DORA · HLÁSENIE INCIDENTOV A ODOLNOSŤ

DORA: hláste incidenty. Riaďte odolnosť.

Praktická príručka pre finančné subjekty: overte pôsobnosť, prepojte hlavné pracovné oblasti a pripravte hlásenie závažných incidentov súvisiacich s IKT.

DORA sa uplatňuje od 17. januára 2025, ale nie na každý podnik.

Pri každej právnickej osobe overte článok 2 vrátane výnimiek a zjednodušených požiadaviek. Zmluva so zákazníkom sama osebe automaticky nemení poskytovateľa IKT na finančný subjekt podľa DORA; ďalšie povinnosti môžu vyplývať zo zmluvy a rámca dohľadu nad kritickými poskytovateľmi IKT služieb tretích strán.

Päť prepojených pracovných oblastí

Riadenie rizík IKT
Usporiadajte zodpovednosti, inventáre, ochranu, detekciu, reakciu a obnovu.

Incidenty
Zaznamenávajte, klasifikujte a interne eskalujte incidenty; závažné prípady hláste.

Testovanie odolnosti
Udržiavajte primeraný program testovania s kritickými funkciami a závislosťami.

Tretie strany IKT
Riaďte registre, zmluvy, koncentračné riziká, dohľad a možnosti ukončenia.

Učenie a zdieľanie
Využívajte poznatky z incidentov; informácie o kybernetických hrozbách možno zdieľať.

Lehoty na hlásenie závažného incidentu IKT

4 h / 24 h
Úvodné oznámenie
Čo najskôr; do 4 h od klasifikácie ako závažný a najneskôr 24 h od zistenia.

72 h
Priebežná správa
Najneskôr 72 h od úvodného oznámenia, aj keď sa stav nezmenil.

1 mesiac
Záverečná správa
Najneskôr mesiac po priebežnej správe alebo jej poslednej aktualizácii.

Ak sa incident klasifikuje ako závažný až viac ako 24 hodín po tom, čo sa o ňom subjekt dozvedel, úvodné oznámenie sa podá do 4 hodín od tejto klasifikácie. Požadované aktualizácie podávajte bez zbytočného odkladu; overte postup príslušného orgánu a uplatniteľné výnimky.

Závažnosť posúďte podľa stanovených kritérií

Použite kritériá a prahové hodnoty nariadenia (EÚ) 2024/1772: vplyv na kritické služby, trvanie, klientov či transakcie, geografický rozsah, stratu údajov a hospodársky dosah. Zaznamenajte klasifikáciu, dôvody a čas.

OD PRAVIDIEL K JASNEJ REAKCII NA INCIDENT

Šesť krokov na prípravu

Nacvičený postup obmedzí hľadanie a koordináciu, keď tímy a poskytovatelia IKT potrebujú rýchlo potvrdiť spoľahlivé skutočnosti.

01 · Zodpovednosť

Pre každú právnickú osobu určte vedúceho incidentu, zástupcu, kontakt na vedenie a osobu zodpovednú za hlásenie.

02 · Klasifikácia

Podľa príslušných prahov posúďte zasiahnuté kritické služby, trvanie, klientov, transakcie, krajiny, stratu údajov a hospodársky dosah.

03 · Časová os

Zaznamenajte zistenie, vedomosť o udalosti, rozhodnutia o klasifikácii a každé podanie vrátane časového pásma.

04 · Zhromaždenie faktov

Zdokumentujte funkcie a vplyvy, známe príčiny, obmedzenie následkov, poskytovateľov a odhad obnovy.

05 · Následné správy

Pripravte správu do 72 hodín a aktualizácie. Jasne označte odhady a údaje, ktoré sa ešte overujú.

06 · Uzavretie a poučenie

Dokončite analýzu príčin, skutočných vplyvov a nápravných opatrení; preneste poznatky do testov a riadenia dodávateľov.

Čo mať pripravené na prvé hlásenie

ID incidentu a časové údaje · zasiahnutá kritická alebo dôležitá funkcia · počiatočné zdôvodnenie klasifikácie · zasiahnuté krajiny, klienti alebo transakcie · výpadok a vplyv na údaje · okamžité opatrenia · kľúčoví poskytovatelia IKT · kontakt a čas ďalšej aktualizácie. Použite predpísané formuláre a kanál príslušného orgánu.

Dve dôležité rozlíšenia

Incidenty IKT zaznamenávajte a klasifikujte podľa kritérií DORA; závažné incidenty IKT sa hlásia príslušnému orgánu. Významnú kybernetickú hrozbu možno podľa článku 19 oznámiť dobrovoľne. Samostatne overte povinnosti týkajúce sa osobných údajov, zmlúv a iných sektorov.

Oficiálne zdroje · právny stav k 8. októbru 2026

DORA, nariadenie (EÚ) 2022/2554 (najmä čl. 2, 5-19, 28-30, 64) · delegované nariadenie (EÚ) 2024/1772 (kritériá klasifikácie) · delegované nariadenie (EÚ) 2025/301 (lehoty) · vykonávacie nariadenie (EÚ) 2025/302 (formuláre) · EIOPA, prehľad DORA.

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

Hranice

Všeobecná pracovná pomôcka, nie právne poradenstvo, technické vyšetrovanie, posúdenie zhody ani hlásenie orgánu. Pre konkrétnu právnickú osobu overte pôsobnosť, klasifikáciu, orgán, kanál a výnimky.