Hart Advocaten: zes praktische DORA-tips

Christian Wulf - 20 december 2023

DORA stelt zware eisen aan ICT-contracten en de beheersing daarvan. Dit moet begin 2025 allemaal geregeld zijn. In deze column zes praktische tips om ervoor te zorgen dat een instelling DORA-proof is op het punt van ICT-risico's met betrekking tot aanbieders van ICT-diensten.

De AFM verzoekt instellingen al enige tijd om zich tijdig voor te bereiden. Zo heeft de AFM onlangs een tweede publicatie op haar website uitgebracht waarin inhoudelijke aspecten van DORA worden toegelicht. Deze publicatie gaat nader in op het beheren van ICT-risico's van derde aanbieders. De AFM stelt in haar berichtgeving vast dat het voor beleggingsondernemingen – om in de hele keten weerbaar te zijn tegen ICT-verstoringen – belangrijk is om aandacht te besteden aan de risico's van het afnemen van ICT-diensten van derde aanbieders. De AFM verlangt dat beleggingsondernemingen (i) expliciet aandacht besteden aan de ICT-risico's die voortkomen uit het gebruik van diensten van derde aanbieders, (ii) een strategie ontwikkelen voor het beheersen van deze zogenoemde third party risks, en (iii) hun bestaande contracten aanpassen aan de DORA eisen.

DORA treedt inwerking vanaf 17 januari 2025 en dat duurt gevoelsmatig nog enige tijd, maar verkijk je niet op de omvang van de werkzaamheden om te kunnen voldoen aan de nieuwe regels. DORA reguleert niet enkel de operationele weerbaarheid en cyberbeveiliging, maar stelt ook regels voor de governance en het beheer van ICT-risico's. Daarom heb ik zes tips ter voorbereiding:

Tip 1: Inventariseer welke ICT-contracten zijn afgesloten

Alle bestaande ICT-contracten moeten geïnventariseerd worden. Maar wat zijn ICT-contracten? Dat zijn alle overeenkomsten met ondernemingen die ICT-diensten verlenen. Zijn alle contracten verzameld? Leg dan het door DORA verplichte ICT-register aan. In dit register worden alle ICT-contracten vastgelegd. Een standaardmodel van dit informatieregister wordt vastgesteld door de Europese toezichthouders. Dat model moet gebruikt worden. Verwacht wordt dat dit model begin 2024 als voorstel aan de Europese Commissie wordt voorgelegd. Let op: toezichthouders kunnen dit register opvragen.

Tip 2: Maak onderscheid tussen (i) diensten die de kritieke of belangrijke functies ondersteunen, en (ii) diensten die reguliere functies ondersteunen

DORA stelt inhoudelijk eisen aan ICT-contracten. Maar eerst is het nodig om onderscheid te maken tussen (i) reguliere functies en (ii) kritieke of belangrijke functies. Aan kritieke uitbestede functies stelt DORA namelijk zwaardere eisen (zie tip 3).
Wat zijn reguliere en kritieke of belangrijke functies? DORA bevat een definitie van wat

een kritieke functie is, die erop neer komt dat daarvan sprake is indien bij verstoring dit een materiële impact heeft op de financiële prestaties, continuïteit en compliance van de beleggingsonderneming. Of sprake is van een kritieke of belangrijke functie dient door de instelling vooraf zelf te worden vastgesteld. Alles wat geen kritieke of belangrijke functie is, is een reguliere functie.

Tip 3: Beoordeel of de bestaande overeenkomsten beantwoorden aan de aanvullende eisen van DORA

DORA stelt vervolgens eisen aan de inhoud en inrichting van ICT-contracten. Bepaalde verplichtingen gelden altijd, dus zowel voor uitbestede ICT-diensten die reguliere functies ondersteunen als diensten die kritieke of belangrijke functies ondersteunen.

Ieder contract moet bevatten:

- Een volledige beschrijving van geleverde diensten;
- De regio's en/of landen waaraan de diensten moeten worden geleverd en waar gegevens moeten worden verwerkt;
- De mate van gegevensbescherming, in termen van beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit; en
- De beëindigingsrechten en bijbehorende opzegtermijnen.

Ten aanzien van ICT-diensten die kritieke of belangrijke functies ondersteunen, stelt DORA aanvullende eisen aan de inhoud van de overeenkomsten.

Enkele voorbeelden hiervan zijn:

- De rapportageverplichting van de ICT-dienstverlener aan de instelling;
- De verplichting voor de ICT-dienstverlener om een bedrijfsnoodplan te ontwikkelen en te testen;
- Het recht van inspectie en audit door de instelling, die dit overigens ook mag laten doen door een derde partij; en
- Het uitwerken van de geleverde diensten door middel van nauwkeurige prestatiedoelstellingen zodat corrigerende maatregelen kunnen worden getroffen indien de overeengekomen dienstenniveaus niet gehaald worden.

Tip 4: Stel een exit strategie op

DORA stelt een exit beleid verplicht. Allereerst moet een ICT-contract in ieder geval beëindigd kunnen worden als de onderstaande omstandigheden zich voor doen: (i) bij ernstige overtreding van wettelijke voorschriften en (ii) bij klaarblijkelijke zwakheden in verband met het algemeen beheer van het ICT-risico. Maar dat is niet alles. Want bij beëindiging moeten de ICT-functionaliteiten wel doorgaan. Dit vereist ook een exit strategie.

De exit strategie moet erin voorzien dat instellingen de mogelijkheid hebben om contractuele overeenkomsten te beëindigen zonder verstoring van hun bedrijfsactiviteiten en zonder dat afbreuk wordt gedaan aan de continuïteit en de kwaliteit

van aan cliënten geleverde diensten. Dergelijke exit plannen zijn volgens de Europese wetgever alomvattend en moeten gedocumenteerd, getest en regelmatig geëvalueerd worden. Opvallend is dat DORA geen verdere eisen stelt aan de inhoud van de exit strategie. De essentie is natuurlijk dat de ICT-functionaliteiten gewoon doorlopen bij beëindiging van een uitbestede ICT-dienst indien dat een kritieke of belangrijke functie betreft.

Tip 5: Doe onderzoek naar de aanbieder van ICT-diensten

DORA legt ook een due diligence verplichting op. Stel daarom een due diligence-beleid op waarin staat aan de hand van welke criteria dit onderzoek wordt verricht en hoe de uitkomst wordt vastgelegd. Uit DORA is af te leiden dat in ieder geval onderzocht moet worden of het contract kan leiden tot een versterking van het ICT-concentratierisico en of de ICT-dienstverlener buiten de EU gevestigd is. Dat laatste is om vast te stellen of en hoe de regelgeving inzake gegevensbescherming kan worden nageleefd.

Tip 6: Volg de guidance van nationale en Europese toezichthouders

Dit jaar hebben de Europese toezichthouders twee batches aan technische standaarden (RTS) geconsulteerd. Deze standaarden bevatten onder andere het informatieregister. De eerste set aan standaarden zijn al ingediend bij de Europese Commissie en de tweede set zal uiterlijk in juli 2024 worden ingediend. De inhoud van deze sets reikt verder dan de ICT-contracten en omvat eveneens standaarden met betrekking tot het risk management framework, en incidenten classificatie en meldingen. En volg in ieder geval de publicatiereeks van de AFM.

Werk aan de ICT-winkel dus!

Christian Wulf is know how manager bij Hart Advocaten, een van de kennisexperts van Investment Officer die maandelijks een bijdrage levert.

Dit artikel is afkomstig van Investment Officer, een journalistiek platform voor professionals werkzaam in de beleggingsindustrie.

www.investmentofficer.com