DORA: meer veiligheid door wisselwerking tussen toezichtrecht en civiel recht

*Mr. K. Christianen**

1 Inleiding

Op 16 januari 2023 is de Digital Operational Resilience Act[1] (of kortweg DORA) in werking getreden, die vanaf 17 januari 2025 van toepassing zal zijn.[2] Formeel bestaat DORA uit een verordening[3] en een richtlijn.[4] De kernregelgeving omtrent digitale operationele weerbaarheid is opgenomen in de verordening. De richtlijn is bedoeld om bestaande toezichtrechtelijke regelgeving te wijzigen en in lijn te brengen met de verordening. Onderwerp van dit artikel is de DORA-verordening. Daar waar dit artikel spreekt over DORA wordt derhalve bedoeld de DORA-verordening.

DORA reguleert de operationele weerbaarheid en cyberbeveiliging in de Europese financiële markt, en stelt onder meer regels voor de governance[5] en het beheer van ICT-risico's. Vanwege de toenemende digitalisering in de financiële sector ontwikkelen zich evenzo toenemende risico's. Beveiliging van ICT-systemen en digitale weerbaarheid zijn onderdeel van het operationele risico van financiële entiteiten. Voorheen ontbrak regelgeving binnen de EU die deze onderwerpen reguleerde vanuit een sectorbrede visie. Dit zorgde voor een gefragmenteerde aanpak die per lidstaat en sector verschillend kon zijn.

Vanaf 17 januari 2025 moeten financiële entiteiten, alsook hun ICT-dienstverleners, dus voldoen aan de vergaande eisen die DORA hun oplegt. DORA hanteert zowel in de Engelstalige als in de Nederlandstalige tekst de term 'financiële entiteiten' als verzamelnaam voor de financiële instellingen die onder de reikwijdte van DORA vallen. Zodoende spreekt ook dit artikel van financiële entiteiten. Verderop in dit artikel wordt nader beschreven op welke specifieke financiële entiteiten de verordening van toepassing zal zijn.

DORA vloeit voort uit het Digital Finance Package[6] van de Europese Commissie. Dit pakket beoogt een competitieve Europese financiële sector waarin consumenten toegang hebben tot innovatieve financiële producten, waarbij de financiële stabiliteit en de rechten van consumenten zijn gewaarborgd. Hierna volgt een uitgebreidere bespreking van de oorsprong en inhoud van dit pakket.

2 Doelstellingen, ontwikkeling en prioriteiten DORA

2.1 Algemeen

Het doel van DORA is het vergroten van de digitale weerbaarheid in de Europese financiële sector. Daarvoor bevat de verordening een breed palet vereisten aan financiële entiteiten met betrekking tot de beveiliging van hun ICT-systemen. Dit betreft eisen op het gebied van ICT-risicobeheer, de rapportage van ICT-incidenten, het testen van ICT-systemen en de beheersing van risico's van ICT-dienstverleners. Deze eisen betreffen niet alleen interne processen, maar zeker ook diensten

* Mr. K. Christianen is Senior Legal Counsel Contracting & IT bij de Coöperatieve Rabobank U.A. te Utrecht.

1 Verordening (EU) 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.

2 Art. 64 DORA. Gelijktijdig dient per 17 januari 2025 de DORA-richtlijn te zijn omgezet.

3 Verordening (EU) 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.

4 Richtlijn (EU) 2022/2556 van het Europees Parlement en de Raad van 14 december 2022 tot wijziging van de Richtlijnen 2009/65/EG, 2009/138/EG, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 en (EU) 2016/2341 wat betreft digitale operationele weerbaarheid voor de financiële sector (hierna: DORA-richtlijn).

5 Het woord 'governance' komt een aantal keer voor in DORA, waaronder als titelaanhef van art. 5 DORA ('Governance en organisatie'), zowel in de Engelstalige als in de Nederlandstalige tekst, zonder dat een duidelijke omschrijving wordt gegeven. Met governance wordt echter veelal een beheersstructuur bedoeld. Zie bijv. Kamerstukken II 2014/15, 33326, nr. 5, p. 214. Een veelgebruikte definitie van ICT-governance is: '[h]et raamwerk van besluitvorming en verantwoordelijkheid in een organisatie of in een geheel van organisaties zoals een keten of community, om het gewenste resultaat met ICT te realiseren'. Zie bijv. Kamerstukken II 2014/15, 33326, nr. 5, p. 65. Deze Kamerstukken zijn te raadplegen via https://zoek.officielebekendmakingen.nl/kst-33326-5.pdf (laatst benaderd op 10 mei 2023).

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

die door leveranciers aan financiële entiteiten worden geleverd.

De vereisten in DORA zien op ICT-risico's in brede zin, dus niet alleen cyberrisico's (zoals hacks en ransomware), maar ook operationele risico's rondom de technische infrastructuur (zoals uitval van elektriciteit, brand en overstroming). Overigens sluit het een het ander niet uit. Steeds vaker doen hackers pogingen om dergelijke infrastructuur aan te vallen en trachten daarmee een samenleving (gedeeltelijk) te ontwrichten.[7]

DORA tracht eveneens de versnippering van bestaande wet- en regelgeving weg te nemen.[8] De bestaande regelgeving met betrekking tot operationele en cyberrisico's geldt maar voor een beperkt aantal typen dienstenaanbieders, zoals kredietinstellingen en betaalinstellingen.[9] Voor andere financiële dienstverleners hebben enkele lidstaten zelf regelgeving opgesteld, maar veelal ontbrak het aan regels, of waren er slechts algemene normen.

Daarnaast introduceert DORA ook rechtstreeks toezicht op leveranciers van ICT-diensten, naast het toezicht op de instellingen zelf.

2.2 De ontwikkeling van digitale weerbaarheid: van FinTech-actieplan naar DORA

Zoals eerder benoemd is DORA ontstaan uit het Digital Finance Package[10] van de Europese Commissie. Dit pakket uit 2020 is weer gebaseerd op het FinTech-actieplan[11] uit 2018 van de Europese Commissie. FinTech betreft technologische innovatie op het gebied van financiële diensten.[12] De financiële sector wordt gezien als de grootste gebruiker van digitale technologieën en als een belangrijke aanjager van de digitale transformatie van de economie en de samenleving.[13] Door nieuwe technologie veranderen de financiële sector en de wijze waarop consumenten en bedrijven toegang krijgen tot diensten. Dit brengt ook uitdagingen mee omtrent cyberrisico's, bescherming van (persoons)gegevens, consumenten en marktintegriteit.[14] Cyberrisico's tasten het vertrouwen aan en bedreigen de stabiliteit van het financiële stelsel. Het FinTech-actieplan beschrijft dat het van het grootste belang is dat de financiële sector weerbaarder wordt tegen cyberaanvallen, ter bescherming van deze sector, en opdat financiële diensten snel en doeltreffend kunnen worden verricht, alsook dat consumenten en markten vertrouwen houden.[15]

In 2017, ten tijde van het FinTech-actieplan, bleek de financiële sector oververtegenwoordigd doelwit van cyberaanvallen.[16] Alhoewel tegenwoordig wereldwijd niet de financiële sector, maar de maakindustrie de meeste cyberaanvallen te verwerken krijgt, vond in 2022 33% van alle cyberaanvallen op de financiele sector in Europa plaats.[17] Reden genoeg voor Europa om allesbehalve achterover te leunen.

Voor wat betreft de digitale transformatie lijkt de financiële sector het inmiddels ook wel beter te doen dan andere industrieën. In een jaarlijks rapport over trends in cybersecurity van het Amerikaanse IT-bedrijf IBM[18] wordt – in het rapport van februari 2023 – namelijk gesteld dat de financiële sector neigt naar meer vooruitgang wat betreft digitale transformatie en cloudadoptie ten opzichte van andere sectoren.[19] In het rapport wordt verondersteld dat cyberaanvallers daardoor mogelijk harder moeten werken om met succes aanvallen tegen instellingen in de financiële sector uit te voeren.[20]

Hopelijk tilt DORA de digitale weerbaarheid naar een nog hoger niveau, opdat de financiële sector in gezamenlijkheid met zijn leveranciers een afdoende bescherming zal bieden tegen ICT-risico's, zoals maar niet beperkt tot cyberaanvallen.

2.3 Doelstelling en prioriteiten van het Europese Digital Finance Package

Het Digital Finance Package beschrijft de digitale toekomst van het geldwezen. Steeds meer consumenten en bedrijven verkrijgen digitale toegang tot financiële diensten (mede versneld als gevolg van de COVID-19-pandemie), nieuwe technologische innovaties worden in de markt aangeboden, en huidige bedrijfsmodellen veranderen.[21] Omdat meer mensen online van financiële diensten gebruikmaken en werknemers van financiële instellingen op afstand werken, is het volgens de Europese Commissie ook belangrijker geworden om zorg te

7 Zie bijv. https://tweakers.net/nieuws/195518/elektriciteitsnet-van-oekraine-aangevallen-door-russische-hackersgroep.html, www.volkskrant.nl/nieuws-achtergrond/microsoft-russische-hackers-vallen-bondgenoten-oekraine-aan-litouwen-voorbereid-op-afsluiting-stroomvoorziening-door-ruzie-met-rusland~be1e1349/ en www.emerce.nl/wire/cyberaanvallen-infrastructuren-groot-risico-wereldwijde-drinkwatervoorziening (laatst benaderd op 7 mei 2023).

8 Europese Commissie 2020; Fiche 4: Verordening digitale operationele weerbaarheid (DORA), www.rijksoverheid.nl/documenten/vergaderstukken/2020/11/01/fiche-4-verordening-digitale-operationele-weerbaarheid-dora.

9 Europese Commissie 2020; Fiche 4: Verordening digitale operationele weerbaarheid (DORA), p. 2.

10 Europese Commissie 2020.

11 Europese Commissie, FinTech-actieplan: voor een meer concurrerende en innovatieve Europese financiële sector, Brussel, 8 maart 2018, COM(2018)109 final.

12 De Financial Stability Board (FSB) definieert FinTech als technologische innovatie op het gebied van financiële diensten die tot nieuwe bedrijfsmodellen, toepassingen, processen of producten kan leiden, en die een wezenlijke invloed kan hebben op financiële markten en instellingen, en op financiële dienstverlening. Zie www.fsb.org/work-of-the-fsb/financial-innovation-and-structural-change/fintech/ (laatst benaderd op 1 mei 2023).

13 Europese Commissie 2018, p. 2.

14 Europese Commissie 2018, p. 3.

15 Europese Commissie 2018, p. 3.

16 Zie de verwijzing in voetnoot 8 van het FinTech-actieplan naar het rapport van IBM uit 2017 over veiligheidstrends in de financiële sector.

17 IBM, X-Force Threat Intelligence Index 2023, februari 2023, p. 44. Dit rapport is online vindbaar via www.ibm.com/downloads/cas/DB4GL8YM (laatst benaderd op 1 mei 2023).

18 IBM is een van de grootste IT-bedrijven ter wereld.

19 IBM 2023, p. 44.

20 IBM 2023, p. 44.

21 Europese Commissie 2020, p. 1.

 doi: 10.5553/MvV/157457672023033006001

dragen voor een veilige en betrouwbare werking van digitale infrastructuur.[22] Daarbij dienen gebruikers van financiële diensten te worden beschermd tegen risico's die samenhangen met het toegenomen gebruik van het digitale geldwezen.[23]

2.4 Doelstelling Digitale Finance Package

De strategische doelstelling van de Europese Commissie voor het digitale geldwezen komt in de kern op het volgende neer: het digitale geldwezen omarmen en digitale innovatie in de financiële sector in de Europese Unie stimuleren, zodat consumenten en bedrijven kunnen profiteren van de voordelen van het digitale geldwezen, waarbij tegelijkertijd de risico's daarvan beperkt moeten worden.[24]

Van de vier prioriteiten van de Europese Commissie zijn de volgende twee relevant in het kader van DORA: (2) digitale innovatie bevorderen middels een aangepast EU-regelgevingskader, en (4) het adresseren van uitdagingen en risico's omtrent digitale transformatie.[25]

Prioriteit 2: digitale innovatie bevorderen middels aangepast EU-regelgevingskader

Innovaties die gebruikmaken van *distributed ledger technology* (DLT)[26] – denk aan cryptoactiva en bijbehorende blockchains – of *artificial intelligence* (AI) kunnen bijdragen aan een verbetering van financiële diensten.[27] Het regelgevingskader dient verantwoord gebruik van dergelijke technologieën mogelijk te maken.[28] Regelmatige toetsing en aanpassing van Europese wetgeving en toezichtpraktijken horen daarbij om digitale innovatie in veranderende marktomstandigheden te kunnen bijbenen.[29]

De EU-strategie benoemt dat het gebruik van cloudcomputinginfrastructuur bevorderd moet worden.[30] Cloudcomputing draagt namelijk bij aan het snel en flexibel opschalen en overschakelen op een modulaire IT-architectuur. Dit bevordert vervolgens samenwerking en sluit het beste aan bij digitale toepassingen die zijn ontworpen voor de cloud. Opdat banken en financiële dienstverleners de vruchten kunnen plukken van clouddiensten, in een 'streng beveiligde klantgerichte omgeving', is inmiddels via DORA een toezichtskader voor cruciale externe aanbieders van IT-diensten ontwikkeld.

Prioriteit 4: adresseren uitdagingen en risico's omtrent digitale transformatie

In het Digital Finance Package wordt aangenomen dat financiele diensten vaker worden aangeboden in versnipperde digitale ecosystemen met daarin onderling verbonden digitaledienstverleners die deels buiten de financiële regelgeving en het financieel toezicht vallen.[31] Voor de bestaande regelgevings- en toezichtskaders kan het volgens de Europese Commissie daardoor moeilijker zijn om belangrijke belangen te borgen, zoals financiële stabiliteit, consumentenbescherming, marktintegriteit, eerlijke concurrentie en beveiliging. Teneinde betere financiële producten voor consumenten en bedrijven voort te brengen uit het digitale geldwezen dienen deze risico's volgens de Europese Commissie te worden aangepakt.[32]

De Europese Commissie stelt dat IT-bedrijven zich vaker bezighouden met het leveren van financiële diensten en technologische oplossingen, zoals hardware-, software- en cloudoplossingen voor de financiële sector.[33] Volgens de Commissie zullen IT-bedrijven daarom naar verwachting een integraal onderdeel worden van het gehele financiële ecosysteem, waardoor ook risico's zullen toenemen. Naast voordelen (zoals gebruiksgemak) signaleert ook De Nederlandsche Bank (DNB) risico's die samenhangen met de opkomst van grote techbedrijven (zoals Apple en Google) in de financiële sector (met bijvoorbeeld Apple Pay of Google Pay).[34]

De Europese Commissie ziet risico's op individueel klantniveau (polishouders, beleggers, depositohouders) alsook risico's met betrekking tot de financiële stabiliteit en concurrentie op financiële markten. In de ogen van de Europese Commissie dienen regelgeving en toezicht daarom evenredig te zijn.[35]

De EU stelt dat zij zich niet kan veroorloven dat er twijfels zouden rijzen omtrent de operationele weerbaarheid en beveiliging van digitale financiële infrastructuur en diensten. Specifiek wordt in de EU-strategie benoemd dat 'ook het risico dat geld van cliënten wordt gestolen of hun gegevens in gevaar worden gebracht, zoveel mogelijk [moet] worden beperkt'.[36]

22 Europese Commissie 2020, p. 1.
23 Europese Commissie 2020, p. 1.
24 Europese Commissie 2020, p. 3.
25 Europese Commissie 2020, p. 4-20.
26 Zie voor een eenvoudige uitleg over DLT www.ecb.europa.eu/ecb/educational/explainers/tell-me-more/html/distributed_ledger_technology.nl.html (laatst benaderd op 29 april 2023).
27 Europese Commissie 2020, p. 10.
28 Uit het Digital Finance Package is niet alleen DORA ontstaan, maar ook een regelgevingskader voor markten in cryptoactiva (MiCA), namelijk: Voorstel voor een verordening van het Europees Parlement en de Raad betreffende markten in cryptoactiva en tot wijziging van Richtlijn (EU) 2019/1937, COM(2020)593 final. Art. 3 lid 1 onder (2) MiCA definieert een cryptoactief, of cryptoasset, als een digitale weergave van waarde of rechten die elektronisch kan worden overgedragen en opgeslagen, met gebruikmaking van DLT of vergelijkbare technologie.
29 Europese Commissie 2020, p. 5.
30 Europese Commissie 2020, p. 11.
31 Europese Commissie 2020, p. 5.
32 Europese Commissie 2020, p. 5.
33 Europese Commissie 2020, p. 17.
34 Zie www.dnb.nl/algemeen-nieuws/nieuwsbericht-2021/opkomst-bigtechs-zorgt-voor-gebruiksgemak-maar-er-zijn-ook-risico-s/ (laatst benaderd op 10 mei 2023) naar aanleiding van het DNB-rapport 'Veranderend landschap, veranderend toezicht. Ontwikkelingen in de relatie tussen BigTechs en financiële instellingen', gepubliceerd op 24 juni 2021 en raadpleegbaar via www.dnb.nl/media/eb5oxjke/veranderend-landschap-veranderend-toezicht.pdf (laatst benaderd op 10 mei 2023).
35 Europese Commissie 2020, p. 17.
36 Europese Commissie 2020, p. 20.

3 DNB: toezicht rondom cyberweerbaarheid speerpunt

DNB meldde begin 2022 dat verzekeraars en pensioenfondsen onvoldoende zicht hebben op het langer worden van de uitbestedingsketens.[37] Later dat jaar meldde DNB dat zij cyberdreigingen ziet toenemen, terwijl de basismaatregelen van instellingen die onder haar toezicht staan niet altijd op orde zijn.[38] Uit haar onderzoek blijkt dat ruim een derde van de instellingen geen inzicht heeft in de uitbestedingsketen.[39] Derhalve ontbreekt volgens DNB een goed beeld van de staat van het onderhoud van kritieke systemen in de keten. Dit terwijl instellingen sterk afhankelijk zijn van maatregelen in de gehele uitbestedingsketen, waaronder monitoring.[40]

DNB concludeert eind 2022 dat 32% van de instellingen (in dit verband: Nederlandse verzekeraars, pensioenfondsen, PUO's en PPI's[41]) gebruikmaakt van een of meer kritieke IT-systemen die niet langer door leveranciers worden voorzien van beveiligingsupdates.[42] Omdat dit percentage in 2021 nog 42% bedroeg, trekt DNB daaruit de voorzichtige conclusie dat instellingen aandacht hebben voor deze verouderde systemen en ze bijvoorbeeld uitfaseren. De praktijk leert dat een migratie naar nieuwe(re) systemen veel tijd kan kosten (soms zelfs meerdere jaren), zeker als het gaat om complexe IT-infrastructuur en software die verweven zijn met andere systemen binnen de instelling.

Voor DNB blijft risicobeheersing op het gebied van informatiebeveiliging, uitbesteding en cybersecurity onverminderd belangrijk voor een beheerste en integere bedrijfsvoering door financiële instellingen.[43] Toezicht rondom cyberweerbaarheid lijkt in 2023 een speerpunt voor DNB, omdat zij in haar toezichtsactiviteiten voor 2023 niet alleen wijst op de beheersing van uitbestedingsrisico's, maar in het bijzonder uitdrukkelijk wijst op haar aandacht voor de implementatie van DORA.[44]

4 Harmonisatie en samenhang met bestaande EU-regelgeving rondom cyberbeveiliging

Naast DORA bestaan meerdere andere regelgevende kaders rondom cybersecurity. Vanwege de harmoniserende aard en het ruime toepassingsbereik van DORA hangt zij met verschillende andere wetgevingskaders samen. Hierna volgen ter illustratie enkele voorbeelden.[45]

4.1 Netwerk- en Informatiebeveiligingsrichtlijn (NIS 2)

De Netwerk- en Informatiebeveiligingsrichtlijn (NIS 1)[46] uit 2016 was het eerste horizontale kader voor EU-cyberbeveiliging dat mede van toepassing is op bepaalde financiële entiteiten.[47] NIS 1 beoogt de totstandbrenging van een hoog gemeenschappelijk niveau van cyberbeveiliging, om zo de werking van de interne markt te verbeteren.[48] Alhoewel door NIS 1 vooruitgang is geboekt bij het vergroten van het niveau van digitale weerbaarheid van de Unie, ontstonden ook wezenlijke implementatieverschillen tussen lidstaten.[49] Dit leidde tot de totstandkoming van de NIS 2-richtlijn,[50] die op 16 januari 2023 in werking is getreden (DORA is diezelfde dag in werking getreden) en uiterlijk op 17 oktober 2024 door lidstaten moet zijn geïmplementeerd. In NIS 2 wordt het toepassingsbereik fors vergroot, worden beveiligingseisen aangescherpt en handhavings- en toezichtsbevoegdheden uitgebreid.[51] DORA is een nadere uitwerking van NIS 2, specifiek voor de financiële sector.[52] In DORA wordt DORA uitdrukkelijk als een *lex specialis* van NIS 2 benoemd.[53] Tegelijkertijd is consistentie tussen DORA en NIS 2 beoogd. De Europese wetgever stelt namelijk dat het cruciaal is om een sterke relatie te handhaven tussen de financiële sector en het in NIS 2 vastgelegde horizontale cybersecuritykader.[54] Doel hiervan is het realiseren van samenhang met de nationale cybersecuritystrategieën en informatie-uitwisseling met financiële toezichthouders omtrent cyberincidenten die gevolgen hebben voor andere sectoren die onder NIS 2 vallen.[55] Daarnaast heeft te gelden dat het in

37 Zie www.dnb.nl/nieuws-voor-de-sector/toezicht-2022/verzekeraars-hebben-onvoldoende-zicht-op-langer-wordende-uitbestedingsketens/ en www.dnb.nl/nieuws-voor-de-sector/toezicht-2022/pensioenfondsen-hebben-onvoldoende-zicht-op-langer-wordende-uitbestedingsketens/ (laatst benaderd op 5 mei 2023).

38 Zie www.dnb.nl/nieuws-voor-de-sector/toezicht-2022/dnb-ziet-cyberdreiging-toenemen-terwijl-basismaatregelen-niet-altijd-op-orde-zijn/ (laatst benaderd op 5 mei 2023).

39 Zie www.dnb.nl/nieuws-voor-de-sector/toezicht-2022/dnb-ziet-cyberdreiging-toenemen-terwijl-basismaatregelen-niet-altijd-op-orde-zijn/ (laatst benaderd op 5 mei 2023).

40 Zie www.dnb.nl/nieuws-voor-de-sector/toezicht-2022/dnb-ziet-cyberdreiging-toenemen-terwijl-basismaatregelen-niet-altijd-op-orde-zijn/ (laatst benaderd op 5 mei 2023).

41 PUO is de afkorting van pensioenuitvoeringsorganisatie; PPI is de afkorting van premiepensioeninstelling.

42 Zie www.dnb.nl/nieuws-voor-de-sector/toezicht-2022/dnb-ziet-cyberdreiging-toenemen-terwijl-basismaatregelen-niet-altijd-op-orde-zijn/ (laatst benaderd op 5 mei 2023).

43 Middels de Wft houdt DNB hierop reeds toezicht.

44 Zie de DNB Benchmarkrapportage informatiebeveiliging 2022 d.d. 18 april 2023, p. 11.

45 Zie voor een meer omvattende opsomming van Europese en nationale regelingen op het gebied van (ICT-)risicobeheer 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.

46 Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie.

47 Overweging 15 DORA. Het betreft de volgende financiële entiteiten waarop NIS van toepassing is: kredietinstellingen, handelsplatformen en centrale tegenpartijen.

48 Art. 1 lid 1 NIS 1.

49 Overweging 2 en 4 NIS 2.

50 Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gemeenschappelijk 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).

51 N. Brouwer & J. van Mil, Cybersecurity in Europa. De herziene Netwerk- en Informatiebeveiligingsrichtlijn (NIS 2), NJB 2023, afl. 10, p. 752-755.

52 Brouwer & Van Mil 2023, p. 757.

53 Overweging 16 DORA.

54 Overweging 16 DORA.

55 Overweging 16 DORA.

 doi: 10.5553/MvV/157457672023033006001

DORA vastgelegde oversightkader voor kritieke[56] aanbieders van ICT-diensten (waaronder cloudproviders[57]) complementair is aan het toezicht op cloudproviders onder NIS 2.[58]

4.2 Richtlijn weerbaarheid kritieke entiteiten

Gelijktijdig met NIS 2 en DORA is op 27 december 2022 ook de 'richtlijn weerbaarheid kritieke entiteiten'[59] gepubliceerd. Deze richtlijn is van toepassing op entiteiten uit diverse sectoren (zoals energie, vervoer, gezondheid en drinkwater) die van cruciaal belang zijn voor vitale maatschappelijke functies en economische activiteiten. Dergelijke kritieke entiteiten moeten risico's in kaart brengen die de levering van essentiële diensten aanzienlijk kunnen verstoren. Tevens moeten deze entiteiten passende maatregelen nemen om hun weerbaarheid te waarborgen en verstorende incidenten melden aan de bevoegde autoriteiten.

DORA gaat in op de sterke verwevenheid tussen de digitale en fysieke weerbaarheid van financiële entiteiten. Vanwege deze verwevenheid is volgens de Europese wetgever een coherente aanpak nodig met betrekking tot de weerbaarheid van kritieke entiteiten.[60] Omdat de fysieke weerbaarheid van financiële entiteiten breed wordt aangepakt in de in DORA genoemde verplichtingen inzake ICT-risicobeheer en -rapportage, mogen de in hoofdstuk 3 en 4 van de richtlijn weerbaarheid kritieke entiteiten vastgelegde verplichtingen niet van toepassing zijn op financiële entiteiten die onder het toepassingsbereik van deze richtlijn vallen.[61]

4.3 Payment Services Directive (PSD 2)

Ter vermindering van administratieve lasten en mogelijk overlappende rapportageverplichtingen voor financiële entiteiten mag de verplichting tot het melden van incidenten op grond van de bestaande PSD 2-richtlijn niet langer van toepassing zijn op betaaldienstaanbieders die onder het toepassingsbereik van DORA vallen.[62] Zodoende moeten kredietinstellingen, instellingen voor elektronisch geld, betalingsinstellingen en aanbieders van rekeninginformatiediensten (zoals bedoeld in art. 33 lid 1 van de PSD 2-richtlijn) vanaf de datum van inwerkingtreding van DORA krachtens DORA alle betalingsgerelateerde operationele of beveiligingsincidenten melden die eerder op grond van de PSD 2-richtlijn werden gemeld, ongeacht of dergelijke incidenten ICT-gerelateerd zijn.[63]

4.4 EBA Guidelines on outsourcing arrangements

In DORA wordt verwezen naar bestaande richtsnoeren inzake uitbesteding, zoals de EBA-richtsnoeren inzake uitbesteding van 2019 en de ESMA-richtsnoeren over uitbesteding aan aanbieders van clouddiensten van 2021.[64] Daarbij wordt in de overwegingen gesteld dat ondanks inspanningen middels dergelijke richtsnoeren de bestrijding van systeemrisico's door blootstelling van de financiële sector aan een beperkt aantal kritieke derde aanbieders van ICT-diensten onvoldoende aan de orde komt.[65] Dit wordt verergerd door ontbrekende mandaten en instrumenten in nationale regelgeving voor toezichthouders ten behoeve van inzicht in afhankelijkheden (van ICT-leveranciers) en concentratierisico's.[66] Derhalve is in DORA een oversightkader voor kritieke ICT-leveranciers opgenomen.[67]

4.5 Cyber Resilience Act (CRA)

Daarnaast is er in september 2022 ook een Europees wetsvoorstel gepresenteerd voor een nieuwe verordening met betrekking tot cyberbeveiligingsvereisten voor producten met digitale elementen (Cyber Resilience Act, of kortweg CRA).[68] Momenteel bestaat er namelijk nog geen Europese wetgeving met een verplichting voor fabrikanten of producenten om digitale producten te beveiligen.[69] De CRA bevat cyberbeveiligingsbepalingen voor fabrikanten, importeurs en distributeurs van producten met digitale elementen.[70] In relatie tot DORA kan worden gesteld dat de CRA gericht is op IT-producten (met digitale elementen), en dat DORA gericht is op IT-diensten (binnen de financiële sector).

5 Inhoud DORA

5.1 Toepassingsgebied DORA

DORA geldt kort gezegd voor vrijwel de gehele financiële markt en haar leveranciers. Het toepassingsgebied omvat de in

56 Zie art. 3 sub 23 DORA, waarin 'kritieke derde aanbieder van ICT-diensten' is gedefinieerd als een derde aanbieder van ICT-diensten die overeenkomstig art. 31 DORA is aangewezen als cruciaal.
57 DORA en NIS 2 spreken over 'aanbieders van cloudcomputingdiensten', in de praktijk doorgaans cloudproviders genoemd.
58 Overweging 20 DORA.
59 Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten en tot intrekking van Richtlijn 2008/114/EG van de Raad.
60 Overweging 19 DORA.
61 Overweging 19 DORA.
62 Overweging 23 DORA.
63 Overweging 23 DORA.
64 Overweging 30 DORA.
65 Overweging 30 DORA.
66 Overweging 30 DORA.
67 Overweging 31 DORA.
68 Voorstel voor een verordening van het Europees Parlement en de Raad betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordening (EU) 2019/1020, COM(2022)454 final.
69 N. Brouwer & M. Reijneveld, De ontwikkeling van cyberveiligheid in Europa. Voorstel voor de Cyber Resilience Act, NJB 2023, afl. 10, p. 758.
70 Voorstel voor een verordening van het Europees Parlement en de Raad betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordening (EU) 2019/1020, COM(2022)454 final, p. 11-12.

art. 2 benoemde 'financiële entiteiten',[71] zoals onder meer banken, betaalinstellingen en verzekeraars. Bepaalde kleinere financiële entiteiten zijn uitgezonderd.[72] Daarnaast is de verordening ook rechtstreeks van toepassing op zogenaamde 'derde aanbieders van ICT-diensten',[73] zijnde ondernemingen die ICT-diensten verlenen aan de financiële entiteiten. In de wereld van ICT-/IT- en outsourcingscontracten worden dergelijke ondernemingen doorgaans (ICT-/IT-)leveranciers genoemd, hierna kortweg leveranciers.[74]

Dat onder de reikwijdte van DORA dus tevens leveranciers vallen, heeft meerdere consequenties. Ten eerste moeten overeenkomsten tussen financiële entiteiten en leveranciers voldoen aan de vereisten die daarvoor gelden in DORA. Ten tweede komen kritieke leveranciers onder rechtstreeks toezicht te staan. Hierover later meer.

Een leverancier van ICT-diensten kan als kritieke leverancier worden aangewezen vanwege de relevantie van zijn diensten voor de financiële sector.[75] Deze kritieke leveranciers komen onder rechtstreeks toezicht[76] van een van de volgende Europese toezichthoudende autoriteiten (ESA's):[77] de Europese Bankautoriteit (EBA), de Europese Autoriteit voor Verzekeringen en Bedrijfspensioenen (EIOPA) of de Europese Autoriteit voor effecten en markten (ESMA).[78]

Sinds de kredietcrisis zijn door deze ESA's al richtsnoeren ontwikkeld om de markt financieel weerbaar te maken tegen bepaalde operationele risico's, zoals ICT-risico's en uitbestedingsrisico's. Zo hebben met betrekking tot ICT-risico's banken reeds de EBA-richtsnoeren inzake ICT en risicobeheer op het gebied van veiligheid[79] en verzekeraars de EIOPA-richtsnoeren betreffende beveiliging en governance van informatie- en communicatietechnologie.[80] En met betrekking tot uitbesteding hebben banken reeds de EBA-richtsnoeren inzake uitbesteding,[81] verzekeraars de EIOPA-richtsnoeren voor uitbesteding aan aanbieders van clouddiensten[82] en effecteninstellingen de ESMA-richtsnoeren inzake uitbesteding aan aanbieders van clouddiensten.[83]

DORA zorgt voor codificatie, harmonisatie en uniformering van verschillende regels rondom de beheersing van ICT-risico's binnen de financiële sector.[84] Alhoewel de bestaande richtsnoeren inzake uitbesteding naar verwachting naast DORA zullen blijven bestaan vanwege de afwijkende reikwijdte,[85] zullen de bestaande aanbevelingen van Europese en/of nationale toezichthouders mogelijk worden aangepast, alhoewel dat nog onduidelijk is.[86]

Zelfs als bestaande ICT-contracten (met een uitbestedingscomponent) recentelijk nog zijn aangepast conform de uitbestedingsregels van toezichthouders, en momenteel daarmee compliant zijn, dienen deze contracten aangepast te worden aan de verplichtingen die DORA aan ICT-contracten stelt (zie tevens hierna).[87]

71 DORA is van toepassing op de volgende in art. 2 DORA genoemde entiteiten, die op grond van art. 2 lid 2 DORA gezamenlijk als 'financiële entiteiten' worden aangeduid: kredietinstellingen (sub a), betaalinstellingen, met inbegrip van bij Richtlijn (EU) 2015/2366 vrijgestelde betaalinstellingen (sub b), aanbieders van rekeninginformatiediensten (sub c), instellingen voor elektronisch geld, met inbegrip van krachtens Richtlijn 2009/110/EG vrijgestelde instellingen voor elektronisch geld (sub d), beleggingsondernemingen (sub e), aanbieders van cryptoactivadiensten met een vergunning op grond van de Verordening van het Europees Parlement en de Raad betreffende markten in cryptoactiva en tot wijziging van Verordeningen (EU) nr. 1093/2010 en (EU) nr. 1095/2010 en Richtlijnen 2013/36/EU en (EU) 2019/1937 ('de verordening betreffende markten in cryptoactiva') en emittenten van *asset-referenced tokens* (sub f), centrale effectenbewaarinstellingen (sub g), centrale tegenpartijen (sub h), handelsplatformen (sub i), transactieregisters (sub j), beheerders van alternatieve beleggingsinstellingen (sub k), beheermaatschappijen (sub l), aanbieders van datarapporteringsdiensten (sub m), verzekerings- en herverzekeringsondernemingen (sub n), verzekeringstussenpersonen, herverzekeringstussenpersonen en nevenverzekeringstussenpersonen (sub o), instellingen voor bedrijfspensioenvoorziening (sub p), ratingbureaus (sub q), beheerders van kritieke benchmarks (sub r), aanbieders van crowdfundingdiensten (sub s) en securitisatieregisters (sub t).

72 Art. 2 lid 3 DORA.

73 Art. 2 lid 1 sub u en art. 3 sub 19 DORA.

74 Alhoewel de terminologie van ICT (informatie- en communicatietechnologie) en IT (informatietechnologie) verschilt, worden deze termen steeds vaker als synoniem door elkaar gebruikt. De term IT is naar de mening van de auteur een bredere, overkoepelende term voor hardware, software, randapparatuur en netwerken. De term ICT verwijst eerder naar het specifieke domein van digitale apparatuur of diensten rondom communicatie. In die zin kan ICT als onderdeel van IT worden gezien. Aangezien DORA consequent spreekt over ICT zal dit artikel daarbij aansluiten, ondanks de voorkeur van de auteur om te spreken over IT.

75 DORA spreekt over 'kritieke derde aanbieder van ICT-diensten' (art. 3 sub 23), hetgeen een leverancier van ICT-diensten betreft die is aangewezen als 'cruciaal' (art. 31).

76 Zie art. 33 DORA.

77 In de Nederlandstalige tekst van DORA (zie overweging 7) wordt de afkorting ETA's gehanteerd voor Europese toezichthoudende autoriteiten. In de praktijk wordt echter vaak ook in Nederlandstalige teksten de Engelstalige afkorting ESA's gebruikt als aanduiding voor European Supervisory Authorities, zoals gehanteerd in de Engelstalige tekst van DORA (logischerwijs eveneens in overweging 7).

78 Zie afdeling II DORA met betrekking tot het oversightkader voor kritieke derde aanbieders van ICT-diensten. Art. 31 DORA beschrijft de wijze waarop een ESA als 'lead overseer' voor de betreffende kritieke derde aanbieder wordt aangesteld.

79 EBA/GL/2019/04.

80 EIOPA-BoS-20/600.

81 EBA/GL/2019/02.

82 EIOPA-BoS-20-002.

83 ESMA50-164-4285.

84 S. Uiterwijk & J.V. Willems, DORA – een Europees kader voor de beheersing van ICT-risico's binnen de financiële sector, Bb 2023/10.

85 P.M. van Vliet, DORA en outsourcing – een vergelijking tussen DORA en de EBA/EIOPA Guidelines, FR 2023, afl. 5, p. 198; Uiterwijk en Willems 2023.

86 Van Vliet 2023, p. 198.

87 Zie in dit kader ook W.A.K. Rank, DORA: veiligheid door veerkracht?, Financial Investigator 2023, afl. 3, p. 67.

 doi: 10.5553/MvV/157457672023033006001

Uitbesteden versus DORA

Een wezenlijk verschil tussen DORA en bestaande regelgeving rondom digitale weerbaarheid is het feit dat DORA zich in de verhouding tussen financiële entiteiten en leveranciers niet beperkt tot uitbesteding van diensten, maar álle ICT-diensten omvat die leveranciers aan financiële entiteiten leveren. DORA is evenwel complementair aan de bestaande uitbestedingsvoorschriften zoals neergelegd in sectorale wet- en regelgeving, waardoor financiële ondernemingen zowel aan DORA als aan de uitbestedingsvoorschriften moeten voldoen.[88] Dit betekent dat nadrukkelijke zorgvuldigheid is vereist bij het contracteren van leveranciers van ICT-diensten. Niet alleen moet worden beoordeeld of sprake is van uitbesteding, en of DORA toepasselijk is, maar ook welke specifieke contractuele verplichtingen moeten worden opgenomen in het desbetreffende ICT-contract. Zowel bij het juridische uitbestedingskader als bij DORA moet namelijk ook worden beoordeeld of sprake is van kritieke of belangrijke functies dan wel van 'reguliere' functies die door de ICT-dienst worden ondersteund. In het geval van kritieke of belangrijke functies moeten aanmerkelijk zwaardere verplichtingen voor leveranciers in het ICT-contract worden opgenomen. Ondanks het feit dat grotere leveranciers over het algemeen wel bekend zijn met op financiële instellingen toepasselijke wet- en regelgeving (zoals de EBA-richtsnoeren inzake uitbesteding), staan deze leveranciers vanwege de vergaande verplichtingen (zoals bijvoorbeeld onbeperkte auditrechten)[89] doorgaans niet te springen om daaraan contractueel gebonden te worden.

De kern van het bestaande juridische kader voor uitbesteding door financiële ondernemingen is opgenomen in art. 3:18 en 4:16 Wet op het financieel toezicht (Wft).[90] In art. 1:1 Wft is 'uitbesteden' gedefinieerd als:

> 'het door een financiële onderneming verlenen van een opdracht aan een derde tot het ten behoeve van die financiële onderneming verrichten van werkzaamheden: (a) die deel uitmaken van of voortvloeien uit het uitoefenen van haar bedrijf of het verlenen van financiële diensten; of (b) die deel uitmaken van de wezenlijke bedrijfsprocessen ter ondersteuning daarvan'.

Kort gezegd betekent dit dat het moet gaan om een dienst die oorspronkelijk door de financiële onderneming zelf zou worden uitgevoerd.[91] Zelfs als de financiële onderneming de dienst nooit eerder heeft uitgevoerd en vanaf het begin een derde heeft ingeschakeld.[92] Voorbeelden van uitbesteding zijn clouddiensten, de ontwikkeling van software, of vermogensbeheer.[93]

In art. 3 sub 21 DORA is 'ICT-diensten' 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'.

Deze definitie van ICT-diensten moet breed worden opgevat.[94] Onder deze definitie vallen in ieder geval over-the-top-diensten, die onder de categorie elektronische-communicatiediensten vallen.[95] Het gaat hierbij om diensten die via internet worden aangeboden zonder dat deze verbonden zijn met een specifieke telecom- of internetprovider.[96] Hierbij kan worden gedacht aan bijvoorbeeld clouddiensten (Amazon Web Services, Microsoft Azure, Google Cloud) en online communicatietools (Microsoft Teams, Zoom). Uitsluitend een beperkte categorie analoge telefoondiensten is uitgezonderd.[97]

Het feit dat DORA een ruimer toepassingsbereik heeft dan de bestaande uitbestedingsregels wordt ook specifiek in de overwegingen van DORA benoemd, waarin is beschreven dat DORA in aanvulling op de bestaande voorschriften voor uitbesteding geldt.[98] Vanwege het afwijkende toepassingsbereik en de afwijkende definities in DORA respectievelijk het juridische uitbestedingskader (zoals de EBA-richtsnoeren inzake uitbesteding) zal bij het inschakelen van een derde de financiële onderneming zowel moeten beoordelen of sprake is van een ICT-dienst alsook of de ICT-dienst kwalificeert als uitbesteding. Voor beide situaties gelden afzonderlijke regimes met betrekking tot de verplichtingen die in de onderliggende overeenkomsten moeten worden opgenomen. Zoals hiervoor reeds aangestipt, is daarbij ook de kwalificatie als kritieke of belangrijke functies relevant. Dit moet per situatie worden beoordeeld, omdat de definities van kritieke of belangrijke functies in de richtsnoeren alsook in DORA van elkaar verschillen.[99] Alhoewel niet geheel duidelijk is hoe de verschillende definities ten opzichte van elkaar moeten worden uitgelegd, zou vanwege de brede reikwijdte van DORA (die breder toepasselijk is dan de richtsnoeren inzake uitbesteding) de DORA-definitie als uitgangspunt kunnen dienen omwille van de eenduidigheid in kernbegrippen, zoals kritieke of belangrijke functies.

Daarnaast bestaan er ook verschillen tussen DORA en het uitbestedingskader met betrekking tot eisen aan de inhoud van de overeenkomst tussen de financiële entiteit en de leverancier. Zo stelt DORA een aantal verplichtingen aan elke ICT-dienst-

88 Overweging 29 DORA.
89 Zie bijv. par. 13.3 van de EBA-richtsnoeren inzake uitbesteding, maar ook art. 30 lid 3 sub e onder i DORA.
90 Van Vliet 2023, p. 191.
91 Van Vliet 2023, p. 193.
92 Van Vliet 2023, p. 193.
93 Van Vliet 2023, p. 193.
94 Overweging 35 DORA.
95 Overweging 35 DORA.
96 Van Vliet 2023, p. 193.
97 Overweging 35 DORA.
98 Overweging 29 DORA.
99 Van Vliet 2023, par. 3.

overeenkomst (of kortweg: ICT-contract), die momenteel in beginsel alleen gelden bij uitbesteding van kritieke of belangrijke functies.[100] Dit betekent dat financiële entiteiten de bestaande overeenkomsten met leveranciers opnieuw tegen het licht zullen moeten houden om te beoordelen of deze op grond van DORA aangepast moeten worden, zelfs als deze recentelijk nog zijn aangepast aan de uitbestedingsrichtsnoeren.

5.2 Governance en ICT-risicobeheer

DORA ziet op governance en beheer van ICT-risico's en hanteert daarvan een ruime definitie.[101] Kort gezegd is een ICT-risico elke omstandigheid omtrent het gebruik van ICT-systemen die de beveiliging van het ICT-systeem, processen of diensten in gevaar kan brengen. Het grote belang van governance en beheer van deze risico's wordt bovendien onderstreept doordat DORA de eindverantwoordelijkheid daarvan uitdrukkelijk bij het leidinggevend orgaan (in Nederland in beginsel: bestuur en raad van commissarissen[102]) van de financiële entiteit legt. Het praktische gevolg daarvan is dat het bestuur primair verantwoordelijk is voor naleving van de verplichtingen in DORA, en dat de raad van commissarissen daarop toezicht houdt.[103] Deze verantwoordelijkheid omvat onder meer de eindverantwoordelijkheid voor het beheer van ICT-risico's, de vaststelling van duidelijke taken en verantwoordelijkheden voor alle ICT-gerelateerde functies, alsook het bepalen van het passende risicotolerantieniveau voor het ICT-risico (ook wel *risk appetite* genoemd).[104] In juridische zin kan deze verantwoordelijkheid mogelijk met zich meebrengen dat niet-naleving van de verplichtingen die voortvloeien uit DORA eventuele consequenties met zich mee zou kunnen brengen in het kader van bestuurdersaansprakelijkheid,[105] of bijvoorbeeld maatregelen van toezichthouders zou kunnen opleveren.

In de huidige praktijk worden de dagelijkse werkzaamheden rondom ICT-governance veelal toegewezen aan de bestuurder die daarvoor doorgaans intern verantwoordelijk is – zoals de chief technology officer (CTO) of de chief innovation and technology officer (CITO). Met de inwerkingtreding van DORA draagt echter het gehele leidinggevend orgaan van de financiële entiteit de verantwoordelijkheid voor ICT-governance. Vanzelfsprekend zijn daarvoor kennis en vaardigheden met betrekking tot ICT-risico's nodig. Zodoende verplicht DORA alle leden van het leidinggevend orgaan om actief voldoende kennis en vaardigheden te onderhouden (onder meer door het verplicht regelmatig volgen van specifieke opleidingen),[106] zodat zij in staat zijn om ICT-risico's en de gevolgen daarvan voor de financiële entiteit te begrijpen en te beoordelen.[107]

5.3 ICT-incidenten

Hoofdstuk 3 van DORA ziet op het beheer, de classificatie en de rapportage van ICT-gerelateerde incidenten. Een ICT-incident is kort gezegd een gebeurtenis die de beveiliging van een ICT-systeem in gevaar brengt en een nadelig effect heeft op de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van gegevens of diensten.[108]

Financiële entiteiten moeten ICT-incidenten detecteren, beheren en melden.[109] Zij moeten deze ICT-incidenten alsook cyberdreigingen registreren en classificeren.[110] Deze vaststelling is nodig vanwege de meldplicht die geldt voor ernstige ICT-incidenten. Overigens gelden voor bepaalde ICT-incidenten al meldplichten op grond van andere wetgeving. De meldplicht in DORA geldt niet voor significante cyberdreigingen, waarvoor een vrijwillig meldingsregime geldt. Een significante cyberdreiging wordt beschreven als een cyberdreiging[111] (in de zin van de 'Cyberbeveiligingsverordening'[112])[113] waarvan de technische kenmerken erop wijzen dat zij kan leiden tot een ernstig ICT-incident of een ernstig betalingsgerelateerd operationeel of beveiligingsincident.

Een ICT-incident kwalificeert als 'ernstig' als het grote nadelige gevolgen heeft voor de ICT-systemen die kritieke of belangrijke functies van de financiële entiteit ondersteunen.[114] Melding en rapportage van ernstige ICT-incidenten vinden plaats aan de voor die entiteit bevoegde toezichthouder.[115] Financiële entiteiten moeten bij een ernstig ICT-incident ook hun cliënten onverwijld informeren, indien dit gevolgen voor de financiële belangen van deze cliënten heeft.[116]

100 Van Vliet 2023, p. 195.
101 Zie art. 3 sub 5 DORA: 'ICT-risico: elke redelijkerwijs aan te wijzen omstandigheid met betrekking tot het gebruik van netwerk- en informatiesystemen die, indien zij zich voordoet, de beveiliging van het netwerk- en informatiesysteem, van technologieafhankelijke instrumenten of processen, van verrichtingen en processen, of van de levering van de diensten in gevaar kan brengen, door schadelijke effecten met zich mee te brengen in de digitale of fysieke omgeving'.
102 T.W.G. de Wit & G. Verschuuren, ICT-risicobeheer met DORA, FR 2023, afl. 5, p. 163.
103 De Wit & Verschuuren 2023, p. 163.
104 Art. 5 lid 2 DORA; De Wit & Verschuuren 2023, p. 163.
105 T.W.J. Hoeben & T.W. Beenen, DORA's intragroep aspecten, FR 2023, afl. 5, p. 187.
106 Zie art. 5 lid 4 DORA, waarin dit uitdrukkelijk wordt benoemd.
107 Art. 5 lid 4 DORA.
108 Zie art. 3 sub 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'.
109 Art. 17 DORA.
110 Art. 17 en 18 DORA.
111 Cyberdreiging is in art. 2 sub 8 Cyberbeveiligingsverordening gedefinieerd als: 'elke potentiële omstandigheid, gebeurtenis of actie die netwerk- en informatiesystemen, de gebruikers van dergelijke systemen en andere personen kan schaden, verstoren of op andere wijze negatief kan beïnvloeden'.
112 Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening).
113 Art. 3 sub 12 DORA en art. 2 sub 8 Cyberbeveiligingsverordening.
114 Art. 3 sub 10 DORA.
115 Art. 19 en 46 DORA.
116 Art. 19 lid 3 DORA.

 doi: 10.5553/MvV/157457672023033006001

De rapportageverplichting in DORA is bedoeld om de rapportage van ICT-incidenten te harmoniseren en om te voorkomen dat dergelijke incidenten door een financiële entiteit bij meerdere toezichthouders moeten worden gemeld.[117]

Alhoewel harmonisatie van meldplichten en rapportageverplichtingen is beoogd, vervangt DORA niet de bestaande verplichtingen daaromtrent uit de Wft of de Algemene verordening gegevensbescherming (AVG).[118] Dit betekent in de praktijk dat het mogelijk is dat een ICT-incident bij verschillende toezichthouders moet worden gemeld, afhankelijk van de aard van het incident.

Indien sprake is van een significante cyberdreiging moet een financiële entiteit haar cliënten in kennis stellen van passende beschermingsmaatregelen die zij kunnen nemen.[119]

5.4 Testen operationele weerbaarheid

DORA wijdt hoofdstuk 4 aan het testen van digitale operationele weerbaarheid. Het testprogramma van een financiële entiteit moet een risicogebaseerde benadering hanteren, en rekening houden met het veranderende landschap van het ICT-risico, specifieke blootstellingsrisico's en de kritieke aard van verleende diensten.[120] Het uitvoeren van passende tests dient minstens eenmaal per jaar plaats te vinden op alle ICT-systemen die kritieke of belangrijke functies ondersteunen.[121] DORA noemt daarbij verschillende voorbeelden van passende tests, zoals penetratietests, netwerkbeveiligingsbeoordelingen en scanningsoftwareoplossingen. Door de bevoegde autoriteiten nog te bepalen grotere financiële entiteiten moeten zelfs om de drie jaar dreigingsgestuurde penetratietests (*thread led penetration testing* – TLPT) uitvoeren op ICT-systemen die kritieke of belangrijke functies van een financiële entiteit ondersteunen.[122] Aan dergelijke TLPT-tests moeten leveranciers verplicht meewerken, voor zover het ICT-diensten betreft die kritieke of belangrijke functies ondersteunen.[123]

5.5 Beheer van risico's van aanbieders van ICT-diensten

DORA vestigt nadrukkelijk aandacht op het beheer van risico's die samenhangen met het gebruik van ICT-diensten van leveranciers. ICT-diensten is zodoende een belangrijk begrip in DORA. Kort gezegd zijn ICT-diensten alle digitale en gegevensdiensten die doorlopend via ICT-systemen worden verleend.[124] Alleen traditionele analoge telefoondiensten zijn daarbij uitgezonderd.

DORA strekt zich in haar toepassingsbereik daarmee uitdrukkelijk verder uit dan ICT-diensten die als uitbesteding kwalificeren (zie tevens hiervoor).

5.6 Implicaties voor overeenkomsten

Feitelijk vallen daardoor alle doorlopend geleverde ICT-diensten onder DORA, en daarmee praktisch ook alle bijbehorende ICT-contracten. Art. 30 DORA omvat een lange lijst met vereisten die worden gesteld aan dergelijke contracten. Daarbij bestaat een onderscheid tussen diensten die de kritieke of belangrijke functies (hierna: KOB-functies) van financiële entiteiten ondersteunen, en diensten die overige functies (reguliere functies) ondersteunen. Een kritieke of belangrijke functie houdt in DORA kort gezegd in een functie die bij verstoring materiële impact heeft op de financiële prestaties, continuïteit en compliance van de financiële entiteit.[125] De kwalificatie van kritieke of belangrijke functie dient door de financiële entiteit zelf vooraf te worden vastgesteld op basis van de definitie en omschrijving daarvan in DORA, hetgeen niet altijd eenvoudig is.

Er geldt een standaardset verplichtingen voor álle overeenkomsten inzake het gebruik van ICT-diensten (dus voor reguliere én KOB-functies).[126] Voor contracten met betrekking tot ICT-diensten die KOB-functies ondersteunen (hierna: KOB-contracten), komt daarbovenop een extra set verplichtingen.[127]

Ongeacht of de ICT-diensten van een leverancier KOB-functies van de financiële entiteit ondersteunen, in alle gevallen moeten de ICT-contracten tussen leverancier en financiële entiteit verschillende relevante bepalingen bevatten. Hieronder vallen met name de volledige beschrijvingen van functies en diensten, van de locaties waar dergelijke functies worden geleverd en waar data worden verwerkt, alsook een indicatie van de beschrijvingen van het dienstverleningsniveau.[128] Andere essentiële elementen om monitoring door de financiële entiteit van het ICT-risico van leveranciers mogelijk te maken, zijn contractuele bepalingen waarin wordt gespecificeerd hoe leveranciers de toegankelijkheid, beschikbaarheid, integriteit, beveiliging en bescherming van persoonsgegevens verzekeren, en bepalingen voor de vaststelling van de relevante garanties inzake de toegang, het herstel en de teruggave in geval van insolventie, afwikkeling of stopzetting van de bedrijfsactiviteiten van de leverancier.[129] Ook van belang zijn contractuele bepalingen waarin van de leverancier wordt verlangd dat deze ondersteuning biedt bij ICT-incidenten in verband met de verleende diensten, en wel zonder extra kosten of tegen kosten die voorafgaand zijn afgesproken, alsmede contractuele bepalin-

117 Art. 20 DORA; Uiterwijk & Willems 2023, p. 4.
118 Uiterwijk & Willems 2023, p. 4.
119 Art. 19 lid 3 DORA.
120 Art. 24 DORA.
121 Art. 24 lid 6 DORA.
122 Art. 26 DORA.
123 Art. 30 lid 3 sub d DORA.
124 Art. 3 sub 21 DORA.
125 Zie art. 3 sub 22 DORA: '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'.
126 Art. 30 lid 2 DORA.
127 Art. 30 lid 3 DORA.
128 Art. 30 lid 2 DORA.
129 Art. 30 lid 2 DORA.

gen waarin de leverancier wordt verplicht volledig samen te werken met de bevoegde autoriteiten en de afwikkelingsautoriteiten van de financiële entiteit, en bepalingen omtrent beëindigingsrechten en de bijbehorende minimumopzegtermijnen voor de beëindiging van de ICT-contracten, in overeenstemming met de verwachtingen van de bevoegde autoriteiten en de afwikkelingsautoriteiten.[130]

Verplichtingen voor overeenkomsten inzake ICT-diensten die KOB-functies ondersteunen[131]

In aanvulling op dergelijke contractuele bepalingen, en om ervoor te zorgen dat financiële entiteiten volledige controle behouden over alle ontwikkelingen op het niveau van leveranciers die hun ICT-beveiliging negatief kunnen beïnvloeden, moeten de KOB-contracten ook voorzien in het volgende:

- specificatie van de volledige beschrijvingen van het dienstenniveau, inclusief precieze kwantitatieve en kwalitatieve prestatiedoelstellingen, opdat zonder onnodige vertraging corrigerende maatregelen kunnen worden getroffen indien de overeengekomen dienstenniveaus niet gehaald worden;
- de relevante kennisgevingsperioden en rapportageverplichtingen van de leverancier in geval van ontwikkelingen met een potentiële materiële impact op het vermogen van de leverancier om zijn respectieve ICT-diensten daadwerkelijk te leveren;
- een verplichting voor de leverancier om bedrijfsnoodplannen uit te voeren en te testen en te beschikken over ICT-beveiligingsmaatregelen, -instrumenten en -beleidsmaatregelen die een veilige dienstverlening mogelijk maken, en om deel te nemen en volledig mee te werken aan de TLPT die uitgevoerd wordt door de financiële entiteit.[132]

KOB-contracten moeten tevens bepalingen bevatten inzake rechten van toegang, inspectie en audit door de financiële entiteit of een aangewezen derde, alsook het recht om kopieën te maken.[133] Dit zijn essentiële instrumenten voor de permanente monitoring door de financiële entiteit van de prestaties van de leverancier, evenals de volledige medewerking van de dienstverlener tijdens inspecties. Tevens moet de autoriteit van de financiële entiteit het recht hebben om (na kennisgeving) de leverancier te inspecteren en te auditen, onder het voorbehoud van de bescherming van vertrouwelijke informatie.[134]

Dergelijke contracten moeten ook voorzien in specifieke exitstrategieën die met name verplichte overgangsperioden mogelijk maken waarin de leverancier de relevante diensten moet blijven verrichten om zo het risico op verstoringen bij de financiële entiteit te beperken, dan wel de financiële entiteit in staat te stellen daadwerkelijk over te stappen naar andere leveranciers, of anders over te gaan op alternatieve interne oplossingen, een en ander in overeenstemming met de complexiteit van de verleende ICT-dienst.[135] Daarnaast moeten financiële entiteiten die binnen het toepassingsgebied van Richtlijn 2014/59/EU vallen, ervoor zorgen dat de relevante ICT-contracten degelijk en volledig afdwingbaar zijn in geval van afwikkeling van die financiële entiteiten.[136] Daarom moeten die financiële entiteiten erop toezien dat, in overeenstemming met de verwachtingen van de afwikkelingsautoriteiten, hun ICT-contracten afwikkelingsbestendig zijn.[137] Zolang zij aan hun betalingsverplichtingen blijven voldoen, moeten die financiële entiteiten er onder meer voor zorgen dat hun ICT-contracten clausules bevatten voor niet-beëindiging, niet-opschorting en niet-wijziging op grond van herstructurering of afwikkeling.[138]

Met betrekking tot de beschrijving van dienstverlening vereist DORA van dergelijke KOB-contracten bijvoorbeeld een precieze beschrijving van de kwantitatieve en kwalitatieve prestatiedoelstellingen (service levels) waaraan de leverancier moet voldoen, monitoring door de financiële entiteit, en de mogelijkheid tot correctieve actie zonder vertraging.[139] Met betrekking tot incidentmanagement vereist DORA van dergelijke KOB-contracten bijvoorbeeld het invoeren en testen van bedrijfsnoodplannen door leveranciers.

In aanvulling op beëindigingsrechten (met minimumopzegtermijnen) die in overeenstemming met toezichtsvereisten dienen te zijn (art. 30 lid 2 sub h DORA), moeten KOB-contracten bovendien een exitstrategie bevatten met een passende overgangsperiode (art. 30 lid 3 sub f DORA).

In aanvulling op medewerkingsverplichtingen (toepasselijk voor alle ICT-contracten) ten behoeve van toezichthouders (art. 30 lid 2 sub g DORA) moeten KOB-contracten bovendien zeer uitgebreide monitoringsrechten bevatten, waaronder onbeperkte rechten van toegang, inspectie en audit voor de financiële entiteit, haar ingeschakelde derden en de toezichthouder (art. 30 lid 3 sub e DORA). Bovendien – en dat is vrij uitzonderlijk en verstrekkend – omvat dit ook het recht om kopieën van kritieke stukken te maken. Ook dienen gedetailleerde auditafspraken te worden opgenomen in KOB-contracten (art. 30 lid 3 sub e onder iii DORA) en gelden medewerkingsverplichtingen voor de leverancier (art. 30 lid 3 sub e onder iv DORA).

5.7 Toezicht op kritieke aanbieders van ICT-diensten

Zoals hiervoor reeds besproken, zullen leveranciers die als 'kritiek' worden aangewezen onder rechtstreeks toezicht komen van EBA, EIOPA of ESMA. Dit is afhankelijk van het onderdeel van de financiële markt waarop de leverancier het meest actief is. Of een leverancier als 'kritiek' wordt gekwalificeerd,

130 Art. 30 lid 2 DORA.
131 Art. 30 lid 3 DORA.
132 Art. 30 lid 3 DORA.
133 Art. 30 lid 3 sub e onder i DORA.
134 Art. 30 lid 3 sub e onder iii DORA.
135 Art. 30 lid 3 sub f onder i en ii DORA.
136 Overweging 74 DORA.
137 Overweging 74 DORA.
138 Overweging 74 DORA.
139 Vgl. art. 30 lid 3 sub a DORA (voor alle contracten) met art. 30 lid 2 sub a DORA (voor KOB-contracten).

 doi: 10.5553/MvV/157457672023033006001

hangt onder meer af van de afhankelijkheid van financiële entiteiten van de ICT-diensten en de vervangbaarheid van de leverancier.[140]

6 Conclusie

Gelet op het brede toepassingsbereik van DORA zullen de daarin opgenomen verplichtingen behoorlijke impact (kunnen) hebben op financiële entiteiten. Omdat DORA met ingang van 17 januari 2025 van toepassing zal zijn, betekent dit het nodige werk om te voldoen aan deze verordening.[141] Niet alleen om de interne organisatie klaar te stomen voor een compliant governancebeleid met betrekking tot ICT-risico's, maar ook met betrekking tot de vereiste contractuele afspraken met leveranciers van ICT-diensten aan financiële entiteiten. Het feit dat het bestuur van financiële entiteiten de eindverantwoordelijkheid krijgt toebedeeld in DORA, zal dit thema hoog genoeg op de agenda's plaatsen, is mijn verwachting (hetgeen vermoedelijk precies de bedoeling van de wetgever zal zijn).

140 Art. 31 lid 2 DORA.
141 Zo ook Rank 2023, p. 67.