Digitale weerbaarheid en contractuele complexiteit

Een analyse van de DORA en de EBA-Guidelines

*Mr. K. Vonk en mr. L. Leemeijer**

1 Inleiding en leeswijzer

In 2010 is de digitale agenda voor Europa door de Europese Commissie gepubliceerd.[1] Het doel van deze agenda was het geven van een impuls aan innovatie en economische groei en het verbeteren van het dagelijkse leven van zowel burgers als ondernemingen.[2] Ook het verwijderen van regelgevingsobstakels in digitale markten is genoemd als doelstelling.[3] Sinds de publicatie van de digitale agenda in 2010 is er een grote hoeveelheid aan Europese (voorstellen voor) regelgeving met betrekking tot de digitale sector bij gekomen.[4] Deze uit de digitale agenda voortvloeiende wet- en regelgeving schrijft niet alleen voor hoe organisaties intern moeten zijn ingericht, maar bepaalt in toenemende mate ook de inhoud van overeenkomsten tussen professionele partijen. Voorbeelden hiervan zijn de Platform-2-Business Verordening[5] en de Algemene verordening gegevensbescherming (AVG).[6] In dit artikel gaan wij in op de Digital Operational Resilience Act (hierna: de DORA).[7] Ook deze verordening is een voorbeeld van Europese wetgeving die ingrijpt op overeenkomsten tussen professionele partijen.

De DORA vloeit net als de Markets in Crypto-assets Regulation[8] en de Distributed Ledger Technology 'DLT' Regulation[9] voort uit het Digital Finance Package van de Europese Commissie,[10] en hangt samen met wet- en regelgeving zoals de tweede Network and Information Security 'NIS 2'-richtlijn[11] en richtsnoeren zoals die van de Europese Bankautoriteit (EBA): de EBA Guidelines on outsourcing arrangements[12] (hierna: de EBA-Guidelines).

Met de DORA wordt beoogd om 'digitale operationele weerbaarheid' te bereiken door middel van het vaststellen van uniforme vereisten met betrekking tot de beveiliging van netwerken informatiesystemen die bedrijfsprocessen van financiële entiteiten ondersteunen.[13] De DORA is specifiek van toepassing op de in art. 2 lid 1 sub a t/m t DORA genoemde financiele entiteiten, zoals banken en verzekeraars (hierna: financiële entiteiten),[14] en op 'derde ICT-leveranciers', die ICT-diensten leveren aan deze financiële entiteiten (hierna: ICT-leveranciers). Vanaf 17 januari 2025 moeten financiële entiteiten en ICT-leveranciers voldoen aan de DORA.

Over de DORA, meer in het bijzonder over de oorsprong, doeleinden en verplichtingen, de plaatsing van de DORA binnen het Digital Finance Package en de verhouding met samen-

* Mr. K. Vonk is als advocaat werkzaam bij Brinkhof te Amsterdam. Mr. drs. L. Leemeijer is als advocaat werkzaam bij Brinkhof te Amsterdam.

1 COM/2010/0245 final.

2 COM/2010/0245 final, par. 1.

3 COM/2010/0245 final, par. 1.

4 Een overzicht van deze 'wall of EU digital regulation' is te vinden op de website www.bruegel.org/dataset/dataset-eu-legislation-digital-world. Met deze toenemende regeldruk kan de vraag worden gesteld of de hiervoor genoemde doelstellingen kunnen worden behaald, zie ook L. Leemeijer, Contractsvrijheid versus Europese regelgeving in de digitale sector, Computerrecht 2024, afl. 4. p. 239-240.

5 Verordening (EU) 2019/1150. Deze verordening bevat o.a. verplichtingen ten aanzien van algemene voorwaarden, zie art. 3.

6 Verordening (EU) 2016/679. Deze verordening schrijft voor dat verwerkingsverantwoordelijken een overeenkomst moeten sluiten met verwerkers en stelt eisen aan de inhoud daarvan (art. 28 lid 3).

7 Verordening (EU) 2022/2554. Overigens vloeien veel van de verplichtingen uit de DORA voort uit bestaande *regulatory guidance* van de EBA, ESMA en EIOPA in het kader van uitbestedingen. Belangrijk verschil is echter dat de DORA, anders dan voornoemde guidance, ook rechtstreeks van toepassing is op ICT-leveranciers (art. 2 lid 1 sub u DORA).

8 Verordening (EU) 2023/1114.

9 Verordening (EU) 2022/858.

10 Europese Commissie, EU-strategie voor het digitale geldwezen, Brussel 24 september 2020, COM(2020)591 final.

11 Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn). De DORA is een *lex specialis* ten opzichte van de NIS 2-richtlijn, overweging 16 DORA.

12 EBA Guidelines on outsourcing arrangements, EBA/GL/2019/02, 25 februari 2019.

13 Art. 1 lid 1 DORA.

14 Art. 2 lid 2 DORA.

hangende Europese regelgeving is al veel geschreven.[15] In dit artikel concentreren wij ons op enkele praktische vragen en knelpunten die zich voordoen bij de uitvoering van de DORA, waarbij wij ons beperken tot de verplichtingen uit de DORA die betrekking hebben op de contracten tussen financiële entiteiten en ICT-leveranciers.

Veel van de verplichtingen uit de DORA bouwen voort op bestaande *regulatory guidance* van de EBA, de Europese Autoriteit voor Verzekeringen en Bedrijfspensioenen (EIOPA)[16] en de Europese Autoriteit voor effecten en markten (ESMA)[17] in het kader van uitbestedingen.[18] De meest verstrekkende bestaande richtsnoeren zijn de EBA-Guidelines.[19] Net als de DORA zijn de EBA-Guidelines gericht op het versterken van operationele weerbaarheid van financiële entiteiten. Omdat veel overeenkomsten tussen financiële entiteiten en ICT-leveranciers als 'uitbesteding' kwalificeren, zijn in veel gevallen zowel de EBA-Guidelines als de DORA van toepassing.

Hoewel beide instrumenten inhoudelijk sterk overeenkomen, zijn er ook verschillen. Zo introduceert de DORA verplichtingen die niet in de EBA-Guidelines voorkomen en bevatten de EBA-Guidelines omgekeerd verplichtingen die niet in de DORA voorkomen.[20] Ook zijn er diverse bepalingen die op het eerste gezicht gelijkenissen vertonen, maar die in de praktijk op belangrijke punten verschillen. Naleving van de EBA-Guidelines impliceert daarom niet automatisch conformiteit met de DORA, en omgekeerd.

Een groot aantal financiële entiteiten in Europa – banken, betaalinstellingen en elektronischgeldinstellingen – zullen naar verwachting reeds voldoen aan de EBA-Guidelines.[21] Dit roept de vraag op wat er onder de DORA meer en anders geregeld moet worden ten opzichte van de verplichtingen onder de EBA-Guidelines.[22] Om deze vraag volledig te kunnen beantwoorden is een transponeringstabel nodig, aan de hand waarvan een *gap*-analyse tussen de EBA-Guidelines en de DORA kan worden gemaakt. Omdat een dergelijk inzicht cruciaal is voor het identificeren van de stappen om zowel aan de EBA-Guidelines als aan de DORA te voldoen, zullen wij enkele in het oog springende *gaps* aan de orde stellen. Het doel van dit artikel is vooral om onduidelijkheden en knelpunten inzichtelijk te maken, en om de praktijkjurist die met de uitvoering van de DORA aan de slag moet, praktische handvatten te bieden. Vanwege deze meer praktische insteek zullen wij een aantal aspecten buiten beschouwing laten. Zo zullen wij overlap tussen de twee instrumenten niet behandelen.[23] Ook zullen bepalingen die wel in de EBA-Guidelines voorkomen, maar niet (ook) in de DORA, niet aan de orde komen. Verder zullen wij aspecten buiten beschouwing laten die zowel in de DORA als in de EBA-Guidelines ontbreken.[24] Wij richten ons tot slot specifiek op de bepalingen van de EBA-Guidelines

15 Zie bijv. K. Christianen, DORA: meer veiligheid door wisselwerking tussen toezichtrecht en civiel recht, MvV 2023, afl. 6, p. 197-207; L.C. Brederveld & A.J.P. de Boer, Exploring DORA: een verkenning van de vereisten aan contracten tussen financiële instellingen en derde ICT-aanbieders, Tijdschrift voor Internetrecht 2024, afl. 2, p. 50-62; T.W.G. de Wit & G. Verschuuren, ICT-risicobeheer met DORA, FR 2023, afl. 5, p. 161-170; J.P. Broekhuizen & L.C. Brederveld, Systemische dimensies van de regulering van ICT-risico's in de Digital Operational Resilience Act (DORA), FR 2023, afl. 5, p. 171-179; T.W.J. Hoeben & T.W. Beenen, DORA's intragroep aspecten, FR 2023, afl. 5, p. 181-189; J.G.C.M. Galle, Cybersecurity door beheerste bedrijfsvoering en daarop gericht toezicht (met DORA als aanjager), FR 2023, afl. 7/8, p. 238-242; P.M. van Vliet, DORA en outsourcing – een vergelijking tussen DORA en de EBA/EIOPA Guidelines, FR 2023, afl. 5, p. 190-198; S. Kourmpetis, Management of ICT Third Party Risk under the Digital Operational Resilience Act, in: L. Böffel & J. Schürger (red.), Digitalisation, Sustainability, and the Banking and Capital Markets Union. Thoughts on Current Issues of EU Financial Regulation, Cham: Palgrave Macmillan 2023, p. 211-226; E. Kun, Challenges in Regulating Cloud Service Providers in EU Financial Regulation: From Operational to Systemic Risks, and Examining Challenges of the New Oversight Regime for Critical Cloud Service Providers under the Digital Operational Resilience Act, Computer Law & Security Review 2024/52; T. Contzen, Contracting under the EBA Guidelines on Outsourcing Arrangements. A Best Practice for the Digital Transformation of Financial and Other Institutions, Computer Law Review International 2020, afl. 2, p. 50-56; V. Begozzi, M. Oldani & F. Terrizzano, The Growing Importance of Digital Risk & Governance, Risk Management Magazine 2023/18, afl. 2, p. 27-36; L.B.G. Hillen & M.H. Kok, DORA: van theorie naar praktijk, TOP 2024/159, afl. 3, p. 29-36.

16 EIOPA Guidelines on outsourcing to cloud service providers, 6 februari 2020.

17 ESMA Guidelines on outsourcing to cloud service providers, 10 mei 2021.

18 In de DORA wordt ook verwezen naar deze bestaande guidelines (overweging 30 DORA).

19 De ESMA Guidelines on outsourcing to cloud service providers en de EIOPA Guidelines on outsourcing to cloud service providers zien net als de EBA-Guidelines op het uitbesteden van diensten. De EBA-Guidelines zijn het meest verstrekkend omdat deze niet uitsluitend betrekking hebben op uitbestedingen aan aanbieders van clouddiensten en strengere regels bevatten. Om deze reden beperken wij ons in dit artikel tot de EBA-Guidelines.

20 Een voorbeeld hiervan is dat de EBA-Guidelines in par. 75 vereisen dat financiële verplichtingen expliciet worden opgenomen in contracten tussen partijen, terwijl de DORA geen dergelijke verplichting oplegt. In de praktijk is dit verschil echter vaak beperkt van betekenis, aangezien commerciële partijen doorgaans grote waarde hechten aan de contractuele vastlegging van dergelijke verplichtingen. Een ander voorbeeld is par. 75 (k) EBA-Guidelines die vereist dat partijen afspraken maken over verzekeringen, zoals de vraag of de leverancier al dan niet een verzekering afsluit en welke dekking van toepassing is. De DORA stelt een dergelijke expliciete eis niet.

21 De compliancedeadline was op 25 april 2019, zie www.eba.europa.eu/activities/single-rulebook/regulatory-activities/internal-governance/guidelines-outsourcing.

22 In het vervolg van dit artikel zullen wij er gemakshalve van uitgaan dat reeds wordt voldaan aan de verplichtingen onder de EBA-Guidelines.

23 Overlappende verplichtingen achten wij minder relevant, omdat ze doorgaans al zullen zijn opgenomen in de overeenkomsten die financiële entiteiten hebben gesloten met ICT-leveranciers.

24 Zowel de DORA als de EBA-Guidelines bevatten bijv. nog steeds geen concrete richtlijnen om de kwaliteit en consistentie van beveiligingsstandaarden te waarborgen. Hoewel er in de recent gepubliceerde Regulatory Technical Standards bij het rapporteren van ICT-incidenten naar ISO-normen wordt verwezen, ontbreekt verdere verwijzing naar technische normen. Door dit gebrek aan harmonisatie moet men terugvallen op bestaande wetgeving en jurisprudentie, zie Hof Amsterdam 9 mei 2017, ECLI:NL:GHAMS:2017:1764, r.o. 3.2.6; Rb. Rotterdam 26 april 2017, ECLI:NL:RBROT:2017:3566, r.o. 4.5-4.6; Rb. Amsterdam 18 december 2019, ECLI:NL:RBAMS:2019:9635, r.o. 4.5; zie ook W.F.R. Rinzema & F.B. Melis, Hoe kan de kwaliteit van ICT-systemen juridisch meetbaar worden gemaakt?, Computerrecht 2014/150.

 doi: 10.5553/MvV/157457672024034010004

en de DORA die betrekking hebben op het contracteren. Andere regulatoire aspecten van de twee regelgevingsinstrumenten laten we buiten beschouwing.

Het artikel is als volgt opgebouwd. In paragraaf 2 gaan wij dieper in op de belangrijkste verschillen tussen de DORA en de EBA-Guidelines en de praktische knelpunten die uit deze verschillen voortvloeien. In paragraaf 3 sluiten wij af met een conclusie en analyse.

2 Praktische uitdagingen bij naleving DORA naast EBA-Guidelines

2.1 Juridische bindendheid

Een eerste verschil tussen de DORA en de EBA-Guidelines ligt in de juridische bindendheid van beide instrumenten. De DORA is een Europese verordening, wat betekent dat zij rechtstreekse werking heeft binnen de lidstaten van de Europese Unie.[25] Dit houdt in dat de DORA, zonder verdere omzetting in nationale wetgeving, rechtstreeks van toepassing is op financiële entiteiten en ICT-diensten, zoals hieronder verder uiteengezet in paragraaf 2.2.

De EBA-Guidelines zijn, zoals de naam aangeeft, richtlijnen die zijn opgesteld door de toezichthoudende autoriteit, de EBA. Deze richtlijnen dienen als een instrument voor het toezicht door de EBA, en zijn bedoeld om verwachtingen ten aanzien van naleving te verduidelijken en te harmoniseren binnen de financiële sector. Echter, in tegenstelling tot de DORA hebben de EBA-Guidelines geen bindende wettelijke status. Zij vormen geen juridisch afdwingbaar recht en verplichten de nationale toezichthouders niet tot naleving. Hoewel rechters deze richtlijnen kunnen beschouwen als relevante gezichtspunten of interpretatieve kaders bij de beoordeling van zaken,[26] zijn zij niet verplicht om hun oordeel hieraan te toetsen.

In de praktijk betekent dit dat wanneer zowel de DORA als de EBA-Guidelines van toepassing zijn op een contract tussen een financiële instelling en een ICT-leverancier, en er sprake is van tegenstrijdige of in ieder geval verschillende bepalingen, de bepalingen van de DORA voorrang hebben. Financiële entiteiten moeten daarom bij conflicterende bepalingen de voorschriften van de DORA volgen.

Toch is dit in de praktijk niet altijd eenvoudig. De Nederlandsche Bank (DNB) is in Nederland de aangewezen toezichthouder voor de naleving van de EBA-Guidelines. In het Concept Uitvoeringsbesluit DORA wordt zowel DNB als de Autoriteit Financiële Markten (AFM) aangewezen om toe te zien op de naleving van de DORA.[27] Dit kan leiden tot de situatie waarbij een financiële entiteit aan de ene kant door de toepasselijkheid van de EBA-Guidelines onder het toezicht valt van DNB en aan de andere kant door de toepasselijkheid van de DORA onder het toezicht van de AFM. Hierdoor kan de situatie voorkomen dat de toezichthouders verschillende of zelfs tegenstrijdige verwachtingen hebben vanwege de soms uiteenlopende bepalingen van beide instrumenten. Omdat de DORA voorrang heeft, gelet op haar status, adviseren wij financiële entiteiten om in deze situatie altijd de verplichtingen onder de DORA te volgen.

2.2 Toepassingsgebied

Een tweede belangrijk onderscheid tussen de DORA en de EBA-Guidelines ligt in hun respectieve toepassingsgebieden.

De EBA-Guidelines zijn van toepassing wanneer kredietinstellingen, beleggingsondernemingen, betalingsinstellingen en instellingen voor elektronisch geld een functie of dienst uitbesteden.[28] 'Uitbesteding' wordt in paragraaf 12 van de EBA-Guidelines als volgt gedefinieerd:

> 'een overeenkomst van om het even welke vorm tussen een instelling, een betalingsinstelling of een instelling voor elektronisch geld en een dienstverlener op grond waarvan deze dienstverlener een proces, een dienst of een activiteit verricht die anders door de instelling, betalingsinstelling of instelling voor elektronisch geld zelf zou worden verricht'.

Enerzijds is het toepassingsbereik van de DORA beperkter dan dat van de EBA-Guidelines, omdat de EBA-Guidelines betrekking hebben op alle uitbestedingen, terwijl de DORA zich alleen richt op de levering en afname van ICT-diensten. Anderzijds is het toepassingsbereik van de DORA breder dan het toepassingsbereik van de EBA-Guidelines, aangezien de DORA van toepassing is op de levering van alle 'ICT-diensten' aan in art. 2 lid 1 sub a t/m t DORA genoemde 'financiële entiteiten'.[29] Naast kredietinstellingen, beleggingsondernemingen, betalingsinstellingen en instellingen voor elektronisch geld, waarop de EBA-Guidelines eveneens van toepassing zijn, omvat deze lijst nog zestien andere financiële

25 Art. 288 Verdrag betreffende de werking van de Europese Unie, Rome, 25 maart 1957.

26 Zie bijv. Rb. Den Haag 9 september 2024, ECLI:NL:RBDHA:2024:14477, r.o. 4.7, waarin de rechtbank aansluit bij richtsnoeren van de European Data Protection Board voor de definitie van 'geautomatiseerd besluit', omdat de AVG daarover geen verduidelijking biedt.

27 Zie art. I(B) Concept Uitvoeringsbesluit DORA, 22 mei 2024, waarin specifiek staat aangegeven voor welke marktpartijen de AFM wordt aangewezen als bevoegde autoriteit in de zin van de DORA, en voor welke partijen DNB wordt aangewezen als bevoegde autoriteit in de zin van de DORA.

28 Instellingen zoals gedefinieerd in art. 4 lid 1 punt 3 van Verordening (EU) 575/2013; betalingsinstellingen als gedefinieerd in art. 4 punt 4 van Richtlijn (EU) 2015/2366; instellingen voor elektronisch geld in de zin van art. 2 punt 1 van Richtlijn 2009/110/EU.

29 Art. 2 lid 1 sub u en art. 3 (19) DORA.

entiteiten.[30] Hierdoor kan de DORA van toepassing zijn op uitbestedingen die niet onder het toepassingsbereik van de EBA-Guidelines vallen.

Daarnaast beperkt de DORA zich niet alleen tot uitbestedingen van ICT-diensten, maar omvat de DORA de levering van alle ICT-diensten door ICT-leveranciers aan financiële entiteiten.[31] 'ICT-diensten' worden in de 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'.[32]

Hoewel diverse ICT-diensten, zoals clouddiensten, reeds onder het toepassingsbereik van de EBA-Guidelines vielen,[33] is het toepassingsbereik van de DORA met deze definitie breder.

De DORA geldt bovendien niet alleen voor financiële entiteiten die een ICT-dienst afnemen, maar ook voor 'derde aanbieders van ICT-diensten'.[34] De verplichtingen van de DORA zijn dus rechtstreeks van toepassing op deze aanbieders wanneer zij ICT-diensten leveren en contracteren met financiële entiteiten.[35] Dit is een belangrijk verschil tussen de DORA en de EBA-Guidelines. Waar financiële entiteiten de op hen rustende verplichtingen contractueel moeten doorleggen aan ICT-leveranciers om compliant te zijn met de EBA-Guidelines,[36] zijn ICT-leveranciers onder de DORA zelf (ook) verplicht zich te houden aan de regelgeving. Doordat de DORA rechtstreeks verplichtingen oplegt aan ICT-leveranciers ten aanzien van contractuele afspraken, zal dit het onderhandelingsproces voor financiële entiteiten vergemakkelijken.[37] Omdat ook intragroepleveranciers van ICT-diensten expliciet onder de DORA vallen,[38] moet er rekening mee worden gehouden dat de DORA ook in sommige intragroepcontracten moet worden geïmplementeerd. Zo kan een moedermaatschappij bijvoorbeeld centrale IT-diensten inkopen en deze via een intragroepcontract beschikbaar stellen aan groepsmaatschappijen die onder de reikwijdte van de DORA vallen, waardoor de moedermaatschappij als ICT-leverancier onder de DORA gaat gelden en het contract tussen de moedermaatschappij en de dochtermaatschappijen zal moeten voldoen aan de vereisten van de DORA.[39]

Tot slot is er een verschil tussen de geografische toepassingsgebieden van de EBA-Guidelines en de DORA. De EBA-Guidelines zijn primair van toepassing op financiële entiteiten gevestigd in de Europese Unie, maar omdat sommige verplichtingen daaruit contractueel moeten worden doorgelegd aan ICT-leveranciers, raken de EBA-Guidelines ook ICT-leveranciers die buiten de Europese Unie zijn gevestigd. De DORA is niet alleen van toepassing op financiële entiteiten, maar ook rechtstreeks op 'in derde landen gevestigde ICT-leveranciers' en 'ICT-subcontractanten uit derde landen',[40] zoals omschreven in art. 3 lid 24 en 28 DORA. Hiermee wordt verwezen naar ICT-leveranciers die buiten de Europese Unie gevestigd zijn, maar hun ICT-diensten aanbieden aan financiële entiteiten binnen de Europese Unie.[41] Wanneer een dergelijke aanbieder door de Europese toezichthoudende autoriteiten – in Nederland DNB – wordt aangewezen als 'kritieke derde aanbieder van ICT-diensten',[42] dan dient deze aanbieder binnen twaalf maanden na de aanwijzing een dochteronderneming in de Europese Unie te vestigen.[43]

Bovengenoemde verschillen maken dat de praktijkjurist er goed aan doet om een inventarisatie te maken van alle bestaande en nieuwe ICT-contracten en na te gaan in hoeverre

30 Namelijk: aanbieders van rekeninginformatiediensten, aanbieders van cryptoactivadiensten, centrale effectenbewaarinstellingen, centrale tegenpartijen, handelsplatformen, transactieregisters, beheerders van alternatieve beleggingsinstellingen, beheermaatschappijen, aanbieders van datarapporteringsdiensten, verzekerings- en herverzekeringsondernemingen, verzekeringstussenpersonen, herverzekeringstussenpersonen en nevenverzekeringstussenpersonen, instellingen voor bedrijfspensioenvoorziening, ratingbureaus, beheerders van kritieke benchmarks, aanbieders van crowdfundingsdiensten en securisatieregisters.

31 Met uitzondering van traditionele analoge telefoondiensten.

32 Art. 3 (21) DORA.

33 Zie DNB Circulaire Cloud Computing, 2011/643815, 6 december 2011.

34 Art. 2 lid 1 sub u DORA. De DORA definieert derde aanbieders van ICT-diensten als: 'een onderneming die ICT-diensten verleent', art. 3 (19) DORA.

35 Zie anders Van Vliet 2023, p. 190.

36 Par. 5, 9 en 10 EBA-Guidelines. Zie over de praktische problemen die hierbij kunnen ontstaan W. van Angeren & E.C. Hangelbroek, Hoe zet je contractuele verplichtingen door naar subleveranciers bij een uitbesteding?, MvV 2021, afl. 10, p. 349-355.

37 Hier staat tegenover dat de verplichtingen uit de DORA nog steeds redelijk algemeen zijn. De inhoud van SLA's etc. is nog steeds ter vrije onderhandeling tussen partijen.

38 Overweging 63 DORA.

39 Zie ook M. Kok, Derden onder de DORA: wanneer trekt de mist op?, 17 oktober 2024, www.finnius.com.

40 De DORA hanteert de termen 'uitbesteding', 'onderaanbesteding', 'onderaanneming' en 'subcontracteren' (en variaties daarop) door elkaar. Wij zullen voor het overige van dit artikel 'onderaanneming' aanhouden.

41 Zie ook overweging 67 en 81 DORA.

42 Art. 3 (23) jo. art. 31 lid 12 jo. lid 1 sub a DORA. De DORA maakt onderscheid tussen ICT-leveranciers en kritieke ICT-leveranciers. Onder art. 31 DORA kunnen ICT-leveranciers door de 'lead overseer' (gedefinieerd in art. 3 (61) DORA) worden aangewezen als 'cruciaal' voor (een) financiële entiteit(en), wat deze aanbieders onder de definitie van 'kritieke derde aanbieder van ICT-diensten' doet vallen (art. 3 (23) DORA). Dit is nieuw en bestaat niet in de EBA-Guidelines. Kritieke ICT-leveranciers komen vervolgens ook onder rechtstreeks toezicht te staan van een 'lead overseer'. Deze wordt per kritieke aanbieder van ICT-diensten geselecteerd uit een van de volgende Europese toezichthoudende autoriteiten: de EBA, de EIOPA of de ESMA. Conform art. 31 lid 1 sub b DORA wordt als *lead overseer* aangewezen de autoriteit die verantwoordelijk is voor de financiële entiteiten die samen over het grootste aandeel van de totale activa beschikken ten opzichte van de waarde van de totale activa van alle financiële entiteiten die gebruik maken van de diensten van de betrokken kritieke aanbieder van ICT-diensten, zoals resulteert uit de som van de individuele balansen van de financiële entiteiten. Zie hierover ook Christianen 2023.

43 Art. 31 lid 12 DORA.

 doi: 10.5553/MvV/157457672024034010004

ICT-diensten (respectievelijk geleverd of ontvangen) onder de EBA-Guidelines en de DORA vallen. Deze inspanning zou moeten leiden tot een overzicht van (1) bestaande contracten waarop de EBA-Guidelines en de DORA niet van toepassing zijn, (2) bestaande (uitbestedings)contracten waarop de EBA-Guidelines niet van toepassing zijn, maar de DORA wel, (3) bestaande (uitbestedings)contracten waarop zowel de EBA-Guidelines als de DORA van toepassing zijn, (4) nieuw te sluiten contracten waarop alleen de DORA van toepassing is, en (5) nieuw te sluiten (uitbestedings)contracten waarop zowel de DORA als de EBA-Guidelines van toepassing zijn.

Iedere situatie vereist een andere opvolging bij het opnemen van de verplichtingen uit de DORA in de contracten tussen financiële entiteiten en ICT-leveranciers. Bestaande contracten waarop de EBA-Guidelines niet van toepassing zijn maar de DORA wel, moeten worden aangevuld met alle verplichtingen uit de DORA die betrekking hebben op de contractuele verhouding tussen financiële entiteiten en ICT-leveranciers. Bestaande contracten waarop de EBA-Guidelines van toepassing zijn, moeten worden aangevuld met de verplichtingen uit de DORA die boven op die van de EBA-Guidelines komen. Dit kan op verschillende manieren, bijvoorbeeld door middel van een addendum op bestaande contracten, het sluiten van een geheel nieuw contract, of het ter hand stellen en van toepassing verklaren van een set 'DORA terms and conditions' door de financiële instelling aan al haar ICT-leveranciers. Zoals wij in de inleiding van dit artikel aangaven, kan een gapanalyse tussen de DORA en EBA-Guidelines inzichtelijk maken wat er precies aan dergelijke contracten moet worden toegevoegd.

Praktisch gezien zijn er twee benaderingen voor het aanpassen van bestaande contracten. De eerste optie is om het contract grondig te herzien en maatwerkoplossingen door te voeren die voldoen aan de DORA. De tweede optie is een meer pragmatische aanpak, waarbij partijen een addendum (laten) opstellen met de verplichte DORA-bepalingen en dit addendum vervolgens toevoegen aan de bestaande contracten. Voor al bestaande contracten waarin de EBA-Guidelines al zijn verwerkt, kan worden volstaan met een DORA-addendum. Een addendum kan ook praktisch zijn bij het afsluiten van nieuwe contracten voor ICT-diensten. Bij nieuwe uitbestedingen van ICT-diensten kan worden gedacht aan een combinatieaddendum, waarin zowel de verplichtingen van de EBA-Guidelines als de verplichtingen van de DORA worden verwerkt. Dit addendum zou ook kunnen worden gebruikt voor nieuwe contracten waarop alleen de DORA van toepassing is. Indien de financiële instelling opteert voor het ter hand stellen (toesturen) en van toepassing verklaren van een set 'DORA terms and conditions' neemt deze ons inziens een risico, aangezien het lastig zal zijn om deze set goed te laten aansluiten bij alle bestaande ICT-contracten, en omdat ernstig rekening gehouden zal moeten worden met de mogelijkheid dat een of meerdere ICT-leveranciers de set met voorwaarden niet of niet volledig zullen accepteren. Voor alle scenario's is het aan te raden om een 'DORA-checklist' op te (laten) stellen, aan de hand waarvan de contracterende partijen zorgvuldig kunnen controleren of alle verplichte afspraken uit de DORA daadwerkelijk in de overeenkomst zijn opgenomen. Daarnaast adviseren wij voor elk scenario om tijdig overleg te voeren met de contractspartij om de nodige wijzigingen door te voeren.

2.3 Nieuwe verplichtingen onder de DORA

De DORA bevat diverse nieuwe verplichtingen die niet zijn opgenomen in de EBA-Guidelines. De belangrijkste zijn de volgende.

Ondersteuning bij incidenten

De DORA verplicht partijen om contractueel overeen te komen dat de ICT-leverancier in het geval van een ICT-incident[44] zonder extra kosten of tegen een vooraf bepaalde kostprijs ondersteuning moet verlenen.[45] Dit biedt financiële entiteiten zekerheid over de kosten en beschikbaarheid van ondersteuning tijdens ICT-incidenten. Deze verplichting is een goed voorbeeld van hoe de DORA de positie van financiële entiteiten versterkt door ook rechtstreeks eisen te stellen aan ICT-leveranciers. Voorheen zouden financiële entiteiten mogelijk ook hebben gewild dat bij een ICT-incident bijstand werd verleend, maar zonder de uitdrukkelijke wettelijke verplichting om dit met zoveel woorden overeen te komen,[46] was dit sterk afhankelijk van de onderhandelingspositie van de financiële entiteit.

Beschrijving van de te leveren functies en ICT-diensten in één schriftelijk document

Onder de DORA moeten alle ICT-diensten en functies die door de ICT-leverancier worden geleverd, op een 'duidelijke en volledige' manier worden omschreven in het contract tus-

44 Art. 3 lid 8 DORA: '"ICT-gerelateerd incident": één gebeurtenis of een reeks gekoppelde gebeurtenissen die niet door de financiële entiteit zijn gepland en die de beveiliging van de netwerk- en informatiesystemen in gevaar brengen en een nadelig effect hebben op de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van gegevens of op de door de financiële entiteit verleende diensten'; art. 3 lid 10 DORA: '"ernstig ICT-gerelateerd incident": een ICT-gerelateerd incident met grote nadelige gevolgen voor de netwerk- en informatiesystemen die kritieke of belangrijke functies van de financiële entiteit ondersteunen'.

45 Art. 30 lid 2 sub f DORA.

46 Verplichtingen om afspraken te maken in het kader van cyberincidenten waren al aanwezig in bestaande wetgeving. Zo vereist de AVG van de verwerkingsverantwoordelijke en verwerker dat zij passende technische en organisatorische maatregelen nemen om een passend beveiligingsniveau te waarborgen, waaronder wordt begrepen 'het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot persoonsgegevens tijdig te herstellen' (art. 32 lid 1 sub c AVG). Een ander voorbeeld is art. 8 Wet beveiliging netwerk- en informatiesystemen, dat vereist dat een aanbieder van een essentiële dienst en diens digitale dienstverlener passende maatregelen moeten nemen om incidenten die de beveiliging van de voor de verlening van de betrokken dienst gebruikte netwerk- en informatiesystemen aantasten te voorkomen en de gevolgen van dergelijke incidenten zo veel mogelijk te beperken, teneinde de continuïteit van die dienst te waarborgen. Deze verplichtingen zijn echter minder breed van toepassing en eisen bovendien niet dat contractueel moet worden vastgelegd dat bij een ICT-incident de ICT-leverancier ondersteuning moet verlenen.

sen de financiële entiteit en de ICT-leverancier.[47] De EBA-Guidelines vereisen een 'heldere' beschrijving van de uitbestede functies die als kritiek of belangrijk worden beschouwd.[48] Het feit dat de DORA een duidelijke/heldere omschrijving eist voor alle functies en ICT-diensten (en niet alleen voor kritieke of belangrijke functies) lijkt een goede ontwikkeling, aangezien contractuele helderheid/duidelijkheid[49] en compleetheid over welke diensten precies geleverd moeten worden in het algemeen zullen leiden tot minder geschillen. Niet geheel duidelijk is wat wordt bedoeld met het woord 'volledig' en hoe deze verplichting zich verhoudt tot veelvoorkomende praktijken, zoals Agile, waarbij de diensten vaak niet tot in detail wordt gespecificeerd. Daarnaast zou dit voor de ICT-leverancier een argument kunnen zijn om te betogen dat voor een beroep op niet expliciet overeengekomen verplichtingen, zoals verplichtingen die in zorgplichtjurisprudentie zijn aangenomen,[50] geen of minder plaats is. Een dergelijk standpunt zou ertoe kunnen leiden dat de zorgplicht van ICT-leveranciers bij een ICT-contract dat onderhevig is aan de DORA nauwer wordt gekoppeld aan de schriftelijk overeengekomen verplichtingen. Daarmee zouden de flexibiliteit en impliciete uitbreiding van verplichtingen van de leverancier op grond van de zorgplicht die voortvloeit uit art. 7:401 BW – en daarmee tegelijkertijd de bescherming van de financiële entiteit – worden beperkt. Dit lijkt ons niet wenselijk en ook niet de bedoeling van de DORA.

Art. 30 lid 1 DORA vereist dat alle rechten en plichten van zowel de financiële entiteit als de ICT-leverancier op een duidelijke wijze moeten worden toegewezen en schriftelijk moeten worden vastgelegd in één schriftelijk document. Dit document moet voor beide partijen beschikbaar zijn, hetzij op papier, hetzij in een ander duurzaam, toegankelijk en downloadbaar formaat. In de praktijk bestaan ICT-overeenkomsten veelal uit een hoofdcontract met meerdere bijlagen, of bestaan ze uit raamovereenkomsten, waaronder later nadere overeenkomsten of addenda worden gesloten. Naar de letter van art. 30 lid 1 DORA lijken contractstructuren bestaande uit meerdere samenhangende documenten niet meer toelaatbaar. Dit betekent dat om te voldoen aan de DORA alle contractdocumenten in één enkel document moeten worden geïntegreerd. Hetzelfde geldt als een overeenkomst wijzigt. In de praktijk vinden wijzigingen veelal plaats via een addendum. Het lijkt erop dat dit onder de DORA niet is toegestaan en dat elke wijziging steeds in het hoofddocument moet worden verwerkt.

Daarnaast kan worden afgevraagd of het gebruik van hyperlinks in contracten straks nog is toegestaan. In de praktijk wordt door ICT-leveranciers vaak gebruik gemaakt van hyperlinks om te verwijzen naar externe documenten, zoals beleidsdocumenten of (algemene) voorwaarden die als een onderdeel van de overeenkomst worden beschouwd. De vraag rijst in hoeverre er dan nog sprake is van één schriftelijk document, en of met het gebruik van hyperlinks wordt voldaan aan het vereiste van een 'downloadbaar, duurzaam en toegankelijk formaat'. Hyperlinks kunnen immers onderhevig zijn aan wijzigingen, verouderde inhoud weergeven of verwijzen naar een pagina met meerdere documenten, waarbij het soms zelfs niet duidelijk is welke documenten van toepassing zijn op de overeenkomst.

De tekst van de DORA laat ook onduidelijkheid bestaan over wie de eindverantwoordelijkheid draagt voor bovengenoemde verplichtingen. Is dit primair de taak van de financiële entiteit om ervoor te zorgen dat deze afspraken schriftelijk worden vastgelegd,[51] is het de taak van de ICT-leverancier, of is het een gezamenlijke verantwoordelijkheid en moeten beide partijen een actieve rol spelen in het opstellen en vastleggen van de wederzijdse rechten en plichten? Ons inziens verplicht de DORA zowel de ICT-leverancier als de financiële entiteit om verantwoordelijkheid te nemen voor de schriftelijke vastlegging van hun rechten en verplichtingen.[52] Hoewel een gezamenlijke verantwoordelijkheid logisch is, zou het nuttig zijn als de DORA specificeert hoe deze taakverdeling eruitziet. Een duidelijke verdeling, waarbij de financiële entiteit eindverantwoordelijk is voor de naleving en de ICT-leverancier een ondersteunende verplichting heeft, zou ons inziens de praktische uitvoering vergemakkelijken en aansluiten bij de algehele gedachte achter de DORA.

Threat-led penetration testing en permanente monitoring

De EBA-Guidelines verplichten financiële entiteiten in paragraaf 94 om, 'waar relevant',[53] ervoor te zorgen dat zij in staat zijn om beveiligingspenetratietesten uit te voeren om de effectiviteit van geïmplementeerde cyber- en interne ICT-beveiligingsmaatregelen en -processen te beoordelen. Deze verplichting om penetratietesten uit te voeren impliceert dat een verplichting tot medewerking door de leverancier moet worden

47 Art. 30 lid 2 sub a DORA. In hetzelfde artikel staat dat in het contract moet worden aangegeven of 'uitbesteding' van een ICT-dienst die een kritieke of belangrijke functie ondersteunt, is toegestaan en, zo ja, onder welke voorwaarden. NB In de Engelstalige versie van de DORA wordt verwezen naar 'subcontracting', in de Nederlandstalige versie: 'uitbesteding'. 'Onderaanneming' was wat ons betreft een betere vertaling geweest, zie ook noot 40.

48 Par. 75 (a) EBA-Guidelines.

49 We gaan ervan uit dat met helderheid en duidelijkheid hetzelfde bedoeld wordt.

50 Zie bijv. E.C. Hangelbroek & L. Leemeijer, De 'bijzondere' zorgplicht van de IT-dienstverlener: twee zwaluwen maken nog geen zomer?, Computerrecht 2024, afl. 1, p. 5-6.

51 Dit zou mogelijk kunnen worden afgeleid uit art. 4 lid 2 DORA. In dit artikel wordt in het kader van het evenredigheidsbeginsel bij de toepassing van de verplichtingen onder de DORA immers enkel naar financiële entiteiten verwezen, en niet (ook) naar ICT-leveranciers.

52 Zoals besproken in par. 2.2 van dit artikel is de DORA immers ook rechtstreeks van toepassing op de ICT-leverancier.

53 Wat met de toevoeging 'waar relevant' wordt bedoeld, blijkt niet duidelijk uit de tekst van de EBA-Guidelines dan wel de EBA-richtsnoeren inzake de beoordeling van het ICT-risico in het kader van SREP, waarnaar in par. 94 EBA-Guidelines wordt verwezen; zie www.eba.europa.eu/documents/10180/1954038/9df6f925-3de8-4d31-96ce-fbd0fb828628/Guidelines%20on%20ICT%20Risk%20Assessment%20under%20SREP%20(EBA-GL-2017-05)_NL.pdf.

 doi: 10.5553/MvV/157457672024034010004

vastgelegd in de contractuele afspraken tussen financiële entiteiten en ICT-leveranciers. De DORA legt verdergaande verplichtingen op met betrekking tot het uitvoeren van specifieke geavanceerde tests: *threat-led penetration tests* (TLPT's).[54] Art. 30 lid 2 sub d DORA schrijft voor dat de contractuele afspraken over het gebruik van ICT-diensten die kritieke of belangrijke functies ondersteunen, in ieder geval moeten omvatten dat de ICT-leverancier 'volledig' zal meewerken aan de TLPT van de financiële entiteit. Hoe dergelijke TLPT's eruit zullen zien en aan welke vereisten deze tests moeten voldoen, wordt in meer detail uitgewerkt in art. 26 en 27 DORA.

Naast de specifieke vereisten omtrent TLPT's moeten de overeenkomsten tussen financiële entiteiten en ICT-leveranciers op grond van art. 30 lid 3 sub e DORA het recht van de financiële entiteit bevatten om de prestaties van de ICT-leverancier 'permanent te monitoren'. Dit recht omvat onbeperkte toegang tot en inspectie en audit van de ICT-leverancier door de financiële entiteit, een door deze entiteit aangestelde derde partij, of de bevoegde autoriteit. De uitoefening van dit recht mag niet worden belemmerd door andere afspraken en omvat tevens het recht om ter plaatse kopieën te maken van relevante documenten die cruciaal zijn voor de activiteiten van de ICT-leverancier.[55] Hoewel het niet met zoveel woorden wordt geduid in de bepalingen van de DORA, lijken het onbeperkte toegangsrecht en het recht om ter plaatse kopieën te maken van documenten erop te wijzen dat ook toegang tot de bedrijfslocaties van ICT-leveranciers, waaronder externe datacenters, moet worden verleend. In paragraaf 87 van de EBA-Guidelines is ook een verplichting opgenomen om een onbeperkt auditrecht overeen te komen, maar deze verplichting geldt in principe[56] alleen voor uitbestedingen van kritieke of belangrijke functies.

In de praktijk is er vanuit ICT-leveranciers vaak weerstand tegen brede auditrechten en het uitvoeren van penetratietests (zoals TLPT). Deze weerstand is niet onbegrijpelijk. Toegang tot bedrijfslocaties van de ICT-leverancier ten behoeve van audits bijvoorbeeld, brengt immers niet alleen operationele lasten met zich mee, maar ook beveiligingsrisico's. Immers: hoe meer mensen toegang hebben tot datacenters, hoe groter het risico op potentiële beveiligingsinbreuken. Om deze risico's te beperken, laten ICT-leveranciers zichzelf vaak certificeren om aan te tonen dat zij aan bepaalde beveiligingsstandaarden[57] voldoen. Dit maakt het uitvoeren van audits door of namens afnemers minder noodzakelijk. Ook worden soms *pooled audits* aangeboden, waarbij meerdere afnemers gezamenlijk een audit laten uitvoeren bij de ICT-leverancier.[58]

De opstellers van de DORA lijken zich – meer dan de EBA bij het opstellen van de EBA-Guidelines – iets bewuster te zijn geweest van deze praktische bezwaren van ICT-leveranciers. Zo voorziet de DORA expliciet in de mogelijkheid van *pooled testing*.[59] Niet geheel duidelijk is echter of pooled audits ook zijn toegestaan onder de DORA. In art. 30 lid 3 sub e onder (ii) DORA wordt het recht toegekend om andere garantieniveaus overeen te komen 'indien de rechten van andere cliënten worden aangetast'. Hoewel niet duidelijk is wie dit recht precies heeft, welke andere cliënten worden bedoeld (die van de financiële entiteit of die van de ICT-leverancier) en welke garantieniveaus van toepassing zijn, lijkt deze bepaling bedoeld om de inzet van pooled audits te faciliteren als alternatief voor de onbeperkte toegang. Dit laatste staat er echter niet met zoveel woorden. Het vereiste dat overeenkomsten *ten minste* de in art. 30 lid 2 DORA genoemde elementen moeten bevatten,[60] gecombineerd met het gebruik van 'en' in plaats van 'of' in de opsomming, impliceert dat zowel het recht op onbeperkte toegang als het recht om andere garantieniveaus overeen te komen moet worden opgenomen. De DORA lijkt hier dus innerlijk tegenstrijdig.

Een andere innerlijke tegenstrijdigheid is dat art. 30 lid 3 sub e onder (iv) DORA vereist dat contracten tussen financiële entiteiten en ICT-leveranciers details bevatten over het toepassingsgebied, de te volgen procedures en de frequentie van inspecties en audits, waarbij de term 'frequentie' een beperking suggereert op hoe vaak audits mogen worden uitgevoerd, maar de DORA tegelijkertijd in art. 30 lid 3 sub e onder (i) 'onbeperkte toegang' eist.

Bewustmakingsprogramma's en opleidingen

Art. 13 lid 6 DORA legt financiële entiteiten de verplichting op om bewustmakingsprogramma's op het gebied van ICT-beveiliging en opleidingen inzake digitale operationele weerbaarheid te ontwikkelen. Financiële entiteiten moeten ICT-leveranciers integreren in hun relevante opleidingsprogramma's.[61] Overeenkomsten met ICT-leveranciers moeten dus minimaal de voorwaarden bevatten voor deelname door het personeel van de ICT-leverancier aan de bewustmakings- en opleidingsprogramma's van de financiële entiteit. De EBA-Guidelines leggen geen vergelijkbare verplichtingen met betrekking tot bewustmakingsprogramma's en opleidingen op. Omdat in de DORA niet wordt toegelicht wat precies onder 'bewustmakingsprogramma' wordt verstaan, is niet duidelijk wat er precies in de overeenkomst moet komen te staan om compliant te zijn.

54 JC 2024-29, 17 juli 2024, Draft Regulatory Technical Standards specifying elements related to threat led penetration tests under Article 26(11) of Regulation (EU) 2022/2554, overweging 13.

55 Welke documenten cruciaal zijn voor de activiteiten van de ICT-leverancier blijkt niet uit de tekst van de DORA.

56 Zie par. 88 EBA-Guidelines voor wat geldt voor uitbesteding van niet-kritieke of niet-belangrijke functies.

57 Zie bijv. ISAE-verklaringen.

58 Bijkomend voordeel hiervan is dat de kosten van deze relatief lager liggen.

59 Art. 26 lid 4 DORA. Pooled testing en joint testing worden ook beschreven in art. 14 van de Draft Regulatory Technical Standards specifying elements related to threat led penetration tests under Article 26(11) of Regulation (EU) 2022/2554.

60 En in het geval van ICT-diensten die kritieke of belangrijke functies ondersteunen ook de in art. 30 lid 3 DORA genoemde elementen.

61 Art. 30 lid 2 sub i DORA.

2.4 Nuanceverschillen

De EBA-Guidelines en de DORA bevatten diverse bepalingen die op het eerste gezicht op elkaar lijken, maar toch van elkaar verschillen. Voorbeelden zijn de gehanteerde terminologie van 'kritieke of belangrijke functies', contractuele afspraken over opzegging, en rapportageverplichtingen, bedrijfscontinuïteitsplannen en onderaanneming.[62] Deze – soms subtiele – verschillen kunnen voor verwarring zorgen en maken naleving voor financiële entiteiten en ICT-leveranciers complex. Hieronder zullen wij dit illustreren aan de hand van twee voorbeelden die het meest in het oog springen.

Terminologie: kritieke of belangrijke functies

Zowel de EBA-Guidelines als de DORA hanteren het begrip 'kritieke of belangrijke functie', maar er zijn verschillen in de manier waarop dit begrip wordt gedefinieerd en toegepast. In de EBA-Guidelines wordt dit gedefinieerd als 'een functie die als kritiek of belangrijk wordt beschouwd zoals beschreven in hoofdstuk 4 van deze richtsnoeren'. Het gaat hier om functies waarvan de verstoring invloed heeft op de prestaties of verplichtingen van een financiële entiteit, zonder expliciet in te gaan op de bredere gevolgen voor de financiële stabiliteit of economie.

De DORA geeft in art. 3 (22) een uitgebreidere definitie van een 'kritieke of belangrijke functie':

> 'een functie 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 wezenlijk 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 diensten'.[63]

Hoewel de strekking van de begrippen vergelijkbaar is, zijn er verschillen in de uitwerking ervan. Waar de EBA-Guidelines zich voornamelijk richten op functies waarvan de verstoring invloed heeft op de prestaties of verplichtingen van een financiële entiteit, wordt onder de DORA een bredere definitie gehanteerd die ook de continuïteit van de ICT-diensten, de naleving van vergunningen of de verplichtingen onder toepasselijke wetgeving omvat. Dit betekent in de praktijk dat financiële entiteiten die naast de EBA-Guidelines ook onder de DORA vallen, een grotere reeks functies als kritiek of belangrijk moeten beschouwen, wat leidt tot meer en strengere verplichtingen. Wij adviseren financiële entiteiten en ICT-leveranciers om in kaart te brengen welke ICT-diensten als kritiek of belangrijk beschouwd moeten worden, en om dit mee te nemen in hun overeenkomsten en addenda (zie ook par. 1).

Verschillen in opzegrechten

De EBA-Guidelines schrijven in paragraaf 98 financiële entiteiten voor om afspraken te maken met betrekking tot het beëindigen van hun uitbestedingsovereenkomst. Ook de DORA legt deze verplichting in art. 28 lid 7 aan financiële entiteiten en ICT-leveranciers op. Hoewel de voorschriften op het eerste gezicht vergelijkbaar zijn, zijn er ook belangrijke verschillen in de mate van strengheid en de voorwaarden waaronder beëindiging moet kunnen plaatsvinden.

Een van de voornaamste verschillen is de ernst van de overtreding die beëindiging rechtvaardigt. Onder de EBA-Guidelines moet in de uitbestedingsovereenkomst de mogelijkheid worden opgenomen voor de financiële entiteit om de uitbestedingsovereenkomst te beëindigen bij *iedere* overtreding van wet- en regelgeving of contractuele bepalingen, ongeacht de ernst daarvan. Dit biedt de financiële entiteit meer flexibiliteit en een ruimere basis om de uitbesteding te beëindigen, hetgeen een hogere mate van risicobeheersing vanuit de financiële entiteit mogelijk maakt. Deze benadering kan echter ook leiden tot minder zekerheid voor ICT-leveranciers, die geconfronteerd kunnen worden met beëindiging bij zelfs een relatief kleine tekortkoming, hetgeen in de praktijk niet of nauwelijks aanvaard zal worden. Onder de DORA moet in de overeenkomst worden opgenomen dat deze mag worden beëindigd als er sprake is van een *ernstige overtreding* van wet- en regelgeving of een overtreding van contractuele verplichtingen door de ICT-leverancier.[64] Dit betekent dat de DORA een zekere mate van proportionaliteit hanteert:[65] niet elke overtreding leidt tot het recht de overeenkomst te mogen beëindigen, maar alleen die overtredingen die als 'ernstig' kunnen worden gekwalificeerd. Onder de DORA heeft de ICT-leverancier dus meer comfort dan onder de EBA-Guidelines.

Zowel uit de DORA als uit de EBA-Guidelines wordt overigens niet duidelijk of met de term 'beëindigen' opzegging of ontbinding wordt bedoeld. Dit is een in de praktijk zeer relevant verschil, gelet op de verschillende rechtsgevolgen die naar Nederlands recht gelden. Bij ontbinding ontstaan op grond van art. 6:271 BW ongedaanmakingsverplichtingen, plus daarnaast op grond van art. 6:277 BW een schadevergoedingsplicht voor de partij waarvan de tekortkoming de ontbinding heeft veroorzaakt. Deze rechtsgevolgen gelden echter niet per se bij opzegging. In dat geval blijven de eerder uitgevoerde prestaties doorgaans in stand, en ontstaat er – tenzij anders overeengekomen – niet standaard een ongedaanmakingsverplichting of schadevergoedingsplicht. Wanneer de beëindiging als ontbinding wordt beschouwd, zou dat kunnen betekenen dat de ICT-leverancier verplicht is om prestaties ongedaan te maken,

62 Zie over opzegging: art. 28 lid 8 en 30 lid 2 sub h DORA en par. 75 (m), 75 (q), 78 (q), 98 en 99 EBA-Guidelines, over rapportageverplichtingen: art. 28 en 30 lid 3 DORA en par. 75 (j) EBA-Guidelines, over bedrijfscontinuïteitsplannen: art. 6, 11 en 30 lid 3 sub c DORA en par. 48 en 75 (l) EBA-Guidelines, en over onderaanneming: art. 30 lid 2 sub a DORA en par. 75 (e) en 76 t/m 80 EBA-Guidelines.

63 Art. 3(22) DORA.

64 Art. 28 lid 7 sub a DORA.

65 Zie in dit kader ook art. 4 lid 2 DORA.

 doi: 10.5553/MvV/157457672024034010004

en dat hij mogelijk een schadevergoeding moet betalen als zijn tekortkoming aanleiding was voor de beëindiging.

Vanuit het perspectief van een financiële entiteit zou het op basis van het voorgaande gunstig kunnen zijn om 'beëindigen' uit te leggen als ontbinding in plaats van opzegging, omdat dat van rechtswege meer rechtsmiddelen biedt, zoals ongedaanmaking van verrichte prestaties (lees: terugbetaling van gedane betalingen) en een schadevergoedingsplicht voor de ICT-leverancier in geval van zijn tekortkoming. Voor de ICT-leverancier is dit daarentegen nadelig, omdat deze uitleg kan leiden tot een terugbetalingsverplichting en een verplichting om schade te vergoeden.

Een tweede verschil is dat onder de EBA-Guidelines beëindigingsrechten moeten worden opgenomen in de overeenkomst voor het geval er zwakheden zijn met betrekking tot het management en de beveiliging van vertrouwelijke, persoonlijke of anderszins gevoelige data of informatie.[66] Onder de DORA moeten beëindigingsrechten worden opgenomen voor het geval er sprake is van 'klaarblijkelijke zwakheden van de ICT-leverancier in verband met zijn algemeen beheer van het ICT-risico',[67] hetgeen een ruimer beëindigingsrecht lijkt te impliceren dan onder de EBA-Guidelines.

Een derde verschil doet zich voor met betrekking tot beëindiging vanwege een wijziging van de overeenkomst. Volgens de EBA-Guidelines mag een overeenkomst door de financiële entiteit worden beëindigd als er sprake is van 'wijzigingen die materieel zijn en gevolgen hebben voor de uitvoering van de overeenkomst of de dienstverlener', zoals bijvoorbeeld wijzigingen van onderaannemers.[68] Onder de DORA moet beëindiging mogelijk zijn bij elke 'materiële wijziging' die de overeenkomst of de situatie van de ICT-leverancier 'nadelig beïnvloed[t], ongeacht de omvang of impact hiervan'. Dit impliceert zowel een beperking als een verruiming ten opzichte van de EBA-Guidelines, maar met name dat laatste.[69]

Art. 30 lid 2 sub h DORA, tot slot, vereist dat overeenkomsten met betrekking tot het gebruik van ICT-diensten ten minste beëindigingsrechten en bijbehorende minimumopzegtermijnen moeten bevatten, 'in overeenstemming met de verwachtingen van zowel de bevoegde autoriteiten als de afwikkelingsautoriteiten'.[70] Een uitdaging die voortvloeit uit deze bepaling is het gebrek aan duidelijkheid over wat precies wordt bedoeld met de 'verwachtingen van de bevoegde autoriteiten en de afwikkelingsautoriteiten'. Deze verwachtingen worden niet nader gespecificeerd in de tekst van de DORA of in een technische standaard, waardoor onzekerheid bestaat over hoe financiële entiteiten en ICT-leveranciers deze bepalingen in de praktijk moeten interpreteren en implementeren.[71] Zonder nadere duiding is het voor partijen moeilijk om te bepalen welke specifieke voorwaarden en opzegtermijnen als voldoende worden beschouwd door de autoriteiten. Dit gebrek aan duidelijkheid kan leiden tot uiteenlopende interpretaties en uitvoeringswetten, hetgeen de uniformiteit en rechtszekerheid in de sector in de praktijk kan ondermijnen. Daarnaast roept deze onduidelijkheid vragen op over de mate van flexibiliteit die financiële entiteiten hebben bij het onderhandelen over beëindigingsrechten en opzegtermijnen. Kunnen zij bijvoorbeeld zelf bepalen welke opzegtermijnen in hun specifieke omstandigheden redelijk en haalbaar zijn, of moeten zij zich strikt houden aan de (nog ongespecificeerde) verwachtingen van de autoriteiten? Bovendien, wat gebeurt er als de verwachtingen van de bevoegde autoriteiten afwijken van die van de afwikkelingsautoriteiten?[72] Deze potentiële discrepanties kunnen leiden tot conflicten en juridische en praktische uitdagingen bij de uitvoering en handhaving van contractuele afspraken.[73]

66 Par. 98 (d) EBA-Guidelines.

67 Hierbij wordt in het bijzonder gekeken naar de manier waarop de ICT-leverancier zorgt voor de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van persoonlijke of anderszins gevoelige gegevens of niet-persoonsgebonden gegevens, zie art. 28 lid 7 sub c DORA. Dit legt indirect ook eisen op met betrekking tot de bewijsvoering bij beëindiging omwille van zwakheden in het ICT-beheer van de ICT-leverancier. De DORA vereist dat dergelijke zwakheden duidelijk en aantoonbaar zijn; ze moeten 'klaarblijkelijk' zijn. Dit betekent dat er objectief bewijs moet zijn om aan te tonen dat de ICT-beheerprocessen van de ICT-leverancier zwakheden bevatten. Deze bepaling zorgt ervoor dat ICT-leveranciers beschermd zijn tegen beëindiging op basis van onduidelijke of subjectieve oordelen, hetgeen een eerlijkere behandeling bevordert. Het legt echter ook een extra last op de financiële entiteit om dit bewijs te kunnen leveren.

68 Par. 98 (c) EBA-Guidelines.

69 Er is ook sprake van een beperking omdat onder de DORA (indien geïmplementeerd in de overeenkomst) – anders dan onder de EBA-Guidelines (indien geïmplementeerd in de overeenkomst) – niet kan worden opgezegd als er sprake is van een wijziging die wel materieel is, maar waarvan de gevolgen niet nadelig worden beïnvloed. Hoewel in de meeste gevallen de financiële entiteit de overeenkomst pas zal willen beëindigen als er sprake is van nadelige gevolgen, kan deze beperking relevant zijn voor de situatie waarin de financiële entiteit om een andere reden van de overeenkomst af wil, en hiervoor een grondslag nodig heeft.

70 Art. 30 lid 2 sub h DORA maakt gebruik van de term 'contractuele overeenkomst', wat lijkt op een vertaalfout uit het Engels. In dit artikel hanteren wij daarom de termen 'overeenkomst' en 'contract'.

71 Hoewel in overweging 71 DORA wel wordt verwezen naar de 'verwachtingen van zowel de bevoegde autoriteiten als de afwikkelingsautoriteiten', wordt hierbij geen toelichting gegeven over de betekenis en/of invulling van dit criterium; ook de Regulatory Technical Standards geven hier geen verdere verduidelijking over.

72 Afwikkelingsautoriteiten in de zin van art. 3 Richtlijn 2014/59/EU. De Nederlandse afwikkelingsautoriteit is DNB.

73 NB Het is onduidelijk of het beëindigingsrecht alleen van toepassing is op de financiële entiteit zelf of ook op de ICT-leverancier, zie Brederveld en De Boer, die suggereren dat het gebruik van het meervoud 'beëindigingsrechten' zou kunnen wijzen op rechten voor zowel de financiële entiteit als de ICT-leverancier. Ze merken echter terecht op dat er onduidelijkheid blijft over hoe zwaar de bijzin weegt, en dat de DORA hierover geen verdere helderheid verschaft, zie Brederveld & De Boer 2024.

3 Conclusie en analyse

De DORA vormt een belangrijke nieuwe stap in de Europese regelgeving, specifiek gericht op het versterken van de digitale operationele weerbaarheid van financiële entiteiten. Hoewel er aanzienlijke overlap bestaat tussen de DORA en bestaande instrumenten zoals de EBA-Guidelines, kent de DORA een breder toepassingsbereik en introduceert de DORA enkele nieuwe verplichtingen die van invloed zijn op zowel bestaande als toekomstige contractuele relaties tussen financiële entiteiten en ICT-leveranciers. Dit maakt dat een goed begrip van beide instrumenten en van de (nuance)verschillen tussen beide instrumenten cruciaal is om te kunnen beoordelen in hoeverre bestaande en nieuw te sluiten contracten voldoen aan de verplichtingen onder de DORA. Een gap-analyse, waarin de verschillen tussen de DORA en de EBA-Guidelines inzichtelijk worden, en een checklist aan de hand waarvan de contracterende partijen kunnen controleren of alle verplichte afspraken uit de DORA daadwerkelijk in de overeenkomst zijn opgenomen, kunnen hierbij praktische hulpmiddelen zijn.

Deze praktische hulpmiddelen nemen de discrepanties tussen beide instrumenten echter niet weg. Letterlijke overname van sommige contractbepalingen die in de EBA-Guidelines verplicht worden gesteld, betekent dat daarmee niet wordt voldaan aan de DORA, en andersom. Dit kan problemen geven bij handhaving door toezichthouders. Zo heeft DNB, in haar rol als toezichthouder, onlangs bij een financiële instelling aangegeven dat financiële entiteiten de volledige tekst van paragraaf 98 van de EBA-Guidelines met betrekking tot beëindigingscriteria een-op-een moeten opnemen in uitbestedingsovereenkomsten. Dit staat echter op gespannen voet met de beëindigingsbepalingen die op grond van de DORA in de overeenkomst moeten worden opgenomen (zie hierover par. 2.4). Het overnemen van paragraaf 98 uit de EBA-Guidelines leidt tot (gedeeltelijke) non-compliance met art. 28 lid 7 DORA.

In dit kader lijkt het goed nieuws dat de EBA heeft aangegeven de EBA-Guidelines te zullen updaten, zodat deze rekening houden met ('take into account') de DORA.[74] Welke wijzigingen precies zullen worden doorgevoerd, wanneer dit zal gebeuren, en of daarmee alle discrepanties tussen de EBA-Guidelines en de DORA zullen verdwijnen, blijft voorlopig onduidelijk. De onzekerheid over hoe financiële entiteiten en ICT-leveranciers compliant kunnen worden en blijven met zowel de DORA als de EBA-Guidelines, blijft dus voorlopig bestaan. Zoals aangegeven in paragraaf 2.1, adviseren wij om bij inconsistenties tussen de DORA en de EBA-Guidelines voorlopig de DORA te volgen.

Echter, ook als de EBA-Guidelines volledig in lijn zouden worden gebracht met de DORA, betekent dit niet dat het voor financiële entiteiten en ICT-leveranciers eenvoudig is om te voldoen aan de regels. Zoals uit een aantal voorbeelden in dit artikel blijkt, bevat de DORA zelf ook diverse onduidelijkheden die verduidelijking behoeven. Gezien het feit dat de DORA een Europese verordening is, zal uiteindelijk jurisprudentie van het Hof van Justitie van de Europese Unie richting geven aan de interpretatie ervan. Dit zal waarschijnlijk enige tijd duren. Tot die tijd zullen financiële instellingen en ICT-leveranciers moeten opereren met enige onzekerheid en met de op dit moment door toezichthouders gepubliceerde technische standaarden.[75] Los van het feit dat deze technische standaarden – enkele uitzonderingen daargelaten[76] – de in dit artikel gesignaleerde onduidelijkheden vooralsnog niet wegnemen, kan worden afgevraagd in hoeverre het wenselijk is dat toezichthouders (deels) verantwoordelijk worden voor de uitleg en interpretatie van de wet. Gesteld kan worden dat dit niet een

74 JC 2023-84, 10 januari 2024, 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. 28. NB Het gebruik van de term 'rekening houden met' suggereert niet dat de EBA-Guidelines volledig in lijn zullen worden gebracht met de DORA.

75 JC 2023-67, 27 november 2023, on 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 as mandated by Article 30(5) of Regulation (EU) 2022/2554; JC 2023-83, 10 januari 2024, on Draft Regulatory Technical Standards specifying the criteria for the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation (EU) 2022/2554; JC 2023-84, 10 januari 2024, 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; JC 2023-85, 10 januari 2024, on 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; JC 2023-86, 10 januari 2024, Draft Regulatory Technical Standards to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554; JC 2024-29, 17 juli 2024, Draft Regulatory Technical Standards specifying elements related to threat led penetration tests under Article 26(11) of Regulation (EU) 2022/2554; JC 2024-33, 17 juli 2024, Draft Regulatory Technical Standards on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents and Draft Implementing Technical Standards on the standard forms, templates and procedures for financial entities to report a major incident and to notify a significant cyber threat; JC 2024-35, 17 juli 2024, Draft Regulatory Technical Standards on harmonisation of conditions enabling the conduct of the oversight activities; JC 2024-54, 17 juli 2024, Draft Regulatory Technical Standard on the harmonisation of conditions enabling the conduct of the oversight activities under Article 41(1)(c) of Regulation (EU) 2022/2554.

76 Zie noot 25, 52 en 57.

 doi: 10.5553/MvV/157457672024034010004

taak is voor de uitvoerende macht.[77] Daar komt bij dat toezichthouders in de praktijk zelf ook lijken te worstelen met de onduidelijkheden.

Met de DORA is een nieuwe stap richting digitale weerbaarheid van financiële instellingen gezet, maar 'the proof of the pudding is in the eating'.

77 Zo heeft de Autoriteit Persoonsgegevens op grond van zogenoemde 'normuitleg' lang het standpunt ingenomen dat een zuiver commercieel belang nooit een gerechtvaardigd belang kan zijn in de zin van art. 6 AVG, zie https://autoriteitpersoonsgegevens.nl/uploads/imported/normuitleg_gerechtvaardigd_belang.pdf. Hier is veel kritiek op geweest, zie bijv. G.J. Zwenne & R. van Eijk, Privacytoezichthouder neemt opmerkelijk afstand van de marktwerking, Het Financieele Dagblad 24 december 2019, W. Heck & P. Olsthoorn, Beschermt de autoriteit persoonsgegevens privacy, of verstoord ze de vrije markt?, NRC Handelblad 3 juli 2022, en in HvJ EU 4 oktober 2024, ECLI:EU:C:2024:857 oordeelde het Hof dat een commercieel belang wel degelijk een gerechtvaardigd belang in de zin van de AVG kan zijn. Een verschil met de technische standaarden die richting moeten geven aan de DORA is dat de wetgever in de tekst van de DORA de ESA's expliciet deze bevoegdheden heeft gegeven.