NIS2 – Checklista dla przedsiębiorstw

Czy Twoja firma jest gotowa na nowe obowiązki w zakresie cyberbezpieczeństwa?

Wprowadzenie

Dyrektywa **NIS2 (Network and Information Security Directive)** weszła w życie w 2025 roku i znacząco rozszerza obowiązki w zakresie cyberbezpieczeństwa. Obejmuje nie tylko infrastrukturę krytyczną, ale również wiele firm z sektora **MŚP**, które przetwarzają dane klientów, świadczą usługi cyfrowe lub są częścią łańcucha dostaw.

Celem tego materiału jest umożliwienie Ci szybkiej samooceny – **czy Twoja organizacja podlega pod NIS2**, a jeśli tak – **czy jest gotowa na kontrolę i spełnienie wymogów**.

KWESTIONARIUSZ WSTĘPNEJ KWALIFIKACJI

Czy Twoja firma podlega obowiązkowi wdrożenia NIS2?

Dyrektywa NIS2 obejmuje szeroki zakres organizacji — nie tylko operatorów infrastruktury krytycznej, ale również firmy świadczące usługi istotne dla gospodarki lub przetwarzające dane wrażliwe.
Odpowiedz na poniższe pytania, aby wstępnie określić, czy Twoja firma może być objęta obowiązkami wynikającymi z NIS2.

1. Wielkość i charakter działalności

Pytanie	TAK	NIE	Notatki
Czy Twoja firma zatrudnia powyżej 50 pracowników?	☐	☐	
Czy roczny obrót Twojej firmy przekracza 10 mln euro (lub równowartość w PLN)?	☐	☐	
Czy świadczycie usługi o znaczeniu dla funkcjonowania innych przedsiębiorstw lub sektora publicznego (np. IT, logistyka, energia, finanse, zdrowie)?	☐	☐	

2. Zakres i charakter usług IT

Pytanie	TAK	NIE	Notatki
Czy Twoja firma świadczy usługi cyfrowe (np. hosting, przetwarzanie danych, utrzymanie systemów, rozwój oprogramowania)?	☐	☐	
Czy zarządzasz lub utrzymujesz infrastrukturę krytyczną lub jej elementy (np. sieci, systemy produkcyjne, usługi łączności)?	☐	☐	
Czy Twoje systemy IT przetwarzają dane osobowe, finansowe lub inne dane wrażliwe klientów lub partnerów?	☐	☐	

3. Rola w łańcuchu dostaw

Pytanie	TAK	NIE	Notatki
Czy Twoja firma jest kluczowym dostawcą usług lub technologii dla innych podmiotów (np. operatorów sieci, firm finansowych, publicznych instytucji)?	☐	☐	
Czy odbiorcy Twoich usług wymagają od Ciebie certyfikatów lub potwierdzeń bezpieczeństwa IT (np. ISO 27001, audytów)?	☐	☐	

4. Obowiązki regulacyjne

Pytanie	TAK	NIE	Notatki
Czy już dziś podlegasz przepisom dotyczącym bezpieczeństwa informacji, np. RODO, KSC, ISO 27001, audytom branżowym?	☐	☐	
Czy posiadasz formalnie wyznaczoną osobę odpowiedzialną za bezpieczeństwo informacji lub IT (np. Inspektor, CISO, vCISO)?	☐	☐	

Wstępna interpretacja wyników:

- **0–2 odpowiedzi TAK:** Prawdopodobnie nie podlegasz bezpośrednio pod NIS2, ale możesz być zobowiązany jako **podwykonawca** w łańcuchu dostaw.
- **3–5 odpowiedzi TAK:** Twoja firma **może podlegać** pod wymogi NIS2 – warto przeprowadzić wstępną analizę i audyt ryzyka.
- **6+ odpowiedzi TAK:** Twoja firma **z dużym prawdopodobieństwem jest objęta Dyrektywą NIS2**. Zalecane jest rozpoczęcie procesu wdrożenia zgodności.

2. CHECKLISTA ZGODNOŚCI Z NIS2

Czy Twoja firma jest gotowa?

Wypełnij checklistę, aby sprawdzić, czy Twoje procesy, procedury i dokumentacja spełniają wymogi NIS2.

1. Audyt ryzyka

Pytanie	TAK	CZĘŚCIOWO	NIE	Notatki
Czy przeprowadzono analizę ryzyk w obszarze IT i procesów biznesowych?	☐	☐	☐	
Czy posiadamy aktualną dokumentację polityk bezpieczeństwa informacji?	☐	☐	☐	
Czy regularnie przeglądamy i aktualizujemy rejestr zagrożeń oraz incydentów?	☐	☐	☐	

2. Środki techniczne i organizacyjne

Pytanie	TAK	CZĘŚCIOWO	NIE	Notatki
Czy mamy wdrożone procedury backupu i odtwarzania danych?	☐	☐	☐	
Czy stosujemy kontrolę dostępu i szyfrowanie danych?	☐	☐	☐	
Czy monitorujemy i logujemy zdarzenia w systemach IT?	☐	☐	☐	
Czy posiadamy plan ciągłości działania (BCP) i odtwarzania po awarii (DRP)?	☐	☐	☐	
Czy dostępy uprzywilejowane (np. administratorzy) są regularnie weryfikowane?	☐	☐	☐	

3. Zarządzanie incydentami

Pytanie	TAK	CZĘŚCIOWO	NIE	Notatki
Czy firma posiada plan reagowania na incydenty bezpieczeństwa?	☐	☐	☐	
Czy wiemy, jak zgłosić incydent do odpowiedniego CSIRT w ciągu 24h?	☐	☐	☐	
Czy pracownicy wiedzą, jak rozpoznać i zgłosić potencjalny incydent?	☐	☐	☐	

4. Łańcuch dostaw

Pytanie	TAK	CZĘŚCIOWO	NIE	Notatki
Czy weryfikujemy dostawców i partnerów pod kątem bezpieczeństwa IT?	☐	☐	☐	
Czy umowy z partnerami zawierają zapisy o cyberbezpieczeństwie i reagowaniu na incydenty?	☐	☐	☐	

5. Szkolenia i kultura bezpieczeństwa

Pytanie	TAK	CZĘŚCIOWO	NIE	Notatki
Czy pracownicy są regularnie szkoleni z zakresu cyberbezpieczeństwa?	☐	☐	☐	
Czy zarząd zna swoje obowiązki wynikające z dyrektywy NIS2?	☐	☐	☐	
Czy w organizacji istnieje kultura zgłaszania błędów i incydentów bez obaw o konsekwencje?	☐	☐	☐	

6. Gotowość na kontrolę

Pytanie	TAK	CZĘŚCIOWO	NIE	Notatki
Czy posiadamy pełną dokumentację spełnienia wymogów NIS2 (polityki, raporty, procedury)?	☐	☐	☐	
Czy wyznaczono osobę odpowiedzialną za cyberbezpieczeństwo (np. vCISO)?	☐	☐	☐	

Pytanie	TAK	CZĘŚCIOWO	NIE	Notatki
Czy procesy bezpieczeństwa są zgodne z przepisami RODO w zakresie danych osobowych?	☐	☐	☐	

3. PODSUMOWANIE I REKOMENDACJE

Jeśli na choć jedno pytanie w powyższych sekcjach odpowiedziałeś **„NIE”** lub **„CZĘŚCIOWO”**, Twoja firma **nie jest w pełni przygotowana** do wdrożenia NIS2.
Dyrektywa wymaga nie tylko posiadania polityk i procedur, ale również ich **udokumentowania, testowania i nadzoru**.

---

4. CO DALEJ?

Skorzystaj z bezpłatnej konsultacji z ekspertem **Cedepe Consulting (vCISO)**, który:

- określi, czy Twoja firma podlega NIS2,
- przeprowadzi analizę luk w obecnym systemie bezpieczeństwa,
- zaproponuje plan działań wdrożeniowych krok po kroku.

Umów konsultację wstępną lub napisz to nas: cedepeconsulting@cedepe.pl

Cedepe Consulting
Eksperckie wsparcie w obszarze **cyberbezpieczeństwa, HR i finansów**