Informacja o ustawie z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (druki sejmowe nr 1955 i 2139),

Podpisana ustawa zmienia przepisy obowiązującej ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222 oraz z 2025 r. poz. 1017 i 1069). Celem uchwalonej przez Sejm ustawy jest kompleksowa zmiana obowiązującego w Polsce systemu zapewnienia cyberbezpieczeństwa i podniesienie poziomu odporności na cyberzagrożenia oraz poziomu ochrony informacji w sektorach: publicznym, militarnym i prywatnym, a także wdrożenie do polskiego porządku prawnego dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającą rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 – zwanej dalej „dyrektywa NIS 2" lub „dyrektywą 2022/2555" tak by polskie regulacje z zakresu cyberbezpieczeństwa były spójne z rozwiązaniami przyjętymi na poziomie Unii Europejskiej.

Uchwalona ustawa dostosowuje krajowy system cyberbezpieczeństwa do zmienionego otoczenia cyfrowego i rosnącej skali zagrożeń w cyberprzestrzeni. Zmiany obejmują m.in. rozszerzenie katalogu podmiotów objętych obowiązkami, zastąpienie dotychczasowego podziału na operatorów usług kluczowych i dostawców usług cyfrowych nową kategorią podmiotów kluczowych i podmiotów ważnych, wzmocnienie systemu reagowania na incydenty oraz do-precyzowanie ról organów odpowiedzialnych za cyberbezpieczeństwo.

Ustawa wprowadza nową strukturę krajowego systemu cyberbezpieczeństwa, rozszerza obowiązki podmiotów publicznych i prywatnych w obszarze cyberbezpieczeństwa, określa na nowo kompetencje organów państwowych oraz wprowadza mechanizmy prewencyjne i kontrolne w odniesieniu do podmiotów kluczowych i ważnych. W ustawie wprowadzono też definicję podmiotów kluczowych, czyli tych, których działanie ma istotne znaczenie dla funkcjonowania państwa i gospodarki, oraz podmiotów ważnych, które mimo mniejszej skali działania nadal muszą spełniać obowiązki w zakresie cyberbezpieczeństwa, w tym zgłaszać incydenty i stosować podstawowe procedury ochrony systemów informacyjnych.

Najważniejsze zmiany zawarte w ustawie polegają na:

1) rozszerzeniu katalogu podmiotów krajowego systemu cyberbezpieczeństwa o nowe sektory gospodarki tj. zarządzania technologią informacyjno-komunikacyjną (ICT), przestrzeni kosmicznej, poczty, produkcji, w tym produkcji i dystrybucji chemikaliów, żywności oraz gospodarowania ściekami;
2) nałożeniu obowiązków z zakresu środków zarządzania ryzykiem na podmioty kluczowe oraz podmioty ważne w cyberbezpieczeństwie, dotyczących stosowania odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych służących zarządzaniu ryzykiem dla bezpieczeństwa sieci i systemów informatycznych;
3) uregulowaniu zasad odpowiedzialności kierownika podmiotu kluczowego lub podmiotu ważnego za realizację zadań z zakresu cyberbezpieczeństwa – kierownik takiego podmiotu będzie odpowiedzialny za realizację zadań przez dany podmiot, a w przypadku niewywiązania się z obowiązków na kierownika będą mogły być nałożone kary; kierownik będzie również obowiązany do odbycia stosownego szkolenia z zakresu cyberbezpieczeństwa;
4) wprowadzeniu możliwości zgłaszania incydentów przez podmioty kluczowe i podmioty ważne, za pomocą systemu teleinformatycznego ministra właściwego do spraw informatyzacji, do właściwych zespołów CSIRT sektorowych i CSIRT poziomu krajowego;
5) utworzeniu zespołów CSIRT sektorowych w poszczególnych sektorach gospodarki, które będą wspierać podmioty kluczowe i podmioty ważne w obsłudze incydentów cyberbezpieczeństwa. Utworzenie CSIRT-ów sektorowych ma nastąpić w ciągu 18 miesięcy od wejścia w życie ustawy;
6) wzmocnieniu kompetencji nadzorczych organów właściwych do spraw cyberbezpieczeństwa; wzmocnienie kompetencji obejmuje umożliwienie wydawania ostrzeżeń, wyznaczania urzędnika monitorującego wykonywanie obowiązków przez dany pod-miot kluczowy, nakazywania przeprowadzenia oceny bezpieczeństwa systemu informacyjnego lub audytu bezpieczeństwa;
7) wprowadzeniu kar pieniężnych za niewykonanie obowiązków ustawowych przez podmioty kluczowe lub podmioty ważne, m.in. za niewdrożenie systemu zarządzania bezpieczeństwem informacji czy niezarejestrowanie się w wykazie podmiotów kluczowych i podmiotów ważnych;
8) wprowadzeniu Krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę;

9) rozszerzeniu kompetencji ministra ds. informatyzacji – organ ten będzie mógł dokonać, w drodze decyzji, prawnej identyfikacji dostawcy wysokiego ryzyka, będzie mógł też wydać polecenie zabezpieczające ze wskazaniem zachowania, które ograniczy skutki trwającego incydentu krytycznego;
10) wzmocnieniu pozycji Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa poprzez:
    a. zapewnienie możliwości żądania od organów administracji rządowej informacji niezbędnych do wykonywania jego zadań;
    b. przyznanie uprawnienia do zlecania wykonania badań niezbędnych do realizacji zadań;
    c. wprowadzenie możliwości dokonywania zakupu oprogramowania z zakresu cyberbezpieczeństwa dla uczestników posiedzeń Połączonego Centrum Operacyjnego Cyberbezpieczeństwa;
    d. utrzymanie w mocy rekomendacji mających na celu wzmocnienie poziomu cyberbezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa, jak i uprawnienia do ich wydawania;
11) rozszerzeniu kompetencji zespołów CSIRT poziomu krajowego, w tym CSIRT NASK, co jest związane ze zwiększoną liczbą podmiotów kluczowych i podmiotów ważnych, którym CSIRT NASK będzie udzielał wsparcia w reagowaniu na incydenty;
12) rozwijaniu kompetencji ministra w zakresie edukacji cyberbezpieczeństwa – przewiduje się środki na prowadzenie kampanii edukacyjnych i programów z zakresu cyberbezpieczeństwa.

Ustawa wchodzi w życie po upływie miesiąca od dnia ogłoszenia.

Pomimo, iż Prezydent podpisał ustawę, to jednocześnie podjął decyzję o skierowaniu ustawy do kontroli następczej przez Trybunał Konstytucyjny z następujących powodów.
Wątpliwości budzi objęcie ustawą aż 18 branż gospodarki pogrupowanych w podmioty kluczowe i ważne. Przy czym, rozszerzenie to nie wynika z przepisów europejskich, a jest samodzielną inicjatywą rządu. Zasadne jest zgłoszenie zastrzeżeń również wobec przepisów regulujących zasady uznawania podmiotów za dostawców wysokiego ryzyka (DWR) oraz zasady wydawania tzw. „poleceń zabezpieczających". Przepisy te ingerują w samodzielność funkcjonowania przedsiębiorców, m.in. poprzez nakładanie obowiązku wymiany sprzętu oraz oprogramowania i to bez odszkodowania, i bez zabezpieczenia środków finansowych na ten

cel. Ponadto wadliwy jest system podejmowania decyzji przez organy ds. cyberbezpieczeństwa wobec podmiotów kluczowych i ważnych, z punktu widzenia gwarancji proceduralnych oraz w zakresie ochrony sądowej.
Przewidziany ustawą system kar administracyjnych jest restrykcyjny, a wysokość możliwych do nałożenia kar ma wręcz charakter samodzielnych środków karnych.

Prezydent zdecydował zatem o przekazaniu ustawy do Trybunału Konstytucyjnego celem weryfikacji podniesionych zarzutów dotyczących naruszenia przepisów Konstytucji RP.