



LEGAL UPDATE
We create clarity.

NOWELIZACJA USTAWY O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA

– WDROŻENIE NIS2 ORAZ ZMIANY O SZEROKIM WPŁYWIE NA RYNEK

28 stycznia Senat przyjął nowelizację ustawy o krajowym systemie cyberbezpieczeństwa (UKSC), która trafi teraz do podpisu Prezydenta. Celem zmian jest implementacja w Polsce unijnej dyrektywy NIS2 oraz wytycznych „5G Toolbox” dotyczących bezpieczeństwa sieci piątej generacji. Warto podkreślić, że termin wdrożenia NIS2 upłynął 17 października 2024 roku, co oznacza, że Polska wprowadza nowe regulacje ze znacznym opóźnieniem.

Szerokie rozszerzenie katalogu podmiotów objętych ustawą

Jedną z kluczowych zmian jest znaczące zwiększenie liczby podmiotów objętych regulacją. Obecnie UKSC dotyczy około 400 jednostek. Projekt nowelizacji przewiduje, że po wejściu w życie nowych przepisów liczba ta wzrośnie do ponad **10 tysięcy**.

Zmiana wynika z całkowitej przebudowy dotychczasowego podziału na operatorów usług kluczowych oraz dostawców usług cyfrowych. W ich miejsce pojawiają się dwie nowe kategorie:

- **Podmioty kluczowe**

Obejmują większe organizacje działające z jak: energetyka, transport, automotive, bankowość, infrastruktura cyfrowa, ochrona zdrowia czy woda pitna.

- **Podmioty ważne**

Obejmują głównie średnie firmy, których działalność – choć istotna – nie wiąże się z natychmiastowym ryzykiem zakłócenia systemowego. Przykładowe sektory: usługi pocztowe i kurierskie, gospodarka odpadami, żywność (produkcja, przetwarzanie, dystrybucja).

Nowy mechanizm samoidentyfikacji – obowiązek po stronie przedsiębiorcy

Projekt wprowadza zasadę, zgodnie z którą **to podmiot samodzielnie ocenia**, czy spełnia kryteria „podmiotu kluczowego” lub „podmiotu ważnego”. Identyfikacja ma charakter obowiązkowy i wymaga zgłoszenia do właściwego rejestru. Oznacza to, że przedsiębiorcy – jeszcze przed wejściem nowych przepisów w życie – powinni dokonać wstępnej analizy, czy będą objęci zakresem nowelizacji. Warto mieć również na uwadze, iż nawet jeżeli dany podmiot nie będzie podlegać pod UKSC, to może on zostać objęty audytami prowadzonymi przez swoich klientów w związku z realizacją przez nich obowiązków wynikających z UKSC.



Nowe obowiązki w obszarze bezpieczeństwa informacji

Projekt przewiduje szeroki katalog obowiązków, których centrum stanowi zbudowanie i utrzymanie spójnego systemu zarządzania bezpieczeństwem informacji.

Do kluczowych elementów należą:

- systematyczne szacowanie ryzyka incydentów bezpieczeństwa,
- wdrażanie adekwatnych środków minimalizujących ryzyko,
- ustanowienie procedur efektywnego reagowania na incydenty,
- zapewnienie współpracy z CSIRT,
- obowiązkowe coroczne szkolenia dla kadry kierowniczej podmiotów kluczowych i ważnych.

Nowe wymogi dotyczące technologii ICT i łańcucha dostaw

Istotnym elementem dyrektywy NIS2 jest wprowadzenie wymogów dotyczących zarządzania ryzykiem w łańcuchu dostaw, przy czym proponowana nowelizacja UKSC przewiduje ich zastosowanie w odniesieniu do łańcucha dostaw produktów, usług oraz procesów ICT. Na podmiotach objętych ustawą spoczywać będzie m.in.:

- obowiązek oceny ryzyka w łańcuchu dostaw,
- weryfikacja bezpieczeństwa dostawców i partnerów kluczowych,
- stosowanie procedur kwalifikacji i oceny dostawców „wysokiego ryzyka”,
- uwzględnianie bezpieczeństwa ICT w procesach zakupowych spółki.

Rekomendacje dla przedsiębiorców

W związku z bardzo szerokim zakresem zmian oraz potencjalnie dużym wpływem na działalność operacyjną firm rekomendujemy, aby spółki już teraz:

- **zweryfikowały, czy kwalifikują się jako podmiot kluczowy lub ważny,**
- **dokonały przeglądu obowiązujących procedur bezpieczeństwa,**
- **rozpoczęły przygotowania do wdrożenia nowych procesów i polityk bezpieczeństwa zgodnych z NIS2.**

Nasza Kancelaria pozostaje do Państwa dyspozycji w zakresie:

- analizy kwalifikacji spółki pod nowe kategorie UKSC,
- oceny obecnych procedur cyberbezpieczeństwa,
- przygotowania lub aktualizacji polityk i dokumentacji zgodnej z NIS2,
- wsparcia w budowie systemów zgodności oraz budowania cyberodporności organizacyjnej.

Zapraszamy do kontaktu!

SDZLEGAL Schindhelm

Kancelaria Prawna Schampera, Dubis, Zając i Wspólnicy sp.j.

ul. Kazimierza Wielkiego 3

50-077 Wrocław

tel.: +48 71 326 51 40

e-mail: piotr.wyszumirski@sdzlegal.pl

e-mail: wroclaw@sdzlegal.pl

www.schindhelm.com