PRACODAWCY RP

NIS 2, DORA nowe obowiązki przedsiębiorców

•W 2023 r. weszła w życie Dyrektywa NIS 2, która zmieni kształt cyberbezpieczeństwa w Państwach Członkowskich Unii Europejskiej. Dla sektorów transportu oraz zaopatrzenia w wodę pitną i jej dystrybucji oznacza to wzrost podmiotów, które będą zobowiązane zastosować szereg rozwiązań z zakresu cyberbezpieczeństwa.

3 kwietnia 2026 r. weszła w życie nowelizacja ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2026 poz. 20 t.j., z uwzględnieniem zmian wprowadzonych ustawą z 23 stycznia 2026 r., Dz.U. 2026 poz. 252)

01

Najważniejsze zmiany - Trzy regulacje, jeden cel — różne mechaniki

•**Dyrektywa NIS2** — dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii. Jako dyrektywa wymaga transpozycji do prawa krajowego — i to właśnie zrobiła znowelizowana ustawa o KSC.

Ustawa o KSC — ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2026 poz. 20 t.j.) ze zmianą z 23 stycznia 2026 r. (Dz.U. 2026 poz. 252). Polski akt, w którym znajdują się konkretne obowiązki dla podmiotów kluczowych i ważnych.

Rozporządzenie DORA — rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego. Obowiązuje bezpośrednio (od 17 stycznia 2025 r.), bez konieczności transpozycji, w sektorze finansowym.

Kogo obejmuje ustawa o KSC po nowelizacji

Zgodnie z art. 4 ustawy krajowy system cyberbezpieczeństwa obejmuje m.in. podmioty kluczowe, podmioty ważne, CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowe, organy właściwe do spraw cyberbezpieczeństwa, Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa oraz Kolegium do Spraw Cyberbezpieczeństwa. Sercem systemu są jednak dwie kategorie podmiotów rynkowych: **podmioty kluczowe i podmioty ważne**, zdefiniowane w art. 5 ustawy.

Art. 5 ust. 1 ustawy wskazuje, że podmiotem kluczowym jest m.in. osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej wskazana w załączniku nr 1 do ustawy, która przewyższa wymogi dla średniego przedsiębiorstwa określone w rozporządzeniu Komisji (UE) nr 651/2014, a także — niezależnie od wielkości — m.in. dostawca usług DNS, kwalifikowany dostawca usług zaufania, podmiot krytyczny, rejestr nazw domen najwyższego poziomu (TLD), podmiot świadczący usługi rejestracji nazw domen, podmiot publiczny wskazany w załączniku nr 1 oraz operator obiektu energetyki jądrowej.

Art. 5 ust. 1 ustawy wskazuje, że podmiotem kluczowym jest m.in. osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej wskazana w załączniku nr 1 do ustawy, która przewyższa wymogi dla średniego przedsiębiorstwa określone w rozporządzeniu Komisji (UE) nr 651/2014, a także — niezależnie od wielkości — m.in. dostawca usług DNS, kwalifikowany dostawca usług zaufania, podmiot krytyczny, rejestr nazw domen najwyższego poziomu (TLD), podmiot świadczący usługi rejestracji nazw domen, podmiot publiczny wskazany w załączniku nr 1 oraz operator obiektu energetyki jądrowej.

UWAGA

Dostawca usług zarządzanych w zakresie cyberbezpieczeństwa (MSSP, art. 5 ust. 1 pkt 3) podlega ustawie już od progu małego przedsiębiorcy (czyli od ok. 10 zatrudnionych osób i 2 mln EUR obrotu). To istotnie niższy próg niż ogólna zasada NIS2 (średni przedsiębiorca, czyli ok. 50 osób i 10 mln EUR). Każdy mniejszy MSSP, który dotąd uważał, że temat cyberbezpieczeństwa go nie dotyczy, powinien tę kwestię przeanalizować — szczegółowo wracamy do niej w wpisie o klasyfikacji podmiotu kluczowego i ważnego.

Kalendarz wdrożenia — terminy, których nie wolno przegapić

Nowelizacja KSC wprowadziła konkretną oś czasu, w której podmioty muszą zrealizować swoje obowiązki. Punktem startu jest **3 kwietnia 2026 r.** — dzień wejścia w życie ustawy.

Zgodnie z art. 16 ustawy:

- **12 miesięcy** — termin na realizację obowiązków rozdziału 3 (system zarządzania bezpieczeństwem informacji, dokumentacja, raportowanie incydentów, struktury wewnętrzne) od dnia spełnienia przesłanek uznania za podmiot kluczowy lub ważny;
- **24 miesiące** — termin na przeprowadzenie pierwszego audytu bezpieczeństwa systemu informacyjnego dla podmiotów kluczowych (art. 15 ust. 1 KSC).

Dla podmiotów istniejących w dniu wejścia w życie ustawy oba terminy liczy się od 3 kwietnia 2026 r. — czyli **3 kwietnia 2027 r.** to deadline na pełne wdrożenie systemu bezpieczeństwa, a **3 kwietnia 2028 r.** to ostateczny termin na pierwszy audyt. Do tego dochodzi termin z art. 7c ust. 1 — **6 miesięcy na złożenie wniosku o wpis do wykazu** od dnia spełnienia przesłanek (czyli dla istniejących podmiotów: do około października 2026 r.).

Etap	Termin	Co trzeba zrobić	Podstawa
Rejestracja w wykazie	~3 października 2026 r.	Złożenie wniosku o wpis do wykazu podmiotów kluczowych i ważnych w systemie S46	art. 7c ust. 1 KSC
Wdrożenie obowiązków rozdziału 3	3 kwietnia 2027 r.	System zarządzania bezpieczeństwem (art. 8), dokumentacja (art. 10), procedury incydentowe (art. 11), struktury wewnętrzne (art. 14)	art. 16 pkt 1 KSC
Pierwszy audyt podmiotu kluczowego	3 kwietnia 2028 r.	Audyt bezpieczeństwa systemu informacyjnego z art. 15 ust. 1	art. 16 pkt 2 KSC

Wysokie kary — także osobiste. Art. 73 ust. 3 KSC wprowadza karę do **10 000 000 EUR lub 2% przychodów** dla podmiotu kluczowego (w zależności od tego, która kwota jest wyższa, nie niższą jednak niż 20 000 zł), a art. 73 ust. 4 — do **7 000 000 EUR lub 1,4% przychodów** (nie mniej niż 15 000 zł) dla podmiotu ważnego. Art. 73 ust. 5 dopuszcza karę nawet do **100 000 000 zł** w razie naruszeń powodujących bezpośrednie i poważne cyberzagrożenie dla obronności, bezpieczeństwa państwa lub zdrowia ludzi. Art. 73a ust. 4 dopuszcza karę dla kierownika prywatnego podmiotu w wysokości **do 300% wynagrodzenia** obliczanego jak ekwiwalent za urlop. To realna zmiana modelu odpowiedzialności — i temat odrębnego wpisu w naszym cyklu.

Co zmieniła nowelizacja z 23 stycznia 2026 r.?

Rozszerzenie zakresu podmiotowego. Zamiast wąskiej kategorii „operatorów usług kluczowych" i „dostawców usług cyfrowych" znanej z poprzedniej wersji ustawy, mamy dwa nowe pojęcia — podmiot kluczowy i podmiot ważny — i istotnie szersze sektory wymienione w załączniku nr 1 i nr 2. Załącznik nr 1 obejmuje m.in. energetykę, transport, bankowość i infrastrukturę rynków finansowych, zdrowie, wodę pitną, ścieki, infrastrukturę cyfrową, zarządzanie usługami ICT i ICT Security, administrację publiczną oraz przestrzeń kosmiczną. Załącznik nr 2 dokłada m.in. pocztę i usługi kurierskie, gospodarkę odpadami, chemię, produkcję żywności, dostawców usług cyfrowych i działalność badawczą.

Nowe obowiązki kierownika. Art. 8c ustawy wprowadza wprost zasadę, że **kierownik podmiotu kluczowego lub ważnego ponosi odpowiedzialność za wykonywanie obowiązków w zakresie cyberbezpieczeństwa** — i to odpowiedzialność, której nie da się delegować. Art. 8d wymienia pięć konkretnych zadań kierownika, art. 8e wprowadza obowiązek corocznego, udokumentowanego szkolenia. Tematowi temu poświęcamy odrębny wpis o art. 8c–8e.

System zarządzania bezpieczeństwem — 14 obszarów. Art. 8 ust. 1 pkt 2 wymienia 14 obszarów (lit. a–n), które każdy podmiot kluczowy lub ważny musi wdrożyć w ramach systemu zarządzania bezpieczeństwem informacji. Od polityk szacowania ryzyka, przez bezpieczeństwo łańcucha dostaw, plany ciągłości działania, monitoring w trybie ciągłym, kryptografię, aż po podstawowe zasady cyberhigieny i polityki kontroli dostępu.

Surowe terminy raportowania incydentów. Art. 11 ust. 1 ustawy wymaga zgłoszenia wczesnego ostrzeżenia w ciągu **24 godzin** od momentu wykrycia incydentu poważnego, pełnego zgłoszenia w ciągu **72 godzin**, a sprawozdania końcowego w ciągu **miesiąca** od dnia zgłoszenia. Te terminy są tożsame z terminami DORA i NIS2 — i są bardzo krótkie. To temat, do którego wracamy w wpisie o procedurach incydentowych.

Jaka jest maksymalna kara z KSC?

Dla podmiotu kluczowego — do 10 000 000 EUR lub 2% przychodów (art. 73 ust. 3), nie mniej niż 20 000 zł. Dla podmiotu ważnego — do 7 000 000 EUR lub 1,4% przychodów (art. 73 ust. 4), nie mniej niż 15 000 zł. Przy naruszeniu powodującym poważne cyberzagrożenie — do 100 000 000 zł (art. 73 ust. 5).

Czy zarząd odpowiada osobiście za cyberbezpieczeństwo w KSC?

Tak. Art. 8c ust. 1 KSC wprowadza osobistą odpowiedzialność kierownika podmiotu kluczowego lub ważnego za wykonywanie obowiązków cybersec. Art. 73a ust. 4 dopuszcza karę pieniężną dla kierownika prywatnego do 300% wynagrodzenia, dla publicznego — do 100% (art. 73a ust. 5).

Czy podmiot finansowy podlega KSC, czy DORA?

Podmioty z sektora bankowości i infrastruktury rynków finansowych (załącznik nr 1 do KSC) podlegają zarówno KSC, jak i DORA, ale art. 8i ust. 1 KSC wyłącza dla nich większość obowiązków technicznych — zastępuje je rozporządzenie 2022/2554 (DORA). Z KSC pozostają obowiązki administracyjne (rejestracja, kierownik, szkolenia, KRK, cyberhigiena, polecenie zabezpieczające).

Najważniejsze działania do podjęcia na starcie

Decyzja klasyfikacyjna zarządu — czy jesteśmy podmiotem kluczowym, ważnym czy w ogóle nie objętym ustawą? Trzeba przeanalizować załączniki nr 1 i 2 oraz progi wielkościowe z rozporządzenia 651/2014/UE. W razie wątpliwości — wpisać podmiot z ostrożności, bo art. 7j pozwala organowi wpisać podmiot z urzędu, a obowiązki ciążą od dnia spełnienia przesłanek z art. 5, a nie od dnia wpisu.

Wyznaczenie odpowiedzialnych — kto w organizacji jest „kierownikiem podmiotu kluczowego lub ważnego" w rozumieniu art. 2 pkt 8a KSC (zwykle: cały zarząd), kto jest osobą delegowaną do spraw cyberbezpieczeństwa, kto będzie wśród minimum dwóch osób kontaktowych z art. 9 ust. 1 pkt 1.

Kick-off projektu wdrożeniowego — formalna decyzja zarządu o uruchomieniu projektu, budżet, harmonogram, kamienie milowe (rejestracja → wdrożenie → audyt).

Przegląd dokumentacji ICT — czy mamy aktualną inwentaryzację aktywów, czy mamy politykę bezpieczeństwa, plan ciągłości działania, procedurę zarządzania incydentami. Każdy z tych dokumentów będzie dowodem dla organu nadzorczego, że system z art. 8 KSC istnieje, a nie tylko jest na papierze.

PRACODAWCY RP

Podziękowanie