Aan de slag met DORA: Beheer van ICT-risico van derde aanbieders

December 2023

Dit is de tweede editie in een reeks AFM-publicaties over de Digital Operational Resilience Act (DORA). Deze reeks is bedoeld voor alle ondernemingen die vanaf 2025 aan deze Europese verordening moeten voldoen. In deze editie gaan we in op het beheren van ICT-risico's van derde aanbieders. Op deze manier kunnen ondernemingen analyseren waar ze staan op dit vlak en welke stappen ze eventueel nog moeten zetten om aan de verordening te voldoen.

Lees verder

AFM

Inhoud

01 De rol van derde aanbieders in DORA

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, waaronder voor het beheren van de risico's die voortkomen uit het gebruik van derde aanbieders (ofwel *third party* risk). Ondernemingen kunnen nu al analyseren of ze op dit punt aan de DORA-vereisten voldoen om vervolgens (indien nodig) tot actie over te gaan. Om in januari 2025 aan DORA te voldoen, is het raadzaam zo vroeg mogelijk te beginnen.

DORA besteedt veel aandacht aan het zogeheten *third party risk* om ketenrisico's zo veel mogelijk te beperken. De vereisten zijn terug te vinden in hoofdstuk V (artikel 28 t/m 44) van de verordening. Deze artikelen gaan onder meer in op de benodigde beleidsstukken, risicoanalyses en contractuele bepalingen. Daarnaast wordt ook het oversight-kader voor kritieke derde aanbieders van ICT-diensten omschreven.

Een deel van de onderwerpen wordt op dit moment door de *European Supervisory Authorities* (ESA's) in meer detail uitgewerkt in Regulatory en Implementing Technical Standards (RTS en ITS). Op het moment van publicatie van deze editie zijn enkele van deze producten al door de ESA's aan de markt voorgelegd ter consultatie. De bijbehorende tijdslijnen zijn in tabel 1 opgenomen.

In de volgende secties staan we stil bij de genoemde artikelen en bespreken waar organisaties nu al mee kunnen starten om tijdig aan DORA te voldoen. Ook behandelen we op welke wijze proportionaliteit terugkomt binnen dit onderwerp.

Tabel 1

Aanvullende uitwerkingen	Onderwerp	Afgerond
RTS voor artikel 28(1)	Policy on ICT services performed by 3rd parties	Uiterlijk januari 2024
ITS voor artikel 28(9)	Templates for the register of information	Uiterlijk jan 2024
RTS voor artikel 30(5)	Elements when sub-contracting critical or important functions	Uiterlijk juli 2024
Call for advice t.b.v. artikel 31(8)	Criticality criteria	September 2023
Selectie van kritieke ICT-dienstverleners t.b.v. artikel 31	n.v.t.	Geen tijdslijn gecommuniceerd
Guidelines t.b.v. artikel 32(7)	Cooperation between ESA's and CA's regarding the structure of oversights	Uiterlijk juli 2024
RTS voor artikel 41	Information on oversight conduct	Uiterlijk juli 2024
Call for advice t.b.v. artikel 43(2)	Oversight fees	September 2023

02 Aan de slag met *third party risk*

Basisbeginselen voor het beheren van ICT-risico van derde aanbieders

Ondernemingen kunnen nu al aan de slag met:

- Het kader voor ICT-risicobeheer (waaronder op het gebied van uitbestedingen);
- De strategie voor het beheersen van ICT-risico's van derde aanbieders;
- Het register van alle contractuele overeenkomsten met derde aanbieders van ICT-diensten;
- De exit-strategie, in het geval dat derde aanbieders kritieke of belangrijke functies ondersteunen.

Artikel 28 en 29 van DORA beschrijven verschillende basisbeginselen voor het beheersen van *third party risk*. Om in de hele keten weerbaar te zijn tegen cyberdreigingen en ICT-verstoringen, is het belangrijk om aandacht te besteden aan de risico's van het afnemen van ICT-diensten van derde aanbieders. Deze artikelen gaan in op de maatregelen die een onderneming zou moeten treffen voorafgaand aan het sluiten van een overeenkomst met een derde aanbieder. Hierbij gelden dezelfde eisen voor externe overeenkomsten als voor overeenkomsten binnen dezelfde groep *(intragroup agreements).*

Om te beginnen moeten ondernemingen expliciet aandacht besteden aan de ICT-risico's die voortkomen uit het gebruiken van diensten van derde aanbieders. Deze risicoanalyse staat niet op zichzelf, maar moet onderdeel zijn van het organisatiebrede kader voor ICT-risicobeheer. Daarnaast verwacht DORA dat ondernemingen een strategie ontwikkelen voor het beheersen van *third party risks,* waarbij de risico's van het uitbesteden van kritieke diensten regelmatig worden herzien. Micro-ondernemingen zijn uitgezonderd[1] van de verplichting om deze strategie te ontwikkelen.

Alle contractuele overeenkomsten voor het leveren van ICT-diensten moeten worden vastgelegd in een register. Ondernemingen moeten daarbij opnemen of de afgenomen diensten kritieke of belangrijke activiteiten ondersteunen. Toezichthouders kunnen dit register opvragen. Het register is van belang voor de interne beheersing van een instelling, maar zal ook door de ESA's worden gebruikt om kritieke dienstverleners (ofwel CTPP's: Critical Third Party service Provider) van de Europese Unie aan te wijzen. Zie hiervoor ook sectie 4 van deze DORA-update.
Daarnaast vereist DORA dat ondernemingen jaarlijks aan de toezichthouder rapporteren welke *third party* ICT-overeenkomsten dat jaar zijn afgesloten. Overeenkomsten met betrekking tot kritieke of belangrijke functies moeten ook tussendoor actief gemeld worden bij de toezichthouder.

Voorafgaand aan het afsluiten van overeenkomsten met derde aanbieders moeten verschillende aspecten worden geanalyseerd, zoals het benodigde ICT-beveiligingsniveau en de gewenste frequentie en scope van audits en inspecties. Het is ook belangrijk om rekening te houden met eventuele concentratierisico's. Verdere onderuitbesteding door de dienstverlener kan hier ook invloed op hebben. Ondernemingen moeten daarnaast ook over een exit-strategie beschikken wanneer derde aanbieders kritieke of belangrijke functies ondersteunen. Daarbij moet rekening worden gehouden met risico's die zich bij de dienstverlener voor kunnen doen, zoals een verstoring van de levering, verslechtering van de kwaliteit of de (voortijdige) beëindiging van de overeenkomst.

1 Dit geldt ook voor ondernemingen uit de eerste alinea van art 16(1): kleine en niet-verweven beleggingsondernemingen, betalingsinstellingen die krachtens Richtlijn (EU) 2015/2366 zijn vrijgesteld; instellingen die krachtens Richtlijn 2013/36/EU zijn vrijgesteld en waarvoor de lidstaten hebben besloten de in artikel 2, lid 4, van deze verordening bedoelde optie niet toe te passen; instellingen voor elektronisch geld die krachtens Richtlijn 2009/110/EG zijn vrijgesteld, en kleine instellingen voor bedrijfspensioenvoorziening.

De ESA's ontwikkelen momenteel een standaardmodel voor het register van contractuele overeenkomsten. Ook worden de uitgangspunten voor *third party risk management* verder uitgewerkt in een RTS. In tabel 2 zijn de tijdslijnen hiervoor opgenomen. Op het moment van publicatie zijn deze stukken al door de ESA's gepubliceerd ter consultatie.

Tabel 2

Aanvullende uitwerkingen	Beschrijving	Afgerond
RTS voor artikel 28(1)	Policy on ICT services performed by 3rd parties	Uiterlijk januari 2024
ITS voor artikel 28(9)	Templates for the register of information	Uiterlijk januari 2024

Belangrijke contractuele bepalingen om schriftelijk vast te stellen

Ondernemingen kunnen nu al aan de slag met:

- De analyse of bestaande contractuele overeenkomsten in lijn zijn met de vereisten uit DORA.

In artikel 30 van DORA zijn verschillende bepalingen opgenomen die ondernemingen op moeten nemen in contractuele overeenkomsten met derde aanbieders. Hierbij wordt onderscheid gemaakt tussen onderdelen die in alle overeenkomsten moeten worden opgenomen, en aanvullende verplichtingen voor overeenkomsten die kritieke of belangrijke functies ondersteunen.

Voorbeelden van onderdelen die altijd in overeenkomsten moeten worden opgenomen zijn:

- De rechten en plichten van beide partijen;
- Een volledige beschrijving van geleverde diensten;
- De regio's en/of landen waaraan de diensten moeten worden geleverd en gegevens moeten worden verwerkt;
- Het te leveren dienstenniveau;
- De mate van gegevensbescherming, in termen van beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit;
- De bijstand bij incidenten;
- De beëindigingsrechten en bijbehorende opzegtermijnen.

Daarnaast moet bij het uitbesteden van diensten die kritieke of belangrijke functies ondersteunen, aanvullend bijvoorbeeld het volgende worden vastgelegd:

- De rapportageverplichting van de dienstverlener;
- De verplichting voor de dienstverlener om bedrijfsnoodplannen te ontwikkelen en te testen;
- De verplichting om mee te werken aan eventuele *Thread Lead Penetration Tests* (TLPT's) van de financiële instelling[2];
- Het recht van inspectie en audit door de financiële entiteit of een daartoe aangestelde derde partij;
- Ook worden aanvullende en verdiepende eisen gesteld aan de bepalingen die voor alle uitbestedingen moeten gelden, zoals het uitwerken van de geleverde diensten door middel van nauwkeurige prestatiedoelstellingen.

Micro-ondernemingen kunnen met de dienstverlener overeenkomen dat audits en inspecties worden uitgevoerd door een door de dienstverlener aangewezen onafhankelijke partij, in plaats van dat micro-ondernemingen deze zelf uitvoeren Hierbij moeten micro-ondernemingen wel altijd de benodigde informatie kunnen opvragen bij deze partij.

2 Zie ook artikel 26 van DORA: een deel van de ondernemingen wordt verplicht om geavanceerde tests uit te voeren op basis van *Thread Lead Penetration Testing*.

Ter aanvulling van deze vereisten werken de ESA's momenteel de voorwaarden uit voor het onderuitbesteden van diensten die kritieke of belangrijke functies ondersteunen. In tabel 3 zijn de tijdslijnen hiervoor opgenomen.

Tabel 3

Aanvullende uitwerkingen	Beschrijving	Afgerond
RTS voor artikel 30(5)	Elements when sub-contracting critical or important functions	Uiterlijk juli 2024

Kritieke derde aanbieders van ICT-diensten nu ook onder toezicht

Een groot deel van de ICT-diensten van de financiële sector wordt uitbesteed aan een beperkt aantal ICT-dienstverleners. Dit brengt concentratierisico's met zich mee. DORA maakt het daarom mogelijk om toezicht te houden op deze dienstverleners. Ze zijn namelijk cruciaal zijn voor de stabiliteit van de Europese financiële sector. Momenteel hebben deze artikelen nog geen directe invloed op financiële ondernemingen. Uiteindelijk zal dit toezicht ondernemingen meer zekerheid kunnen geven over de digitale weerbaarheid van uitbestedingspartners. Artikel 31 t/m 44 beschrijven dit nieuwe mandaat in het zogeheten *oversight*-kader.

De ESA's zijn momenteel aan het selecteren welke dienstverleners onder dit kader zullen vallen. De aanwijzing zullen zij onder andere baseren op de systeeminvloed van de dienstverlener, en de mate van afhankelijkheid en substitueerbaarheid van deze dienst. Per dienstverlener zal een *lead overseer* worden aangewezen die verantwoordelijk is voor het toezicht. Afhankelijk van de sector die het meest wordt bediend, is dit de ESMA, EIOPA of EBA. Het uiteindelijke toezicht zal worden uitgevoerd door een team van Europese en nationale toezichthouders. Zie tabel 4 voor een overzicht van onderdelen die nog verder worden uitgewerkt.

Tabel 4

Aanvullende uitwerkingen	Beschrijving	Afgerond
Call for advice t.b.v. artikel 31(8)	Criticality criteria	September 2023
Selectie van kritieke ICT-dienstverleners t.b.v. artikel 31	n.v.t.	Geen tijdslijn gecommuniceerd
Guidelines t.b.v. artikel 32(7)	Cooperation between ESA's and CA's regarding the structure of oversights	Uiterlijk juli 2024
RTS voor artikel 41	Information on oversight conduct	Uiterlijk juli 2024
Call for advice t.b.v. artikel 43(2)	Oversight fees	September 2023

03 **Vooruitblik**

De komende tijd worden de RTS'en en ITS'en verder ontwikkeld volgens de tijdslijnen die in de vorige secties zijn opgenomen. De ESA's zullen deze via publieke consultatie ook voorleggen aan ondernemingen in de financiële sector, waarbij er op de stukken gereageerd kan worden.

De AFM bereidt zich in de tussentijd voor op het uitvoeren van DORA-toezicht. In de volgende publicaties uit deze reeks zal dieper worden ingegaan op deelonderwerpen uit de verordening. De volgende editie zal in het eerste kwartaal van 2024 worden gepubliceerd.

Voor een verdere uitwerking over *third party risk* in DORA kunnen de volgende pagina's worden geraadpleegd:

- ESAs Report on the landscape of ICT third-party providers in the EU (eba.europa.eu)
- Nieuwsbericht over de consultatie van de eerste set policy products (RTS en ITS) (esma.europa.eu)
- Verdere vragen? Neem contact op met het ondernemersloket van de AFM

Heeft u vragen of opmerkingen over deze publicatie?

Stuur een e-mail naar: redactie@afm.nl

Autoriteit Financiële Markten
Postbus 11723 | 1001 GS Amsterdam

Telefoon
020 797 2000

www.afm.nl

Dataclassificatie
AFM-Publiek

Volg ons: →

De AFM maakt zich sterk voor eerlijke en transparante financiële markten. Als onafhankelijke gedragstoezichthouder dragen wij bij aan duurzaam financieel welzijn in Nederland.