Dyrektywa NIS2 ostatecznie wdrożona w Polsce

Co powinni wiedzieć przedsiębiorcy

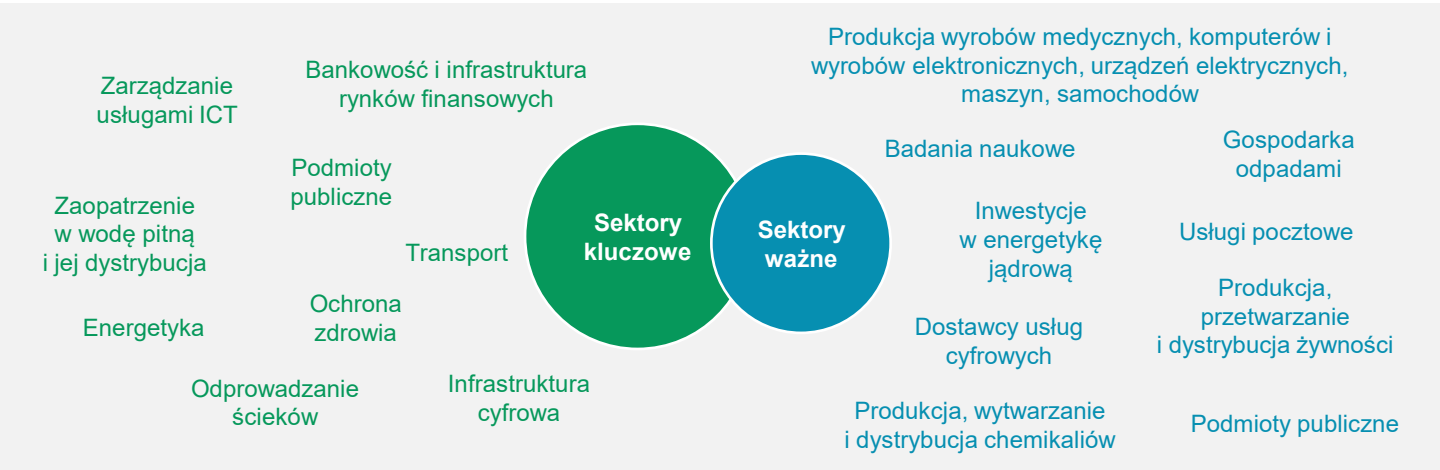
19 lutego 2026 r. Prezydent Rzeczypospolitej Polskiej podpisał ustawę o zmianie ustawy o krajowym systemie cyberbezpieczeństwa („**UKSC**"), wdrażającą dyrektywę (UE) 2022/2555 („**Dyrektywa NIS2**"). Podpis Prezydenta stanowi ostatni etap procesu legislacyjnego przed wejściem w życie nowych przepisów.

Nowe prawo wejdzie w życie po upływie miesięcznego *vacatio legis* liczonego od dnia ogłoszenia UKSC w Dzienniku Ustaw. W praktyce oznacza to, że znowelizowana UKSC zacznie obowiązywać na początku kwietnia 2026 r.

Dla przedsiębiorstw prowadzących działalność w Polsce oznacza to przejście z etapu monitorowania procesu legislacyjnego do etapu wdrożeniowego oraz konieczność rozpoczęcia uporządkowanego procesu zapewnienia zgodności z nowymi obowiązkami wynikającymi z UKSC.

NAJWAŻNIEJSZE ZMIANY REGULACYJNE WZGLĘDEM REŻIMU NIS1

- Zastąpienie dotychczasowych kategorii operatorów usług kluczowych i dostawców usług cyfrowych nowymi kategoriami podmiotów kluczowych oraz podmiotów ważnych.
- Istotne rozszerzenie katalogu sektorów objętych regulacją. Oprócz energetyki, transportu, ochrony zdrowia i bankowości, UKSC obejmuje obecnie m.in. produkcję i dystrybucję żywności, sektor chemiczny, usługi pocztowe i kurierskie, gospodarkę odpadami, infrastrukturę cyfrową oraz sektor kosmiczny. Poniżej znajduje się pełna lista sektorów:



- Wzmocnienie uprawnień nadzorczych organów właściwych do spraw cyberbezpieczeństwa, w tym możliwość nakazania przeprowadzenia audytu bezpieczeństwa oraz wydawania wiążących poleceń w związku z incydentami.
- Utworzenie sektorowych zespołów reagowania na incydenty bezpieczeństwa komputerowego wspierających obsługę incydentów i koordynację działań.
- Przypisanie odpowiedzialności kierownikom podmiotów kluczowych i ważnych, w tym wprowadzenie obowiązku odbywania szkoleń.

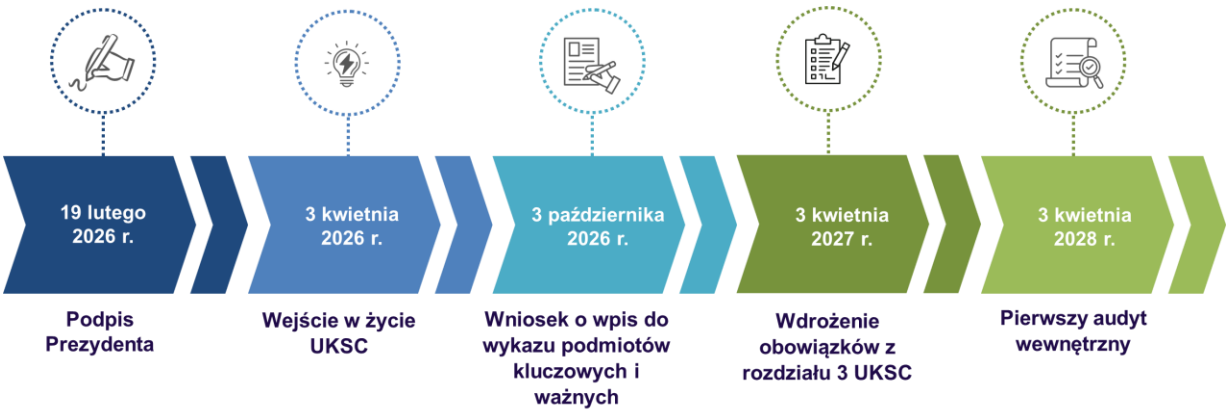
ADDLESHAW GODDARD

Dyrektywa NIS2 ostatecznie wdrożona w Polsce

Co powinni wiedzieć przedsiębiorcy

HARMONOGRAM WDROŻENIA

1. 19 lutego 2026 r. – podpis Prezydenta.
2. 3 kwietnia 2026 r. – wejście w życie UKSC po upływie miesięcznego vacatio legis. 3 października 2026 r. – złożenie wniosku o wpis do wykazu podmiotów kluczowych i podmiotów ważnych.
3. 3 kwietnia 2027 r. – wdrożenie oraz zapewnienie zgodności z obowiązkami w zakresie zarządzania ryzykiem w cyberbezpieczeństwie określonymi w rozdziale 3 UKSC.
4. 3 kwietnia 2028 r. – przeprowadzenie pierwszego audytu przez podmioty, które w dniu wejścia w życie UKSC spełniają przesłanki uznania za podmiot kluczowy.



PIERWSZY KROK – SAMOOCENA PODMIOTU

Przedsiębiorcy powinni teraz przejść od etapu analizy potencjalnych zmian do etapu wdrożenia nowych reguł na gruncie znowelizowanej UKSC. Punktem wyjścia powinno być przeprowadzenie samooceny podmiotu w celu ustalenia, czy kwalifikuje się on jako podmiot kluczowy lub podmiot ważny w rozumieniu UKSC. Ocena ta może być złożona i wymagać analizy klasyfikacji sektorowej, progów wielkościowych oraz charakteru świadczonych usług.

DZIAŁANIA COMPLIANCE

Podmioty objęte zakresem UKSC powinny w szczególności:

- wdrożyć adekwatne środki techniczne i organizacyjne dostosowane do skali działalności, rodzaju usług oraz profilu ryzyka,
- dokonać przeglądu i przetestować mechanizmy wykrywania i raportowania incydentów,
- przeprowadzić kompleksową analizę łańcucha dostaw, w tym pod kątem korzystania z rozwiązań dostawców uznanych za dostawców wysokiego ryzyka,
- zapewnić udokumentowany nadzór kierownictwa nad obszarem cyberbezpieczeństwa,
- zapewnić spójność wdrożenia UKSC z innymi reżimami regulacyjnymi, w szczególności z rozporządzeniem DORA, RODO oraz innymi regulacjami cyfrowymi UE.

ADDLESHAW GODDARD

Dyrektywa NIS2 ostatecznie wdrożona w Polsce

Co powinni wiedzieć przedsiębiorcy

SANKCJE I RYZYKO NADZORCZE

Naruszenie obowiązków wynikających z UKSC może skutkować nałożeniem wysokich administracyjnych kar pieniężnych, ukształtowanych analogicznie do modelu przyjętego w RODO.

Co do zasady:

- na podmioty kluczowe może zostać nałożona kara pieniężna w wysokości do 10 mln euro albo do 2% przychodów z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa;
- na podmioty ważne może zostać nałożona kara pieniężna w wysokości do 7 mln euro albo do 1,4% przychodów z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa

UKSC przewiduje również możliwość nałożenia kary do 100 mln zł w sytuacji, gdy naruszenie powoduje bezpośrednie i poważne cyberzagrożenie dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego albo życia i zdrowia ludzi, lub stwarza ryzyko powstania poważnej szkody majątkowej bądź istotnych utrudnień w świadczeniu usług.

ODPOWIEDZIALNOŚĆ ZARZĄDU

UKSC wprowadza model dodatkowej odpowiedzialności kierownictwa podmiotu kluczowego lub ważnego oraz wzmacnia znaczenie cyberbezpieczeństwa jako obszaru wymagającego nadzoru na poziomie zarządu. Kierownik podmiotu kluczowego lub ważnego (zarząd) jest zobowiązany do zapewnienia wdrożenia oraz skutecznego nadzoru nad środkami zarządzania ryzykiem w cyberbezpieczeństwie oraz do zapewnienia zgodności działalności podmiotu z obowiązkami wynikającymi z UKSC. Kadra zarządzająca będzie zatem ponosić bezpośrednią odpowiedzialność za realizację obowiązków w na gruncie UKSC. W UKSC przewidziano kary pieniężne dla kadry zarządzającej za naruszenia obowiązków wynikających z ustawy.

UKSC wprowadza również obowiązek odbywania regularnych szkoleń przez kierownictwo i wprost wyklucza możliwość przeniesienia odpowiedzialności za zadania z zakresu cyberbezpieczeństwa na niższe szczeble w organizacji. W świetle rozszerzonych uprawnień nadzorczych oraz wysokiego poziomu sankcji, obszar cyberbezpieczeństwa wymaga realnego i udokumentowanego nadzoru na poziomie kierownictwa (zarządu) podmiotów objętych UKSC.

JAK MOŻEMY POMÓC

Doradzamy w zakresie mapowania i wdrożenia obowiązków wynikających z Dyrektywy NIS2 na poziomie unijnym oraz z UKSC w Polsce. Wspieramy Klientów w szczególności w zakresie:

- oceny, czy obowiązki wynikające z Dyrektywy NIS2 i UKSC mają zastosowanie do danego podmiotu,
- identyfikacji konkretnych wymogów regulacyjnych,
- wdrożenia polityk, procedur i dokumentacji w obszarze cyberbezpieczeństwa,
- doradztwa w zakresie prawnych aspektów obsługi i raportowania incydentów,
- przeglądu umów z dostawcami produktów i usług ICT,
- prowadzenia szkoleń dla kierownictwa oraz zespołów IT z nowych wymogów regulacyjnych.

KONTAKT

SZYMON SIENIEWICZ
Counsel
Head of TMT/IP
Tel +48 22 526 5042
Mob +48 665 052 724
szymon.sieniewicz@aglaw.com

ADDLESHAW GODDARD