



In het kort:

- Vergroten weerbaarheid financiële instellingen
- Strengere eisen aan contracten tussen financiële instellingen en hun IT-leveranciers
- Register- en rapportageverplichting m.b.t. contracten met IT-leveranciers
- Direct toezicht op kritieke IT-leveranciers



Vereiste acties o.a.:

- Diverse specifieke acties vereist voor financiële instellingen
- Aanscherpen contracten met IT-leveranciers



Geldt vanaf:

17 januari 2025

WAT WORDT GEREGLD?

De [DORA](#) staat voor de verordening betreffende de digitale operationele weerbaarheid voor de financiële sector. De DORA beoogt de financiële sector robuuster te maken, en legt daartoe strengere verplichtingen op aan financiële instellingen. Zo stelt de DORA strenge eisen aan contracten met IT-leveranciers (strenger dan de [EBA guidelines](#)), die in de praktijk zullen resulteren in hogere eisen aan IT-leveranciers. Afhankelijk van hoe kritiek of belangrijk de uitbestede functie is gelden o.a. eisen ten aanzien van de beschrijving van rechten, plichten en de dienstverlening, SLA, gegevensbescherming, exit, bijstand bij incidenten, medewerking aan bepaalde PEN-tests van de financiële instelling, en rapportage- en auditverplichtingen. Daarnaast komen bepaalde kritieke IT-leveranciers zelf onder toezicht te staan.

VOOR WIE GELDEN DEZE REGELS?

De regels gelden primair voor alle spelers in de financiële sector, zoals banken, verzekeraars, beheermaatschappijen en handelsplatforms. Indirect hebben de regels ook gevolgen voor hun IT-leveranciers. Daarnaast komen bepaalde kritieke IT-leveranciers zelf ook onder toezicht te staan. Deze leveranciers worden geselecteerd.

VANAF WANNEER GELDEN DEZE REGELS?

De DORA is op 14 december 2022 vastgesteld. De deadline voor implementatie van de DORA door financiële instellingen is 17 januari 2025.

IS ER AANVERWANTE WET- EN REGELGEVING?

O.a. de NIS2-richtlijn en de AVG.

MEER INFORMATIE?

Neem gerust contact met ons op, of check de Vondst 'Tech & Digital' Cheatsheet: [Tech & Digital Cheatsheet - Vondst](#).