DORA · INCIDENT-REPORTING UND RESILIENZ

DORA: Vorfälle melden. Resilienz steuern.

Der kompakte Praxisleitfaden für Finanzunternehmen: Geltungsbereich klären, wichtige Arbeitsbereiche verbinden und den Meldeablauf für schwere IKT-Vorfälle vorbereiten.

DORA gilt seit dem 17. Januar 2025 - aber nicht pauschal für jedes Unternehmen.

Prüfen Sie die konkrete Rechtseinheit anhand von Artikel 2, einschließlich Ausnahmen und vereinfachter Anforderungen. IKT-Dienstleister werden durch einen Kundenvertrag nicht automatisch selbst zum Finanzunternehmen unter DORA; zusätzliche Pflichten können aus Vertrag und dem Aufsichtsrahmen für kritische IKT-Drittdienstleister entstehen.

Fünf Arbeitsbereiche greifen ineinander

IKT-Risikomanagement

Verantwortung, Inventar, Schutz, Erkennung, Reaktion und Wiederherstellung organisieren.

Vorfälle

Vorfälle erfassen, einstufen, intern eskalieren und schwere Fälle melden.

Resilienztests

Ein angemessenes Testprogramm pflegen; kritische Funktionen und Abhängigkeiten einbeziehen.

IKT-Drittparteien

Register, Verträge, Konzentrationsrisiken, Überwachung und Ausstiegsoptionen steuern.

Lernen & Teilen

Erkenntnisse nach Vorfällen nutzen; Informationen zu Cyberbedrohungen können geteilt werden.

Meldezeitplan bei einem schweren IKT-Vorfall

4 h / 24 h

Erstmeldung

So früh wie möglich; binnen 4 h ab Einstufung als schwerwiegend, spätestens 24 h ab Kenntnis.

72 h

Zwischenbericht

Spätestens 72 h nach der Erstmeldung - auch ohne Statusänderung.

1 Monat

Abschlussbericht

Spätestens einen Monat nach dem Zwischenbericht oder dessen letzter Aktualisierung.

Wird ein Vorfall erst mehr als 24 Stunden nach Kenntnis als schwerwiegend eingestuft, ist die Erstmeldung binnen 4 Stunden nach dieser Einstufung abzugeben. Danach sind erforderliche Aktualisierungen ohne unangemessene Verzögerung einzureichen; Vorgaben der zuständigen Aufsicht und Ausnahmen mitprüfen.

Schweregrad anhand fester Kriterien prüfen

Bewerten Sie den Vorfall anhand der Kriterien und Schwellen aus Verordnung (EU) 2024/1772 - etwa Auswirkungen auf kritische Dienste, Dauer, Kunden oder Transaktionen, geografische Ausbreitung, Datenverlust und wirtschaftlichen Schaden. Halten Sie Einstufung und Begründung mit Zeitstempel fest.

VOM REGELWERK ZUM KLAREN VORFALLABLAUF

Sechs Schritte für den Ernstfall

Ein geübter Ablauf reduziert Such- und Abstimmungsschleifen, wenn mehrere Teams und IKT-Anbieter schnell dieselben belastbaren Fakten brauchen.

01 · Zuständigkeit

Benennen Sie je Rechtseinheit Incident Lead, Stellvertretung, Managementkontakt und Meldeverantwortliche.

02 · Einstufung

Bewerten Sie betroffene kritische Dienste, Dauer, Kunden, Transaktionen, Länder, Datenverlust und wirtschaftliche Auswirkungen anhand der geltenden Schwellen.

03 · Zeitlinie

Halten Sie Entdeckung, Kenntnis, Einstufungsentscheidung und jede Einreichung mit Zeitzone nachvollziehbar fest.

04 · Fakten sammeln

Dokumentieren Sie betroffene Funktionen, Auswirkungen, Ursache soweit bekannt, Eindämmung, Dienstleister und Wiederherstellungsprognose.

05 · Folgeberichte

Bereiten Sie 72-Stunden-Bericht und Aktualisierungen vor. Kennzeichnen Sie Schätzungen und offene Fakten klar.

06 · Abschluss & Lernen

Ergänzen Sie Ursachenanalyse, tatsächliche Auswirkungen und Abhilfemaßnahmen; führen Sie Erkenntnisse in Tests und Lieferantensteuerung zurück.

Was im ersten Meldepaket griffbereit sein sollte

Vorfall-ID und Zeitstempel · betroffene kritische oder wichtige Funktion · erste Einstufungsbegründung · betroffene Länder, Kunden oder Transaktionen · Ausfallzeit und Datenfolgen · Sofortmaßnahmen · wichtige IKT-Dienstleister · Kontakt und nächster Aktualisierungstermin. Nutzen Sie die vorgeschriebenen Formate und den Meldekanal der zuständigen Behörde.

Zwei wichtige Abgrenzungen

Erfassen Sie IKT-bezogene Vorfälle und stufen Sie sie nach den DORA-Kriterien ein; an die Aufsicht zu melden sind schwere IKT-Vorfälle. Eine signifikante Cyberbedrohung kann nach Artikel 19 freiwillig gemeldet werden. Datenschutz-, Vertrags- und andere sektorale Meldepflichten separat prüfen.

Offizielle Quellen · Rechtsstand 8. Oktober 2026

DORA, Verordnung (EU) 2022/2554 (insb. Art. 2, 5-19, 28-30, 64) · Delegierte Verordnung (EU) 2024/1772 (Einstufungskriterien) · Delegierte Verordnung (EU) 2025/301 (Fristen) · Durchführungsverordnung (EU) 2025/302 (Meldeformate) · EIOPA, DORA-Überblick.

Offizielle Texte: 2022/2554 · 2024/1772 · 2025/301 · 2025/302 · EIOPA

Geltungsgrenzen

Allgemeine Arbeitshilfe, keine Rechtsberatung, technische Untersuchung, Konformitätsbewertung oder Meldung an eine Behörde. Scope, Klassifizierung, zuständige Aufsicht, Meldekanal und Ausnahmen für die konkrete Rechtseinheit prüfen.