

**Alert
prawny**

Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa wdrażająca dyrektywę NIS 2

28 stycznia Sejm i Senat **uchwalił nowelizację ustawy o krajowym systemie cyberbezpieczeństwa (UKSC), która implementuje dyrektywę NIS 2.** Ustawa oczekuje obecnie na podpis Prezydenta i ma wejść w życie po upływie 14 dni od dnia ogłoszenia.

Kogo dotyczą nowe przepisy?

Nowe przepisy obejmą **podmioty kluczowe oraz podmioty ważne**, przy czym kwalifikacja następować będzie na podstawie dwóch kryteriów: wielkościowego oraz sektorowego.

Kryterium wielkościowe

Co do zasady jako podmioty kluczowe i ważne będą kwalifikować się **średnie i duże przedsiębiorstwa**, tj. podmioty zatrudniające co najmniej 50 pracowników lub osiągające roczny obrót powyżej 10 mln EUR, lub całkowity bilans roczny przekraczający 10 mln EUR. **Przy obliczaniu progów wielkości przedsiębiorstwa należy uwzględnić dane przedsiębiorstw partnerskich i powiązanych**, co w praktyce może powodować objęcie regulacją również mniejszych podmiotów należących do większych struktur organizacyjnych.

Kryterium sektorowe

Dodatkowo warunkiem objęcia ustawą jest **prowadzenie działalności w jednym z sektorów wskazanych w załącznikach do ustawy**. Sektory te obejmują w szczególności:

- › energetykę,
- › transport (lotniczy, kolejowy, wodny, drogowy),
- › bankowość, infrastrukturę rynków finansowych,
- › opiekę zdrowotną,
- › zaopatrzenie w wodę pitną i odprowadzanie ścieków,
- › infrastrukturę cyfrową oraz zarządzanie usługami ICT,
- › przestrzeń kosmiczną,
- › usługi pocztowe i kurierskie,
- › gospodarowanie odpadami,
- › produkcję, wytwarzanie i dystrybucję chemikaliów,
- › produkcję, przetwarzanie i dystrybucję żywności,
- › produkcję wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro,
- › produkcję komputerów, wyrobów elektronicznych i optycznych,
- › produkcję urządzeń elektrycznych oraz maszyn i urządzeń, gdzie indziej niesklasyfikowanych,
- › produkcję pojazdów samochodowych, przyczep, naczep i pozostałego sprzętu transportowego,
- › działalność badawczo-naukową (organizacje badawcze).

W konsekwencji **katalog podmiotów objętych regulacją jest istotnie szerszy niż w dotychczasowym stanie prawnym** i obejmuje wiele przedsiębiorstw, które dotąd nie podlegały przepisom ustawy o krajowym systemie cyberbezpieczeństwa.

Przedsiębiorcy powinni samodzielnie dokonać oceny, czy spełniają kryteria wielkościowe oraz sektorowe objęcia regulacją.

Kluczowe obowiązki

Nowelizacja UKSC nakłada na podmioty kluczowe i ważne obowiązek wdrożenia kompleksowego **systemu zarządzania bezpieczeństwem informacji**, obejmującego zarówno środki techniczne, jak i organizacyjne. W szczególności wymagane będzie:

- › zarządzanie ryzykiem w obszarze cyberbezpieczeństwa oraz regularna identyfikacja i ocena zagrożeń,
- › wdrożenie odpowiednich środków technicznych i organizacyjnych, w tym przyjęcie i utrzymywanie polityk, procedur i dokumentacji bezpieczeństwa,
- › zapewnienie ciągłości działania i planów reagowania kryzysowego,
- › monitorowanie, wykrywanie i obsługa incydentów oraz ich zgłaszanie w ustawowych terminach do właściwych organów,
- › prowadzenie regularnych testów, audytów oraz szkoleń pracowników,
- › zapewnienie bezpieczeństwa łańcucha dostaw, w tym weryfikację i nadzór nad dostawcami usług ICT,
- › dostosowanie umów z dostawcami i podwykonawcami poprzez wprowadzenie wymogów bezpieczeństwa i obowiązków raportowych,
- › sprawowanie nadzoru przez kadrę zarządzającą nad realizacją obowiązków oraz przypisanie odpowiedzialności wewnątrz organizacji.

W praktyce wdrożenie przepisów wymagać będzie nie tylko zmian technicznych, lecz także uporządkowania procesów wewnętrznych, dokumentacji oraz relacji kontraktowych z dostawcami.

Nadzór i sankcje

Nadzór nad wykonywaniem obowiązków wynikających z UKSC sprawować będą właściwe organy krajowego systemu cyberbezpieczeństwa, wyposażone w szerokie **kompetencje nadzorcze i środki egzekwowania przepisów**. Organ te będą uprawnione m.in. do:

- › żądania informacji, dokumentów i wyjaśnień,
- › przeprowadzania kontroli i audytów, w tym w siedzibie podmiotu,
- › wydawania poleceń lub nakazów naprawienia uchybień, lub usunięcia naruszeń,
- › wystosowania ostrzeżeń dotyczących naruszeń.

W przypadku naruszeń możliwe będzie nałożenie **administracyjnych kar pieniężnych**, których wysokość uzależniona będzie od kategorii podmiotu:

Podmiot kluczowy od 20 000 zł do 10 mln EUR lub 2% przychodów (stosuje się kwotę wyższą) 	Podmiot ważny od 15 000 zł do 7 mln EUR lub 1,4% przychodów (stosuje się kwotę wyższą) 	Sankcja nadzwyczajna do 100 mln zł 	Sankcja wobec kierownika do 300% otrzymywanego przez ukaranego wynagrodzenia 
---	---	---	---

Administracyjne kary pieniężne będą mogły być nakładane po upływie 2 lat od wejścia w życie ustawy, co daje organizacjom czas na wdrożenie wymaganych środków, jednak nie zwalnia z obowiązku rozpoczęcia przygotowań niezwłocznie po wejściu w życie przepisów.

Jak możemy pomóc?

Zapewniamy wsparcie prawne w przygotowaniu organizacji do spełnienia nowych obowiązków wynikających z nowelizacji UKSC, w szczególności w zakresie dostosowania dokumentacji, procesów wewnętrznych oraz relacji kontraktowych.

Zakres wsparcia obejmuje w szczególności:

- › weryfikację czy przepisy mają zastosowanie do danej organizacji (kwalifikacja jako podmiot kluczowy lub ważny),
- › analizę luki oraz opracowanie rekomendacji działań dostosowawczych,
- › przygotowanie i aktualizację polityk, procedur oraz pozostałej dokumentacji wewnętrznej wymaganej przepisami,
- › dostosowanie umów z dostawcami i podwykonawcami,
- › wsparcie w opracowaniu procedur zgłaszania incydentów i współpracy z organami nadzorczymi,
- › doradztwo prawne w toku kontroli, postępowań nadzorczych oraz przy interpretacji obowiązków ustawowych,
- › szkolenia dla personelu i kadry zarządzającej.

Kluczowi doradcy

Ekspertki z Praktyki IP&TMT



dr Aleksandra Auleytner

Partner, Szefowa Praktyki IP&TMT

E: Aleksandra.Auleytner@dzp.pl

T: +48 660 440 306



Karolina Kulikowska-Gruszecka

Senior Associate

E: Karolina.Kulikowska-Gruszecka@dzp.pl

T: +48 660 440 314