

Dyrektywa NIS2

nowe wymagania cyberbezpieczeństwa dla podmiotów gospodarczych.

Unijna dyrektywa NIS2 (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555) - regulacja znacząco zaostrożająca wymagania w zakresie cyberbezpieczeństwa dla wielu sektorów gospodarki, w tym dla podmiotów związanych z wyrobami medycznymi do diagnostyki in vitro (IVD). Producenci IVD spełniający kryteria wielkości przedsiębiorstwa (co najmniej średnie) automatycznie stają się podmiotami ważnymi, a w określonych sytuacjach mogą zostać uznani za podmioty kluczowe.

Poniższa tabela podsumowuje najważniejsze obowiązki, różnice między statusami podmiotów oraz rolę producentów, dystrybutorów i importerów w nowym reżimie prawnym.

Zagadnienie	Wyjaśnienie
Co to jest NIS 2?	To unijna dyrektywa mająca na celu zapewnienie wysokiego wspólnego poziomu cyberbezpieczeństwa w całej UE. W Polsce wdraża ją nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (KSC).
Po co te zmiany?	Aby zwiększyć odporność gospodarki na ataki hakerskie, chronić dane pacjentów oraz zapewnić ciągłość dostaw produktów i usług , których brak mógłby zagrozić zdrowiu publicznemu.
Od kiedy obowiązuje?	Przepisy powinny być stosowane od 18 października 2024 r. Podmioty spełniające kryteria będą miały 6 miesięcy na wdrożenie obowiązków od dnia wejścia w życie nowelizacji.
Klasy podmiotów	Podmioty dzielą się na kluczowe (podlegające kontroli prewencyjnej i następczej) oraz ważne (kontrolowane głównie po wystąpieniu incydentu).
Rola Producenta IVD	Podmioty produkujące wyroby IVD są wymienione jako sektor ważny . Stają się nimi automatycznie, jeśli są co najmniej średnim przedsiębiorstwem .
Rola Dystrybutora i Importera	Są zdefiniowani jako „ dostawcy sprzętu lub oprogramowania ”. Muszą spełniać wymogi bezpieczeństwa narzucane im w umowach przez szpitale i producentów (zarządzanie łańcuchem dostaw).
Progi wielkości (GBER)	Średnie przedsiębiorstwo : zatrudnienie < 250 osób i obrót ≤ 50 mln EUR lub bilans ≤ 43 mln EUR. Duże przedsiębiorstwo : powyżej tych progów.
Główny obowiązek (SZBI)	Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji , co obejmuje m.in. szacowanie ryzyka, plany ciągłości działania oraz dbanie o bezpieczeństwo łańcucha dostaw.
Zgłaszanie incydentów	Obowiązek raportowania incydentów poważnych: wczesne ostrzeżenie w 24h , zgłoszenie pełne w 72h, sprawozdanie końcowe po miesiącu.
Małe i mikroprzedsiębiorstwa	Podmioty zatrudniające mniej niż 50 osób są co do zasady wyłączone , chyba że pełnią unikalną, strategiczną funkcję (np. są jedynym dostawcą krytycznej usługi) lub organ wyda decyzję o ich włączeniu ze względu na ryzyko systemowe lub zagrożenie dla zdrowia publicznego.