TOEZICHT DORA UPDATE 6

DORA vooruitzicht: Wat te verwachten in het komende jaar

In het kort Dit is de laatste editie in een reeks AFM-publicaties over de Digital Operational Resilience Act (DORA). Deze reeks is bedoeld voor alle ondernemingen die vanaf 2025 aan de Europese verordening moeten voldoen. In deze editie kijken we naar de verwachtingen voor 2025. Ook staan we stil bij een aantal praktische zaken.

1. Inleiding

DORA heeft als doel dat financiële instellingen ICT-risico's beter beheersen en daarmee weerbaarder worden tegen cyberdreigingen en ICT-verstoringen. Hiervoor beschrijft de verordening verschillende vereisten op het gebied van ICT. Om op 17 januari 2025 aan DORA te voldoen, is het belangrijk om de implementatie van de DORA vereisten zo snel mogelijk af te ronden.

Vanaf 17 januari 2025 is DORA van toepassing. Op dat moment moeten alle financiële ondernemingen die onder DORA vallen, voldoen aan de vereisten in de verordening en de nadere regelgeving. In de voorgaande edities hebben we steeds een onderdeel van DORA uitgelicht en besproken wat er wordt verwacht van ondernemingen. Deze laatste editie willen we gebruiken om toe te lichten wat ondernemingen kunnen verwachten in 2025. Hierbij zullen we toelichten op welke manier de AFM toezicht zal houden op DORA en welke informatieverzoeken ondernemingen kunnen verwachten vanuit de Europese toezichthouders (EIOPA, ESMA en EBA – samen de ESAs). Daarnaast zullen wij in deze editie een aantal praktische zaken bespreken, zoals de manier waarop ondernemingen informatie moeten aanleveren bij de AFM.

Het afgelopen jaar hebben de ESAs zich beziggehouden met de ontwikkeling van de *Regulatory Technical Standards* (RTS) en *Implementing Technical Standards* (ITS). De RTS'en en ITS'en zijn in twee batches verdeeld en zijn inmiddels allemaal aan de Europese Commissie voorgelegd. De Europese Commissie neemt het uiteindelijke besluit over het al dan niet aannemen van deze nadere regelgeving. De RTS'en en ITS in de eerste batch zijn al geadapteerd en zijn daarmee definitief. Onderdeel van deze eerste batch was de ITS voor het informatieregister (*register of information*), welke onlangs is geadapteerd door de Europese Commissie. Voor de RTS'en en ITS in de tweede batch is er nog geen besluit genomen door de Europese Commissie. De verwachting is echter dat deze op hoofdlijnen gelijk zullen blijven.

Om tijdig te voldoen aan de vereisten in DORA is het belangrijk dat ondernemingen al begonnen zijn met de implementatie van de vereisten in de verordening en de RTS'en en gebruikmaken van de templates in de ITS'en. Aangezien de nadere regelgeving op hoofdlijnen gelijk zal blijven, kunnen ondernemingen nu al aan de slag met de implementatie van deze vereisten. Ondernemingen die wachten tot het besluit van de Europese Commissie om te beginnen met de implementatie, zullen naar alle waarschijnlijkheid niet op tijd voldoen aan de DORA-vereisten.

JANUARI 2025

AFM

2. Vooruitblik 2025

2.1 Wat kunt u verwachten in 2025

Ondernemingen kunnen nu al aan de slag met:
- Vullen van het *register of information;*
- Inrichten van processen om incidenten te melden.

Wanneer DORA van toepassing wordt, zullen de nationale toezichthouders beginnen met hun toezichtwerkzaamheden voor DORA. Denk hierbij aan het opzetten van onderzoeken om vast te stellen of ondernemingen voldoen aan de vereisten, maar ook het verzamelen en controleren van informatie die vanuit de ESAs wordt opgevraagd.

Informatieregister

De eerste uitvraag waar ondernemingen mee te maken zullen krijgen in 2025, is het *register of information*. De nationale toezichthouders dienen het informatieregister uiterlijk 30 april 2025 aan te leveren bij de ESAs. Om de registers tijdig aan te kunnen leveren bij de ESAs, zal de AFM snel nadat DORA van toepassing, wordt een informatieverzoek versturen naar alle ondernemingen die een vergunning hebben bij de AFM en onder DORA vallen. Om het register op tijd te kunnen delen, moeten ondernemingen al bezig zijn met het opstellen hiervan.

De AFM en DNB zullen het volledige *register of information* op jaarlijkse basis opvragen bij ondernemingen. De AFM en DNB zullen vervolgens de informatieregisters controleren op de volledigheid waarna deze worden doorgestuurd naar de ESAs. Wanneer velden ontbreken of niet zijn ingevuld, kan het register niet worden gedeeld met de ESAs en zal de onderneming het volledige informatieregister opnieuw moeten delen met de toezichthouder. Het is daarom belangrijk om te controleren of het register volledig is, voordat deze met de AFM of DNB wordt gedeeld.

Op basis van de informatie uit de registers, zullen de ESAs de ICT-dienstverleners aanwijzen die als kritiek worden gezien voor de financiële sector. Bij de aanwijzing van de kritieke ICT-dienstverleners, kijken de ESAs naar het (systemische) effect op de stabiliteit, continuïteit en kwaliteit van de financiële dienstverlening in het geval van een ernstige verstoring bij de ICT-dienstverlener. Daarnaast kijken de ESAs bij het bepalen van de kritieke ICT-dienstverleners naar het belang van de financiële entiteiten voor de sector die afhankelijk zijn van de derde aanbieder van ICT-diensten. Tot slot wordt rekening gehouden met de mate waarin financiële entiteiten afhankelijk zijn van de ICT-diensten en de vervangbaarheid van de derde aanbieder van ICT-diensten. De ESAs zullen zelf toezicht houden op de aangewezen kritieke ICT-dienstverleners. Hoofdstuk 5, afdeling 2 (artikel 31-44) van de verordening beschrijft onder meer de taken en bevoegdheden van de ESAs die toezicht gaan houden op deze kritieke ICT-dienstverleners. Daarnaast wordt in dit hoofdstuk beschreven op welke manier toezicht kan worden gehouden op deze ondernemingen.

ICT-gerelateerde incidenten

Een andere verplichting voor ondernemingen is het melden van ernstige ICT-incidenten. Wanneer een ICT-gerelateerd incident heeft plaatsgevonden moeten ondernemingen aan de hand van criteria [1] bepalen of er sprake is van een ernstig ICT-incident. Op het moment dat een onderneming heeft bepaald dat er sprake is geweest van een ernstig ICT-incident, moeten zij dit binnen 4 uur bij de relevante toezichthouder (AFM of DNB) melden. De (Europese) toezichthouder kan aan de hand van de initiële melding en de vervolgrapportages, bepalen of het een ICT-incident betreft dat invloed heeft op de hele sector. Op basis van deze beoordeling kan de toezichthouder bepalen of er aanvullende maatregelen moeten worden genomen. Daarnaast kunnen ondernemingen significante cyberdreigingen op vrijwillige basis melden.

1 Zie de RTS voor het classificeren van ICT-gerelateerde incidenten (Regulatory Technical Standards (RTS) en Implementing Technical Standards (ITS))

TLPT

Een aantal ondernemingen zullen worden aangewezen voor *threat led penetration testing* (TLPT). Voor deze ondernemingen gelden, naast de bovenstaande verplichtingen, aanvullende vereisten met betrekking tot het testen van de digitale operationele weerbaarheid. Ondernemingen hoeven alleen aan deze vereisten te voldoen wanneer ze hiervan op de hoogte worden gebracht door de toezichthouder middels een aanwijzingsbrief. Zodra de RTS voor TLPT wordt goedgekeurd door de Europese Commissie, zal de AFM contact opnemen met de ondernemingen die worden aangewezen voor TLPT. In overleg met de onderneming wordt gepland wanneer de test plaatsvindt.

2.2 Wat gaat de AFM doen?

Ondernemingen kunnen nu al aan de slag met:
- Toegang tot het DORA-portaal controleren.

Net als veel ondernemingen heeft de AFM zich de afgelopen tweeënhalf jaar voorbereid op de komst van DORA. Een groot onderdeel van dit programma bestond uit het voorbereiden van de sector op DORA. Denk hierbij aan verschillende publicaties (zoals de DORA-updates), gesprekken met ondernemingen tijdens seminars en een-op-een gesprekken met ondernemingen.

Daarnaast heeft de AFM zich intern voorbereid op het toezicht op DORA. Zo is er een DORA-portaal ontwikkeld waar ondernemingen meldingen kunnen doen bij de AFM, maar is er ook veel tijd besteed aan het voorbereiden van onze toezichthouders op DORA. In het eerste kwartaal van 2025 wordt het DORA-programma bij de AFM afgerond. Vanaf dat moment zal de AFM overgaan op doorlopend DORA-toezicht. Onze toezicht werkzaamheden zullen vanaf dat moment voor het grootste deel bestaan uit het uitvoeren van onderzoeken, het behandelen van ICT-incidenten, de verwerking van het *register of information* en het beoordelen van vergunningsaanvragen.

DORA-onderzoeken

Om vast te stellen of ondernemingen voldoen aan de vereisten zullen zowel thematische onderzoeken als instellingsgerichte onderzoeken worden uitgevoerd. Bij een thematisch onderzoek zullen een aantal ondernemingen worden geselecteerd en ligt de focus op een onderwerp uit DORA. Dit kan bijvoorbeeld een onderzoek zijn naar *business continuity management* of het controleren van overeenkomsten met ICT-dienstverleners.

Tijdens een instellingsgericht onderzoek zal slechts één onderneming worden geselecteerd en zullen stukken worden opgevraagd die betrekking hebben op een onderdeel uit DORA (bijvoorbeeld ICT-risicobeheer of het testen van de digitale operationele weerbaarheid). Dit type onderzoek kan per instelling verschillen. In beide gevallen blijft het uitgangspunt dat er op risico's gebaseerd en proportioneel toezicht zal worden gehouden. Dit betekent dat de AFM toezichtcapaciteit zal inzetten waar de grootste risico's worden verwacht.

Meldingen

Een tweede onderdeel van ons DORA-toezicht, is het behandelen van ICT-incidentmeldingen. Op het moment dat een ernstig ICT-gerelateerd incident heeft plaatsgevonden, moeten ondernemingen 4 uur na de classificatie van het incident een eerste kennisgeving delen via het DORA-portaal. Daarnaast moet een tussentijds verslag en eindverslag respectievelijk 72 uur en 1 maand na de classificatie van het incident worden gedeeld met de AFM.

De AFM zal bij de beoordeling van deze rapportages kijken naar de volledigheid van het incidentenrapport. Daarnaast wordt beoordeeld of het incident (en de impact hiervan) voldoende worden beschreven in de rapportage. Wanneer dit niet het geval is, zal de AFM aanvullende informatie opvragen om dit te achterhalen. Naast de meldingen voor ernstige ICT-gerelateerde incidenten, kunnen financiële ondernemingen op vrijwillige basis cyberdreigingen melden. Beide soorten meldingen zullen voornamelijk worden gebruikt om te bepalen of er ICT-incidenten hebben plaatsgevonden of cyberdreigingen actief zijn die impact (kunnen) hebben op de financiële sector.

Nieuwe overeenkomsten met ICT-dienstverleners dienen eveneens te worden gemeld bij de AFM. Deze kunnen net als ICT-incidenten en cyberdreigingen in het DORA-portaal worden gemeld. Bij het melden van een overeenkomst met een ICT-dienstverlener, kunnen ondernemingen kiezen of het gaat om een nieuwe overeenkomst of dat er een bestaande overeenkomst is waarbij de functie die deze ICT-dienst ondersteunt, belangrijk of kritiek is geworden. Afhankelijk van deze keuze zal er worden gevraagd naar het type ICT-dienst dat wordt uitbesteed of de functie die belangrijk of kritiek is geworden. Net als bij ernstige ICT-incidenten, zal de AFM de melding beoordelen en eventueel extra informatie opvragen.

Financiële instellingen die onder DORA vallen en een vergunning hebben bij de AFM krijgen vanaf 17 januari 2025 toegang tot de DORA-pagina in het portaal van de AFM. Dit zal onderdeel zijn van het AFM-portaal waar ondernemingen nu al toegang tot hebben. Wanneer u op 17 januari 2025 geen toegang tot de DORA-pagina heeft, is het belangrijk om dit op tijd te melden, zodat u de verplichte meldingen in dit portaal kunt doorgeven.

Vergunningsaanvragen

Voor ondernemingen die onder DORA gaan vallen, toetst de AFM sinds 1 augustus 2024 een aantal DORA-vereisten tijdens de vergunningsaanvraag. Het doel hiervan is om ondernemingen die in aanloop naar januari 2025 een vergunning verkrijgen, te ondersteunen in het tijdig voldoen aan de DORA-vereisten. Tijdens de vergunningsaanvraag wordt onder meer gekeken naar het bestaan van bepaalde beleidstukken en procedures die verplicht zijn onder DORA. Na 17 januari 2025 zal de AFM deze vereisten blijven toetsen tijdens vergunningsaanvragen. Het kan daarom helpen om voor de vergunningsaanvraag al te kijken aan welke DORA vereisten de onderneming moet gaan voldoen. Tijdens de vergunningsaanvraag worden bestuurders getoetst op hun kennisniveau en vaardigheden om ICT-risico's te begrijpen en beoordelen. DORA verwacht van bestuurders dat zij zelf over deze kennis en vaardigheden beschikken en dat zij regelmatig opleidingen volgen die hen in staat stellen om ICT-risico's adequaat te kunnen beheren.

TLPT

De ondernemingen die worden aangewezen voor TLPT zullen na adaptie van de TLPT RTS door de Europese Commissie een bericht krijgen van de AFM dat zij een verplichte TLPT moeten uitvoeren. Vervolgens bepalen de testmanagers van de AFM, in overleg met de onderneming, in welke periode deze test moet worden uitgevoerd. De testmanagers begeleiden tijdens de voorbereiding en de uitvoering van de testwerkzaamheden de onderneming om te waarborgen dat de test voldoet aan de vereisten in de verordening en de RTS. Alle rapportages die, als onderdeel van de test, moeten worden gedeeld met de testmanagers, moeten worden ingediend in het DORA-portaal. Na de succesvolle afronding van de test, ontvangt de onderneming een attest, waarmee kan worden aangetoond dat er is voldaan aan de vereisten met betrekking tot TLPT.

3. Vooruitblik

Dit was de laatste editie in de reeks DORA-updates van de AFM. In de komende periode zullen de laatste RTS'en en ITS'en worden beoordeeld door de Europese Commissie. Voor meer informatie over de ontwikkelingen in de wet- en regelgeving kunt u de DORA-pagina op de AFM-website raadplegen. Daarnaast kunt u de ontwikkelingen op de website van de ESAs in de gaten houden:

- Digital Operational Resilience Act (DORA) - AFM
- Digital Operational Resilience Act (DORA) - EBA
- Digital Operational Resilience Act (DORA) - EIOPA
- Digital Operational Resilience Act (DORA) - ESMA

Verdere vragen?

Neem contact op met het ondernemersloket van de AFM.