PoradyODO.pl
OCHRONA DANYCH ■ CYBERBEZPIECZEŃSTWO

NIS 2 a rola CSIRT

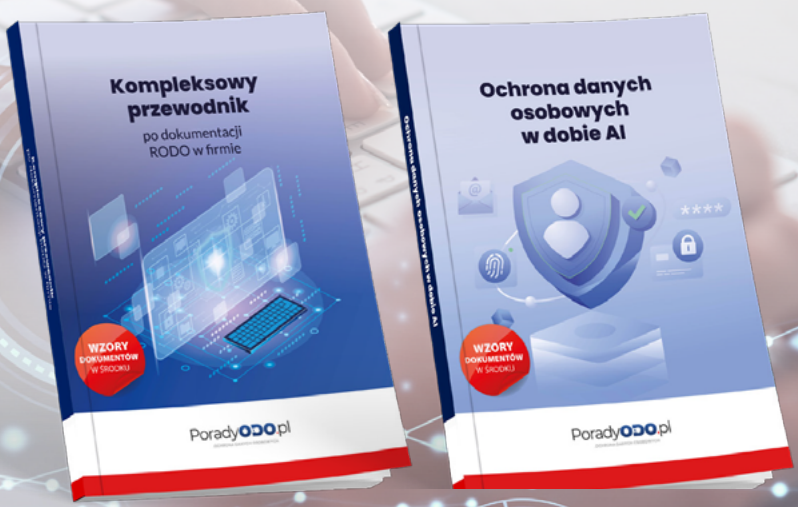
w zarządzaniu incydentami cyberbezpieczeństwa

PoradyODO.pl

.OCHRONA DANYCH OSOBOWYCH

Wszystko, czego potrzebujesz!

Nowoczesne rozwiązania w jednym miejscu!



Nasza biblioteczka to zbiór najlepszych książek i e-booków, które pomogą Ci w codziennej pracy z dokumentacją ochrony danych osobowych.

Sprawdź już dziś!

NIS 2 a rola CSIRT w zarządzaniu incydentami cyberbezpieczeństwa

Autorzy: Ewa Lewańska,
Redakcja: Anna Śmigulska-Wojciechowska
Korekta: Zespół
Koordynator produkcji: Mariusz Jezierski
Koordynator projektów wydawniczych: Anna Jagodzińska
Content & Publishing Leader: Marta Grabowska-Peda

Projekt graficzny okładki: Agnieszka Makowska
Zdjęcie na okładce: Freepick
Skład i łamanie: Agnieszka Makowska

Wydanie I
Stan prawny: marzec 2026 r.
ISBN: 978-83-8409-645-1
Kod produktu: 1BG59

Wydawca:
Wiedza i Praktyka sp. z o.o.
03-918 Warszawa, ul. Łotewska 9a
tel. 22 518 29 29, faks 22 617 60 10
www.wip.pl

Publikacja uwzględnia stan prawny obowiązujący na dzień 16 marca 2026 r.

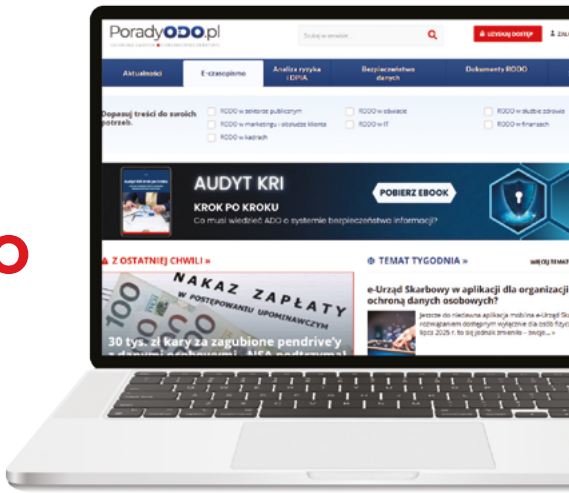
Spis treści

PoradyODO.pl

OCHRONA DANYCH ■ CYBERBEZPIECZEŃSTWO

Twój profesjonalny portal zgodny z RODO

Zawsze aktualna wiedza, praktyczne wzory i porady ekspertów w jednym miejscu.



Oferta specjalna

– 14 dni darmowego dostępu!

Skorzystaj z kuponu i sprawdź wszystkie możliwości portalu.

W ramach dostępu otrzymasz:

- **Możliwość zadania 3** pytań w miesiącu naszym ekspertom.
- **Listy kontrolne** do szybkiej weryfikacji zgodności z RODO.
- **Gotowe wzory dokumentów**, w pełni edytowalne i zgodne z przepisami.
- **Baza porad ekspertów** z praktycznymi rozwiązaniami dla Twojej organizacji.
- **Profesjonalne wideoszkolenia** dla poszerzenia i zdobycia wiedzy.
- **24/7 dostęp do stale aktualizowanej bazy wiedzy** z aktualnościami i top tematami.

PoradyODO.pl – zawsze aktualna baza wiedzy, aktów prawnych, dokumentów oraz porad ekspertów. Twoje centrum wiedzy o ochronie danych osobowych.

NIS 2 a rola CSIRT w zarządzaniu incydentami cyberbezpieczeństwa

Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa implementująca dyrektywę NIS 2 wprowadza istotne zmiany w zarządzaniu incydentami cyberbezpieczeństwa, porządkując odpowiedzialność podmiotów kluczowych i ważnych, operatorów usług kluczowych oraz wzmacniając rolę zespołów CSIRT. Reagowanie na incydenty cyberbezpieczeństwa staje się integralnym elementem formalnego systemu bezpieczeństwa państwa, z jasno zdefiniowanymi kompetencjami, obowiązkami raportowania i kanałami współpracy zgodnymi z wymogami NIS 2.

Ważne miejsce w tym systemie zajmują **Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego (Computer Security Incident Response Team, CSIRT)**, czyli wyspecjalizowane podmioty systemowe, działające na poziomie krajowym, a niedługo także sektorowym. To właśnie im ustawa przypisuje zadania koordynacyjne, analityczne i wspierające w obsłudze incydentów.

CSIRT-y krajowe

Ustawa w aktualnym brzmieniu wskazuje trzy zespoły o charakterze krajowym, pełniące funkcję filarów systemu:

- CSIRT GOV, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego – odpowiedzialny za infrastrukturę administracji rządowej oraz infrastrukturę krytyczną o kluczowym znaczeniu dla państwa;
- CSIRT MON, prowadzony przez Ministra Obrony Narodowej – właściwy dla resortu obrony narodowej oraz jednostek organizacyjnych mu podległych;
- CSIRT NASK, prowadzony przez Naukową i Akademicką Sieć Komputerową (NASK-PIB) – odpowiedzialny za pozostałe podmioty krajowego systemu

cyberbezpieczeństwa, w tym jednostki samorządu terytorialnego oraz sektor prywatny

Zespoły te tworzą fundament państwowego reagowania na incydenty cyberbezpieczeństwa, pełniąc funkcję centralnych punktów reagowania i wymiany informacji. Ich zadania obejmują m.in.:

- analizę incydentów,
- koordynację działań w przypadku zdarzeń o większej skali,
- wymianę informacji z innymi państwami członkowskimi UE,
- współpracę z podmiotami krajowego systemu cyberbezpieczeństwa.

CSIRT-y sektorowe

Kluczowym elementem systemu są Sektorowe Zespoły Cyberbezpieczeństwa (SZC), które po wykazaniu pełnej zdolności operacyjnej, pełnią funkcję CSIRT-ów sektorowych w rozumieniu dyrektywy NIS 2 (Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555). Ustawa definiuje je jako Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego, działające na poziomie sektora lub podsektora, ustanowione przez organ właściwy do spraw cyberbezpieczeństwa dla danego sektora lub podsektora.

CSIRT sektorowe mają odpowiadać na potrzebę uwzględnienia specyfiki poszczególnych sektorów gospodarki i administracji. Inaczej bowiem wygląda krajobraz zagrożeń w energetyce, inaczej w ochronie zdrowia, finansach czy transporcie. Zadaniem CSIRT sektorowego jest zatem zapewnienie reagowania osadzonego w realiach danego sektora przy jednoczesnym zachowaniu spójności z systemem krajowym.

Jak będą powstawać CSIRT sektorowe?

Ustawodawca przewidział dwa mechanizmy powstawania CSIRT-ów sektorowych:

1. **Tworzenie od podstaw** – organ właściwy ustanawia CSIRT sektorowy w terminie 18 miesięcy od wejścia w życie nowelizacji i zapewnia mu zdolność operacyjną.