FINNIUS

DORA – een nieuwe fase voor cybersecurity in de Europese financiële sector

9 mei 2022

8 MINUTEN

Inleiding

Vorig jaar schreef ik een Finnius Vindt blog over cybersecurity in de financiële sector. Aanleiding vormde een reeks ransomware incidenten in Nederland en de VS. In mijn blog stond ik stil bij het versnipperde en weinig concrete wettelijk kader voor cybersecurity in de financiële sector, en noteerde dat financiële instellingen zoals banken, vermogensbeheerders en verzekeraars het momenteel vooral moeten doen met guidance van toezichthouders AFM, DNB, EBA en ESMA. Ik sloot af met een blik naar de toekomst, te weten naar DORA, de verordening betreffende digitale operationele veerkracht voor de financiële sector.

Intussen heeft het onderwerp cybersecurity alleen maar verder aan relevantie gewonnen. Zo publiceerde DNB op 23 december 2021 op haar website dat ruim 15% van de Nederlandse pensioenfondsen en verzekeraars heeft laten weten in 2021 te zijn geconfronteerd met aanzienlijke financiële schade door beveiligingsincidenten en datalekken. Volgens DNB moet onder andere de weerbaarheid tegen cyberaanvallen worden versterkt en is daar dringend aandacht voor nodig.[1]

Gelet op het grote belang van DORA voor en de te verwachten impact van DORA op de gehele financiële sector zoom ik in deze blog verder in op deze nieuwe verordening, waarvan de definitieve tekst op dit moment wordt uitonderhandeld in Brussel.

Wat is er bijzonder aan DORA?

DORA is om meerdere redenen bijzonder:

1. Het is voor het eerst dat binnen het financieel toezichtrecht op EU-niveau een omvangrijke set aan cybersecurity regels wordt geïntroduceerd, die straks in iedere lidstaat rechtstreeks (dus in beginsel[2] zonder omzetting in nationale wetten) van toepassing is.
2. De reikwijdte van de DORA-regels zal zich uitstrekken tot een groot aantal type financiële spelers (alhoewel sommige instellingen, zoals AIFMD-light beheerders, in de laatste versie van het voorstel zijn vrijgesteld). Doel is dat voor het overgrote deel van de Europese financiële sector in beginsel dezelfde eisen op het vlak van ICT gaan gelden. Ik zeg bewust ‘in beginsel’, omdat in het meest recente DORA-voorstel van 19 november 2021 relatief veel aandacht wordt besteed aan het proportionaliteitsbeginsel.
3. Het bestuur van financiële ondernemingen krijgt in DORA een centrale en actieve rol toebedeeld bij de beheersing van ICT-risico’s. Zo moet het bestuur alle regelingen met betrekking tot het ICT-risicobeheer goedkeuren, dient zij toezicht te houden op de uitvoering van die regelingen en moet zij regelmatig opleidingen volgen over ICT-risicobeheersing.
4. Voor het eerst wordt ook een belangrijke groep niet-financiële dienstverleners onder het toezicht van financiële toezichthouders gebracht, namelijk de zogeheten ‘cruciale aanbieders van ICT-diensten’. Denk bijvoorbeeld aan de grote techbedrijven die clouddiensten aanbieden. Om effectief toezicht mogelijk te maken moeten deze ICT-aanbieders straks op

grond van DORA (ook) gevestigd zijn in de EU.

Een korte tour door DORA aan de hand van vier kernbegrippen

DORA staat bol van lastig leesbare definities en lange bepalingen. Een erg toegankelijke verordening is zij daarom niet. Wat dan in ieder geval helpt is om de kernbegrippen uit DORA goed voor ogen te hebben. Veel voorschriften in DORA vormen een uitwerking van, althans hebben betrekking op, deze kernbegrippen.

Hierna zal ik een aantal belangrijke aspecten uit het meest recente DORA-voorstel kort uitlichten aan de hand van de volgende vier DORA-kernbegrippen: 'ICT-risicobeheer', 'ICT-risico's', 'ICT-incidenten' en 'derde aanbieders van ICT-diensten'.[3]

(i) ICT-risicobeheer

Een van dé kernbepalingen uit DORA houdt in dat financiële ondernemingen moeten zorgen voor een "*solide, alomvattend en goed gedocumenteerd*" kader voor ICT-risicobeheer. Dit betekent dat ondernemingen moeten beschikken over adequate strategieën, beleidsdocumenten, procedures en protocollen om informatie, software en hardware te beschermen tegen ICT-risico's.

De in DORA opgenomen regels over ICT-risicobeheer zijn geïnspireerd op internationale, nationale en door de sector vastgestelde normen, richtsnoeren en aanbevelingen. De daarin verankerde grondgedachte is dat ICT-risicobeheer moet voorzien in de volgende functies: (i) identificatie, bescherming en voorkoming, (ii) detectie, respons en herstel, (iii) scholing en ontwikkeling en (iv) communicatie richting stakeholders. Met betrekking tot ieder van deze functies bevat DORA voorschriften, waarbij in een aantal gevallen de nadere uitwerking van deze voorschriften wordt overgelaten aan de Europese toezichthouders EBA, ESMA en EIOPA (de ESAs).

(ii) ICT-risico's

ICT-risicobeheer gaat logischerwijs over ICT-risico's. Maar wat valt daar allemaal onder? In DORA zijn ICT-risico' als volgt gedefinieerd:

"*elke redelijkerwijs aan te wijzen omstandigheid of gebeurtenis met een potentieel nadelig effect op de netwerk- en informatiesystemen (…) die, indien zij zich voordoet, de beveiliging of het functioneren in gevaar kan brengen van de netwerk- en informatiesystemen, technologieafhankelijke instrumenten of processen, de exploitatie en het procesverloop, of de levering van de diensten, waarbij de integriteit of beschikbaarheid van gegevens, software of enig andere component van ICT-diensten en infrastructuren wordt aangetast, of waarbij een inbreuk op*

de vertrouwelijkheid, een beschadiging van fysieke ICT-infrastructuur of andere nadelige effecten worden veroorzaakt”

Over moeilijk leesbare en ruim geformuleerde definities gesproken. Financiële ondernemingen zullen zelf in hun beleid structuur in de identificatie van ICT-risico’s moeten aanbrengen, bijvoorbeeld door deze te rubriceren naar aard of potentiële impact. Duidelijk is in ieder geval dat ICT-risico’s zowel kunnen zien op kwaadwillige als niet-kwaadwillige gebeurtenissen, op gebeurtenissen van zowel buiten de organisatie als van binnenuit en op zowel digitale als fysieke ICT-infrastructuur van de onderneming.

(iii) (Ernstige) ICT-incidenten

Een ander DORA-kernbegrip is ‘ICT-incident’. In DORA wordt ICT-incident als volgt omschreven:

“*een eenmalig voorval of een reeks aan gerelateerde voorvallen onvoorzien door de financiële onderneming in de netwerk- en informatiesystemen, met een nadelig gevolg voor de integriteit, beschikbaarheid, vertrouwelijkheid, continuïteit of authenticiteit van de door de financiële onderneming verleende financiële diensten*”

DORA schrijft voor hoe financiële ondernemingen met ICT-incidenten om moeten gaan. DORA geeft daarnaast ook criteria om te bepalen of sprake is van een ‘ernstig ICT-incident’, welke criteria door de ESAs nader moeten worden uitgewerkt. Indien sprake is van een ernstig ICT-incident, dan moet deze straks op grond van DORA door de financiële onderneming aan de bevoegde toezichthouder en, onder omstandigheden, aan cliënten worden gemeld. Hoe dat precies in zijn werk moet gaan en binnen welke tijdsperiode de melding dient plaats te vinden, zal door de ESAs worden uitgewerkt.

(iv) Derde aanbieders van ICT-diensten

Financiële ondernemingen maken in toenemende mate gebruik van ICT-diensten van derde partijen. DORA verplicht daarom dat financiële ondernemingen die gebruikmaken van ‘derde aanbieders van ICT-diensten’ de daaraan verbonden risico’s goed in kaart brengen en monitoren. Ook voorziet DORA in minimumeisen waaraan uitbestedingsovereenkomsten met dergelijke partijen moeten voldoen. Derde aanbieders van ICT-diensten zijn in beginsel alle ondernemingen die:

“*digitale en gegevensdiensten verlenen, waaronder cloud computing, verstrekken van gegevens, gegevensinvoer, gegevensopslag, gegevensverwerking en rapportagediensten, gegevensmonitoring, op gegevens gebaseerde bedrijfs- en beslissingsondersteunende diensten,*

hardware ‘as a service’ en hardware diensten met inbegrip van technische ondersteuning via software of firmware updates door de hardware aanbieder”

Voorts voorziet DORA in aanvullende regels voor de uitbesteding van zogeheten cruciale of belangrijke functies aan derde aanbieders. Dat zijn functies waarbij het wegvallen daarvan wezenlijk afbreuk zou doen aan de naleving van de wettelijke verlichtingen door de financiële onderneming, of aan haar financiële prestaties dan wel aan de kwaliteit en beschikbaarheid van haar diensten en activiteiten.

Derde aanbieders die zo belangrijk zijn voor financiële ondernemingen dat zij door de ESAs als ‘cruciale aanbieder’ worden aangemerkt, komen onder rechtstreeks toezicht van EBA, ESMA of EIOPA te staan (de zogeheten ‘Lead Overseer’).

Wanneer treedt DORA in werking?

Op dit moment zijn de onderhandelingen in Brussel over de definitieve tekst van DORA nog gaande. De verwachting is dat de finale tekst in de komende maanden definitief wordt. De Europese Commissie heeft voorgesteld om DORA 12 maanden nadien van toepassing te laten zijn, dus medio 2023. De Raad heeft in haar voorstel van 19 november 2021 echter voorgesteld om een periode van 24 maanden aan te houden, waardoor DORA medio 2024 van toepassing zou worden. De definitieve toepassingsdatum zullen we binnenkort weten. Hoe dan ook doen financiële ondernemingen er goed aan om zich alvast voor te bereiden op de in DORA neergelegde eisen. Want dat DORA een belangrijke verordening gaat worden waar ook toezichthouders in Nederland veel aandacht voor zullen hebben, lijdt geen twijfel.

Naschrift 11 mei 2022: op 10 mei 2022 hebben vertegenwoordigers van het Europees Parlement een ‘provisional deal’ gesloten met de Raad over DORA. De deal houdt onder meer in dat DORA 24 maanden na inwerkingtreding van toepassing wordt in alle EU-lidstaten.

[1] https://www.dnb.nl/nieuws-voor-de-sector/2021/resultaat-jaarlijkse-onderzoeken-naar-cyber-nu-gepubliceerd-in-ib-monitor-2021/.

[2] Op het gebied van handhavingsbevoegden worden lidstaten in DORA opgedragen om op nationaal niveau te zorgen voor adequate regelingen.

[3] Vertaald vanuit de laatste Engelstalige versie van 19 november 2021.

Specialisten

Laurens Hillen

T +31 (0)20 767 01 80
T +31 (0)20 767 01 84 (direct)
M +31 (0)6 21 663 776
laurens.hillen@finnius.com