DORA · ZGŁASZANIE INCYDENTÓW I ODPORNOŚĆ

DORA: zgłaszaj incydenty. Zarządzaj odpornością.

Praktyczny przewodnik dla podmiotów finansowych: potwierdź zakres, połącz główne obszary pracy i przygotuj zgłaszanie poważnych incydentów związanych z ICT.

DORA stosuje się od 17 stycznia 2025 r., ale nie do każdej firmy.

Sprawdź każdą osobę prawną pod kątem art. 2, w tym wyłączeń i uproszczonych wymogów. Umowa z klientem nie czyni automatycznie dostawcy ICT podmiotem finansowym podlegającym DORA; dodatkowe obowiązki mogą wynikać z umowy i ram nadzoru nad krytycznymi zewnętrznymi dostawcami ICT.

Pięć powiązanych obszarów pracy

Zarządzanie ryzykiem ICT

Uporządkuj odpowiedzialność, wykazy, ochronę, wykrywanie, reagowanie i odtwarzanie.

Incydenty

Rejestruj, klasyfikuj i eskaluj incydenty; zgłaszaj poważne przypadki.

Testowanie odporności

Prowadź proporcjonalny program testów obejmujący krytyczne funkcje i zależności.

Zewnętrzni dostawcy ICT

Zarządzaj rejestrem, umowami, koncentracją, monitorowaniem i planami wyjścia.

Uczenie się i wymiana

Wykorzystuj wnioski z incydentów; informacje o cyberzagrożeniach można wymieniać.

Terminy zgłoszeń poważnego incydentu ICT

4 h / 24 h

Zgłoszenie wstępne

Jak najszybciej; w 4 h od klasyfikacji jako poważny, najpóźniej 24 h od uzyskania wiedzy.

72 h

Sprawozdanie pośrednie

Najpóźniej 72 h po zgłoszeniu wstępnym, nawet jeśli status się nie zmienił.

1 miesiąc

Sprawozdanie końcowe

Najpóźniej miesiąc po sprawozdaniu pośrednim lub jego ostatniej aktualizacji.

Jeżeli incydent zostanie uznany za poważny ponad 24 godziny po uzyskaniu wiedzy przez podmiot, zgłoszenie wstępne należy złożyć w ciągu 4 godzin od tej klasyfikacji. Wymagane aktualizacje przekazuj bez zbędnej zwłoki; sprawdź procedurę właściwego organu i mające zastosowanie wyjątki.

Oceń powagę według określonych kryteriów

Zastosuj kryteria i progi z rozporządzenia (UE) 2024/1772: wpływ na usługi krytyczne, czas trwania, klientów lub transakcje, zasięg geograficzny, utratę danych i skutki gospodarcze. Zapisz klasyfikację, uzasadnienie i czas.

OD PRZEPISÓW DO JASNEJ REAKCJI NA INCYDENT

Sześć kroków przygotowania

Przećwiczony proces ogranicza szukanie informacji i uzgodnienia, gdy zespoły i dostawcy ICT muszą szybko ustalić wiarygodne fakty.

01 · Odpowiedzialność

Dla każdej osoby prawnej wskaż lidera incydentu, zastępcę, kontakt zarządczy i osobę odpowiedzialną za zgłoszenia.

02 · Klasyfikacja

Oceń wpływ na usługi krytyczne, czas trwania, klientów, transakcje, kraje, utratę danych i skutki gospodarcze według właściwych progów.

03 · Oś czasu

Zapisz wykrycie, uzyskanie wiedzy, decyzje klasyfikacyjne i każde zgłoszenie wraz ze strefą czasową.

04 · Zbieranie faktów

Udokumentuj funkcje i skutki, znane przyczyny, ograniczanie skutków, dostawców i prognozę odtworzenia.

05 · Kolejne raporty

Przygotuj raport po 72 godzinach i aktualizacje. Wyraźnie oznacz szacunki i informacje w trakcie weryfikacji.

06 · Zamknięcie i wnioski

Dokończ analizę przyczyn, ustal rzeczywiste skutki i działania naprawcze; przenieś wnioski do testów i nadzoru dostawców.

Informacje gotowe do pierwszego zgłoszenia

Identyfikator incydentu i znaczniki czasu · dotknięta funkcja krytyczna lub ważna · wstępne uzasadnienie klasyfikacji · dotknięte kraje, klienci lub transakcje · przerwa i wpływ na dane · natychmiastowe działania · kluczowi dostawcy ICT · kontakt i termin kolejnej aktualizacji. Użyj wymaganych formularzy i kanału właściwego organu.

Dwa ważne rozróżnienia

Rejestruj i klasyfikuj incydenty ICT zgodnie z kryteriami DORA; poważne incydenty ICT należy zgłaszać organowi. Istotne cyberzagrożenie można zgłosić dobrowolnie na podstawie art. 19. Osobno sprawdź obowiązki dotyczące danych osobowych, umów i innych sektorów.

Źródła urzędowe · stan prawny na 8 października 2026 r.

DORA, rozporządzenie (UE) 2022/2554 (w szczególności art. 2, 5-19, 28-30, 64) · rozporządzenie delegowane (UE) 2024/1772 (kryteria klasyfikacji) · rozporządzenie delegowane (UE) 2025/301 (terminy) · rozporządzenie wykonawcze (UE) 2025/302 (formularze) · EIOPA, przegląd DORA.

Akty urzędowe: 2022/2554 · 2024/1772 · 2025/301 · 2025/302 · EIOPA

Granice

Ogólna pomoc w pracy, nie porada prawna, dochodzenie techniczne, ocena zgodności ani zgłoszenie do organu. Sprawdź zakres, klasyfikację, organ, kanał i wyjątki dla konkretnej osoby prawnej.