RAPPORT ANALYSE

DORA-update 7

In het kort - De afgelopen anderhalf jaar stond voor veel financiële ondernemingen in het teken van de implementatie van de Digital Operational Resilience Act (DORA). Van de uitvraag van het informatieregister en de eerste ervaringen met het DORA-toezicht tot aan verdere verduidelijkingen in de onderliggende regelgeving: de sector heeft in korte tijd belangrijke stappen gezet. Tegelijkertijd zien wij een aantal verbeterpunten waar ondernemingen nog mee aan de slag kunnen. In deze DORA-update blikken we terug op de belangrijkste ontwikkelingen, ervaringen en aandachtspunten sinds de invoering van DORA.

AUGUSTUS | 2026

AFM

Inhoudsopgave

1. DORA-informatieregister

Uitvraag

De AFM heeft twee keer het informatieregister (register of information) uitgevraagd bij alle DORA-plichtige ondernemingen. In het eerste jaar werd 40% van de registers goedgekeurd door de European Banking Authority (EBA). In 2026 is dit gestegen naar 94% van de registers.

De uitvraag naar het informatieregister was de eerste (en grootste) uitvraag waar ondernemingen mee te maken kregen nadat DORA van toepassing werd. Tijdens deze jaarlijkse uitvraag, vraagt de EBA aan alle nationale toezichthouders om de informatieregisters van DORA-plichtige ondernemingen op te vragen en met hen te delen. De EBA gebruikt deze registers vervolgens om te bepalen welke kritieke derde-aanbieders van ICT-diensten onder het toezicht van de Europese toezichthouders komen te staan (zie DORA Oversight activiteiten' hieronder).

Aangezien ondernemingen al in het eerste kwartaal van 2025 hun informatieregister moesten aanleveren, was er nog veel onduidelijkheid over het xBRL-CSV-formaat en de wijze waarop het register moest worden ingevuld. Wij hebben daarom voor 2025 besloten dat wij eenmalig de conversie naar xBRL-CSV op ons zouden nemen. Dit betekende dat instellingen hun informatieregister in Excel konden aanleveren, waardoor zij meer tijd konden besteden aan het juist invullen van het register. Uiteindelijk werd 40% van de aangeleverde registers in 2025 goedgekeurd door de EBA.

Voor de uitvraag in 2026 moesten ondernemingen voor het eerst zelf het informatieregister in xBRL-CSV aanleveren. Tegelijkertijd hebben wij het proces aan onze kant zodanig ingericht dat de registers automatisch naar de EBA werden verstuurd en de feedback automatisch werd opgehaald. Hierdoor konden ondernemingen zo vaak als nodig een nieuwe versie indienen. In 2026 werd 94% van de informatieregisters goedgekeurd door de EBA. Deze stijging ten opzichte van 2025 kan (deels) worden verklaard doordat ondernemingen in het tweede jaar beter wisten wat zij konden verwachten van de uitvraag. Daarnaast merkten wij dat veel ondernemingen in 2026 gebruikmaakten van externe partijen die de conversie naar xBRL-CSV verzorgden en hen hielpen bij het invullen van het register.

Q&A sessie

Tijdens de uitvraag van het informatieregister in 2026 organiseerden wij een Q&A-sessie waarbij ondernemingen de mogelijkheid kregen om vragen te stellen over het register. Het doel hiervan was om in een korte tijd zoveel mogelijk vragen te beantwoorden. Daarnaast hielp de Q&A-sessie ons om vast te stellen waar de grootste knelpunten lagen bij het invullen van het register.

Na de deadline hebben we aan de hand van de Q&A-sessie en de ingediende registers een overzicht gemaakt van de meest voorkomende fouten en hoe deze kunnen worden opgelost. Dit overzicht is opgenomen in de vragen en antwoorden van de Q&A-sessie (pdf, 240 kB).[1]

[1] https://www.afm.nl/~/profmedia/files/onderwerpen/dora/20260305-qa-dora-sessie.pdf

DORA Oversight activiteiten

De European Supervisory Authorities (EBA, EIOPA en ESMA – gezamenlijk de ESAs) hebben op basis van hun analyse van de informatieregisters uit de verschillende lidstaten een lijst opgesteld van negentien kritieke derde-aanbieders van ICT-diensten.[2] Deze ondernemingen komen onder het directe toezicht van de ESA's te staan (het DORA Oversight Framework). Als nationale toezichthouder dragen wij bij aan Joint Examination Teams (JETs) die DORA Oversight activiteiten uitvoeren bij verschillende kritieke derde-aanbieders van ICT-diensten.

De DORA Oversight activiteiten kunnen worden onderverdeeld in de volgende onderdelen:

- Doorlopende reguliere monitoring. Dit omvat onder meer periodieke informatieverzameling en een doorlopende dialoog met *Critical ICT Third-Party Providers* (CTPPs) over de actuele stand van zaken en opkomende risico's, zoals operationele incidenten of nieuwe dreigingen.
- Algemene onderzoeken. Dit zijn meer diepgaande onderzoeken naar specifieke risicogebieden. Deze worden uitgevoerd overeenkomstig het toezichtplan en zijn gericht op het aanpakken van nieuw geïdentificeerde aandachtspunten of het beoordelen van herstelmaatregelen naar aanleiding van eerdere onderzoeken.
- Inspecties. Inspecties zijn vergelijkbaar met algemene onderzoeken, maar zijn ingrijpender en gericht op een diepgaande beoordeling van de risico's die dienstverleners voor financiële instellingen vormen. Inspecties omvatten onder meer de bevoegdheid om dossiers, gegevens en andere relevante documentatie op te vragen.
- Informatieverzoeken. Dit biedt de mogelijkheid om informatie bij CTPPs op te vragen zonder een algemeen onderzoek of inspectie te starten. Informatieverzoeken kunnen bijvoorbeeld worden ingezet om een specifieke situatie te verduidelijken waarvoor toezichthouders aanvullende informatie of toelichting van de CTPP nodig hebben.
- Aanbevelingen. Aanbevelingen richten zich op geconstateerde tekortkomingen bij een CTPP binnen specifieke beoordelingsgebieden. De opvolging van aanbevelingen vindt plaats via de doorlopende monitoring en rapportages waarin de getroffen maatregelen en doorgevoerde verbeteringen naar aanleiding van de aanbevelingen worden beschreven.

Meer informatie over de DORA Oversight activiteiten zijn te vinden in de richtlijn die de ESAs eerder hebben gepubliceerd.[3]

[2] The European Supervisory Authorities designate critical ICT third-party providers under the Digital Operational Resilience Act | European Banking Authority

[3] JC 2025 29 Guide on DORA oversight activities

2. DORA-toezicht

In 2025 heeft hebben wij ons in het toezicht op de naleving van de DORA-vereisten gericht op het ICT-risicobeheer (hoofdstuk II van de verordening). Tijdens onze onderzoeken hebben wij beleidsstukken en procedures van ondernemingen opgevraagd en beoordeeld in hoeverre deze documenten voldoen aan de eisen die DORA stelt. Daarbij viel op dat financiële entiteiten niet altijd beschikken over alle beleidsstukken en procedures die op grond van DORA vereist zijn. Daarnaast voldeden niet alle aangeleverde beleidsstukken en procedures aan de vereisten van de verordening en de gedelegeerde Verordening (EU) 2024/1774 van de Commissie.

Wij adviseren ondernemingen daarom periodiek een self-assessment uit te voeren, waarbij wordt nagegaan of de bestaande beleidsstukken en procedures voldoen aan de DORA-vereisten. Door dit regelmatig te doen, bijvoorbeeld tijdens de verplichte evaluatie van het ICT risk management framework, kunnen financiële entiteiten er ook voor zorgen dat hun beleid en procedures aansluiten bij actuele risico's en de feitelijke werkwijze van de onderneming.

Verder merken wij op dat financiële entiteiten die onderdeel uitmaken van een grotere groep, vaak gebruikmaken van beleidsstukken en procedures die op groepsniveau worden opgesteld. In veel gevallen is dit efficiënter dan wanneer individuele ondernemingen binnen de groep zelf beleid ontwikkelen. De DORA-plichtige onderneming (vergunninghouder) blijft echter altijd verantwoordelijk voor de naleving van de DORA-vereisten. Het is daarom van belang dat ondernemingen zelf controleren of alle relevante DORA-vereisten volledig zijn verwerkt in hun beleidsstukken en procedures.

Tot slot constateren wij dat de meeste ondernemingen voldoende maatregelen hebben getroffen om (mogelijke) verstoringen tijdig te signaleren. Tegelijkertijd zien wij dat ondernemingen vaak nog onvoldoende preventieve maatregelen hebben ingericht om dergelijke verstoringen te voorkomen. Met name op het gebied van logische toegangsbeveiliging en patch- en vulnerabilitymanagement zijn nog verbeteringen mogelijk.

TLPT

De eerste ondernemingen zijn in 2025 gestart met Threat-Led Penatration Testing (TLPT). Dit betreft uitgebreide tests waarbij tactieken, technieken en procedures die in de praktijk door dreigingsactoren (zoals hackers) worden gebruikt, worden nagebootst. Deze tests vinden plaats onder begeleiding van de TLPT-testmanagers van de AFM.

Ondernemingen die wij hebben aangewezen voor TLPT moeten periodiek een test uitvoeren die voldoet aan de vereisten van DORA. Gedurende de test controleren de DORA TLPT-testmanagers of de werkzaamheden worden uitgevoerd overeenkomstig de vereisten uit de gedelegeerde verordening (EU) 2025/1190 van de Commissie.[4] Aan het einde van de test ontvangen ondernemingen een attestatie waarmee zij kunnen aantonen dat zij met succes een TLPT-test hebben uitgevoerd.

Na afronding van de test worden de resultaten, waaronder de *Test Summary* en het *Remediation Plan*, gedeeld met de toezichtafdelingen van de AFM. Hierdoor kunnen de bevindingen en de uitvoering van het herstelplan worden opgevolgd.

[4] Delegated regulation - EU - 2025/1190 - EN - EUR-Lex

DORA-meldingen

In 2025 hebben wij 123 DORA-meldingen ontvangen van ondernemingen die onder ons toezicht staan. Hiervan hadden 65 meldingen betrekking op ernstige ICT-gerelateerde incidenten. 54 meldingen gingen over nieuwe overeenkomsten met ICT-dienstverleners. Vier meldingen betroffen significante cyberdreigingen.

Aangezien het aantal incidentmeldingen achterblijft bij onze verwachtingen, adviseren wij ondernemingen om (nogmaals) te controleren of het incidentenproces juist is ingericht. Daarbij is het van belang dat het proces zodanig is ingericht dat incidenten tijdig kunnen worden gedetecteerd, geregistreerd, beheerst, geclassificeerd en gemeld.

Drie type meldingen

In DORA worden drie typen meldingen onderscheiden die ondernemingen doorlopend moeten of kunnen doen aan de toezichthouder. Het eerste type melding betreft ernstige ICT-gerelateerde incidenten. Deze moeten uiterlijk vier uur na de classificatie van het incident, of binnen 24 uur na de detectie ervan, worden gemeld. Vervolgens moet uiterlijk 72 uur na de initiële melding een tussentijds verslag worden ingediend. Uiterlijk één maand na de classificatie moet een eindrapportage worden aangeleverd.

Gezien deze strakke termijnen is het van belang dat ondernemingen hun incidentenproces zodanig inrichten dat verplichte meldingen tijdig bij de toezichthouder kunnen worden ingediend.

Naast het melden van incidenten zijn ondernemingen op grond van DORA verplicht om ten minste eenmaal per jaar alle nieuwe overeenkomsten te melden die zijn gesloten met derde-aanbieders van ICT-diensten. Tot slot kunnen ondernemingen op vrijwillige basis significante cyberdreigingen melden die relevant zijn voor de financiële sector.

Meer informatie over de verplichtingen met betrekking tot DORA-meldingen is te vinden in de artikelen 18, 19 en 28, derde lid, van de verordening en de gedelegeerde verordening inzake het melden van ernstige ICT-gerelateerde incidenten en significante cyberdreigingen[5].

[5] Delegated regulation - EU - 2025/301 - EN - EUR-Lex

3. Ontwikkelingen voor verzekeringstussenpersonen

Lange tijd bestond onduidelijkheid over de wijze waarop moet worden bepaald of verzekeringstussenpersonen onder DORA vallen. De ESAs hebben hierover inmiddels meer duidelijkheid gegeven in Q&A DORA099[6] en DORA237[7].

In de verordening is namelijk een uitzondering opgenomen voor kleine en middelgrote verzekeringstussenpersonen (minder dan 250 fte en een jaaromzet van minder dan €50 miljoen en/of een balanstotaal van minder dan €43 miljoen). Omdat het bemiddelen in verzekeringen voor sommige verzekeringstussenpersonen slechts een beperkt onderdeel van hun activiteiten vormt, ontstond de vraag hoe deze criteria moeten worden toegepast op ondernemingen waarbij het bemiddelen in verzekeringen niet de primaire activiteit is. Daarnaast bestond onduidelijkheid over de wijze waarop het aantal fte, de jaaromzet en het balanstotaal moeten worden berekend voor ondernemingen die deel uitmaken van een groep.

Q&A DORA237 geeft antwoord op de vraag hoe het aantal fte, de jaaromzet en het balanstotaal moeten worden berekend wanneer het bemiddelen in verzekeringen slechts een beperkt deel van de totale activiteiten van een onderneming vormt. Uit het antwoord van EIOPA blijkt dat in beginsel de cijfers van de gehele onderneming moeten worden meegenomen bij deze beoordeling. Vanuit het proportionaliteitsbeginsel moeten ondernemingen waarvan de verzekeringsbemiddelingsactiviteiten slechts een beperkte omvang hebben, echter uitsluitend rekening houden met de activiteiten en middelen die worden ingezet voor die verzekeringsactiviteiten.

Voor verzekeringstussenpersonen die deel uitmaken van een groep, moet eerst worden vastgesteld of sprake is van een financiële groep of een niet-financiële groep. Wanneer een onderneming deel uitmaakt van een niet-financiële groep, moet enkel worden gekeken naar de individuele onderneming. Voor financiële entiteiten die wel deel uitmaken van een financiële groep, moet worden gekeken naar het belang dat zij hebben in andere ondernemingen of het belang dat andere ondernemingen in haar houden.

Wanneer een onderneming tussen de 25% en 50% van de aandelen of stemrechten van een andere onderneming bezit, worden deze ondernemingen aangemerkt als partnerondernemingen (*partner entities*). In dat geval moeten het aantal fte, de jaaromzet en het balanstotaal van de partneronderneming naar rato worden meegenomen in de berekening van de drempelwaarden. Bij verbonden ondernemingen (*linked entities*), waarbij sprake is van een meerderheidsbelang of zeggenschap, moeten het aantal fte, de jaaromzet en het balanstotaal van de verbonden onderneming volledig worden meegenomen in de berekening.

[6] 3100 - DORA099 - European Insurance and Occupational Pensions Authority
[7] DORA237 - 3350 - European Insurance and Occupational Pensions Authority

4. Tot slot

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

Verdere vragen? Neem contact op met het ondernemersloket van de AFM.

Links naar eerdere publicaties:
Publicaties
Handelssystemen vragen om scherpere ICT-risicobeheersing onder DORA
SREP Marktbeeld: beheersing vraagt meer dan alleen beleid
Preparations for reporting of DORA registers of information | European Banking Authority