DORA · HLÁŠENÍ INCIDENTŮ A ODOLNOST

DORA: hlaste incidenty. Řiďte odolnost.

Praktický průvodce pro finanční subjekty: ověřte působnost, propojte hlavní pracovní oblasti a připravte hlášení závažných incidentů souvisejících s ICT.

DORA se používá od 17. ledna 2025, ale ne na každý podnik.

U každé právnické osoby ověřte článek 2 včetně výjimek a zjednodušených požadavků. Smlouva se zákazníkem sama o sobě z poskytovatele ICT automaticky nedělá finanční subjekt podle DORA; další povinnosti mohou vyplývat ze smlouvy a rámce dohledu nad kritickými poskytovateli ICT služeb třetích stran.

Pět propojených pracovních oblastí

Řízení rizik ICT
Uspořádejte odpovědnosti, inventáře, ochranu, detekci, reakci a obnovu.

Incidenty
Zaznamenávejte, klasifikujte a interně eskalujte incidenty; závažné případy hlaste.

Testování odolnosti
Udržujte přiměřený program testování zahrnující kritické funkce a závislosti.

Třetí strany ICT
Řiďte registry, smlouvy, koncentrační rizika, dohled a možnosti ukončení.

Učení a sdílení
Využívejte poznatky z incidentů; informace o kybernetických hrozbách lze sdílet.

Lhůty pro hlášení závažného incidentu ICT

4 h / 24 h
Počáteční oznámení
Co nejdříve; do 4 h od klasifikace jako závažný a nejpozději 24 h od zjištění.

72 h
Průběžná zpráva
Nejpozději 72 h od počátečního oznámení, i když se stav nezměnil.

1 měsíc
Závěrečná zpráva
Nejpozději měsíc po průběžné zprávě nebo její poslední aktualizaci.

Je-li incident klasifikován jako závažný až více než 24 hodin poté, co se o něm subjekt dozvěděl, počáteční oznámení se podává do 4 hodin od této klasifikace. Požadované aktualizace podávejte bez zbytečného odkladu; ověřte postup příslušného orgánu a použitelné výjimky.

Závažnost posuďte podle stanovených kritérií

Použijte kritéria a prahové hodnoty nařízení (EU) 2024/1772: dopad na kritické služby, dobu trvání, klienty či transakce, geografický rozsah, ztrátu dat a hospodářský dopad. Zaznamenejte klasifikaci, důvody a čas.

OD PRAVIDEL K JASNÉ REAKCI NA INCIDENT

Šest kroků k připravenosti

Procvičený postup omezuje dohledávání a koordinaci, když týmy a poskytovatelé ICT potřebují rychle potvrdit spolehlivé skutečnosti.

01 · Odpovědnost

Pro každou právnickou osobu určete vedoucího incidentu, zástupce, kontakt vedení a osobu odpovědnou za hlášení.

02 · Klasifikace

Podle příslušných prahů vyhodnoťte zasažené kritické služby, dobu trvání, klienty, transakce, země, ztrátu dat a hospodářský dopad.

03 · Časová osa

Zaznamenejte zjištění, vědomost o události, rozhodnutí o klasifikaci a každé podání včetně časového pásma.

04 · Shromáždění faktů

Zdokumentujte funkce a dopady, známé příčiny, omezení následků, poskytovatele a odhad obnovy.

05 · Následné zprávy

Připravte zprávu do 72 hodin a aktualizace. Jasně označte odhady a dosud ověřované údaje.

06 · Uzavření a poučení

Dokončete analýzu příčin, skutečných dopadů a nápravných opatření; promítněte zjištění do testů a řízení dodavatelů.

Co mít připravené pro první hlášení

ID incidentu a časové údaje · zasažená kritická nebo důležitá funkce · počáteční důvody klasifikace · zasažené země, klienti nebo transakce · výpadek a dopady na data · okamžitá opatření · klíčoví poskytovatelé ICT · kontakt a čas další aktualizace. Použijte předepsané formuláře a kanál příslušného orgánu.

Dvě důležitá rozlišení

Incidenty ICT zaznamenávejte a klasifikujte podle kritérií DORA; závažné incidenty ICT se hlásí příslušnému orgánu. Významnou kybernetickou hrozbu lze podle článku 19 oznámit dobrovolně. Samostatně ověřte povinnosti týkající se osobních údajů, smluv a jiných sektorů.

Oficiální zdroje · právní stav k 8. říjnu 2026

DORA, nařízení (EU) 2022/2554 (zejm. čl. 2, 5-19, 28-30, 64) · nařízení v přenesené pravomoci (EU) 2024/1772 (kritéria klasifikace) · nařízení v přenesené pravomoci (EU) 2025/301 (lhůty) · prováděcí nařízení (EU) 2025/302 (formuláře) · EIOPA, přehled DORA.

Oficiální texty: 2022/2554 · 2024/1772 · 2025/301 · 2025/302 · EIOPA

Hranice

Obecná pracovní pomůcka, nikoli právní poradenství, technické šetření, posouzení shody ani hlášení orgánu. Pro konkrétní právnickou osobu ověřte působnost, klasifikaci, orgán, kanál a výjimky.