DORA · INCIDENTMELDING EN WEERBAARHEID

DORA: meld incidenten. Stuur op weerbaarheid.

Praktische gids voor financiële entiteiten: bepaal de reikwijdte, verbind de belangrijkste werkgebieden en bereid meldingen van ernstige ICT-incidenten voor.

DORA geldt sinds 17 januari 2025, maar niet automatisch voor elk bedrijf.

Toets elke rechtspersoon aan artikel 2, inclusief uitsluitingen en vereenvoudigde vereisten. Een klantcontract maakt een ICT-aanbieder niet automatisch zelf tot een financiële entiteit onder DORA; contractuele verplichtingen en het toezichtskader voor kritieke ICT-dienstverleners kunnen aanvullende verplichtingen meebrengen.

Vijf samenhangende werkgebieden

ICT-risicobeheer

Organiseer verantwoordelijkheid, inventaris, bescherming, detectie, respons en herstel.

Incidenten

Registreer, classificeer en escaleer incidenten intern; meld ernstige gevallen.

Weerbaarheidstests

Houd een evenredig testprogramma bij met kritieke functies en afhankelijkheden.

ICT-derden

Beheer registers, contracten, concentratierisico's, toezicht en uitstapmogelijkheden.

Leren en delen

Gebruik lessen uit incidenten; informatie over cyberdreigingen kan worden gedeeld.

Meldtermijnen bij een ernstig ICT-incident

4 u / 24 u

Eerste melding

Zo snel mogelijk; binnen 4 u na classificatie als ernstig en uiterlijk 24 u na kennisname.

72 u

Tussenrapport

Uiterlijk 72 u na de eerste melding, ook als de status niet is veranderd.

1 maand

Eindrapport

Uiterlijk een maand na het tussenrapport of de laatste actualisering daarvan.

Wordt een incident pas meer dan 24 uur na kennisname als ernstig geclassificeerd, dan moet de eerste melding binnen 4 uur na die classificatie worden gedaan. Dien vereiste updates zonder onnodige vertraging in; controleer de procedure van de bevoegde autoriteit en toepasselijke uitzonderingen.

Beoordeel de ernst aan de hand van criteria

Pas de criteria en drempels van Verordening (EU) 2024/1772 toe: impact op kritieke diensten, duur, klanten of transacties, geografische spreiding, gegevensverlies en economische impact. Leg de classificatie, motivering en tijd vast.

VAN REGELGEVING NAAR EEN HELDERE INCIDENTAANPAK

Zes stappen om voorbereid te zijn

Een geoefend proces beperkt zoek- en afstemmingswerk wanneer teams en ICT-aanbieders snel dezelfde betrouwbare feiten nodig hebben.

01 · Eigenaarschap

Wijs per rechtspersoon een incidentleider, vervanger, managementcontact en meldverantwoordelijke aan.

02 · Classificatie

Beoordeel getroffen kritieke diensten, duur, klanten, transacties, landen, gegevensverlies en economische impact volgens de toepasselijke drempels.

03 · Tijdlijn

Leg ontdekking, kennisname, classificatiebesluiten en iedere indiening met tijdzone vast.

04 · Feiten verzamelen

Documenteer functies en gevolgen, bekende oorzaken, indamming, aanbieders en herstelprognose.

05 · Vervolgmeldingen

Bereid het 72-uursrapport en updates voor. Maak schattingen en nog te controleren informatie herkenbaar.

06 · Afronden en leren

Voltooi oorzaakanalyse, werkelijke impact en herstelmaatregelen; verwerk lessen in tests en leveranciersbeheer.

Houd dit gereed voor de eerste melding

Incident-ID en tijdstippen · getroffen kritieke of belangrijke functie · eerste onderbouwing van de classificatie · getroffen landen, klanten of transacties · uitval en data-impact · directe maatregelen · belangrijkste ICT-aanbieders · contactpersoon en tijd van volgende update. Gebruik de voorgeschreven formats en het kanaal van de bevoegde autoriteit.

Twee belangrijke onderscheidingen

Registreer en classificeer ICT-incidenten volgens de DORA-criteria; ernstige ICT-incidenten moeten aan de autoriteit worden gemeld. Een significante cyberdreiging kan op grond van artikel 19 vrijwillig worden gemeld. Controleer privacy-, contractuele en andere sectorale meldplichten afzonderlijk.

Officiële bronnen · rechtsstand 8 oktober 2026

DORA, Verordening (EU) 2022/2554 (met name art. 2, 5-19, 28-30, 64) · Gedelegeerde Verordening (EU) 2024/1772 (classificatiecriteria) · Gedelegeerde Verordening (EU) 2025/301 (termijnen) · Uitvoeringsverordening (EU) 2025/302 (meldformats) · EIOPA, DORA-overzicht.

Officiële teksten: 2022/2554 · 2024/1772 · 2025/301 · 2025/302 · EIOPA

Grenzen

Algemene praktische hulp, geen juridisch advies, technisch onderzoek, conformiteitsbeoordeling of melding aan een autoriteit. Controleer reikwijdte, classificatie, bevoegde autoriteit, meldkanaal en uitzonderingen voor de specifieke rechtspersoon.