Legacy Turn
Grupa LT Mastery

SERIA: LEGACYTURN

UoKSC i NIS2 w Praktyce

Praktyczny podręcznik implementacji krajowego systemu cyberbezpieczeństwa
Frameworki, procedury i audyt
dla zarządów, IT i *compliance*

Piotr Szymczyk

grupy LT Mastery

SERIA LEGACYTURN

UoKSC i NIS2 w praktyce

Praktyczny podręcznik implementacji Krajowego Systemu Cyberbezpieczeństwa

Frameworki, procedury, audyt dla zarządów, IT i compliance

„Bezpieczeństwo nie jest produktem, który się kupuje. To proces, który się buduje”

- Bruce Schneier

Piotr Szymczyk · LegacyTurn · 2026

UoKSC i NIS2 w praktyce

Praktyczny podręcznik implementacji Krajowego Systemu Cyberbezpieczeństwa

Seria: LegacyTurn - Cyberbezpieczeństwo i Compliance

Wydanie: Pierwsze, 2026

Autor: Piotr Szymczyk

Konsultant cyberbezpieczeństwa, audytor, wykładowca, trener

E-mail: biuro@legacyturn.com

Tel.: +48 600 390 516

www.legacyturn.com

ISBN: 978-83-981562-0-2

Spis Treści

O serii LegacyTurn

LegacyTurn to seria wydawnicza o cyberbezpieczeństwie dla organizacji i pracowników, którzy wolą działać niż czytać komentarze do ustaw. Każdy tytuł piszę tak, żeby czytelnik wiedział co robić dalej. Seria powstała po to, żeby zrozumieć nie tylko co regulacja mówi, ale jak ją wdrożyć, udokumentować i obronić przed audytorem. Dość często wplatają mi się angielskie słowa w moją prozę, gdyż cyberbezpieczeństwo i nowoczesne zarządzanie (Cyber Governance) to dziedziny, w których angielskie nazewnictwo stało się globalnym standardem. W tej książce świadomie rezygnuję z siłowego i sztucznego tłumaczenia niektórych pojęć na język polski, np.:

Kiedy manager, prawnik czy inżynier stają w obliczu incydentu, nie szukają „oprogramowania wymuszającego okup", lecz reagują na ransomware. Nie audytują „zgodności z przepisami", tylko sprawdzają compliance.

Żeby książka przygotowała Cię do realnych rozmów w biznesie i z audytorami, wszędzie tam, gdzie polskie odpowiedniki brzmią archaicznie lub nieprecyzyjnie, posługuję się powszechnie przyjętym żargonem branżowym.

Sześć cech, które odróżniają tę serię od innych publikacji o NIS2 i UoKSC:

1. każdy rozdział jest napisany językiem konkretnej roli - Zarządu, IT/Security, Compliance, Audytu, OT/ICS, HR i Legal/Procurement. Czytasz to co dotyczy Ciebie, nie całą ustawę.
2. traktuj tę książkę jak przewodnik, w którym każdy rozdział żyje własnym życiem. Możesz czytać je osobno i w dowolnym momencie, a i tak dostaniesz komplet informacji o tym, co trzeba zrobić w danym kroku. Jeśli po drodze trafisz na podobne myśli lub informacje – bez obaw, to nie jest błąd! Niektóre kwestie powtarzam celowo, żeby każdy rozdział bronił się sam, będąc jednocześnie elementem większej całości.
3. całość została wzbogacona o dodatkowe rozdziały dotyczące regulacji DORA, RODO, AI Act, a także roli czynnika ludzkiego (pracowników) w obszarze Security. Ich celem jest przedstawienie szerszego kontekstu oraz zobrazowanie wzajemnych zależności pomiędzy omawianymi przepisami
4. tabele, checklisty i frameworki do użycia bezpośrednio w organizacji - nie „co mówi przepis" ale „co masz zrobić w przysłowiowy poniedziałek"
5. każda sekcja kończy się tym czego szuka audytor KSC - nie domyślasz się, po prostu wiesz
6. seria uwzględnia stan prawny na moment wydania, z oznaczeniem datowanym

INNE TYTUŁY SERII LEGACYTURN

Tytuł	Dla kogo	Status
UoKSC i NIS2 w praktyce	Wszystkie role - kompletny przewodnik operacyjny	Ta książka
NIS2 dla Zarządu	CEO, członkowie zarządu, dyrektorzy generalni	W przygotowaniu
Audyt KSC w praktyce	Audytorzy wewnętrzni i zewnętrzni KSC	W przygotowaniu
Cyber Resilience Act dla producentów	Producenci sprzętu i oprogramowania (CRA)	W przygotowaniu
DORA dla sektora finansowego	Banki, ubezpieczyciele, instytucje płatnicze	W przygotowaniu
NIS2 szablony - wersja PREMUM	Compliance, IT/Security - gotowe do użycia	W przygotowaniu
Cyberbezpieczeństwo w obszarze IT/OT, NIS2, CRA	IT/OT, Producenci Sprzętu	W przygotowaniu

Od Autora

Powyższa lista to dopiero początek. Seria LegacyTurn nie powstaje za biurkiem teoretyka. Kolejne książki będę pisał na bieżąco - na podstawie tego, co wynika z moich szkoleń i wdrożeń NIS2. Jeśli podczas warsztatu widzę, że konkretna branża lub rola ma problem z jakimś przepisem, po prostu usiadam i piszę dedykowany podręcznik. Masz temat z obszaru cyberbezpieczeństwa, którego nikt jeszcze prosto nie opisał? Napisz na biuro@legacyturn.com - następna książka może być odpowiedzią na Twoje wyzwanie.

Kontakt LegacyTurn.com

Wprowadzenie

Dlaczego powstała ta książka

Prezes jednej z polskich firm energetycznych opowiedział mi historię z zeszłego roku. Dostał telefon od „audytora z ministerstwa". Mężczyzna był uprzejmy, znał szczegóły, wiedział, jak nazywają się kluczowe systemy. Poprosił o pilny dostęp do dokumentacji. Prezes przekazał dane. Trzy godziny później CSIRT NASK zadzwonił z pytaniem czy wiedzą, że ktoś właśnie mapuje ich sieć OT.

Żaden firewall tego nie zatrzymał. Zatrzymałaby to wiedza, wiedza, że takie rozmowy się zdarzają, że istnieje procedura weryfikacji, że pracownicy wiedzą komu zgłaszać podejrzenia. Tych rzeczy nie da się kupić w sklepie z oprogramowaniem.

Regulacje cybernetyczne UE eksplodowały. W ciągu kilku lat pojawiły się: NIS2, nowelizacja UoKSC, Cyber Resilience Act (CRA), DORA, AI Act, CER i inne. Każda nakłada kolejne obowiązki, mówi nieco innym językiem i dotyczy nieco innych podmiotów. Rzeczywistość organizacyjna jest jeszcze inna niż rzeczywistość regulacyjna.

Zarząd chce wiedzieć, co mu grozi i co ma zrobić. Dział IT - co wdrożyć i jak udokumentować. Audytor - co sprawdzić i jakich dowodów szukać. Prawnik - jakie klauzule wpisać do umów. HR - jakie szkolenia zorganizować. Tej książki brakowało na rynku: przewodnika, który mówi do każdej roli jej własnym językiem.

> **Ważna informacja prawna**
>
> Ta książka nie jest komentarzem prawnym ani oficjalną wykładnią przepisów. Jest podręcznikiem operacyjnym dla profesjonalistów, którzy muszą działać i wdrażać skuteczne rozwiązania, a nie tylko teoretycznie rozumieć ustawę.
>
> Zawarte tu analizy, szablony i wskazówki odzwierciedlają najlepszą wiedzę i praktyczne doświadczenie autora, jednak każda organizacja posiada unikalną specyfikę prawną i technologiczną. Treść tej publikacji nie zastępuje indywidualnej porady prawnej ani dedykowanego audytu zgodności.

Co zyskujesz czytając tę książkę

To nie jest książka, którą czyta się raz i odkłada na półkę. To narzędzie pracy do którego warto sięgnąć, gdy audytor ogłasza kontrolę, gdy prezes pyta o ryzyko, gdy CISO składa wniosek o budżet.

Jeśli Twoja rola to:	Po przeczytaniu...
Zarząd	Będziesz wiedział jakie pytania zada Ci audytor KSC, które dokumenty musisz podpisać osobiście i jak chronić się przed odpowiedzialnością do 300% wynagrodzenia
IT / Security	Masz kompletny plan wdrożenia 10 obszarów art. 8 UoKSC, wiesz od czego zacząć (MFA), jak zbudować „analizę niezgodności" i co przygotować dla audytora
Compliance	Masz matrycę 14 obowiązkowych polityk, rytm PDCA na cały rok i narzędzia do walki z „fake compliance", czyli tzw. pozorną zgodnością
Audytor	Masz listę 15 pytań audytowych, TOP 5 niezgodności i mapę zakresu audytu KSC wg szablonu Ministerstwa Cyfryzacji
OT / ICS	Rozumiesz, dlaczego Twoje środowisko rządzi się innymi prawami niż IT i co konkretnie zrobić z każdym z 10 obszarów art. 8

Cyberbezpieczeństwo jako ryzyko biznesowe

Przez lata cyberbezpieczeństwo było problemem działu IT. Zarządy delegowały ten temat w dół struktury i wracały do niego po incydentach. NIS2 i UoKSC zamknęły tę drogę. Osoby kierujące podmiotem kluczowym lub ważnym ponoszą osobistą odpowiedzialność za poziom cyberbezpieczeństwa organizacji. Kary sięgają 300% wynagrodzenia kierownika. Organizacja może zostać ukarana grzywną do 10 milionów euro lub 2% globalnego obrotu.

Cyberatak może zatrzymać produkcję, zablokować infrastrukturę krytyczną i sparaliżować usługi kluczowe. Wyciek danych narusza RODO, NIS2 i reputację jednocześnie. Incydent u dostawcy ICT może mieć skutki równie dotkliwe jak incydent wewnętrzny. Brak dokumentacji jest traktowany przez organy nadzoru tak samo poważnie jak brak wdrożenia.

> Cyberbezpieczeństwo stało się ryzykiem biznesowym klasy A - obok ryzyka finansowego, operacyjnego i reputacji firmy. To nie jest tylko zmiana kosmetyczna.

Jak korzystać z tego podręcznika

Książka jest zbudowana warstwowo. Możesz czytać ją od początku do końca albo korzystać selektywnie, zależnie od roli i potrzeb. Każdy rozdział jest zaprojektowany jako niezależna jednostka. Możesz zacząć od sekcji swojej roli i nie tracić kontekstu.

Struktura książki

Część	Co znajdziesz
Orientacja strategiczna	Mapa regulacji UE, klasyfikacja podmiotów PK/PW, słownik pojęć. Zacznij tutaj, jeśli dopiero wchodzisz w temat
Część 0 - NIS2/UoKSC w praktyce	Klasyfikacja, rejestracja S46, analiza ryzyka, SZBI, incydenty, łańcuch dostaw, audyt, roadmapa wdrożenia. Rdzeń tej książki
Część I - Regulacje pokrewne	CRA, DORA, RODO, AI Act. Dla organizacji objętych więcej niż jednym aktem prawnym
Część II - Human Layer Security	Kultura bezpieczeństwa, szkolenia, insider threat- zagrożenie ze strony pracownika, rola HR w cyberbezpieczeństwie
Część III – Narzędzia, szablony, checklisty	Szablony, matryce, checklisty i narzędzia wdrożeniowe do użycia bezpośrednio w organizacji

Mapa rozdziałów według ról

Poniższa tabela pozwala zbudować własną ścieżkę lektury. Zacznij od rozdziałów kluczowych dla Twojej funkcji, pozostałe traktuj jako kontekst. Nawet czytając z perspektywy jednej roli, warto przejrzeć rozdziały adresowane do innych - cyberbezpieczeństwo to gra zespołowa.

Rola	Kim jesteś	Kluczowe rozdziały dla Ciebie
Zarząd	CEO, członek zarządu, dyrektor generalny, rada nadzorcza	4 (governance i odpowiedzialność), 6 (incydenty i cyberkryzys), 8 (audyt KSC), 9 (roadmapa NIS2)
IT / Security	CISO, administrator sieci, architekt bezpieczeństwa, inżynier SOC	3 (analiza ryzyka), 5 (SZBI i 10 obszarów), 6 (incydenty), 7 (łańcuch dostaw ICT)

Rola	Kim jesteś	Kluczowe rozdziały dla Ciebie
Compliance / IOD	Inspektor ochrony danych, compliance officer, prawnik wewnętrzny	1 (klasyfikacja PK/PW), 2 (rejestracja S46), 5 (SZBI), 12 (RODO i NIS2)
Audyt	Audytor wewnętrzny i zewnętrzny, kontroler, rewident	8 (audyt KSC i metodyka), 8A (pierwsze 48h), 3 (ryzyko), 9A (model dojrzałości)
OT / ICS	Inżynier automatyki, specjalista OT/SCADA, kierownik produkcji	3 (ryzyko OT), 6 (incydenty OT), 5 sekcja OT
HR	Dyrektor HR, specjalista ds. szkoleń, People & Culture	14 (human layer security), 4 (odpowiedzialność personelu), 5 (SZBI)
Legal / Procurement	Radca prawny, kierownik zakupów, category manager ICT	7 (łańcuch dostaw i klauzule), 10 (CRA), 11 (DORA), 2 (rejestracja i S46)

! Nota o obowiązku szkoleniowym (art. 8e UoKSC) Osoby kierujące podmiotem kluczowym lub ważnym są zobowiązane do regularnego uczestnictwa w szkoleniach z cyberbezpieczeństwa minimum raz w roku. Art. 8e ust. 2 UoKSC wymaga „uczestnictwa w szkoleniach” - sama lektura książki nie spełnia tego wymogu. Książka może być jednak jednym z elementów udokumentowanego szkolenia wewnętrznego lub warsztatów, w ramach których kierownictwo zapoznaje się z jej treścią. Kluczowa jest dokumentacja: lista obecności ze szkolenia z datą i podpisami, protokół szkolenia lub zaświadczenie wystawione przez prowadzącego. Brak akredytacji dostawców szkoleń w UoKSC oznacza, że podmiot sam decyduje o formie - pod warunkiem udokumentowania zakresu zgodnego z art. 8e ust. 2.

O autorze

Książka ma jednego autora - praktyka. NIS2 jest zbyt często opisywana przez osoby, które czytały przepisy, ale ich nie wdrażały. Przez ostatnie kilka miesięcy byłem zanurzony w regulacjach, jednocześnie pomagając organizacjom przejść przez klasyfikację, rejestrację S46, analiza niezgodności i pierwsze kroki SZBI. Wynik tej pracy trzymasz w rękach.

Piotr Szymczyk - Technical Project Manager i Konsultant, Audytor Cyberbezpieczeństwa z ponad 25 - letnim doświadczeniem w GRC i bezpieczeństwie informacji. Magister Informatyki i Ekonometrii Uniwersytetu Łódzkiego. Certyfikowany Audytor ISO/IEC 27001, AgilePM Practitioner, absolwent EITCA Academy of Information Security i ITIL 4. Twórca LegacyTurn Grupy LT Mastery, firmy szkoleniowo - konsultingowej specjalizującej się w cyberbezpieczeństwie dla biznesu.

Kontakt do mnie:

biuro@legacyturn.com · linkedin.com/in/piotr - szymczyk - cyber - security

Nota od autora

Niniejsza publikacja opiera się na wieloletniej praktyce zawodowej uzupełnionej o intensywną pracę badawczą prowadzoną bezpośrednio przed wydaniem. Poświęciłem ostatnie kilka miesięcy na analizę tekstów prawnych, wytycznych ENISA, rekomendacji Ministerstwa Cyfryzacji i dokumentacji audytowej, konfrontując je z rzeczywistymi wdrożeniami NIS2 w polskich organizacjach. W tekście świadomie i często korzystam z angielskich słów oraz branżowego żargonu (jak *compliance*, *runbook*, *framework* czy *ransomware*). Robię to celowo. W świecie cyberbezpieczeństwa i prawa unijnego te terminy to globalny standard. Tłumaczenie „na siłę" na język polski na potrzeby książki byłoby sztuczne. Na szkoleniach i podczas audytów i tak rozmawiamy językiem praktyków, a nie podręczników akademickich. Jednocześnie mam pełną świadomość, że żaden pojedynczy podręcznik nie może wyczerpywać całości tak rozległej i dynamicznej materii, jak cyberbezpieczeństwo i prawo cybernetyczne. Ta książka zawiera to, co na dzień wydania uznałem za najważniejsze, najbardziej operacyjne i najlepiej zweryfikowane w mojej codziennej praktyce wdrożeniowej. Nie zawiera wszystkiego i nie aspiruje do bycia jedynym źródłem wiedzy na świecie. Daje Ci jednak solidne, przetestowane ramy (frameworki), które możesz zacząć wdrażać w swojej organizacji od zaraz.

** Nota o współautorstwie technologicznym. Strukturę wybranych tabel, matryc decyzyjnych i checklisty opracowałem z pomocą narzędzi AI. Połączenie wiedzy eksperckiej z analitycznymi możliwościami AI pozwoliło nadać tym elementom maksymalnie skondensowaną, czytelną i pragmatyczną formę, idealną do użycia w warunkach Twojej organizacji.*

- Piotr Szymczyk, Łódź 2026

Rozdział 0

Orientacja strategiczna i ekosystem regulacyjny UE

NIS2 · UoKSC · CRA · DORA · AI Act · RODO · CER · Data Act

„Pierwszym krokiem do mądrości jest nazywanie rzeczy właściwymi imionami”

- Konfucjusz

Piotr Szymczyk · LegacyTurn · 2026

Rozdział 0 - Orientacja strategiczna i ekosystem regulacyjny UE

0.1 Panorama regulacji UE 2024–2028

W latach 2022–2028 wchodzi lub wejdzie w życie co najmniej dziewięć aktów prawnych UE dotyczących cyberbezpieczeństwa, ochrony danych i odporności cyfrowej. To nie przypadek. To świadoma odpowiedź na rosnące zagrożenia i na dekadę, w której państwa członkowskie radziły sobie z nimi każde po swojemu.

Dla organizacji działających w UE oznacza to jedno: nie wystarczy wiedzieć która regulacja Cię dotyczy. Trzeba rozumieć jak regulacje na siebie wpływają, gdzie wymagania się pokrywają, gdzie mogą powstawać konflikty i jak ustawić priorytety wdrożenia. Wskazówka nawigacyjna: jeśli Twoje pierwsze pytanie brzmi „czy NIS2/UoKSC w ogóle mnie dotyczy?" - przejdź bezpośrednio do sekcji 0.3 z drzewkiem decyzyjnym. Jeśli już wiesz, że jesteś PK lub PW i chcesz zrozumieć szerszy ekosystem regulacyjny - czytaj kolejno od 0.1.

9 GŁÓWNYCH REGULACJI UE W OBSZARZE CYBERBEZPIECZEŃSTWA

Akt	Podstawa	Zakres	Kogo dotyczy	Status PL
NIS2	Dyrektywa 2022/2555	Bezpieczeństwo sieci i systemów - fundament ekosystemu	Wszystkie sektory kluczowe i ważne (18 sektorów)	Wdrożona przez UoKSC 2026 (w życie 16.01.2023, termin transpozycji 17.10.2024, PL z opóźnieniem)
UoKSC	Dz.U. 2026 poz. 252	Polska implementacja NIS2 z terminami i sankcjami	Podmioty kluczowe i ważne w Polsce	Obowiązuje od 2026

Akt	Podstawa	Zakres	Kogo dotyczy	Status PL
Rozp. 2024/2690	Rozp. Wyk. KE 2024/2690	Techniczne wymagania zarządzania ryzykiem dla wybranych dostawców ICT	MSP (dostawcy usług zarządzanych IT), MSSP (dostawcy usług cyberbezpieczeństwa), DNS, TLD, chmura (CSP), CDN, DC, platformy cyfrowe, wyszukiwarki, sieci społecznościowe	Bezpośrednio stosowane w UE
CRA	Rozp. UE 2024/2847	Security by design, zarządzanie podatnościami (CVE) dla produktów z elementami cyfrowymi - sprzęt (w tym przemysłowy: PLC, HMI, IoT), oprogramowanie samodzielne i SaaS	Producenci, importerzy, dystrybutorzy HW/SW	Etapowo 2025–2027
DORA	Rozp. UE 2022/2554	Operacyjna odporność cyfrowa sektora finansowego - TLPT, rejestry umów	Banki, ubezpieczyciele, fintech, dostawcy ICT dla finansów	Obowiązuje od 01.2025
AI Act	Rozp. UE 2024/1689	Bezpieczeństwo i przejrzystość systemów AI wg poziomu ryzyka	Dostawcy i firmy wdrażające systemy AI: wszystkich klas (zakazy art. 5 dotyczą wszystkich), wysokiego ryzyka (Zał. III), GPAI (modele ogólnego przeznaczenia)	Etapowo 2024–2026

Akt	Podstawa	Zakres	Kogo dotyczy	Status PL
RODO	Rozp. UE 2016/679	Ochrona danych osobowych - incydenty NIS2 generują równoległy obowiązek	Wszystkie org. przetwarzające dane obywateli UE	Obowiązuje od 2018
CER	Dyrektywa 2022/2557	Odporność fizyczna podmiotów krytycznych - uzupełnienie NIS2 o wymiar fizyczny	Operatorzy infrastruktury krytycznej - 11 sektorów	Termin transpozycji: 17.10.2024; Polska z opóźnieniem (podobnie jak przy NIS2) - brak pełnej implementacji na dzień wydania
Data Act	Rozp. UE 2023/2854	Dostęp do danych i ich dzielenie - bezpieczne udostępnianie danych IoT	Producenci urządzeń IoT, dostawcy usług danych	Obowiązuje od 2025

> ! Rozp. 2024/2690 to akt często pomijany. Dotyczy bezpośrednio MSP (dostawców usług zarządzanych IT), MSSP (dostawców usług cyberbezpieczeństwa), dostawców DNS, TLD, chmury, CDN i platform cyfrowych. Obowiązuje bezpośrednio w całej UE - bez potrzeby implementacji krajowej. Jeśli jesteś MSSP lub dostawcą usług cyfrowych - to Twój akt prawny również.

NIS2 - fundament ekosystemu

Dyrektywa NIS2 (2022/2555) zastąpiła NIS1 z 2016 roku, która okazała się niewystarczająca wobec rosnącej skali zagrożeń. NIS2 rozszerzyła zakres z 7 do 18 sektorów, wprowadziła podział na PK i PW, podniosła sankcje i po raz pierwszy nałożyła osobistą odpowiedzialność na kierownictwo. NIS2 nie jest regulacją techniczną. Jest to regulacja zarządcza.

SANKCJE - porównanie 6 regulacji UE			
Akt	**Kara dla organizacji**	**Kara dla kierownictwa**	**Uwagi**
NIS2 / UoKSC (PK)	Do 10 mln EUR lub 2% globalnego obrotu	Do 300% wynagrodzenia - osobista, niezależna	Egzekucja kar od 3.04.2028. nadzór i decyzje nakazowe od 3.04.2026
NIS2 / UoKSC (PW)	Do 7 mln EUR lub 1,4% globalnego obrotu	Do 300% wynagrodzenia - osobista, niezależna	Tryb nadzoru ex - post. Kary niezależne od kary dla organizacji
CRA	Do 15 mln EUR lub 2,5% globalnego obrotu	Brak osobistych kar dla kierownictwa	Najwyższe kary za braki bezpieczeństwa produktów. Dotyczy producentów
DORA	Do 1% średniego dziennego obrotu za poprzedni rok (art. 50 ust. 1 DORA w zw. z implementacją krajową); nakłada KNF w Polsce wg wytycznych EBA/ESMA/EIOPA	Krajowe sankcje nadzorcze wg KNF (Polska); możliwy zakaz pełnienia funkcji kierowniczych (art. 50 ust. 4 DORA)	DORA ma pierwszeństwo przed NIS2 dla sektora finansowego
AI Act	Do 35 mln EUR lub 7% obrotu (zakazy art. 5) / do 30 mln EUR lub 6% obrotu (systemy wysokiego ryzyka)	Brak osobistych kar dla kierownictwa	Najwyższe sankcje za zakazane zastosowania AI i systemy wys. ryzyka
RODO	Do 20 mln EUR lub 4% rocznego obrotu	Brak osobistych kar (ale odpowiedzialność cywilna)	Incydent NIS2 naruszający dane os. generuje równoległy obowiązek RODO

0.2 Mapa regulacji cybernetycznych UE

Znajomość poszczególnych regulacji to dopiero początek. Organizacje, które wdrażają je osobno, bez koordynacji, tworzą dublującą się biurokrację i przegapiają obszary, gdzie jedno działanie spełnia kilka wymogów naraz.

TIMELINE WDROŻEŃ REGULACJI UE - kto, co i kiedy

Data	Regulacja	Co wchodzi w życie	Kogo dotyczy
2018	RODO	Pełne stosowanie ochrony danych osobowych	Wszystkie organizacje przetwarzające dane osób w UE
01.2025	DORA	Pełne stosowanie dla sektora finansowego	Banki, ubezpieczyciele, fintech, kluczowi dostawcy ICT
02.2025	CRA (częściowo)	Pierwsze obowiązki dla producentów - zgłaszanie podatności	Producenci sprzętu i oprogramowania
2025	Data Act	Obowiązki w zakresie dostępu do danych IoT	Producenci urządzeń IoT, dostawcy usług danych
08.2025	AI Act (częściowo)	Zakazy AI z art. 5 (zakazane zastosowania) + obowiązki dla GPAI (art. 51–56). UWAGA: systemy AI wysokiego ryzyka z Zał. III obowiązują dopiero od 2.08.2026, nie od tej daty	Dostawcy systemów AI, duże modele językowe
04.2026	UoKSC / NIS2 PL	Wejście w życie nowelizacji UoKSC - nadzór aktywny	Wszystkie PK i PW - ex - ante (PK) i ex - post (PW)
05–10.2026	UoKSC - S46	Okno rejestracji PK/PW: 7.05–3.10.2026	Wszystkie PK i PW nie wpisane z urzędu
08.2026	AI Act (pełne)	Pełne stosowanie dla systemów AI wysokiego ryzyka z Załącznika III (dostawcy, firmy wdrażające) - od 2.08.2026	Dostawcy i użytkownicy systemów AI wys. ryzyka

Data	Regulacja	Co wchodzi w życie	Kogo dotyczy
11.12.2027	CRA (pełne)	Pełne wymagania bezpieczeństwa dla wszystkich klas produktów (36 mies. od 11.12.2024). Raportowanie podatności - od 11.09.2026 (21 mies.)	Producenci, importerzy, dystrybutorzy HW/SW
04.2028	UoKSC - kary	Pełna wymagalność kar finansowych dla PK i PW (art. 130 ust. 1 ustawy nowelizującej - Dz.U. 2026 poz. 252: przepis przejściowy - kary egzekwowane po upływie 2 lat od wejścia w życie)	Wszystkie PK i PW - nadzór aktywny już od 2026

> **!** Zacznij teraz. Nie czekaj na deadline Wdrożenie SZBI zajmuje 7–8 miesięcy dla średniej organizacji (50–250 pracowników); dla dużych podmiotów z OT lub wieloma lokalizacjami jest to 12–18 miesięcy. Deadline rejestracji S46 to 3 października 2026. Organizacje, które zaczną wtedy, nie zdążą z 12 - miesięcznym terminem na wdrożenie. Analizę ryzyka zacznij równolegle z rejestracją S46

Obszary wspólne - jedno wdrożenie, wiele efektów

Wiersze z wieloma ✓ to priorytety wdrożeniowe. Zobacz np. zarządzanie ryzykiem i obsługa incydentów pojawiają się w co najmniej pięciu regulacjach naraz. Zacznij od tego obszaru.

Obszar wymagań	NIS2/UoKSC	DORA	CRA	RODO	AI Act	CER
Zarządzanie ryzykiem	✓	✓	✓	✓	✓	✓
Obsługa incydentów	✓	✓	✓	✓	-	-
Łańcuch dostaw / ICT	✓	✓	✓	-	✓	-
Ciągłość (BCP/DR)	✓	✓	✓	-	-	-
Kontrola dostępu i MFA	✓	✓	-	✓	-	-

Obszar wymagań	NIS2/UoKSC	DORA	CRA	RODO	AI Act	CER
Szkolenia / awareness	✓	✓	-	✓	-	✓
Raportowanie do organu	✓	✓	✓	✓	-	✓
Ochrona danych osobowych	✓	-	-	✓	-	-
Testowanie bezpieczeństwa *	✓	✓	-	✓	-	-
Governance / odp. zarządu	✓	✓	-	✓	✓	-
Bezpieczeństwo produktów (by design)	-	-	✓	-	✓	-
Odporność fizyczna	✓	-	-	-	-	✓

** Testowanie bezpieczeństwa w kontekście RODO: art. 32 ust. 1 lit. d RODO wymaga „regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych" - co jest interpretowane przez organów nadzorczych jako obejmujące testy bezpieczeństwa. Należy traktować jako interpretację rozszerzoną art. 32 RODO, nie jako wymaganie wprost.*

Jak regulacje na siebie wpływają - cztery kluczowe relacje

Para regulacji	Relacja i co z niej wynika w praktyce
NIS2 i RODO	Incydent naruszający dane osobowe generuje jednocześnie raport do CSIRT (NIS2: 24h/72h) i do UODO (RODO: 72h). Procedury muszą być skoordynowane - dwie całkowicie niezależne procedury bez punktów styku to błąd operacyjny **Koordynacja oznacza w praktyce:** (1) CISO powiadamia IOD niezwłocznie po potwierdzeniu incydentu - IOD ocenia, czy dotyczą dane osobowe i uruchamia własny zegar 72h do UODO. (2) Jeden Crisis Team podejmuje decyzje dla obu zgłoszeń. (3) Procedura zarządzania incydentami zawiera expressis verbis ścieżkę RODO jako równoległą gałąź decyzyjną - nie osobny dokument
NIS2 i DORA	DORA ma pierwszeństwo w obszarach, które reguluje (zasada subsydiarności). W obszarach nieregulowanych przez DORA obowiązują wymagania NIS2/UoKSC.

Para regulacji	Relacja i co z niej wynika w praktyce
	Dla podmiotów finansowych będących jednocześnie PK/PW konieczna jest mapa zgodności pokazująca które wymaganie pochodzi z której regulacji i który organ je egzekwuje. Dwa równoległe tory raportowania incydentów: KNF (4h/24h/72h wg DORA) i CSIRT NASK (24h/72h wg UoKSC). Ten sam incydent - dwa niezależne formularze
NIS2 i CRA	Łańcuch dostaw produktów cyfrowych: podmiot kluczowy lub ważny może wymagać od dostawcy certyfikatu zgodności CRA jako elementu weryfikacji dostawcy przed nawiązaniem współpracy. CRA tworzy nowy standard rynkowy: produkty cyfrowe bez dokumentacji bezpieczeństwa zgodnej z CRA stają się trudniejsze do zakupu przez PK/PW, bo odpowiedzialność za łańcuch dostaw spoczywa na nabywcy. Klauzule umowne z dostawcami produktów cyfrowych powinny zawierać wymóg zgodności z CRA lub plan dojścia do zgodności z datą
NIS2 i AI Act	Organizacje wdrażające systemy AI wysokiego ryzyka w środowiskach objętych NIS2 muszą zarządzać ryzykiem AI jako integralnym elementem SZBI - nie jako osobnym projektem Shadow AI to nowy wektor ryzyka pojawiający się regularnie w audytach KSC od 2025 roku: niezatwierdzone narzędzia AI używane przez pracowników bez wiedzy IT i Compliance Poważny incydent AI (art. 73 AI Act: 15 dni lub 24h) może jednocześnie być poważnym incydentem KSC (art. 11 UoKSC: 24h). Procedura zgłaszania incydentów musi obejmować oba tory

Stan na czerwiec 2026 r. Relacje między regulacjami mogą być doprecyzowywane przez akty wykonawcze i orzecznictwo organów nadzorczych.

0.3 Który akt dotyczy Twojej organizacji?

Przed wdrożeniem wymagań regulacyjnych organizacja powinna odpowiedzieć sobie na jedno pytanie: *Które przepisy jej dotyczą i w jakim zakresie?*

Odpowiedź wymaga analizy sektorowej, wielkościowej i funkcjonalnej. W praktyce wiele organizacji dowiaduje się o swoim statusie PK lub PW dopiero z pisma organu właściwego. Zachęcam, żebyś nie czekał na tą korespondencję.

Drzewko decyzyjne - czy NIS2 / UoKSC Cię dotyczy?

Krok	Pytanie	Szczegóły	TAK →	NIE →
1	Sektor	Czy działasz w co najmniej jednym z 18 sektorów NIS2? Sprawdź wszystkie kody PKD - nie tylko główny	Idź do kroku 2	Co do zasady NIS2 Cię nie dotyczy, sprawdź wyjątki ustawowe
2	Wielkość	Czy zatrudniasz ≥50 osób LUB osiągasz obrót >10 mln EUR? Licz z podmiotami powiązanymi (rozp. 651/2014)	Idź do kroku 3	Co do zasady poza zakresem, ale: MSP/MSSP lub jedyny dostawca usługi w kraju?
3	Typ PK/PW	Zał.1 + duże → PK. Zał.1 + średnie → PW. Zał.2 + duże/średnie → PW. Infrastruktura cyfrowa (IXP, DNS, TLD, DC, CDN) → PK niezależnie od wielkości. MSP/MSSP (usługi zarządzane IT/cyberbezpieczeństwo) → zawsze PK. Uwaga: zwykła firma IT świadcząca helpdesk lub wdrożenia ERP NIE jest automatycznie PK - musi świadczyć usługi zarządzane (MSP) lub cyberbezpieczeństwo (MSSP)	Ustal PK lub PW Idź do kroku 4	-
4	Wpis z urzędu	Sprawdź wykaz - ksc.gov.pl. NBP, BGK, KNF, PAP i inne instytucje są wpisane automatycznie	Nie składasz S46, ale masz pełne obowiązki UoKSC od dnia wpisu	Złóż wniosek S46 w oknie 7.05 - 3.10.2026
5	Dostawca ICT	Czy dostarczasz produkty lub usługi ICT podmiotom PK/PW? Czy jesteś MSSP, CSP, dostawcą DNS/TLD lub CDN?	Możesz podlegać pośrednio lub bezpośrednio (MSP/MSSP = zawsze PK)	Sprawdź czy klient PK/PW wymaga klauzuli NIS2 w umowie

> Dostawca ICT obsługujący podmiot kluczowy lub ważny nie jest automatycznie PK lub PW. Ale jego incydent może być incydentem PK/PW. I jego umowa musi zawierać klauzule bezpieczeństwa - bo PK/PW odpowiada za łańcuch dostaw.

ROZDZIAŁ 1

Klasyfikacja PK/PW

Kim jesteś w świetle prawa i co z tego wynika

Dla ról: Zarząd · Compliance / IOD · Audyt

„Pierwszym krokiem do mądrości jest nazywanie rzeczy właściwymi imionami”

- Konfucjusz

Piotr Szymczyk · LegacyTurn · 2026

Część I – NIS2 i UoKSC; Rozdział 1 - Klasyfikacja podmiotów kluczowych i ważnych (PK/PW)

1.1 Dlaczego klasyfikacja ma znaczenie operacyjne

Miałem na szkoleniu prezesa firmy z sektora energetycznego. Pytał, kiedy złożyć wniosek S46. Odpowiedziałem: to proszę drugie pytanie - pierwsze brzmi: jakim podmiotem w świetle UoKSC jest Państwa organizacja? Milczał przez chwilę. Potem powiedział: „prosiłem CISO, żeby to sprawdził". To jest błąd. Za błędną klasyfikację nie odpowiada CISO, lecz prezes.

Różnica między PK a PW jest prosta w teorii i kosztowna w praktyce, jeśli się jej nie rozumie. PK to tryb ex - ante: audytor może przyjść w każdej chwili, bez incydentu, bez uprzedzenia. PW to tryb ex - post - zazwyczaj po incydencie lub skardze. „Zazwyczaj" to słowo, które kosztuje organizacje, które wzięły je zbyt dosłownie.

Co równie istotne: klasyfikacja **NIE różnicuje wymagań wdrożeniowych.** Oba typy podmiotów muszą wdrożyć te same 10 obszarów art. 8 UoKSC, prowadzić analizę ryzyka, zarządzać incydentami i zabezpieczyć łańcuch dostaw. Klasyfikacja określa konsekwencje za brak wdrożenia wymogów Ustawy o KSC i co ważne nie zwalnia z obowiązku ich wdrożenia.

> Klasyfikacja PK/PW to decyzja zarządcza, nie działu IT. Zarząd ponosi osobistą odpowiedzialność za błędną klasyfikację - w tym za zaniechanie rejestracji S46 w wymaganym terminie.

1.2 Podmiot kluczowy vs podmiot ważny - porównanie

Poniższa tabela zestawia kluczowe różnice między PK i PW w wymiarze operacyjnym. Oba typy podmiotów mają te same obowiązki wdrożeniowe - różnią się wyłącznie modelem nadzoru, ryzykiem kontroli i wysokością potencjalnych sankcji.

PODMIOT KLUCZOWY vs PODMIOT WAŻNY - kluczowe różnice operacyjne

Kryterium	Podmiot Kluczowy (PK)	Podmiot Ważny (PW)
Nadzór	Ex - ante/ kontrola w każdej chwili, bez incydentu, prewencyjnie	Ex - post/ kontrola po incydencie lub zgłoszeniu/ skardze

Kryterium	Podmiot Kluczowy (PK)	Podmiot Ważny (PW)
Audyt	Pierwszy obowiązkowy audyt w ciągu 24 miesięcy od wpisu; kolejne co 36 miesięcy - niezależnie od incydentów (art. 15 UoKSC)	Po incydencie lub na wniosek organu właściwego - nie prewencyjnie (art. 15 ust. 4 UoKSC)
Kara dla organizacji	Do 10 mln EUR lub 2% globalnego obrotu rocznego	Do 7 mln EUR lub 1,4% globalnego obrotu rocznego
Kara dla kierownika podmiotu	Do 300% wynagrodzenia - osobista, niezależna od kary dla organizacji	Do 300% wynagrodzenia - osobista, niezależna od kary dla organizacji
Sektor	Załącznik 1 + duże przedsiębiorstwo lub MSP/MSSP niezależnie od wielkości	Załącznik 1 + średnie MSP lub Załącznik 2 (duże/ średnie)
Termin rejestracji S46	7 maja – 3 października 2026 lub wpis z urzędu (sprawdź wykaz - ksc.gov.pl)	7 maja – 3 października 2026 lub wpis z urzędu (sprawdź wykaz - ksc.gov.pl)
Wymagania SZBI	IDENTYCZNE dla PK i PW - 10 obszarów art. 8 UoKSC. Klasyfikacja określa model nadzoru i kary - nie zakres obowiązków wdrożeniowych	IDENTYCZNE dla PK i PW - 10 obszarów art. 8 UoKSC. Klasyfikacja określa model nadzoru i kary - nie zakres obowiązków wdrożeniowych

> Kluczowy wniosek: PK i PW mają identyczne obowiązki wdrożeniowe. Klasyfikacja określa wyłącznie model nadzoru i wysokość sankcji.

> ! Kary osobiste są niezależne od kary dla organizacji Nawet jeśli organizacja zostanie ukarana grzywną, kierownik podmiotu, którym w praktyce jest/są: prezes zarządu, CEO, dyrektor generalny; wszyscy członkowie zarządu (jeśli organ wieloosobowy i nie wskazano jednej osoby - odpowiadają wtedy **wszyscy;** likwidator, syndyk, zarządca sukcesyjny, może dodatkowo otrzymać karę do 300% swojego wynagrodzenia. Obie kary są nakładane niezależnie od siebie i co ważne nie ma mechanizmu zaliczenia jednej na poczet drugiej.

1.3 18 sektorów NIS2 - Załącznik 1 i Załącznik 2

NIS1 obejmowała 7 sektorów. NIS2 rozszerzyła to do 18 i podzieliła na dwie listy: Załącznik 1 to sektory wysokiej krytyczności (podstawa dla PK), Załącznik 2 to pozostałe (podstawa dla PW). Nowelizacja UoKSC 2026 dodała OZE - sektor nieobecny w oryginalnej dyrektywie NIS2. Jeśli prowadzisz farmę wiatrakową lub fotowoltaiczną w skali przemysłowej, sprawdź poniższą tabelę - PKD Twojej działalności może znaleźć się na liście podmiotów krytycznych.

18 SEKTORÓW NIS2 - Załącznik 1 (podstawa PK) i Załącznik 2 (podstawa PW)	
Załącznik 1 - sektory wysokiej krytyczności (podstawa PK)	**Załącznik 2 - pozostałe sektory (podstawa PW)**
Energetyka	Usługi pocztowe i kurierskie
Transport	Gospodarka odpadami
Bankowość	Produkcja* - chemia i farmacja
Infrastruktura rynków finansowych	Produkcja* - żywność
Ochrona zdrowia	Produkcja* - wyroby medyczne
Woda pitna	Przemysł* - maszyny i pojazdy
Ścieki	Przemysł* - elektronika
Infrastruktura cyfrowa	Dostawcy usług cyfrowych (wyszukiwarki, platformy handlowe, sieci społ.) - rozszerzony zakres vs NIS1
Zarządzanie usługami ICT (B2B)	OZE - farmy wiatrowe i PV **NOWE
Administracja publiczna	Badania naukowe **NOWE
Przestrzeń kosmiczna **NOWE	

> *Produkcja liczona jako 1 sektor/ przemysł liczony jako 1 sektor
>
> Sprawdź wszystkie kody PKD - nie tylko główny. Organizacja z głównym PKD w sektorze produkcji, ale z dodatkowym kodem w zarządzaniu usługami IT dla klientów biznesowych, może być PK. Jeden kod PKD z sektora kluczowego może przesądzić o klasyfikacji całego podmiotu

1.4 Progi wielkości - reguła size - cap i jej pułapki

Sektor to nie wszystko, trzeba jeszcze spełnić próg wielkości. I tu zaczyna się zamieszanie. Definicja „średniego przedsiębiorstwa" w rozporządzeniu KE 651/2014 to nie to samo co potoczna „średnia firma". Spotykam organizacje z 47 pracownikami, które są de facto dużym przedsiębiorstwem, bo ich spółka matka zatrudnia 400.

REGUŁA SIZE - CAP - progi wielkości dla klasyfikacji PK/PW

Kategoria	Próg wielkości	Skutek dla NIS2/ UoKSC	Wyjątek
Duże ≥ 250 pracowników	≥ 250 pracowników LUB > 50 mln EUR obrotu LUB > 43 mln EUR bilansu	PK (Zał. 1) lub PW (Zał. 2)	MSP/MSSP → zawsze PK niezależnie od wielkości
Średnie 50–249 pracowników	50–249 pracowników LUB 10–50 mln EUR obrotu LUB 10–43 mln EUR bilansu	PW w większości sektorów	PK w infrastrukturze cyfrowej i zarządzaniu ICT (MSP/MSSP)
Małe 10–49 pracowników	10–49 pracowników LUB 2–10 mln EUR obrotu	Zasadniczo wyłączone	Jedyny krajowy dostawca usługi
Mikro < 10 pracowników	< 10 pracowników LUB < 2 mln EUR obrotu	Co do zasady wyłączone	Decyzja organu właściwego lub jedyny dostawca w kraju

> Wystarczy spełnić **jeden** z warunków w kolumnie "Próg wielkości" - pracownicy **LUB** obrót **LUB** bilans. Progi liczone łącznie z podmiotami powiązanymi i partnerskimi wg rozporządzenia 651/2014

Pułapki przy liczeniu progów

Liczenie łącznie w grupie kapitałowej. Jeśli organizacja jest powiązana lub partnerska z innym podmiotem, pracownicy i obrót liczone są łącznie. Spółka

zależna z 40 pracownikami, której matka zatrudnia 300 osób, jest de facto dużym przedsiębiorstwem.

Kryterium alternatywne, nie łączne czyli wystarczy spełnić jeden warunek (pracownicy LUB obrót LUB bilans). Firma z 260 pracownikami i obrotem 8 mln EUR jest dużym przedsiębiorstwem.

Jeden obszar działalności może decydować o całości. Jeśli organizacja faktycznie prowadzi działalność w zakresie sektora kluczowego, cały podmiot może zostać zakwalifikowany jako PK. Decyduje faktyczne prowadzenie działalności, nie samo posiadanie kodu PKD, choć kod PKD jest pierwszym sygnałem do weryfikacji. Organizacja, która posiada kod PKD z sektora energetyki, ale faktycznie nie świadczy żadnej usługi energetycznej, powinna to udokumentować przed złożeniem S46.

Dostawcy usług cyfrowych bez ograniczenia wielkości, do których zaliczają się np. wyszukiwarki, platformy handlowe i sieci społecznościowe podlegają NIS2 niezależnie od liczby pracowników w Polsce.

> **!** Błędna ocena progów = brak rejestracji = sankcja Organizacja, która błędnie uznała, że nie spełnia progów i nie złożyła wniosku S46, naraża się na karę administracyjną. Przy wątpliwościach: konsultacja z organem właściwym lub radcą prawnym.

1.5 Wyjątki ustawowe i jurysdykcja transgraniczna

Wyjątki rozszerzające, którym podlegają podmioty mimo małej skali

Jedyny krajowy dostawca usługi, np. mikro lub małe przedsiębiorstwo będące jedynym dostawcą określonej usługi w Polsce może zostać uznane za PK/PW decyzją organu właściwego.

Organ właściwy może uznać dowolny podmiot za PK/PW, niezależnie od progów, jeśli uzna to za konieczne ze względów bezpieczeństwa.

Dostawcy usług zarządzanych (MSP/MSSP) są zawsze PK, niezależnie od wielkości i bez konieczności spełnienia progów.

Wyjątki zawężające, czyli podmioty które nie podlegają Ustawie mimo spełnienia kryteriów

Służby specjalne i podmioty MON czyli ABW, AW, SKW, SWW i podmioty podległe Ministrowi Obrony Narodowej są wyłączone z zakresu UoKSC.

Niezależne spółki zależne, które są poniżej progów w momencie gdy ich system informacyjny jest w pełni niezależny od spółki matki i nie świadczy usług wspólnie, nie jest PW.

Energetyka jądrowa, czyli wszystkie podmioty z sektora jądrowego stają się PK z dniem uzyskania odpowiedniego zezwolenia na eksploatację, nie z dniem rejestracji działalności.

Jurysdykcja i działalność transgraniczna

Standardowa zasada: rejestracja w danym państwie = jurysdykcja tego państwa. Ale dla MSP, MSSP, CSP, CDN, platform handlowych i wyszukiwarek reguła jest inna: jurysdykcję określa główne miejsce prowadzenia działalności w UE, nie siedziba rejestrowa.

Podstawa prawna tej zasady: art. 26 ust. 2 lit. b NIS2 definiuje „główne miejsce prowadzenia działalności" jako miejsce, w którym podejmowane są główne decyzje w zakresie zarządzania ryzykiem cyberbezpieczeństwa. Konsekwencja praktyczna: spółka z siedzibą w Niemczech, której CISO i zespół bezpieczeństwa podejmują wszystkie decyzje dotyczące SZBI z biura w Warszawie, podlega polskiemu UoKSC, nie niemieckiemu. Holenderski dostawca chmury, którego decyzje bezpieczeństwa zapadają w Amsterdamie, podlega jurysdykcji holenderskiej, nawet jeśli obsługuje polskie PK.

1.6 Klasyfikacja dostawców ICT

Dostawca ICT może być PK, PW albo nie podlegać NIS2 bezpośrednio, a i tak mieć obowiązki przez klauzule umowne swoich klientów. Rozróżnienie ma fundamentalne znaczenie operacyjne: czy organ może przyjść do Ciebie z kontrolą, czy tylko klient może wymagać certyfikatu i prawa do audytu.

Typ dostawcy ICT	Obowiązek NIS2?	Jak podlega wymaganiom?
MSSP / dostawca SOC	TAK - zawsze PK	Wprost wymieniony w Zał. 1 UoKSC jako PK niezależnie od wielkości. Podlega też Rozporządzeniu 2024/2690
MSP (usługi zarządzane IT)	TAK - PK lub PW	Dostawcy usług zarządzanych objęci jako PK w sektorze zarządzania ICT. Sprawdź kody PKD i zakres świadczonych usług

Typ dostawcy ICT	Obowiązek NIS2?	Jak podlega wymaganiom?
Dostawca oprogramowania (SaaS)	Zazwyczaj NIE	Pośrednio przez klauzule umowne klientów PK/PW: certyfikaty bezpieczeństwa, prawo do audytu, obowiązek zgłaszania incydentów
Dostawca chmury (CSP)	TAK - infrastruktura cyfrowa	Krajowi dostawcy chmury objęci jako infrastruktura cyfrowa wg UoKSC. AWS, Azure, GCP podlegają regulacji NIS2 w państwie UE, gdzie mają główne miejsce prowadzenia działalności (np. Azure → Irlandia, AWS → Luksemburg) - nie polskiemu UoKSC bezpośrednio. Polski PK egzekwuje wobec nich wymagania przez klauzule umowne, nie przez organ właściwy.
Integrator / wykonawca IT	Zazwyczaj NIE	Pośrednio przez klauzule umowne. Incydent u integratora z dostępem do infrastruktury PK może być incydentem PK
Dostawca wysokiego ryzyka	Może być wykluczony decyzją Ministra	Minister ds. informatyzacji może wykluczyć dostawcę z rynku PK/PW (art. 66c UoKSC). Wycofanie produktów: 7 lat (4 lata dla telekomunikacji)

> Incydent u dostawcy ICT z dostępem do infrastruktury PK jest traktowany jako incydent tego PK. Klient PK musi wiedzieć o incydencie u dostawcy w ciągu godzin a nie kilku dni. Klauzula obowiązku zgłaszania incydentów przez dostawcę do klienta jest niezbędna w każdej umowie z dostawcą ICT.

1.7 Kwalifikacja grup kapitałowych

Grupy kapitałowe to najtrudniejszy obszar klasyfikacyjny, z jakim się spotykam. Najczęstsze pytanie: czy holding jako taki podlega NIS2? Nie podlega. Podlegają konkretne spółki. Ale, i to duże ale, powiązania kapitałowe wpływają na progi wielkości i na to, czy spółka zależna jest „odrębna” w rozumieniu ustawy.

Scenariusz	Zasada kwalifikacji wg UoKSC
Spółka matka jest PK	Spółki zależne mogą być objęte obowiązkami jako część grupy, jeśli świadczą usługi wspólnie z PK lub ich systemy informacyjne są wzajemnie zależne

Scenariusz	Zasada kwalifikacji wg UoKSC
Spółka zależna spełnia progi	Kwalifikowana samodzielnie, niezależnie od statusu spółki matki. Własny wniosek S46, własne obowiązki wdrożeniowe, własna odpowiedzialność
Spółka zależna poniżej progów, zintegrowana z PK	Jeśli jej system informacyjny jest w pełni niezależny od PK i nie świadczy usług wspólnie, nie jest PW. Jeśli jest zintegrowana może być objęta jako część PK
Holding wielosektorowy	Każda spółka oceniana osobno według sektora, w którym prowadzi działalność. Holding jako taki nie podlega NIS2 - podlegają poszczególne spółki
Dostawca wysokiego ryzyka w grupie	Minister ds. informatyzacji może uznać za dostawcę wysokiego ryzyka całą grupę kapitałową (art. 67b UoKSC)

> Zarząd holdingu, który nie jest formalnie PK ani PW, ale sprawuje nadzór właścicielski nad spółkami zależnymi będącymi PK, powinien rozważyć wdrożenie spójnej polityki cyberbezpieczeństwa dla całej grupy. Incydent w spółce zależnej może dotrzeć do serwerów matki szybciej niż decyzja o segmentacji sieci.

1.8 Wpis z urzędu (ex officio)

Przed złożeniem wniosku S46 zrób jedno: sprawdź wykaz - ksc.gov.pl. Część organizacji jest wpisywana z urzędu, bez ich inicjatywy. NBP, BGK, KNF, PAP i kilkadziesiąt instytucji wymienionych wprost w ustawie dostaje status PK automatycznie. Jeśli jesteś już w wykazie i złożysz wniosek, może to wygenerować komplikacje proceduralne.

WPIS Z URZĘDU - kto nie składa wniosku S46		
Typ podmiotu	**Wniosek S46?**	**Podstawa i uwagi**
Podmioty infrastruktury krytycznej wskazane z urzędu	NIE	Art. 5 UoKSC: organ wpisuje automatycznie w ciągu 6 miesięcy od wejścia w życie (do 03.10.2026). Sprawdź status w systemie S46. Jeśli organ nie wpisał do terminu: złóż wniosek S46 samodzielnie - brak wpisu nie zwalnia z obowiązków KSC, a naruszenia mogą być ukarane po 03.04.2028.

Typ podmiotu	Wniosek S46?	Podstawa i uwagi
MSSP / dostawcy usług zarządzanych cyberbezpieczeństwem	TAK obowiązkowo	Mimo że są zawsze PK, muszą złożyć wniosek S46 w oknie 7.05–3.10.2026
Podmioty wskazane decyzją administracyjną organu	NIE wpis decyzją	Organ właściwy może uznać podmiot za PK/PW decyzją administracyjną i jest to niezależnie od progów. Dotyczy podmiotów strategicznych
NBP, BGK, KNF, PAP i instytucje wymienione w ustawie	NIE z urzędu	Wprost wymienione w Załączniku do UoKSC, automatyczny status PK bez wniosku
Standardowe PK i PW nie wpisane z urzędu	TAK obowiązkowo	Termin: 7 maja do 3 października 2026. Sankcja za brak wniosku: kara administracyjna

> Zanim Twoja organizacja złoży wniosek S46, sprawdź wykaz - ksc.gov.pl. Jeśli jesteś już wpisany z urzędu i złożysz wniosek, organ może potraktować go jako wniosek o zmianę danych, nie jako nowy wpis. Ryzykujesz też błędne liczenie terminów: 12 miesięcy na wdrożenie SZBI biegnie od daty wpisu z urzędu, nie od daty Twojego wniosku.

1.9 Framework: Decision Tree PK/PW

Pięć pytań, przez które prowadzę każdą organizację przed złożeniem wniosku S46. Idź przez nie sekwencyjnie. Każda odpowiedź powinna być poparta dokumentem, a nie tylko wewnętrznym przekonaniem.

DECISION TREE PK/PW - 5 kroków klasyfikacji				
Krok	Pytanie	Szczegóły	TAK →	NIE →
1	Sektor	Czy organizacja działa w co najmniej jednym z 18 sektorów NIS2? Sprawdź wszystkie kody PKD, nie tylko główny	Idź do kroku 2	Co do zasady NIS2 nie dotyczy, ale warto sprawdzić wyjątki ustawowe

Krok	Pytanie	Szczegóły	TAK →	NIE →
2	Wielkość	Czy zatrudniasz ≥50 osób LUB osiągasz obrót >10 mln EUR? Licz łącznie z podmiotami powiązanymi i partnerskimi wg rozp. 651/2014	Idź do kroku 3	Zasadniczo poza zakresem ale sprawdź wyjątki: MSP/MSSP lub jedyny krajowy dostawca usługi
3	Typ PK/PW	Zał. 1 + duże → PK Zał. 1 + średnie → PW Zał. 2 + duże/średnie → PW Infrastruktura cyfrowa (IXP, DNS, TLD, DC, CDN) → PK niezależnie od wielkości. MSP/MSSP → zawsze PK. Zwykła firma IT (helpdesk, wdrożenia) NIE jest automatycznie PK	Ustal PK lub PW - krok 4	n/d
4	Wpis z urzędu	Sprawdź wykaz - ksc.gov.pl. NBP, BGK, KNF, PAP to są wpisy automatyczne	Nie składasz S46, ale masz pełne obowiązki UoKSC od dnia wpisu	Złóż wniosek S46 w oknie 7.05–3.10.2026
5	Dostawca ICT	Czy dostarczasz produkty lub usługi ICT podmiotom PK/PW? Czy jesteś MSSP, CSP, dostawcą DNS/TLD lub CDN?	Możesz podlegać bezpośrednio lub pośrednio/ MSP/MSSP = zawsze PK	Sprawdź czy klient PK/PW wymaga klauzul NIS2 w umowie z Tobą

> ! Kara za brak rejestracji Organizacja, która spełnia kryteria PK/PW i nie złożyła wniosku S46 do 3 października 2026, naraża się na karę administracyjną, niezależnie od tego, czy działała w dobrej wierze. Termin jest nieprzekraczalny.

Uwaga o przypadkach granicznych:

Decision Tree jest narzędziem wstępnym, nie zastępuje analizy prawnej.

Trzy scenariusze wymagają szczególnej uwagi poza standardową ścieżką drzewka:

(1) OZE: kiedy farma fotowoltaiczna lub wiatrowa staje się PK? Próg mocy zainstalowanej określi rozporządzenie wykonawcze; do jego wydania skonsultuj z organem właściwym (Urząd Regulacji Energetyki);

(2) Ochrona zdrowia: prywatna klinika świadcząca usługi dla NFZ, apteka sieciowa, laboratorium diagnostyczne: status PK lub PW zależy od zakresu usług i powiązań kontraktowych z systemem ochrony zdrowia, sprawdź z Ministerstwem Zdrowia jako organem właściwym;

(3) Działalność transgraniczna: spółka zagraniczna bez polskiego oddziału świadcząca SaaS dla polskich PK podlega jurysdykcji państwa UE swojego głównego miejsca działalności, nie bezpośrednio UoKSC. We wszystkich przypadkach granicznych: skonsultuj się z organem właściwym lub radcą prawnym PRZED złożeniem S46.

1.10 Odpowiedzialności w organizacji - RACI

Zarząd - *CEO, Prezes, członkowie zarządu, dyrektorzy generalni*

Klasyfikacja jako PK lub PW nie jest kwestią prestiżu. Jest to decyzja, która bezpośrednio wpływa na Twoją osobistą odpowiedzialność. Jako osoba kierująca podmiotem odpowiadasz za prawidłowość klasyfikacji, terminowe złożenie wniosku S46 i zakres wymagań, które organizacja musi spełnić.

Co Zarząd powinien wiedzieć o klasyfikacji

Klasyfikacja PK/PW to Twoja decyzja, nie dyrektora IT, nie compliance. CISO i prawnicy dostarczają analizę, a Ty ją zatwierdzasz i odpowiadasz za błędy. Błędna klasyfikacja to jest ryzyko kary administracyjnej.

Termin rejestracji S46: 7 maj - 3 październik 2026. Złożenie wniosku jest Twoim obowiązkiem. Podpisujesz wniosek z odpowiedzialnością karną za fałszywe dane (art. 233 KK). Zanim podpiszesz, zweryfikuj każde pole z CISO i prawnikiem.

Sprawdź wykaz - ksc.gov.pl przed złożeniem wniosku. Część organizacji jest wpisywana z urzędu bez ich inicjatywy. Złożenie wniosku przez podmiot już wpisany może prowadzić do komplikacji jak już wcześniej pisałem.

Status PW to nie 'lżejszy wariant'. Wymagania wdrożeniowe są identyczne z PK. Różni je model nadzoru. Organizacja PW, która opóźnia wdrożenie SZBI, ryzykuje, że pierwszy incydent przyniesie jednocześnie: szkodę operacyjną, obowiązek raportowania, kontrolę organu i potencjalnie karę za brak zgodności.

Pięć pytań, które Zarząd powinien zadać przed złożeniem wniosku S46

Czy sprawdziliśmy WSZYSTKIE kody PKD, a nie tylko główny?

Czy progi wielkości były liczone łącznie ze spółkami powiązanymi i partnerskimi?

Czy sprawdziliśmy, czy organizacja jest już wpisana z urzędu w systemie S46?

Czy nasze spółki zależne wymagają osobnych wniosków S46?

Czy decyzja klasyfikacyjna jest udokumentowana z uzasadnieniem na piśmie?

> ! Kara za brak rejestracji Organizacja, która spełnia kryteria PK/PW i nie złożyła wniosku S46 do 3 października 2026, naraża się na karę

> administracyjną - niezależnie od tego, czy działała w dobrej wierze. Termin jest nieprzekraczalny

Konsekwencje dla Zarządu PK vs PW

Jeśli jesteś PK: audytor może pojawić się w każdej chwili, bez incydentu, bez skargi, bez uprzedzenia. Pierwszy obowiązkowy audyt w ciągu 2 lat od rejestracji, kolejne co 3 lata. Zarząd PK musi być przygotowany na pytanie: 'Czy możemy jutro przyjąć audytora?' Jeśli odpowiedź brzmi 'nie' powinien natychmiast uruchomić program gotowości audytowej.

Jeśli jesteś PW: kontrole są zazwyczaj reaktywne ale 'zazwyczaj' to nie 'nigdy'. Pułapka PW polega na tym, że organizacje traktując status PW jako 'lżejszy wariant' opóźniają wdrożenie. A po pierwszym incydencie kontrola jest prawie pewna - i ujawnia brak zgodności.

Compliance / IOD - *Compliance Officers, Inspektorzy Ochrony Danych, prawnicy wewnętrzni*

Dla Compliance klasyfikacja PK/PW to punkt startowy wszystkich dalszych obowiązków czyli rejestracja S46, zakres SZBI, terminy audytów, progi kar. Błędna klasyfikacja nie jest „małym problemem proceduralnym”. To jest fundament, na którym spoczywa cały program compliance NIS2.

Proces klasyfikacji czyli co Compliance musi przeprowadzić:

Analiza sektorowa: sprawdź wszystkie kody PKD organizacji (nie tylko główny) pod kątem 18 sektorów NIS2. Jeden kod PKD z Załącznika 1 może zmienić klasyfikację całej organizacji.

Analiza progów wielkości: oblicz zatrudnienie i obrót łącznie z podmiotami powiązanymi i partnerskimi zgodnie z rozporządzeniem 651/2014. To nie jest prosta arytmetyka lecz praca która wymaga analizy struktury grupy kapitałowej.

Sprawdzenie wyjątków: zweryfikuj, czy organizacja spełnia kryteria MSP/MSSP (zawsze PK), jest jedynym dostawcą usługi (może być PK/PW mimo małej skali) lub jest wpisana z urzędu.

Sprawdzenie wykazu S46: przed złożeniem wniosku zweryfikuj wykaz - ksc.gov.pl, czy organizacja nie jest już wpisana.

Dokumentacja decyzji klasyfikacyjnej: wynik klasyfikacji z uzasadnieniem, analizą PKD i obliczeniem progów musi być przechowany jako dokument wewnętrzny z datą i podpisem zatwierdzającego.

Lista kwalifikacyjna - 10 pytań do samodzielnej weryfikacji

Nr	Pytanie kwalifikacyjne	TAK	NIE
1	Czy Twoja organizacja prowadzi działalność w co najmniej jednym z 18 sektorów NIS2 (Załącznik 1 lub 2 UoKSC)?	☐	☐
2	Czy Twoja organizacja zatrudnia co najmniej 50 osób LUB osiąga obrót powyżej 10 mln EUR (łącznie z podmiotami powiązanymi)?	☐	☐
3	Czy Twoja organizacja dostarcza usługi zarządzane (MSP) lub usługi cyberbezpieczeństwa (MSSP) dla innych podmiotów?	☐	☐
4	Czy Twoja organizacja jest jedynym lub krytycznym dostawcą określonej usługi w Polsce lub regionie?	☐	☐
5	Czy Twoja organizacja figuruje już w wykazie podmiotów w systemie S46 (wpis z urzędu sprawdź wykaz - ksc.gov.pl)?	☐	☐
6	Czy Twoja organizacja jest dostawcą ICT z dostępem do infrastruktury podmiotu kluczowego lub ważnego?	☐	☐
7	Czy Twoja organizacja wchodzi w skład grupy kapitałowej, w której inna spółka jest PK lub PW?	☐	☐
8	Czy wszystkie kody PKD Twojej organizacji (nie tylko główny) były sprawdzone pod kątem 18 sektorów NIS2?	☐	☐
9	Czy wielkość organizacji była liczona łącznie z przedsiębiorstwami powiązanymi i partnerskimi wg rozporz. 651/2014?	☐	☐
10	Czy organ właściwy dla Twojego sektora był konsultowany w przypadku wątpliwości co do klasyfikacji?	☐	☐

> **Interpretacja:** Jeśli na pytania 1 i 2 odpowiedź brzmi TAK, a na pytanie 5 NIE wtedy organizacja powinna złożyć wniosek S46. Jeśli na którekolwiek z pytań 3–7 odpowiedź jest nieznana konieczna jest pogłębiona analiza lub konsultacja prawna.

Audyt - *Audytorzy wewnętrzni i zewnętrzni KSC*

Prawidłowość klasyfikacji PK/PW to jeden z pierwszych obszarów weryfikowanych podczas audytu KSC. Audytor sprawdza nie tylko czy organizacja złożyła wniosek S46, ale czy klasyfikacja jest poprawna i udokumentowana. Błędna klasyfikacja na korzyść, na przykład nieuzasadnione zakwalifikowanie się jako PW zamiast PK, może skutkować nałożeniem obowiązków wstecz.

Co audytor sprawdza w zakresie klasyfikacji

Dokumentacja decyzji klasyfikacyjnej takiej jak: analiza PKD, obliczenie progów wg rozporządzenia 651/2014, uzasadnienie, data i podpis zatwierdzającego. Brak dokumentacji to jest brak dowodu.

Prawidłowość progów wielkości. Czy obrót i zatrudnienie były liczone łącznie z podmiotami powiązanymi? Czy użyto definicji z rozporządzenia 651/2014? Sprawdzenie wszystkich kodów PKD. Czy analiza sektorowa obejmowała wszystkie kody PKD, nie tylko główny? Wpis w systemie S46. Czy organizacja złożyła wniosek w terminie (7.05–3.10.2026) lub jest wpisana z urzędu? Czy dane w S46 są aktualne?

Status dostawców ICT. Czy organizacja prawidłowo oceniła status swoich kluczowych dostawców ICT (MSP/MSSP vs. dostawca pośredni)?

Najczęstsze błędy klasyfikacyjne stwierdzane w audytach

Najczęstszy błąd to progi liczone wyłącznie dla spółki, bez podmiotów powiązanych. Spółka z 48 pracownikami, której matka zatrudnia 400 osób, błędnie uznaje się za wyłączoną.

Sprawdzono tylko główny PKD, podczas gdy, organizacja z dodatkową działalnością w sektorze zarządzania ICT nie zauważyła, że jeden kod PKD kwalifikuje ją jako PK.

Brak dokumentacji decyzji klasyfikacyjnej, gdzie organizacja dokonała prawidłowej klasyfikacji, ale nie ma żadnego dokumentu potwierdzającego analizę. Dla audytora nieudokumentowane to nieistniejące.

Nieaktualne dane w S46, czyli np. zmiana profilu działalności lub przekroczenie progów wielkości nie zostało zgłoszone w ciągu 14 dni. Art. 7 UoKSC wymaga aktualizacji danych w 14 - dniowym terminie.

Kluczowe pytania do zadania podczas audytu klasyfikacji

Proszę pokaż mi dokumentację decyzji klasyfikacyjnej czyli analizę PKD, obliczenie progów, datę i podpis?

Na jakiej podstawie progi były obliczane? Czy uwzględniono podmioty powiązane i partnerskie wg rozporządzenia 651/2014?

Kiedy ostatnio weryfikowano prawidłowość klasyfikacji? Czy po zmianie działalności lub przekroczeniu progu?

Pokaż mi wniosek S46 lub dowód wpisu z urzędu.

Czy organizacja jest dostawcą usług zarządzanych (MSP/MSSP)? Jeśli tak jak jest zakwalifikowana? Dlaczego nie jest zakwalifikowana jako PK?

> Prawidłowa klasyfikacja bez dokumentacji to ryzyko niezgodności. Dokumentacja błędnej klasyfikacji to niezgodność pewna. Cel: prawidłowa klasyfikacja + kompletna dokumentacja z datą. Audytor zawsze pyta 'pokaż mi'

1.11 Podsumowanie rozdziału 1

Status podmiotu ważnego brzmi jak ulga. Mniejszy nadzór, kontrole reaktywne, bez audytora pukającego bez zapowiedzi. I w pewnym sensie to prawda bo model nadzoru jest łagodniejszy. Ale jest w tym pewien paradoks, który warto zobaczyć zanim się odetchnie z ulgą: wymagania wdrożeniowe dla PK i PW są identyczne. Zakres art. 8 UoKSC jest ten sam. SZBI, analiza ryzyka, procedura raportowania incydentów, rejestr dostawców, wszystko to samo. Jedyne co się różni, to kto i kiedy to sprawdzi.

Dla wielu organizacji ta informacja jest w gruncie rzeczy uwalniająca. Nie trzeba się zastanawiać, czy jako PW można sobie odpuścić połowę wymagań. Nie można. Ale też nie trzeba budować czegoś innego niż PK. Jeden program wdrożenia, jeden SZBI, jedna teczka audytowa. Klasyfikacja decyduje o modelu nadzoru, nie o architekturze bezpieczeństwa.

18 sektorów, dwa Załączniki. Najczęstszy błąd przy analizie sektorowej to sprawdzanie tylko głównego kodu PKD. Jeden dodatkowy kod z Załącznika 1, taki jak np. zarządzanie ICT, infrastruktura cyfrowa, dystrybucja energii, może zmienić klasyfikację całej organizacji. OZE to nowy sektor w nowelizacji UoKSC 2026, co oznacza że część firm z branży energetyki odnawialnej po raz pierwszy wchodzi w zakres regulacji.

Progi wielkości są alternatywne: pracownicy LUB obrót LUB suma bilansowa. Przekroczenie jednego progu wystarczy. Ale liczy się je łącznie z podmiotami powiązanymi i partnerskimi według rozporządzenia 651/2014. I tu kryje się więcej niespodzianek niż w samej sektorowości. Grupy kapitałowe wyglądają na papierze jak zbiór małych spółek, a po zsumowaniu okazuje się, że każda z nich przekracza progi samodzielnie.

MSSP i dostawcy usług zarządzanych mają własną regułę: zawsze PK, niezależnie od wielkości i sektora. To nie jest kwestia do analizy, to wprost wynikający z ustawy pewnik.

Przed złożeniem wniosku S46 warto sprawdzić wykaz - ksc.gov.pl, bo część organizacji jest wpisywana z urzędu i nie musi składać wniosku samodzielnie. Okno rejestracyjne to 7 maja do 3 października 2026. Po wpisie każda zmiana danych wymaga aktualizacji w 14 dni.

I ostatnia rzecz, która ma znaczenie nie tylko formalne: udokumentowana decyzja klasyfikacyjna. Chodzi o to, żeby organizacja sama wiedziała dlaczego jest tym

czym jest i który kod PKD był decydujący, jak były liczone progi, kto zatwierdził analizę i kiedy. Nie dla audytora. Dla siebie. Bo klasyfikacja to punkt startowy całego programu zgodności i warto wiedzieć na czym ten punkt stoi.

Miałem klienta, który po godzinie wspólnej analizy struktury grupy i kodów PKD powiedział: to właściwie fajnie, że to wiemy. Wcześniej działaliśmy na przeczuciu. Teraz mamy dokument i wiemy od czego zaczynamy.

I od tego zaczyna się każde sensowne wdrożenie NIS2.

> Następny krok: Rozdział 2 - Rejestracja S46 i obowiązki formalne. Wiesz już, jak klasyfikuje się Twoja organizacja. Teraz dowiedz się, co musisz zrobić i w jakich terminach

Zachęcam również do odwiedzin na naszej stronie głównej oraz Akademii LegacyTurn, która rusza już od lipca 2026

Pozdrawiam i dziękuję,

Piotr Szymczyk