PoradyODO.pl

OCHRONA DANYCH ■ CYBERBEZPIECZEŃSTWO

NIS 2 a RODO

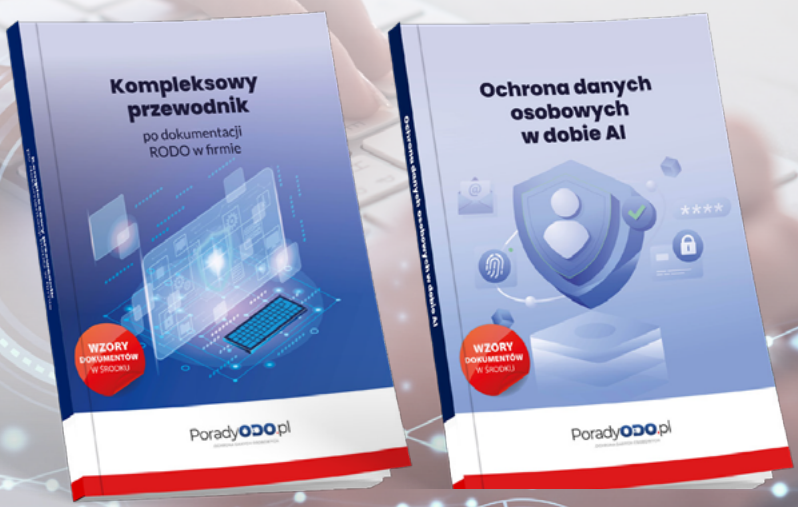
Jak podmioty kluczowe i ważne mają przygotować się na incydenty cyberbezpieczeństwa

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 RODO. Jak podmioty kluczowe i ważne mają przygotować się na incydenty cyberbezpieczeństwa

Autorzy: Ewa Lewańska, Maciej Lipka
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: 978-83-8409-642-0
Kod produktu: 1BG58

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.

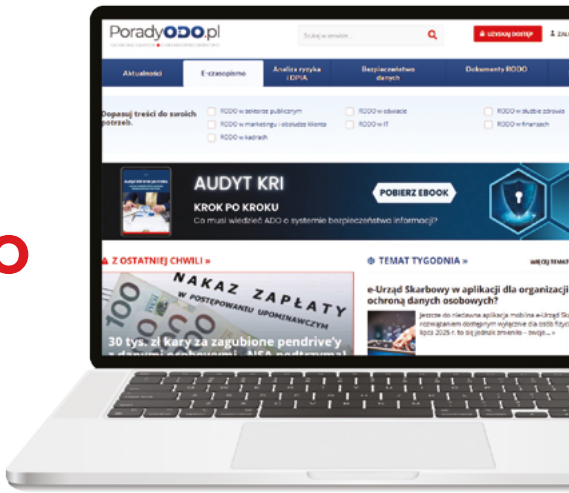
Spis treści

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.

Katalog podmiotów ważnych i kluczowych według ustawy KSC

Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa stanowi istotny etap dostosowania polskiego porządku prawnego do wymogów dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w Unii. W debacie publicznej dominują kwestie zarządzania ryzykiem, raportowania incydentów oraz sankcji, jednak kluczowym elementem pozostaje katalog podmiotów objętych tymi obowiązkami, określający zakres podmiotowy regulacji.

To właśnie katalog podmiotów objętych systemem cyberbezpieczeństwa przesądza o tym, kto w ogóle podlega ustawie i kto zostaje włączony do krajowego systemu cyberbezpieczeństwa. Bez tej kwalifikacji nie powstają obowiązki szczególne, nie uruchamia się nadzór ani nie aktualizują się mechanizmy reagowania na incydenty. Z perspektywy przedsiębiorców omawiany katalog jest więc punktem wyjścia do oceny własnej sytuacji.

Rola katalogu w konstrukcji ustawy

Ustawa o krajowym systemie cyberbezpieczeństwa opiera się na założeniu, że **nie wszystkie podmioty funkcjonujące w gospodarce muszą podlegać jednakowym wymaganiom w zakresie cyberbezpieczeństwa**. Regulacja koncentruje się na tych organizacjach, których działalność ma istotne znaczenie dla funkcjonowania państwa, bezpieczeństwa obywateli lub ciągłości kluczowych usług.

Katalog podmiotów pełni w tym modelu funkcję selekcyjną. Ustawodawca wskazuje sektory i rodzaje działalności, które uznaje za wrażliwe z punktu widzenia odporności systemowej. Dopiero podmioty mieszczące się w tym katalogu podlegają dalszej kwalifikacji oraz szczególnym obowiązkom wynikającym z ustawy.

W nowelizacji katalog został istotnie rozszerzony, co oznacza, że wiele podmiotów, które do tej pory funkcjonowały poza reżimem krajowego systemu cyberbezpieczeństwa, będzie musiało po raz pierwszy zmierzyć się z formalnymi obowiązkami w zakresie bezpieczeństwa systemów informacyjnych.

Podmioty objęte ustawą: nowe podejście sektorowe

Dotychczasowe regulacje były postrzegane jako skierowane przede wszystkim do operatorów infrastruktury krytycznej oraz wybranych dostawców usług cyfrowych. Nowelizacja zmienia tę perspektywę, wprowadzając podejście sektorowe, zbliżone do rozwiązań przyjętych w dyrektywie NIS 2.

Katalog podmiotów został oparty na wybranych sektorach i pod sektorach działalności. Obejmują one zarówno obszary tradycyjnie uznawane za infrastrukturę krytyczną, jak i sektory, których znaczenie dla bezpieczeństwa państwa i ciągłości usług publicznych ujawniło się wraz z postępującą cyfryzacją gospodarki.

Do sektorów objętych ustawą o krajowym systemie cyberbezpieczeństwa należą w szczególności:

- energia (wydobywanie kopalin, energia elektryczna, jądrowa, ciepło, gaz i inne),
- transport (lotniczy, kolejowy, wodny i drogowy),
- bankowość infrastruktura rynków finansowych,
- ochrona zdrowia,
- zaopatrzenie w wodę pitną i jej dystrybucja,
- zbiorowe odprowadzanie ścieków,
- infrastruktura cyfrowa,
- zarządzanie usługami ICT,
- administracja publiczna,
- usługi pocztowe,
- gospodarowanie odpadami (m.in. zbieranie odpadów, transport odpadów, przetwarzanie odpadów),
- produkcja, wytwarzanie oraz dystrybucja chemikaliów,
- produkcja, przetwarzanie oraz dystrybucja żywności,