FINNIUS

Derden onder DORA: wanneer trekt de mist op?

17 oktober 2024

12 MINUTEN

Nog precies 3 maanden vanaf de datum van deze blog en dan is het zo ver: DORA-tijd. Hoewel financiële instellingen die binnen het toepassingsbereik van DORA vallen al hard bezig zijn om tijdig aan alle regels te kunnen voldoen, is er ook nog één en ander niet volledig duidelijk.

De nog bestaande onduidelijkheid is des te lastiger voor partijen van wie nu al (theoretische) DORA-compliance wordt verwacht in beleidsstukken en procedures, bijvoorbeeld omdat zij in een vergunningtraject zitten bij de AFM.[2] Van die partijen wordt een anticiperende houding verwacht, maar daarmee lopen zij wel tegen een aantal vraagstukken aan die nog niet zijn uitgekristalliseerd. Bij het uitblijven van concrete guidance vanuit de Europese of nationale toezichthouder en/of wetgever is het daarom (voorlopig) lastig om de precieze route door het DORA-bos te bepalen.

Met deze blog beoog ik een aantal onduidelijkheden nader te belichten en zo onder de aandacht te brengen bij zowel binnen de DORA-reikwijdte vallende marktpartijen als de toezichthouder. Hierbij ligt de focus op vragen die met uitbesteding te maken hebben, maar er zijn natuurlijk ook andere vragen te bedenken – denk bijvoorbeeld aan het evenredigheidsbeginsel.

DORA en relaties met derden: wie doet wat?

Een deel van de vraagstukken ziet op uitbestedingsstructuren. Wanneer is er nu sprake van een ICT-dienstverleningsrelatie binnen het bereik van DORA? Welke rol wordt door welke partij vervuld? Wie is bijvoorbeeld de ICT-dienstverlener en wie kwalificeert als subcontractor? Hoe moeten deze vragen worden beantwoord in geval van centrale inkoop van ICT diensten binnen een groep? En wat als de uitbestedingsrelatie een non-EU component bevat? Hoe ingewikkelder – en grensoverschrijdender – de structuur, hoe meer vragen er opgeworpen kunnen worden. Dit is niet alleen van belang voor het uitbestedingsbeleid van de financiële instelling, maar ook voor het adequaat bijhouden van het door DORA vereiste informatieregister en het correct doen van verplichte meldingen aan de toezichthouder.[3]

Idealiter is het duidelijk aan te wijzen welke partij welke rol vervult in de keten, maar in de praktijk blijkt dit lang niet zo simpel. Hieronder schets ik twee voorbeeldscenario's die praktische vragen oproepen voor de DORA-compliance van financiële instellingen.

Scenario 1: intra-groepsverhoudingen

Een constructie die voorkomt is het centraal inkopen van bepaalde producten en diensten binnen een groep via één groepsmaatschappij (zoals een holding of moedermaatschappij), welke vervolgens de producten en diensten ter beschikking stelt aan de dochtermaatschappijen. Hierbij is een scenario denkbaar waarin een groepsmaatschappij ICT-diensten inkoopt en deze vervolgt

doorschuift naar dochtermaatschappijen die binnen de reikwijdte van DORA vallen. Dit kan bijvoorbeeld door het sluiten van een contract met de ICT-dienstverlener op eigen naam waarin ligt besloten dat de dienst direct aan de dochtermaatschappijen wordt verleend, of door het op eigen naam sluiten van contracten met de ICT-dienstverlener en het zelf afnemen van die diensten aan de ene kant en aan de andere kant het sluiten van contracten met de dochtermaatschappijen voor het gebruik van de desbetreffende ICT-diensten.

Voordat ik hier nader op in ga, is het goed om eerst de Level 1 tekst van DORA te bekijken – kunnen intra-groepsverhoudingen onder DORA vallen? Het antwoord hierop is ja, zoals wordt bevestigd in overweging 31 van DORA:

"*Aan ICT-dienstverlening binnen een financiële groep zijn specifieke risico's en voordelen verbonden die evenwel niet automatisch aangemerkt mogen worden als minder risicovol dan ICT-dienstverlening door externe aanbieders. Interne ICT-dienstverlening moet derhalve aan hetzelfde regelgevingskader worden onderworpen. Dat neemt niet weg dat bij interne ICT-dienstverlening vanuit de financiële groep zelf, financiële entiteiten een betere grip op intra-groepsaanbieders zouden kunnen hebben, iets waarmee bij de algehele risicobeoordeling rekening gehouden moet worden*."

De ICT intra-groep dienstverlener is voorts in de Level 1 tekst van DORA gedefinieerd als "*een onderneming die deel uitmaakt van een financiële groep en hoofdzakelijk ICT-diensten verleent aan financiële entiteiten binnen dezelfde groep of aan financiële entiteiten die tot hetzelfde institutionele protectiestelsel behoren, met inbegrip van hun moedermaatschappijen, dochterondernemingen, bijkantoren of andere entiteiten die gezamenlijk eigendom zijn of onder gezamenlijke zeggenschap staan*".[4]

Intra-groepsverhoudingen kunnen dus wel degelijk binnen de reikwijdte van DORA vallen. Maar hoe moet daarmee worden omgegaan? De concept-ITS inzake het informatieregister[5] bieden voor dit vraagstuk enige soelaas. In overweging 5 van de concept-ITS (p. 16) staat:

"*In order to capture the full ICT service supply chain, financial entities maintaining the register of information should report information on both the contractual arrangement with their ICT intra-group service provider as well as information on the arrangement stipulated by the ICT intragroup service provider and the ICT third-party providers external to the group as subcontractors.*"

Hier lijkt het dus primair van belang wat er contractueel is afgesproken met de uiteindelijke ICT-dienstverlener en wat de (contractuele) verhoudingen zijn tussen de groepsmaatschappijen. Het uitgangspunt lijkt te zijn dat de ICT intra-groep dienstverlener te gelden heeft als de ICT-dienstverlener van de dochtermaatschappij en de achterliggende externe ICT-dienstverlener als subcontractor moet worden gezien.

Toch is daarmee niet alle onduidelijkheid opgelost, want wanneer is de centrale inkoper van ICT-dienstverlening hier 'hoofdzakelijk' mee bezig? En kan het ook zo zijn dat zowel de inkopende

groepsmaatschappij als de externe ICT-dienstverlener als directe ICT-dienstverlener moeten worden aangemerkt? De concept-ITS lijken te bepalen dat van dit laatste bijvoorbeeld sprake is als de groepsmaatschappij zelf het contract aangaat maar hierin ligt besloten dat de ICT-dienst direct is bestemd voor een bepaalde dochtermaatschappij die onder DORA valt. Daar tegenover staat dat het ook kan dat de tussenliggende groepsmaatschappij ertussenuit valt als het een structuur betreft waarbij de groepsmaatschappij de ICT-dienstverlening contracten aangaat namens de respectievelijke dochtermaatschappijen. In dat geval zal de externe ICT-dienstverlener eerder de directe ICT-dienstverlener van de dochtermaatschappij zijn dan dat deze zou kwalificeren als subcontractor.

Scenario 2: non-EU uitbesteding van gereguleerde diensten

Het kan ook voorkomen dat een financiële instelling binnen de EU een uitbestedingsrelatie heeft met een non-EU partij ten behoeve van andere diensten dan ICT, bijvoorbeeld het (deels) uitbesteden van vermogens- of fondsenbeheer. De non-EU dienstverlener zou in een dergelijk geval op zijn beurt ICT-diensten kunnen inkopen ten behoeve van het uitvoeren van de uitbestede functie, maar valt in tegenstelling tot de financiële instelling zelf niet direct binnen de reikwijdte van DORA. Valt de verhouding dan toch onder DORA? En zo ja, bij wie ligt dan de verantwoordelijkheid voor het naleven van DORA?

ESMA heeft eerder dit jaar in februari in een Q&A over non-EU uitbesteding[6] opgemerkt dat de DORA-compliance met betrekking tot dit soort uitbestedingsrelaties binnen het pakket aan verantwoordelijkheden valt van de onder DORA vallende financiële instelling. Dit betekent dat als de non-EU dienstverlener voor het uitvoeren van de uitbestede functie gebruik maakt van ICT-diensten van derden, de onder DORA vallende financiële instelling zich ervan moet verzekeren dat de non-EU dienstverlener DORA-compliance niet in de weg zit. Dit geldt volgens ESMA ongeacht of de uitbestede functie als kritiek of belangrijk moet worden aangemerkt.

De door ESMA genomen afslag is niet geheel onverwachts, omdat het bij uitbesteding gaat om functies of activiteiten die anders door de financiële instelling zelf zouden worden uitgevoerd. De financiële instelling zou derhalve zelf hoogstwaarschijnlijk ook van ICT-diensten gebruik maken als zij de functie zelf zou uitvoeren. Het ligt daarom in de rede dat de financiële instelling zich voor bepaalde uitbestede functies niet aan DORA kan onttrekken door de functie buiten de EU te laten uitvoeren. Anderzijds wordt het territoriale toepassingsbereik van DORA met deze aanpak – met name door de toenemende digitalisering van allerlei diensten en activiteiten – dusdanig opgerekt dat er vraagtekens kunnen worden gezet bij de proportionaliteit van deze opzet en de vergaande verantwoordelijk die financiële instellingen onder DORA dragen voor de gehele uitbestedingsketen binnen én buiten de EU.

Overigens is de vraag of een uitbesteding (ook) door DORA wordt beheerst, bepaald nog niet uitgekristalliseerd. Tekenend in dit verband is het FAQ document dat de ESA's deze zomer in het kader van de dry run hebben gepubliceerd.[7] In deze FAQ wordt ten aanzien van de reikwijdte van de definitie van ICT-diensten antwoord gegeven op de vraag welke typen dienstverleners die als ICT-dienstverleners moeten worden beschouwd.[8] Hierover zeggen de ESA's dat indien een financiële instelling een vergunning, registratie of anderszins authorisatie nodig heeft om een dienst te verlenen, dit als gereguleerde dienst moet worden gezien en niet als ICT-dienst in de zin van DORA. Op basis van dit antwoord zouden marktpartijen kunnen concluderen dat bepaalde uitbestedingsrelaties ten aanzien van gereguleerde diensten niet onder DORA vallen, terwijl ESMA in haar eigen Q&A aangeeft dat dat niet betekent dat je niet door deze relatie heen moet kijken indien de dienstverlener op zijn beurt wél gebruik maakt van ICT-diensten. Op het verlossende woord moet echter nog even worden gewacht, want het voorgaande antwoord is inmiddels weer ingetrokken in afwachting van formele Q&As na overleg tussen de ESA's en de Europese Commissie (**EC**). Tot die tijd wordt van onder DORA vallende partijen verwacht dat zij hun dienstverleningsovereenkomsten opnemen in het informatieregister op een *best effort* basis.

Enfin, als de voorvraag over de toepassing van DORA bevestigend moet worden beantwoord, is de kous daarmee nog niet af. Er moet immers ook worden vastgesteld wie de directe ICT-dienstverlener is en wie kwalificeert als subcontractor. Ook hier zegt de eerdergenoemde concept-ITS inzake het informatieregister iets over. In overweging 7 (p. 17) staat:

"*In case a financial entity outsources a function or activity to a service provider, and this service provider makes use of ICT services to support this function or activity, the responsibility for ensuring the operational resilience of that function or activity remains with the financial entity. Therefore, for the purpose of the register of information, the service provider should be treated as a direct ICT third-party service provider. In the case where a financial entity or a management entity acting on behalf of the financial entity, outsources all its activity to a service provider, the ICT third-party service providers to that service provider should be treated as a direct ICT third-party service provider of the financial entity or of the management entity, respectively*."

Deze overweging lijkt erop te duiden dat het uitbesteden van een functie of activiteit waarvoor door de dienstverlener (ongeacht waar deze is gevestigd) gebruik wordt gemaakt van ICT-diensten ertoe leidt dat de dienstverlener zelf als ICT-dienstverlener zoals bedoeld in DORA moet worden aangemerkt. De vervolgstap zou dan zijn dat de partij die aan deze dienstverlener ICT-diensten verleent, onder DORA als subcontractor te gelden heeft. Toch is deze redenering niet definitief te noemen: bovenstaande citaat blijft een concept-ITS tekst en is 'slechts' een overweging.

Laatste update over de concept-ITS inzake het informatieregister

Zoals hierboven opgemerkt, zijn de ITS inzake het informatieregister enkel nog in conceptvorm beschikbaar. De laatste stand van zaken is als volgt. Afgelopen juli heeft de EC te kennen gegeven dat zij voornemens is om de conceptversie van de ITS af te keuren, tenzij een aantal wijzigingen wordt doorgevoerd.[9] Dit voornemen was tot 15 oktober 2024 niet gepubliceerd, maar nu wel beschikbaar. Het onderwerp van discussie tussen de EC en de ESA's is het gebruik van identifiers voor ICT-dienstverleners en de proportionaliteit daarvan. Dit is een meer technische discussie op een detailpunt, dus zal niet als gevolg hebben dat van de gehele ITS afscheid wordt genomen. Het zal kan echter wel tot wijzigingen leiden.

Volgens de EC moeten ICT-dienstverleners de keuze krijgen tussen het gebruik van de LEI en EUID, in plaats van enkel het verplichten van de LEI. Daarnaast heeft de EC nog wat kleine wijzigingen voorgesteld zodat de ITS binnen het mandaat van artikel 28(9) DORA blijven. Als reactie op het voornemen tot afwijzing hebben de ESA's op 15 oktober 2024 een opinie gepubliceerd, tezamen met twee documenten met voorgestelde wijzigingen.[10] Volgens de ESA's leidt het toevoegen van een identifier-keuze tot onnodige complexiteit en heeft dit mogelijk negatieve impact op de implementatie van DORA door financiële instellingen. De discussie lijkt met de reactie van de ESA's nog niet tot een einde te zijn gekomen, dus het valt nog te bezien hoe de uiteindelijke ITS eruit komen te zien.

Kortom, het laatste woord is over DORA nog zeker niet gesproken – en de laatste vraag nog niet gesteld. Het is dan ook verstandig om nauwlettend in de gaten te houden hoe de verdere ontwikkeling van de Level 2 regelgeving onder DORA verloopt en of er aanvullende guidance verschijnt. Mochten er toch prangende vragen zijn waarvan het antwoord zich nog onder de DORA-mistbank bevindt, staat het Finnius team uiteraard graag voor u klaar.

[1] Zie over DORA ook het artikel van Laurens Hillen en mijzelf getiteld '*DORA: van theorie naar praktijk*' zoals eerder dit jaar verschenen in het Tijdschrift Ondernemingsrechtpraktijk. Dit artikel is hier te raadplegen.

[2] Denk bijvoorbeeld aan cryptodienstverleners die bezig zijn om een CASP-vergunning onder MiCA te verkrijgen.

[3] Zie artikel 28(3) DORA.

[4] Zie artikel 3(20) DORA.

[5] Zie het Final Report 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 zoals gepubliceerd door de ESAs op 17 januari 2024.

[6] Zie https://www.esma.europa.eu/publications-data/questions-answers/2107.

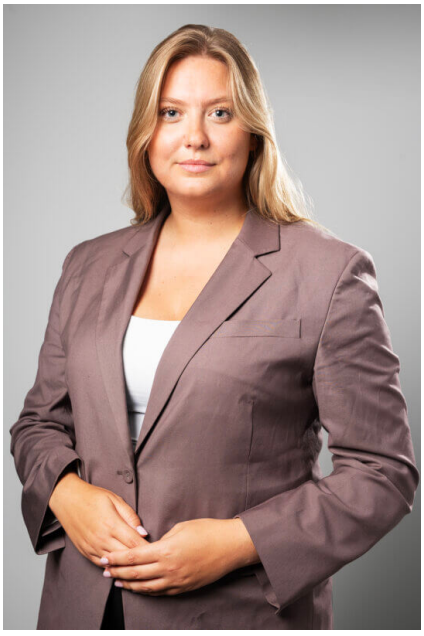
[7] Zie '*Frequently Asked Questions: DORA 2024 Dry Run exercise on reporting of registers of information*', zoals gepubliceerd door de ESAs op 31 mei 2024 en laatst geüpdatete op 29 juli 2024.

[8] Zie vraag 74 van de FAQ, p. 30.

[9] Zie https://finance.ec.europa.eu/document/download/d7f731c6-39a7-42e5-bd4b-f28434b7d51d_en?filename=240723-letter-esma-dora-register-information_en.pdf.

[10] Zie https://www.esma.europa.eu/press-news/esma-news/esas-respond-european-commissions-rejection-technical-standards-registers.

Specialisten



Marise Kok
T +31 (0)20 767 01 80
M +31 (0)6 25 29 82 99

marise.kok@finnius.com