneming en ICT-dienstverleners. Andere externe relaties zijn met klanten en toezichthouders van de financiële onderneming. Voor ieder van de hiervoor genoemde relaties bevat DORA voorschriften. Denk aan gedetailleerde eisen aan de overeenkomsten die een financiële onderneming met haar ICT-dienstverleners sluit, het verplicht informeren van klanten over een ICT-incident en verschillende rapportageverplichtingen jegens de toezichthouder.

DORA is een zogeheten horizontale verordening, want het heeft betrekking op veel verschillende typen financiële ondernemingen en ziet op één specifiek onderwerp: ICT. Voorheen volgden de – zeer beperkte – ICT-regels voor financiële ondernemingen uit afzonderlijke sectorale richtlijnen. Naast de DORA-verordening is er ook een DORA-richtlijn.[5] Deze richtlijn strekt ertoe dat de bestaande sectorale richtlijnen voor wat betreft ICT-vereisten voortaan naar de DORA-verordening verwijzen.[6]

3. Welke ondernemingen worden door DORA geraakt?

Voor financiële ondernemingen is de essentiële eerste stap om vast te stellen in hoeverre zij per 17 januari 2025 binnen de reikwijdte van DORA zullen vallen. Op deze vraag zijn in principe drie antwoorden mogelijk, die we hieronder bespreken.

3.1 Optie 1: DORA is volledig van toepassing

DORA is van toepassing op 'financiële entiteiten' zoals gedefinieerd in DORA.[7] Denk aan banken, verzekeraars, betaalinstellingen, beleggingsondernemingen, beheerders van beleggingsinstellingen, maar ook aanbieders van crowdfundingdiensten en aanbieders van cryptoactivadiensten.

Voor financiële ondernemingen die onder de definitie van 'financiële entiteiten' vallen en geen beroep kunnen doen op een uitzonderingsgrond of verlicht regime, geldt in principe het (vrijwel) volledige DORA-kader. Gelet op het brede toepassingsbereik van DORA en de relatief beperkte uitzonderingen en verlichtingen (zie hierna), zal dit naar verwachting, ook in Nederland, een zeer grote groep financiële ondernemingen betreffen.

3.2 Optie 2: DORA is gedeeltelijk van toepassing

Als een financiële onderneming onder het toepassingsbereik van DORA valt, dan is het mogelijk dat DORA niet volledig maar slechts gedeeltelijk van toepassing is. De Europese wetgever heeft namelijk rekening willen houden met de belasting van DORA voor, kort gezegd, kleinere en/of lichter gereguleerde ondernemingen.

Voor financiële ondernemingen is de essentiële eerste stap om vast te stellen in hoeverre zij per 17 januari 2025 binnen de reikwijdte van DORA zullen vallen

DORA voorziet allereerst in een lichter regime voor zogenoemde 'micro-ondernemingen'. Een micro-onderneming wordt gedefinieerd als '*een financiële entiteit die geen handelsplatform, centrale tegenpartij, transactieregister of centrale effectenbewaarinstelling is, en waar minder dan 10 personen werkzaam zijn en waarvan de jaaromzet en/of en het jaarlijkse balanstotaal niet hoger liggen dan EUR 2 miljoen*'.[8] Verschillende verplichtingen uit DORA zijn niet van toepassing op micro-ondernemingen. Het betreft onder andere de eis om de verantwoordelijkheid voor het beheer van ICT-risico's toe te wijzen aan een controlefunctie,[9] de eis om het kader voor ICT-risicobeheer regelmatig te onderwerpen aan een interne audit,[10] de eis om over een functie voor crisisbeheer te beschikken[11] en eisen betreffende het testen van de eigen ICT-weerbaarheid.[12]

Daarnaast bevat DORA een zogenoemd 'vereenvoudigd kader' voor bepaalde financiële ondernemingen. Het gaat om zogeheten klasse 3 beleggingsondernemingen, vrijgestelde betaal-, elektronischgeld- en kredietinstellingen[13] en kleine instellingen voor bedrijfspensioenvoorziening. Voor deze ondernemingen geldt onder meer een separate, kleinere, set aan regels voor het ICT-risicobeheer.[14]

5 Richtlijn (EU) nr. 2022/2556 van het Europees Parlement en de Raad van 14 december 2022 tot wijziging van de Richtlijnen (EG) nr. 2009/65, (EG) nr. 2009/138, (EU) nr. 2011/61, (EU) nr. 2013/36, (EU) nr. 2014/59, (EU) nr. 2014/65, (EU) nr. 2015/2366 en (EU) nr. 2016/2341 wat betreft digitale operationele weerbaarheid voor de financiële sector. Deze richtlijn strekt tot wijziging van de UCITS-richtlijn, de Solvency II richtlijn, AIFMD, CRD, MiFID II, BRRD, PSD2 en de Pensioenrichtlijn.

6 In oktober 2023 heeft de Nederlandse wetgever het wetsvoorstel voor de implementatie van de DORA-richtlijn gepubliceerd. De implementatie zal plaatsvinden in de Wet op het financieel toezicht (Wft) en onderliggende regelgeving.

7 Art. 2(1) DORA.

8 Art. 3 onder 60 DORA.

9 Art. 6(4) DORA.

10 Art. 6(6) DORA.

11 Art. 11(7) DORA.

12 Art. 24 DORA.

13 Vrijgestelde kredietinstellingen enkel voor zover de lidstaten de lidstaatoptie van art. 2(4) DORA niet hebben toegepast.

14 Art. 16 DORA.

3.3 Optie 3: DORA is niet van toepassing

Sommige financiële ondernemingen vallen geheel niet onder het toepassingsbereik van DORA. Zo is DORA bijvoorbeeld niet van toepassing op (i) AIFMD light-beheerders, (ii) kleine verzekerings- en herverzekeringsondernemingen, (iii) instellingen voor bedrijfspensioenvoorzieningen die pensioenregelingen uitvoeren die samen niet meer dan 15 leden hebben, (iv) van MiFID II uitgezonderde natuurlijke of rechtspersonen en (v) verzekeringstussenpersonen, herverzekeringstussenpersonen en nevenverzekeringstussenpersonen die micro-ondernemingen, kleine of middelgrote ondernemingen zijn.[15] Ook is DORA niet van toepassing op aanbieders van krediet (niet zijnde een bank of verzekeraar) en accountantsorganisaties.

3.4 ICT-dienstverleners

Naast financiële ondernemingen heeft DORA ook – zij het indirect – invloed op ICT-dienstverleners (of in DORA termen: 'derde aanbieders van ICT-diensten').[16] Het gaat hier om elke '*onderneming die ICT-diensten verleent*' aan een financiële onderneming die onder DORA valt.[17] ICT-diensten zijn in DORA gedefinieerd als '*digitale en gegevensdiensten die doorlopend via ICT-systemen aan een of meer interne of externe gebruikers worden verleend, waaronder hardware als dienst en hardwarediensten, met inbegrip van het verlenen van technische ondersteuning via software- of firmware-updates door de hardwareaanbieder, met uitzondering van traditionele analoge telefoondiensten*'.[18] De Europese wetgever heeft duidelijk gemaakt dat de definitie van ICT-diensten breed moet worden opgevat.[19] Het gevolg daarvan is dat partijen die ICT-gerelateerde diensten verlenen aan financiële ondernemingen waarschijnlijk al snel zullen kwalificeren als ICT-dienstverlener in de zin van DORA.[20]

Het is bijzonder dat bepaalde ICT-dienstverleners op grond van DORA direct onder toezicht van financiële toezichthouders komen te staan. Dit is het geval als de ICT-dienstverlener als 'kritiek'[21] wordt aangemerkt.[22] Het gevolg van deze kwalificatie is dat één van de ESA's rechtstreeks toezicht zal uitoefenen op deze ICT-dienstverlener.[23]

4. Wat wordt er van financiële ondernemingen verwacht?

Zoals hiervoor opgemerkt, zien de verplichtingen uit DORA op vier ICT-kernprocessen, waartussen overigens de nodige overlap bestaat. Hieronder zullen deze kernprocessen worden toegelicht. Daarbij moet worden opgemerkt dat financiële ondernemingen die onder een verlicht regime vallen, niet ten volle aan de hierna te bespreken verplichtingen hoeven te voldoen (zie par. 3 hiervoor).

4.1 ICT-risicobeheer raamwerk

De in DORA opgenomen regels over ICT-risicobeheer zijn geïnspireerd op internationale, nationale en door de sector vastgestelde normen, richtsnoeren en aanbevelingen. De grondgedachte is dat het ICT-risicobeheer van een financiële onderneming moet voorzien in de volgende functies: (i) identificatie van het eigen ICT-landschap en de ICT-risico's die dat landschap kunnen bedreigen, (ii) bescherming tegen en het voorkomen van de verwezenlijking van ICT-risico's, (iii) monitoring van de ICT-systemen en detectie van ongewone ICT-activiteiten, (iv) respons en herstel van ICT-systemen en data bij ICT-incidenten, (v) communicatie richting stakeholders bij ICT-incidenten en (vi) scholing en ontwikkeling.[24] Voor ieder van deze functies bevat DORA specifieke eisen.

> Als onderdeel van het toezicht van de ESA's op kritieke ICT-dienstverleners, krijgen de ESA's bevoegdheden om allerlei informatie van deze dienstverleners op te vragen

Een belangrijk onderdeel van het raamwerk is de ICT-strategie, die goed gedocumenteerd moet worden. In deze strategie moet onder meer worden uitgewerkt wat het ICT-risicotolerantieniveau van de financiële onderneming is en hoe het ICT-risicobeheer de bedrijfsdoelstellingen van de onderneming ondersteunt.[25] Een ander belangrijk onderdeel van het ICT-risicobeheer raamwerk is de inbedding daarvan in de organisatie. Het bestuur van een financiële onderneming krijgt in DORA een centrale en actieve rol

15 Zoals gedefinieerd in DORA. Zie art. 2(3) DORA.

16 Opvallend is dat derde aanbieders van ICT-diensten expliciet worden genoemd in art. 2(1) onder u DORA als entiteiten waarop DORA (rechtstreeks) van toepassing is. De verplichtingen uit DORA richten zich namelijk tot financiële entiteiten als genoemd in art. 2(1) DORA (op de bepalingen inzake kritieke derde aanbieders van ICT-diensten na).

17 Art. 3 onder 19 DORA.

18 Art. 3 onder 21 DORA.

19 Overweging 35 DORA.

20 In paragraaf 5 van dit artikel zal nader op de impact van DORA op ICT-dienstverleners worden ingegaan.

21 Op basis van de in art. 31(2) DORA gestelde criteria.

22 Reeds onder toezicht staande financiële ondernemingen die ICT-diensten verlenen aan andere financiële ondernemingen kunnen niet als kritiek worden aangemerkt. De gedachte hierachter is dat deze ondernemingen al aan financieel toezicht zijn onderworpen. Ook ICT-dienstverleners die reeds onderworpen zijn aan bepaalde oversightkaders van de ECB, kunnen niet als kritiek worden aangemerkt, net als intra-groep ICT-dienstverleners en ICT-dienstverleners die uitsluitend in één lidstaat diensten verlenen aan financiële ondernemingen die enkel in die lidstaat actief zijn.

23 Art. 31(1)(b) DORA. Onder welke van de drie ESA's de ICT-dienstverlener uiteindelijk komt te vallen, hangt af van de financiële ondernemingen die diensten afnemen van de dienstverlener.

24 Zie overweging 47 DORA en art. 5 tot en met 16 DORA. Specifieke onderdelen uit het ICT-risicobeheer raamwerk worden nader uitgewerkt in Level 2 regelgeving, zie Gedelegeerde verordening van 13 maart 2024 tot vaststelling van tools, methoden, processen en beleidslijnen voor ICT-risicobeheersing en het vereenvoudigde raamwerk voor ICT-risicobeheersing (ten tijde van het schrijven van dit artikel nog niet gepubliceerd in het Publicatieblad van de EU), zoals geraadpleegd op 4 april 2024.

25 Art. 6(8) en 28(2) DORA.

toebedeeld. Zo moet het bestuur alle regelingen met betrekking tot het ICT-risicobeheer goedkeuren, dient zij toezicht te houden op de uitvoering van die regelingen en moet zij regelmatig opleidingen volgen over ICT-risicobeheersing.[26] Daarnaast moet een financiële onderneming zorgen voor een passende scheiding en onafhankelijkheid van ICT-risicobeheerfuncties (eerste lijn), controlefuncties (tweede lijn) en interne auditfuncties (derde lijn) (*three lines of defense*).

4.2 Omgaan met ICT-gerelateerde incidenten

Het tweede kernproces waarvoor DORA regels stelt, is het omgaan met ICT-gerelateerde incidenten. Een ICT-gerelateerd incident is, kort gezegd, een ongeplande gebeurtenis die de beveiliging van de ICT-systemen van een financiële onderneming in gevaar brengt en een nadelig effect heeft op de gegevens van of de dienstverlening door de onderneming.[27]

Ieder ICT-incident dat wordt gedetecteerd moet door de financiële onderneming worden geregistreerd en geclassificeerd. Dit classificatiesysteem is vrij uitgebreid en nader uitgewerkt in Level 2 regelgeving.[28] Als een ICT-incident als 'ernstig' kwalificeert, gelden er rapportageplichten jegens de AFM of DNB.[29] Een ernstig ICT-incident is een incident met grote nadelige gevolgen voor de ICT-systemen die kritieke of belangrijke functies van de financiële onderneming ondersteunen.[30] Wanneer hiervan sprake is, is eveneens op gedetailleerde wijze uitgewerkt in Level 2 regelgeving.[31]

Een financiële onderneming moet beschikken over een crisiscommunicatieplan en zelfs een woordvoerder aanwijzen.[32] Bij een ernstig ICT-incident dat gevolgen heeft voor de financiële belangen van cliënten, moet de onderneming, zodra zij het incident heeft opgemerkt, haar cliënten onverwijld in kennis stellen van het ernstige ICT-gerelateerde incident en van de maatregelen die zijn genomen om de negatieve gevolgen van het incident te beperken.[33]

4.3 Testen van de eigen ICT-weerbaarheid

Het periodiek testen van de eigen weerbaarheid tegen ICT-risico's is het derde kernproces waarvoor DORA verplichtingen in het leven roept. Een financiële onderneming moet beschikken over een testprogramma. De precieze invulling hiervan wordt overgelaten aan de onderneming, waarbij gedacht kan worden aan (i) kwetsbaarheidsbeoordelingen en -scans, (ii) open source analyses, (iii) netwerkbeveiligingsbeoordelingen, (iv) beoordelingen van fysieke beveiliging, (v) beoordelingen van broncodes, (vi) compatibiliteitstests, (vii) prestatietests, (viii) end-to-end tests en (ix) penetratietests.[34]

Ten minste één keer per jaar moeten er passende tests worden uitgevoerd op alle ICT-systemen en -toepassingen die kritieke of belangrijke functies van de financiële onderneming ondersteunen. De tests moeten worden uitgevoerd door onafhankelijke partijen, maar dat kunnen ook testers zijn die werkzaam zijn bij de financiële onderneming. Wanneer tests worden uitgevoerd door een dergelijke interne tester, moet de onderneming er wel voor zorgen dat belangenconflicten gedurende de hele ontwerp- en uitvoeringsfase van de test worden voorkomen.[35]

Door de bevoegde autoriteiten aangewezen financiele ondernemingen moeten ook ten minste elke drie jaar geavanceerde tests gaan uitvoeren. Het betreft zogeheten *threat led penetration tests* (TLPT).[36] Op dit moment bestaat er in Nederland en in de EU al een raamwerk voor TLPT. Dit raamwerk is in 2016 opgesteld door DNB (genaamd TIBER-NL) en door de ECB en andere Europese centrale banken binnen de EU verder uitgerold (genaamd TIBER-EU). In Nederland doen de circa 30 grootste financiële ondernemingen – denk aan grote banken, verzekeraars, betaalinstellingen en pensioenuitvoerders – op vrijwillige basis mee aan het TIBER programma. De regels uit DORA wijken echter op een aantal punten af van TIBER, waardoor een update van het TIBER-raamwerk is vereist. Zo voorziet TIBER-NL/TIBER-EU niet in het gebruik van interne testers bij TLPT, maar DORA wel. Op basis van de concept Level 2 tekst inzake TLPT lijkt het er vooralsnog op dat slechts een beperkt aantal Nederlandse financiële ondernemingen onder DORA zal worden aangewezen om TLPT uit te voeren.[37]

4.4 Beheer risico's inschakelen ICT-dienstverleners

Tot slot besteedt DORA veel aandacht aan de relatie tussen financiële ondernemingen en ICT-dienstverleners. Dit is logisch. Vanwege de voortschrijdende digitalisering worden financiële ondernemingen voor hun dienstverlening en bedrijfsprocessen in toenemende mate afhankelijk van ICT-

26 Art. 5 DORA. Ook werknemers van de financiële onderneming moeten bewustmakingsprogramma's en opleidingen op het gebied van ICT-beveiliging volgen (art. 13(6) DORA). DNB wijst er in haar nieuwsberichten overigens op dat ook commissarissen ('interne toezichthouders') hun kennisgebied met betrekking tot ICT-risicobeheer op niveau moeten brengen en houden, zie www.dnb.nl.

27 Art. 3(8) DORA.

28 Zie Gedelegeerde verordening van 13 maart 2024 tot nadere bepaling van de criteria voor de classificatie van ICT-gerelateerde incidenten en cyberdreigingen, tot vaststelling van materialiteitsdrempels en tot bepaling van de nadere informatie van verslagen over ernstige incidenten (ten tijde van het schrijven van dit artikel nog niet gepubliceerd in het Publicatieblad van de EU), zoals geraadpleegd op 4 april 2024.

29 Art. 19 DORA. DORA bevat ook regels over de classificatie en vrijwillige melding van significante cyberdreigingen, zie art. 18(2) en 19(2) DORA. Voor significante banken geldt dat DNB een melding van een ernstig ICT-incident doorzendt aan de ECB, zie artikel 19(1) DORA.

30 Art. 3(10) DORA.

31 Zie voetnoot 28.

32 Art. 14 DORA.

33 Art. 19(3) DORA.

34 Art. 25(1) DORA.

35 Art. 24 DORA.

36 Art. 26 DORA.

37 Zie de aanwijzingscriteria in het voorgestelde art. 2 van de concept Level 2 regelgeving in het ESA's consultatierapport '*Draft Regulatory Technical Standards specifying elements related to threat led penetration tests*' van 27 november 2023.

dienstverleners. Bovendien nemen de concentratierisico's daarbij toe door het grootschalig gebruik van ICT-diensten van een relatief kleine maar dominante groep dienstverleners (denk aan de paar Amerikaanse techbedrijven die een groot deel van de markt voor clouddiensten in handen hebben).[38]

Het identificeren en mitigeren van de risico's die gepaard gaan met het gebruik van ICT-dienstverleners – ongeacht of de dienstverlener tot dezelfde groep als de financiële onderneming behoort – is een belangrijk onderdeel van het ICT-risicobeheer.[39] Zo moet de financiële onderneming beschikken over een uitgeschreven strategie aangaande het inschakelen van ICT-dienstverleners. Voor de gevallen waarin een ICT-dienst wordt afgenomen ter ondersteuning van kritieke of belangrijke functies van de financiële onderneming, moet er beleid zijn voor (i) de selectie van de ICT-dienstverlener, (ii) de daarmee te sluiten overeenkomst, (iii) het toezicht op de prestaties van deze dienstverlener en (iv) het exit-plan bij de beëindiging van de overeenkomst.[40] De Level 2 regelgeving stelt gedetailleerde eisen aan dit beleid.[41]

> De belangrijkste DORA-bepalingen waar ICT-dienstverleners indirect door worden geraakt, zijn gelegen in de contractuele sfeer

Een belangrijke – en naar verwachting in de praktijk behoorlijk belastende – verplichting is het informatieregister dat een financiële onderneming moet bijhouden voor alle door haar afgesloten ICT-overeenkomsten. Dit register moet aan zeer gedetailleerde eisen voldoen en kan door de toezichthouder worden opgevraagd.[42] Ook gelden er twee actieve meldplichten naar de toezichthouder. Ten eerste moet een financiële onderneming ten minste jaarlijks aan de toezichthouder rapporteren hoeveel nieuwe ICT-overeenkomsten zij heeft afgesloten en waar deze overeenkomsten betrekking op hebben. Ten tweede moet een financiele onderneming de toezichthouder tijdig in kennis stellen van geplande ICT-overeenkomsten ter ondersteuning van kritieke of belangrijke functies en van het feit dat een functie kritiek of belangrijk is geworden.[43]

DORA stelt ook specifieke eisen aan de overeenkomst zelf die een financiële onderneming sluit met een ICT-dienstverlener, zie hierna.

5. Wat wordt er van ICT-dienstverleners verwacht?

5.1 ICT-dienstverleners waarvan financiële ondernemingen gebruik maken

De belangrijkste DORA-bepalingen waar ICT-dienstverleners indirect door worden geraakt zijn gelegen in de contractuele sfeer. DORA bevat een uitgebreide lijst met elementen die ten minste – de lijst is niet uitputtend – moeten worden opgenomen in overeenkomsten voor het gebruik van ICT-diensten.[44] Hierbij wordt in DORA een onderscheid gemaakt tussen enerzijds ICT-diensten die kritieke of belangrijke functies van een financiële onderneming ondersteunen en anderzijds alle overige ICT-diensten waarvan een financiële onderneming gebruik maakt.

Het indirecte karakter van de impact op ICT-dienstverleners is erin gelegen dat op grond van DORA enkel de financiële onderneming door de toezichthouder formeel kan worden aangesproken op het niet (adequaat) verwerken van de vereiste contractuele elementen in de overeenkomst met een ICT-dienstverlener. De in DORA opgesomde lijst met vereiste contractuele elementen bevat echter verschillende verplichtingen die een financiële onderneming aan haar ICT-dienstverleners moet opleggen. Het gaat daarbij bijvoorbeeld om de verplichting om de financiële onderneming zonder extra kosten (of tegen een vooraf bepaalde kostprijs) bijstand te verlenen in geval van een incident en de verplichting om volledige medewerking te verlenen aan bevoegde autoriteiten en afwikkelingsautoriteiten van de financiële onderneming.[45] Als de ICT-dienstverlener hiermee niet wil of kan instemmen, zal de financiële onderneming geen overeenkomst mogen sluiten met de desbetreffende ICT-dienstverlener.

5.2 ICT-dienstverleners waarvan financiële ondernemingen gebruik maken ter ondersteuning van kritieke of belangrijke functies

De impact op de ICT-dienstverlener zal nog groter zijn als de dienstverlener ICT-diensten verleent ter ondersteuning van functies die door de financiële onderneming als 'kritiek of belangrijk' zijn aangemerkt. 'Kritieke of belangrijke functies' zijn in DORA gedefinieerd als '*functies waarvan de verstoring wezenlijk afbreuk zou doen aan de financiële prestaties van een financiële entiteit of aan de soliditeit of de continuïteit van haar diensten en activiteiten, of waarvan de beëindiging of gebrekkige of mislukte uitvoering wezen-*

38 Zie ook de conclusies van de ESA's in '*Report on the landscape of ICT third-party providers in the EU*' van 19 september 2023.

39 Zie paragraaf 4.1 van dit artikel.

40 Art. 28(2) DORA.

41 Gedelegeerde verordening van 13 maart 2024 tot bepaling van de gedetailleerde inhoud van het beleid met betrekking tot de contractuele overeenkomsten inzake het gebruik van door derde aanbieders verleende ICT-diensten die kritieke of belangrijke functies ondersteunen (ten tijde van het schrijven van dit artikel nog niet gepubliceerd in het Publicatieblad van de EU), zoals geraadpleegd op 4 april 2024.

42 Art. 28(3) DORA. Zie voor de Level 2 eisen aan het informatieregister het finale rapport van de ESA's '*Draft Implementing Technical Standards on the standard templates for the purposes of the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers under Article 28(9) of Regulation (EU) 2022/2554*' van 10 januari 2024.

43 Art. 28(3) DORA.

44 Art. 30 DORA.

45 Art. 30(2)(f-g) DORA.

*lijk afbreuk zou doen aan de permanente naleving door een financiële entiteit van de voorwaarden en verplichtingen uit hoofde van haar vergunning of haar andere verplichtingen uit hoofde van het toepasselijke recht inzake financiële dienste*n'.[46]

Als een overeenkomst met een ICT-dienstverlener op kritieke of belangrijke functies betrekking heeft, moet de financiële onderneming een aantal extra verplichtingen aan de ICT-dienstverlener opleggen. Denk aan de verplichting voor de ICT-dienstverlener om bedrijfsnoodplannen in te voeren en te beschikken over ICT-beveiligingsmaatregelen, -instrumenten en -beleidslijnen en de verplichting om mee te werken aan TLPT door de financiële onderneming.[47] Ook moet de ICT-dienstverlener '*onbeperkte rechten*' verlenen van toegang, inspectie en audit door de financiële onderneming en bevoegde autoriteiten.[48]

Vermeldenswaardig is dat er strenge Level 2 regelgeving in de maak is voor de situatie dat een ICT-dienstverlener op haar beurt andere ICT-dienstverleners inschakelt ten behoeve van de ondersteuning van kritieke of belangrijke functies van een financiële onderneming. Op grond van de voorgestelde regels mag een financiële onderneming alleen onder strikte voorwaarden dergelijk 'subcontracteren' door de ICT-dienstverlener toestaan. Zo is de ICT-dienstverlener in dat geval onder meer verplicht ervoor te zorgen dat (ook) de door haar ingeschakelde derden meewerken aan audits door de financiële onderneming en bevoegde autoriteiten. De financiële onderneming dient de gehele keten van ICT-dienstverleners te monitoren en moet vooraf worden geïnformeerd over materiële wijzigingen in overeenkomsten tussen haar ICT-dienstverlener en door deze ICT-dienstverlener ingeschakelde derden. De financiële onderneming moet ervoor zorgen dat materiële wijzigingen door de ICT-dienstverlener alleen worden doorgevoerd als zij daartegen geen bezwaar heeft.[49]

5.3 Kritieke ICT-dienstverleners

Voor ICT-dienstverleners die door de ESA's als 'kritiek' worden aangemerkt geldt bovenop de voorgenoemde eisen een specifiek 'oversightkader' onder DORA.[50] Zoals in paragraaf 3 opgemerkt, komen deze kritieke ICT-dienstverleners onder rechtstreeks toezicht van de ESA's te vallen. Als onderdeel van het toezicht van de ESA's op kritieke ICT-dienstverleners, krijgen de ESA's bevoegdheden om allerlei informatie van deze dienstverleners op te vragen en ook ter plaatse inspecties uit te voeren. Mochten er na een dergelijk onderzoek verbeterpunten worden geconstateerd, dan kunnen de ESA's aanbevelingen doen aan de kritieke ICT-dienstverleners. Deze aanbevelingen moeten ook daadwerkelijk worden opgevolgd – het niet meewerken door een kritieke ICT-dienstverlener kan er in het *worst case scenario* toe leiden dat de ESA's financiële ondernemingen verbieden om nog langer gebruik te maken van deze dienstverlener.[51] Ook kan de toezichthoudende ESA een dwangsom aan de kritieke ICT-dienstverlener opleggen om zodoende af te dwingen dat er wordt meegewerkt aan onderzoeken en inspecties.[52]

6. Vijf praktische tips bij de voorbereiding op DORA

6.1 Inleiding

De bepalingen in DORA zijn uitgebreid en niet zelden lastig leesbaar door de lange zinnen, de grote hoeveelheid definities en de niet altijd heldere structuur. Dit maakt de implementatie van alle verschillende eisen bepaald geen gemakkelijke opgave, waarbij de grote hoeveelheid Level 2 regels de uitdaging nog groter maakt.

Tegelijkertijd is ICT-risicobeheer voor de meeste financiële ondernemingen gelukkig niet nieuw. Met name financiële ondernemingen die onder toezicht staan van DNB zullen vaak al over uitgebreide beleidsstukken en procedures beschikken om ICT-risico's, als subcategorie van operationele risico's, te beheersen. Dit houdt er onder meer mee verband dat DNB al sinds 2010 een gedetailleerde Q&A Informatiebeveiliging publiceert, die zij eind 2023 voor het laatst heeft geactualiseerd.[53] Voor ondernemingen die de AFM als hoofdtoezichthouder hebben, geldt dat de AFM eind 2019 elf 'Principes voor Informatiebeveiliging' heeft gepubliceerd.[54] Dat document valt echter in het niet bij het DORA-kader, waardoor het in de rede ligt dat (juist) ondernemingen die onder AFM-toezicht vallen hun inspanningen op ICT-risicobeheersingsvlak aanzienlijk zullen moeten intensiveren.

Hoe dan ook, DORA zal vanwege haar reikwijdte, omvang en mate van detail op vrijwel iedere financiële onderneming impact hebben. Hieronder geven wij vijf tips voor een goede voorbereiding op 17 januari 2025 en om de naleving van DORA toetsbaar te maken voor de toezichthouder.

46 Art. 3 onder 22 DORA.

47 Art. 30(2)(c-d) DORA.

48 Art. 30(2)(e) DORA.

49 Aldus de voorgestelde art. 3 tot en met 7 in de concept Level 2 regelgeving zoals opgenomen in het ESA's consultatierapport '*Draft Regulatory Technical Standards to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions*' van 27 november 2023.

50 Hoofdstuk 5, afdeling II DORA. Zie ook S.J.J. Weggelaar, R.M.T.F. Bos-van Zijp & T.W. Zoutendijk, 'Big Tech onder financieel toezicht? Een verkenning van het oversightkader in de Digital Operational Resilience Act', *FR* 2024, nr. 3.

51 Art. 42(6) DORA.

52 Art. 35(6) DORA.

53 DNB, '*Good practices Informatiebeveiliging*' (19 december 2023), te raadplegen via www.dnb.nl.

54 AFM Principes voor Informatiebeveiliging (19 december 2019), te raadplegen via afm.nl. Ook Europese toezichthouders EBA en ESMA hebben de afgelopen jaren relevante guidance gepubliceerd, zie EBA, '*EBA richtsnoeren inzake ICT en risicobeheer op het gebied van veiligheid*' (28 november 2019)', '*EBA richtsnoeren inzake uitbesteding*' (25 februari 2019) en '*EBA aanbevelingen inzake uitbesteding aan aanbieders van clouddiensten*' (28 maart 2018), alle drie te raadplegen via www.eba.europa.eu, en ESMA, '*Richtsnoeren inzake uitbesteding aan aanbieders van clouddiensten*' (10 mei 2021), te raadplegen via www.esma.europa.eu.

6.2 Tip 1: begin bij het begin – in hoeverre is DORA van toepassing?

Allereerst is het essentieel om eerst heel precies in kaart te brengen – of door een adviseur te laten brengen – welke Level 1- en 2-bepalingen wél en welke bepalingen niet op de financiële onderneming van toepassing zijn. Op basis daarvan kan een overzicht worden gemaakt van de beleidstukken, procedures en ICT-rollen waarover de onderneming op grond van DORA moet beschikken. Vervolgens kan aan de hand van dit overzicht en de bestaande 'policy house', procedures en inrichting van de organisatie worden geïdentificeerd welke 'gaps' er zijn.

6.3 Tip 2: maak en documenteer een evenredigheidsbeoordeling

De Europese wetgever heeft onderkend dat DORA op een groot aantal financiële ondernemingen van toepassing is, maar de onderlinge verschillen tussen financiële ondernemingen, onder meer qua omvang en risicoprofiel, aanzienlijk kunnen zijn.[55] Met het oog hierop is in DORA expliciet bepaald dat een financiële onderneming de eisen uit DORA moet toepassen in overeenstemming met het evenredigheidsbeginsel. Dit betekent dat een financiële onderneming haar ICT-gerelateerde voorzieningen en dus inspanningen moet afstemmen op haar omvang, algeheel risicoprofiel, en op de aard, schaal en complexiteit van haar activiteiten.[56] DNB en de AFM moeten bij het uitoefenen van toezicht op de naleving van DORA rekening houden met dit evenredigheidsbeginsel.[57]

> Het vormen van een multidisciplinair team is onontkoombaar bij het maken van een gedegen DORA gap-analyse en het implementeren van alle eisen

Het gaat hier om een algemeen uitgangspunt; de wetgever heeft niet uitgewerkt hoe individuele ondernemingen het evenredigheidsbeginsel concreet moeten interpreteren en toepassen bij de naleving van DORA. Kunnen bepaalde eisen door een onderneming onder omstandigheden geheel achterwege worden gelaten, of gaat het uitsluitend om de diepgang waarin kan worden gevarieerd bij de implementatie van de verplichtingen? Concrete guidance van de ESA's ontbreekt (vooralsnog). Niettemin is het raadzaam dat een onderneming haar omvang, risicoprofiel en de aard, schaal en complexiteit van haar activiteiten analyseert en zich op basis daarvan een opvatting vormt waar haar ICT-inspanningen zich met name op moeten richten en waar het minder kan. Deze exercitie, en de keuzes die de onderneming in dit verband maakt, vormt feitelijk het startpunt van de implementatie van DORA.

55 Overweging 36 DORA.
56 Art. 4(1-2) DORA en overweging 36 DORA.
57 Art. 4(3) DORA.

6.4 Tip 3: betrek van meet af aan het bestuur, ICT-specialisten en juristen

Omdat DORA zo'n technisch onderwerp betreft, is het vormen van een multidisciplinair team onontkoombaar bij het maken van een gedegen gap-analyse en vervolgens de implementatie van alle eisen. Het is van belang dat binnen dit team zowel juridische kennis, risk management expertise als, uiteraard, ICT-kennis voorhanden is.

Daarnaast is het belangrijk dat het bestuur wordt betrokken bij de voorbereiding.[58] Niet alleen omdat het bestuur moet zorgen voor voldoende budget voor de naleving van DORA,[59] maar ook omdat de Europese wetgever het bestuur als eindverantwoordelijk orgaan expliciet een heel aantal ICT-gerelateerde taken heeft toegedicht. Deze taken zijn onder meer:

- de invoering van beleidslijnen om de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens te waarborgen;
- de vaststelling van duidelijke taken voor alle ICT-gerelateerde functies en het zorgen voor goede communicatie en samenwerking tussen die functies;
- de algemene verantwoordelijkheid voor het vaststellen en goedkeuren van de ICT-strategie inclusief bepaling van het passende ICT-risicotolerantieniveau;
- de goedkeuring en de periodieke evaluatie van het ICT-bedrijfscontinuïteitsbeleid, de interne ICT-auditplannen en het beleid inzake het inschakelen van ICT-dienstverleners;
- het opzetten van interne rapportagelijnen die het bestuur in staat stellen informatie in te winnen over ICT-contracten en geplande materiële wijzigingen met betrekking tot ICT-dienstverleners.[60]

6.5 Tip 4: treed tijdig in contact met ICT-dienstverleners

De vierde tip is om bestaande overeenkomsten voor het gebruik van ICT-diensten onder de loep te nemen en tijdig met ICT-dienstverleners in contact te treden om deze overeenkomsten, waar nodig, in lijn te brengen met de eisen uit DORA. Verschillende marktpartijen hebben de ESA's erop gewezen dat in dit kader overgangsrecht zou moeten worden gehanteerd en DORA alleen op nieuwe overeenkomsten of contractverlengingen zou moeten worden toegepast. De ESA's hebben echter bevestigd dat DORA niet voorziet in overgangsrecht en dat de daarin gestelde eisen vanaf 17 januari 2025 op zowel nieuwe als bestaande

58 Noemenswaardig is dat DNB en de AFM in juli 2022 voornemens waren om DORA expliciet op te nemen in de Beleidsregel geschiktheid 2012. Na de publieke consultatie hebben DNB en de AFM besloten om hier vooralsnog van af te zien zolang DORA nog niet van kracht is. Wel heeft de AFM in februari 2024 in de geschiktheidsmatrix een expliciete verwijzing naar DORA opgenomen onder de noemer '*DORA implementatie*', en dienen beoogde dagelijks beleidsbepalers in deze matrix concreet aan te geven in hoeverre zij kennis hebben van DORA-vereisten en ervaring met de inrichting en implementatie daarvan in bedrijfsvoering.
59 Art. 5(2)(g) en overweging 46 DORA.
60 Art. 5(2) DORA.

overeenkomsten met ICT-dienstverleners van toepassing zullen zijn.[61]

DNB heeft in één van haar nieuwsberichten opgemerkt dat financiële ondernemingen moeten nadenken over hoe zij handelen als een ICT-dienstverlener het verwachte niveau niet binnen de termijn gaat halen.[62] Als een ICT-dienstverlener überhaupt niet wil of kan voldoen aan de verplichtingen die DORA indirect aan hem oplegt, dan valt lastig in te zien hoe een financiële onderneming de relatie met deze ICT-dienstverlener kan voortzetten.

6.6 Tip 5: denk in processen

Wanneer de grote hoeveelheid nieuwe verplichtingen begint te duizelen, is het van belang om vanuit een heldere structuur te blijven werken. De vijfde en laatste tip is dan ook om bij de vertaling van de DORA-eisen naar beleid en procedures, te denken in processen en de verschillende stappen binnen dat proces. Het ICT-risicobeheer raamwerk bestaat bijvoorbeeld uit identificatie, preventie, monitoring en detectie, respons, herstel, communicatie en evaluatie. Het volgen van deze stappen geeft structuur en daarmee houvast bij het uitwerken van beleid en procedures ter implementatie van alle nieuwe regels.

Dit artikel is afgesloten op 4 april 2024.

Over de auteurs

Mr. L.B.G. (Laurens) Hillen
Advocaat bij Finnius te Amsterdam.

Mr. M.H. (Marise) Kok
Advocaat bij Finnius te Amsterdam.

61 Zie '*Final report on Draft Regulatory Technical Standards to specify the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers as mandated by Regulation (EU) 2022/2554*', p. 30.

62 Zie het nieuwsbericht van DNB '*DORA; tijd om uit de startblokken te komen*' (31 oktober 2023), te raadplegen via www.dnb.nl.