



Checklist zgodności NIS2 — wersja podstawowa

Wersja 1.0 | Wrzesień 2026 | Zgodna z ustawą o KSC z 23 stycznia 2026 r.

Dyrektywa NIS2 (UE 2022/2555) została wdrożona do polskiego prawa ustawą z 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa. Obejmuje **ponad 10 000 podmiotów** w Polsce — od energetyki i transportu, po produkcję żywności i samorządy. Kary sięgają **10 mln EUR lub 2% obrotu**, a kierownictwo odpowiada osobiście (do 600% wynagrodzenia). Ta checklist pomoże Ci ocenić, czy NIS2 dotyczy Twojej organizacji i jak wygląda Twoja gotowość.

1 Czy NIS2 dotyczy Twojej firmy?

PYTANIE	TAK	NIE
1 Czy działasz w jednym z sektorów NIS2? (energetyka, transport, bankowość, ochrona zdrowia, woda, infrastruktura cyfrowa, ICT, produkcja, żywność, chemia, odpady, poczta, badania, administracja publiczna, przestrzeń kosmiczna)	☐	☐
2 Czy Twoja firma zatrudnia ≥ 50 pracowników lub ma obrót/sumę bilansową ≥ 10 mln EUR?	☐	☐
3 Czy świadczysz usługi DNS, dostawcy chmury, centrum danych, CDN, usługi zaufania, rejestracji domen, lub jesteś dostawcą usług zarządzanych (MSP/MSSP)? (jeśli TAK — podlegasz niezależnie od wielkości)	☐	☐
4 Czy jesteś jednostką samorządu terytorialnego, podmiotem publicznym lub spółką komunalną realizującą zadania użyteczności publicznej?	☐	☐
5 Czy Twoja firma zatrudnia > 250 pracowników lub ma obrót > 50 mln EUR i działa w sektorze o wysokiej krytyczności (Załącznik 1 NIS2)? (jeśli TAK — jesteś podmiotem kluczowym)	☐	☐
6 Czy Twoja firma jest dostawcą ICT dla podmiotów kluczowych/ważnych? (jeśli TAK — pośrednio podlegasz wymogom bezpieczeństwa łańcucha dostaw)	☐	☐

INTERPRETACJA

Jeśli odpowiedziałeś TAK na pytanie 1 + 2 → jesteś podmiotem **ważnym** lub **kluczowym**. Pytanie 3 lub 4 = TAK → podlegasz niezależnie od wielkości. Pytanie 5 = TAK → podmiot **kluczowy** (pełny nadzór, audyt co 2 lata). Pytanie 6 = TAK → wymogi pośrednie z łańcucha dostaw.

A. Zarządzanie ryzykiem i polityki bezpieczeństwa

- ☐ **Polityka bezpieczeństwa informacji** — Czy posiadasz udokumentowaną, zatwierdzoną przez zarząd politykę cyberbezpieczeństwa, aktualizowaną co najmniej raz w roku? [art. 8 ust. 1 pkt 2 UKSC | CyFun ID.GV-1.1]
- ☐ **Inwentaryzacja aktywów** — Czy prowadzisz aktualny rejestr sprzętu IT/OT, oprogramowania i danych krytycznych wraz z ich klasyfikacją wg ważności dla biznesu? [CyFun ID.AM-1.1, ID.AM-2.1, ID.AM-5.1]
- ☐ **Analiza ryzyka** — Czy przeprowadzasz systematyczną ocenę ryzyka (zagrożenia, podatności, prawdopodobieństwo, wpływ) dla swoich systemów informacyjnych? [art. 8 ust. 1 pkt 1 UKSC | CyFun ID.RA-1.1, ID.RA-5.1]
- ☐ **Strategia zarządzania ryzykiem** — Czy posiadasz udokumentowany plan postępowania z ryzykiem (akceptacja, redukcja, transfer) z przypisanym budżetem i zasobami? [CyFun ID.GV-4.1]

B. Ochrona systemów i danych

- ☐ **Kopie zapasowe (backup)** — Czy tworzysz regularne backupy krytycznych danych, przechowywane na oddzielnym systemie, i testujesz ich odtwarzalność? [art. 8 ust. 1 pkt 4 UKSC | CyFun PR.IP-4.1]
- ☐ **Aktualizacje i łatki** — Czy instalujesz patche bezpieczeństwa dla systemów operacyjnych i krytycznych komponentów w ustalonych ramach czasowych? [CyFun PR.MA-1.1]
- ☐ **Segmentacja sieci** — Czy Twoja sieć jest podzielona na strefy bezpieczeństwa (np. VLAN) z firewallami na granicach i kontrolą ruchu między strefami? [CyFun PR.AC-5.1, PR.AC-5.2]
- ☐ **Uwierzytelnianie wieloskładnikowe (MFA)** — Czy stosujesz MFA na systemach dostępnych z internetu (poczta, VPN, pulpity zdalne, panele administracyjne)? [art. 8 ust. 1 pkt 10 UKSC | CyFun PR.AC-3.2]
- ☐ **Kontrola dostępu** — Czy stosujesz zasadę minimalnych uprawnień, oddzielone konta admin, i bezzwłocznie dezaktywujesz konta odchodzących pracowników? [CyFun PR.AC-4.1 – PR.AC-4.4]

C. Wykrywanie i reagowanie na incydenty

- ☐ **Monitoring i logi** — Czy zbierasz i analizujesz logi z firewalli, antywirusów, serwerów i systematycznie przeglądasz je pod kątem anomalii? [CyFun DE.AE-3.1, PR.PT-1.1]
- ☐ **Ochrona przed malware** — Czy masz zainstalowane i automatycznie aktualizowane oprogramowanie antywirusowe/antymalware na wszystkich urządzeniach? [CyFun DE.CM-4.1]
- ☐ **Plan reagowania na incydenty** — Czy posiadasz udokumentowaną procedurę incydentową z przypisanymi rolami, danymi kontaktowymi i ścieżkami eskalacji? [art. 8 ust. 1 pkt 3 UKSC | CyFun RS.RP-1.1]
- ☐ **Zgłaszanie incydentów (24h/72h)** — Czy wiesz, do którego CSIRT zgłaszać incydent poważny i czy Twój zespół potrafi zmieścić się w terminie 24h (ostrzeżenie) i 72h (zgłoszenie)? [art. 11 UKSC]
- ☐ **Lessons learned** — Czy po każdym incydencie przeprowadzasz analizę post-mortem i aktualizujesz procedury na podstawie wniosków? [CyFun RS.IM-1.1]

D. Łańcuch dostaw

- ☐ **Ocena dostawców ICT** — Czy weryfikujesz praktyki cyberbezpieczeństwa kluczowych dostawców (certyfikaty, polityki, zdolność do reakcji na incydenty)? [art. 8 ust. 1 pkt 5 UKSC | art. 21 ust. 2 lit. d NIS2]
- ☐ **Klauzule bezpieczeństwa w umowach** — Czy umowy z dostawcami IT zawierają wymogi dot. bezpieczeństwa, prawo do audytu, obowiązek zgłaszania incydentów i SLA na łatanie podatności? [art. 8 ust. 1 pkt 5 UKSC]

E. Zarządzanie i czynnik ludzki

- ☐ **Odpowiedzialność zarządu** — Czy kierownictwo formalnie zatwierdziło SZBI i świadomie nadzoruje realizację obowiązków z zakresu cyberbezpieczeństwa? [art. 8d UKSC]
- ☐ **Szkolenia kierownictwa** — Czy zarząd/kierownik podmiotu odbywa regularne szkolenia z cyberbezpieczeństwa (identyfikacja ryzyk, ocena środków zarządzania)? [art. 8e UKSC]
- ☐ **Szkolenia pracowników** — Czy wszyscy pracownicy przechodzą regularne szkolenia z cyberhigieny (phishing, hasła, bezpieczne korzystanie z systemów)? [art. 8f UKSC | CyFun PR.AT-1.1]
- ☐ **Plan ciągłości działania** — Czy posiadasz plan BCP/DR obejmujący scenariusze cyber (ransomware, utrata danych, awaria dostawcy) z określonymi RTO/RPO? [art. 8 ust. 1 pkt 4 UKSC | CyFun RC.RP-1.1]

3 Twój wynik

____ / 20
ZAZNACZONYCH

Policz, ile checkboxów z sekcji 2 możesz zaznaczyć jako spełnione. Wpisz wynik i sprawdź, w której kategorii się znajdujesz. Bądź szczery — to narzędzie dla Ciebie, nie dla audytora.

0–5

KRYTYCZNE

6–10

WYMAGA DZIAŁANIA

11–15

DOBRA PODSTAWA

16–20

ZAAWANSOWANY

0–5 · Krytyczne — Twoja organizacja ma poważne luki w cyberbezpieczeństwie. Brak podstawowych zabezpieczeń naraża Cię na incydenty i kary. Potrzebujesz natychmiastowego planu działania.

6–10 · Wymaga działania — Masz pewne podstawy, ale istotne obszary wymagają uzupełnienia. Priorytet: analiza ryzyka, procedury incydentowe, szkolenia i MFA.

11–15 · Dobra podstawa — Większość fundamentów jest na miejscu. Skup się na doskonaleniu: testuj backupy, przeprowadź audyt dostawców, ćwicz scenariusze incydentowe.

16–20 · Zaawansowany — Gratulacje! Twoje zabezpieczenia są solidne. Następny krok: formalizacja SZBI, przygotowanie do audytu zewnętrznego i rejestracja w wykazie podmiotów.

Potrzebujesz wsparcia we wdrożeniu NIS2?

Umów się na bezpłatną konsultację, podczas której ocenimy Twój status NIS2, zidentyfikujemy największe ryzyka i zaproponujemy konkretny plan działania dopasowany do Twojej organizacji i budżetu.

[Umów bezpłatną konsultację →](#)

eurokompas.pl/kontakt

KLUCZOWE TERMINY DO ZAPAMIĘTANIA

- **12 miesięcy** od wejścia w życie — wdrożenie SZBI i środków bezpieczeństwa
- **24 miesiące** — pierwszy audyt (podmioty kluczowe)
- **6 miesięcy** — nowe zasady zgłaszania incydentów
- **2 lata** — pierwsze kary pieniężne mogą być nałożone

Zastrzeżenie: niniejszy dokument ma charakter informacyjny i edukacyjny. Nie stanowi porady prawnej ani audytu zgodności. Opracowano na podstawie Dyrektywy NIS2 (UE 2022/2555), ustawy z 23 stycznia 2026 r. o zmianie ustawy o KSC oraz frameworka CyberFundamentals (CyFun) BASIC Tier opracowanego przez Centre for Cybersecurity Belgium. W celu uzyskania indywidualnej oceny zgodności skontaktuj się z wykwalifikowanym konsultantem. © 2026 Euro Kompas. Wszystkie prawa zastrzeżone.