NASK

Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa – stan po pracach w parlamencie

Zmiany wprowadzone w projekcie nowelizacji na etapie prac parlamentarnych

NASK-PIB
ul. Kolska 12
01–045 Warszawa

NIP: 521 04 17 157
Regon: 010464542
KRS: 0000012938

nask@nask.pl
+48 22 380 82 00
+48 22 380 82 01

nask.pl

NASK

Spis treści

27 stycznia w komisji w Senacie przyjęto projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa (dalej: KSC) bez poprawek w stosunku do tekstu przyjętego w Sejmie. Oznacza to, że aktualnie ustawa została przekazana do podpisu Prezydentowi RP, który decyzję o jej dalszych losach musi podjąć do 19 lutego 2026 r. W trakcie prac parlamentarnych pierwotny, skierowany do Sejmu tekst projektu uległ zmianom, w szczególności w zakresie terminów spełniania obowiązków przez podmioty KSC oraz nakładania kar.

1. Wprowadzenie – pierwotny tekst nowelizacji skierowany do parlamentu

Przedłożony Sejmowi projekt ustawy o zmianie ustawy o KSC, któremu nadano numer druku 1955, stanowi odpowiedź na konieczność implementacji dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 (NIS 2), a tym samym dalszego uszczelnienia ekosystemu bezpieczeństwa państwa w wymiarze cyfryzacji i cyberbezpieczeństwa. Ustawa wdraża także rozwiązania zaproponowane w tzw. 5G Toolbox, nadając im charakter uniwersalny i obejmując nimi więcej sektorów niż wyłącznie sektor telekomunikacji.

2. Główne zmiany w nowelizacji

Zasadniczym celem projektodawcy jest odejście od dotychczasowego, punktowego modelu ochrony zasobów, sieci, systemów i usług na rzecz powszechnego, sektorowego podejścia do cyberodporności oraz zwiększania dojrzałości w tym zakresie już na poziomie sektorowym. Projekt zakłada objęcie reżimem ustawowym szerokiego katalogu podmiotów gospodarczych i publicznych (szacunkowo dziesiątki tysięcy jednostek), w tym także tych które wcześniej nie były częścią KSC. Istotnym elementem projektu jest powiązanie wymogów cyberbezpieczeństwa z bezpieczeństwem łańcucha dostaw, co ma pozwolić na eliminację z polskiego rynku technologii lub urządzeń stanowiących zagrożenie dla bezpieczeństwa państwa, obronności lub porządku publicznego, w ramach tak zwanej procedury uznania za dostawcę wysokiego ryzyka (dalej także jako DWR) czy też podejmowanie innych ekstraordynaryjnych środków na rzecz cyberbezpieczeństwa.

2.1. Zakres podmiotowy

Projekt dokonuje fundamentalnej przebudowy oraz rozszerzenia zakresu podmiotowego ustawy. Dotychczasowa kategoria „operatorów usług kluczowych” (OUK) zostaje zastąpiona dychotomicznym podziałem na **podmioty**

kluczowe i **podmioty ważne**, opartym na kryteriach wielkości przedsiębiorstwa lub krytyczności i znaczenia sektora, w którym działają. Nowa systematyka obejmuje 18 sektorów gospodarki, w niektórych przypadkach rozszerzając te dotychczas objęte (jak energia, ochrona zdrowia czy infrastruktura cyfrowa), ale dodając także nowe jak produkcja, wytwarzanie i dystrybucja chemikaliów, administracja publiczna czy przestrzeń kosmiczna.

Sektor		KSC 2.0 – sektory kluczowe	KSC 2.0 – sektory ważne
	Energia	✓	
	Transport	✓	
	Bankowość	✓	
	Infrastruktura rynków finansowych	✓	
	Ochrona zdrowia	✓	
	Zaopatrzenie w wodę pitną i jej dystrybucja	✓	
	Infrastruktura cyfrowa	✓	
	Ścieki	✓	
	Zarządzanie usługami ICT	✓	
	Administracja publiczna	✓	
	Przestrzeń kosmiczna	✓	

	Usługi pocztowe i kurierskie		✓
	Gospodarowanie odpadami		✓
	Produkcja, wytwarzanie i dystrybucja chemikaliów	✓	
	Produkcja, przetwarzanie i dystrybucja żywności	✓	
	Produkcja	✓	
	Dostawcy usług cyfrowych		✓
	Badania naukowe		✓

✓	sektory, które były objęte ustawą o KSC z 2018 r. i które staną się sektorami kluczowymi
✓	sektory, które były objęte ustawą o KSC z 2018 r. i które staną się sektorami kluczowymi oraz w których zostały zmodyfikowane lub dodane nowe podsektory
✓	nowe sektory, które zostaną objęte przepisami nowelizacji ustawy o KSC

Zmianie ulegnie także procedura identyfikacji podmiotów KSC. Do tej pory operatorzy usług kluczowych byli wyznaczani w drodze decyzji administracyjnej organu właściwego do spraw cyberbezpieczeństwa. Nowelizacja odchodzi jednak od tej zasady i wprowadza samoidentyfikację podmiotów kluczowych i ważnych, nakładając na nie obowiązek samodzielnej rejestracji w wykazie prowadzonym przez ministra właściwego do spraw informatyzacji. Część informacji w wykazie będzie uzupełniana z urzędu przez ministra właściwego do spraw informatyzacji. Natomiast **podmioty zobowiązane będą do złożenia wniosku o wpis do rejestru w terminie 2 miesięcy** od spełnienia przesłanek uznania za podmiot kluczowy lub ważny, czyli od dnia wejścia w życie ustawy.

2.2. System zarządzania bezpieczeństwem informacji

Kluczowym elementem zmian jest także wprowadzenie rozwiniętego i kompleksowego **systemu zarządzania bezpieczeństwem informacji (SZBI)** w podmiotach KSC. Zostaną one zobligowane do wdrożenia proporcjonalnych środków technicznych i organizacyjnych, w tym polityk analizy ryzyka, obsługi incydentów, ciągłości działania oraz bezpieczeństwa łańcucha dostaw. Projektodawca pierwotnie, to znaczy w projekcie

skierowanym do Sejmu, nałożył na podmioty obowiązek wprowadzenia ich w terminie **6 miesięcy** od wpisu do wykazu podmiotów kluczowych i ważnych.

2.3. Procedura uznania za dostawcę wysokiego ryzyka

Znaczącą zmianą w projekcie nowelizacji jest wprowadzenie procedury uznawania dostawcy za **dostawcę wysokiego ryzyka (DWR)**. Minister właściwy do spraw informatyzacji, z urzędu lub na wniosek przewodniczącego Kolegium do Spraw Cyberbezpieczeństwa, po zasięgnięciu opinii Kolegium ds. Cyberbezpieczeństwa, uzyskuje kompetencję do wydania decyzji administracyjnej eliminującej z rynku konkretny sprzęt lub oprogramowanie, wykorzystywane przez ustawowo wskazane podmioty. Postępowanie musi być wszczęte w celu określonym przepisami , tj. ochrony bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego. Procedura uznania za DWR jest wieloetapowa oraz angażuje szereg podmiotów, obejmuje fazy opiniowania oraz ważenia kwestii stopnia zagrożenia i jego wpływu na bezpieczeństwo, a także wieloaspektowej i wielopłaszczyznowej analizy ryzyk dla całego systemu bezpieczeństwa państwa, w tym również podmiotu będącego producentem danych produktów, usług i procesów.

Decyzja o uznaniu za dostawcę wysokiego ryzyka jest wydawana przez ministra właściwego ds. informatyzacji i zawiera w szczególności wskazanie produktów, rodzajów usług lub procesów ICT. Ogłasza się ją w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski” oraz udostępnia w Biuletynie Informacji Publicznej ministra i na stronie internetowej urzędu go obsługującego. Zasadniczą konsekwencją takiej decyzji jest bezwzględny obowiązek wycofania wskazanych rozwiązań w ciągu 4 lat (sektor telekomunikacyjny lub ujęcie w wykazie kategorii funkcji krytycznych) lub 7 lat (pozostałe podmioty).

2.4. Model zgłaszania i obsługi incydentów oraz podatności

Nowelizacja ustawy wprowadza także obowiązek powołania przez organ właściwy do spraw cyberbezpieczeństwa CSIRT sektorowego, właściwego dla danego sektora lub podsektora. Na ich powołanie jest 18 miesięcy. Wprowadza to jednocześnie **kaskadowy model zgłaszania incydentów** – pierwszym punktem kontaktu są CSIRT sektorowe. Niezależnie od tego CSIRT sektorowy ma ustawowy obowiązek przekazać każde wczesne ostrzeżenie, zgłoszenie i sprawozdanie z obsługi incydentu poważnego do właściwego CSIRT krajowego (NASK, GOV lub MON) niezwłocznie, nie później niż w ciągu 8 godzin.

Wprowadzono rozróżnienie na informacje dot. incydentów poważnych, których obowiązek przekazywania do CSIRT sektorowych mają podmioty: wczesne ostrzeżenie w ciągu 24 godzin od wykrycia, pełne zgłoszenie w 72 godziny oraz sprawozdania okresowe i końcowe. Całość komunikacji, w tym obsługa incydentów oraz przekazywanie informacji, ma być realizowana za pośrednictwem centralnego systemu teleinformatycznego (**S46**), którego użycie staje się obligatoryjne, a niekorzystanie z niego naraża podmiot na kary.

W ramach nowych przepisów, wynikających z dyrektywy NIS 2, CSIRT NASK otrzymał rolę koordynatora w procesie skoordynowanego ujawniania podatności (CVD), a także został zobowiązany do stworzenia usługi online dostępnej dla obywateli, pozwalającej sprawdzić, czy ich dane osobowe (np. login, PESEL) nie zostały ujawnione w wyniku wycieku.

W ramach ułatwień dla organów właściwych w zakresie wdrażania obowiązków wynikających z nowelizacji organ właściwy może nie tworzyć odrębnego CSIRT sektorowego, lecz **powierzyć realizację jego zadań** CSIRT-owi poziomu krajowego w drodze porozumienia.

3. Nowelizacja po przejściu procesu parlamentarnego

Finalny kształt projektu nowelizacji ustawy, przyjęty przez Senat i skierowany do podpisu Prezydenta, podtrzymuje konieczność implementacji dyrektywy NIS 2, a tym samym dalszego uszczelnienia ekosystemu bezpieczeństwa państwa w wymiarze cyfryzacji i cyberbezpieczeństwa. W tej kwestii, jak również w zakresie wdrożenia rozwiązań z Toolbox 5G, nie wprowadzono zmian.

To na co należy zwrócić uwagę, to wprowadzenie zmian w zakresie terminów wdrożenia niektórych obowiązków nakładanych na podmioty w drodze ustawy. W szczególności ma to znaczenie dla tych nowych, nieobjętych wcześniej obowiązkami podmiotów, których poziom dojrzałości w zakresie cyberbezpieczeństwa może nie być odpowiedni dla współczesnych wyzwań. Wydłużenie terminów pozwoli na uniknięcie ewentualnych negatywnych skutków potencjalnie zbyt szybkiego wdrażania nowych rozwiązań w zakresie SZBI, nie wpływając przy tym na sam ostateczny cel nowych obowiązków – to znaczy zwiększenie poziomu cyberodporności podmiotów i państwa.

3.1. Zmiany dot. zakresu oraz terminów realizacji obowiązków ustawowych

Kluczową modyfikacją systemową jest zmiana niektórych terminów poprzez ich **wydłużenie** względem pierwotnie planowanych. Ustawodawca wydłużył termin na realizację kluczowych obowiązków (takich jak m.in. wdrożenie SZBI w kształcie przewidzianym nowelizacją) z **6 do 12 miesięcy** od momentu uznania za podmiot kluczowy lub ważny.

Analogicznie wydłużono także czas na podłączenie i rozpoczęcie korzystania z systemu S46 (**do 12 miesięcy**). W przypadku państwowych osób prawnych uznanych za podmioty kluczowe termin na realizację obowiązków z zakresu SZBI wydłużono **z 6 do 12 miesięcy**. Dodatkowo termin na uzupełnienie brakujących danych w wykazie podmiotów kluczowych i ważnych został wydłużony do **6 miesięcy** (pierwotnie były na to 2 miesiące), co stanowi znaczące wydłużenie względem pierwotnie przewidzianej daty.

Istotne zmniejszenie wymagań nastąpiło w obszarze **audytów bezpieczeństwa**. W wersji uchwalonej przez Senat zrezygnowano z nakładania na podmioty ważne bezwzględnego obowiązku przeprowadzania regularnych, cyklicznych audytów zewnętrznych. Obowiązek ten utrzymano obligatoryjnie dla podmiotów kluczowych, przy czym termin na przeprowadzenie pierwszego audytu wydłużono do **24 miesięcy** od spełnienia przesłanek ustawowych.

3.2. Zmiany w definicjach i zakresie podmiotowym

W toku prac parlamentarnych usunięto definicję platformy sieci usług społecznościowych, a zastąpiono ją definicją dostawcy platformy sieci usług społecznościowych, szerszą i ujednoliconą zgodnie z innymi ustawami oraz treścią samej nowelizacji.

Ponadto skorygowano definicję organizacji badawczej, doprecyzowując, że status ten przysługuje podmiotom, których podstawową działalnością jest działalność naukowa, przy jednoczesnym wyłączeniu ich z kategorii podmiotów kluczowych z części rygorystycznych wymogów SZBI na rzecz wymogów z załącznika nr 4. Tym samym wyłączono z niej podmioty, dla których działalność naukowa nie jest działalnością wiodącą. Należy także wspomnieć, że sektor badań naukowych został podzielony pomiędzy dwa organy właściwe – ministra właściwego ds. szkolnictwa wyższego i nauki oraz Ministra Obrony Narodowej. W tym drugim przypadku chodzi o podmioty z sektora badań naukowych, które podlegają Ministrowi Obrony Narodowej lub są przez niego nadzorowane.

3.3. System sankcji, w tym kar pieniężnych

W treści nowelizacji doprecyzowane niektóre zachowania podlegające karze oraz przepisy w tym zakresie, w tym odesłania do naruszeń obowiązków informacyjnych oraz dotyczących poleceń zabezpieczających. Wprowadzono także inne zmiany w systemie sankcji, a konkretnie nakładania kar pieniężnych.

Dodany w toku prac parlamentarnych przepis przejściowy ustanawia swoisty **okres karencji**, zgodnie z którym kary pieniężne za naruszenie ustawy mogą być nałożone po raz pierwszy dopiero po upływie **2 lat** od dnia wejścia w życie ustawy. Jest to fundamentalna zmiana, stanowiąca złagodzenie początkowo przewidzianych przepisów, tworząca swego rodzaju pilotażowy, mniej dotkliwy dla podmiotów okres obowiązywania ustawy. Jednocześnie nie zmniejsza to liczby niezbędnych do wdrożenia obowiązków (np. w zakresie SZBI), a jedynie zapewnia że nie zostaną ukarane najbardziej dotkliwą sankcją.

3.4. Jednostki samorządu terytorialnego

W przypadku sektora JST wprowadzono również pewne zmiany, przykładowo w stosunku do porozumień pomiędzy jednostkami samorządu terytorialnego w sprawie realizacji określonych obowiązków wynikających z ustawy o KSC. Zgodnie z brzmieniem nowelizacji po pracach parlamentarnych mogą one przewidywać powierzenie wykonywania obowiązków dowolnej jednostce, spośród jednostek zawierających porozumienie.

Dodano także istotne zastrzeżenie dotyczące porozumień między jednostkami samorządu terytorialnego. Obowiązujące porozumienia regulujące wspólne wykonywanie zadań z zakresu cyberbezpieczeństwa zachowują moc do czasu wyznaczenia nowej jednostki obsługującej, nie dłużej jednak niż przez 2 lata od wejścia w życie ustawy.

3.5. Inne zmiany w projekcie nowelizacji

- W zakresie finansowania systemu, w toku prac dodano prognozę i limity wydatków budżetowych aż do roku 2035 (pierwotnie do 2034 r.).
- Szereg szczegółowych działań lub zadań CSIRT NASK jako koordynatora CVD zostało usuniętych, jednocześnie rozszerzono katalog podmiotów zgłaszających o jednostki organizacyjne nieposiadające osobowości prawnej (tzw. ułomne osoby prawne);
- Przedstawiciel Prezydenta RP obowiązkowo będzie uczestniczył w pracach nad krajowym planem reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę (zamiast jak to dotychczasowo miało być – fakultatywnie);
- Rozszerzono możliwość udostępniania danych administratora konta podmiotu w systemie S46 na potrzeby postępowań cywilnych i sądowo administracyjnych, a nie tylko karnych.

4. Wnioski i podsumowanie

Zmiany wprowadzone na etapie procesu legislacyjnego w parlamencie mogą nie wydawać się na pierwszy rzut oka znaczne, jednak wprowadzają znaczące ułatwienia dla organizacji objętych obowiązkami na gruncie KSC 2.0 – przede wszystkim przesunięcie terminu na wdrożenie obowiązków przez podmioty kluczowe i ważne do 12 miesięcy. Umożliwi to wdrożenie SZBI oraz innych środków na rzecz zwiększenia cyberodporności i efektywnej obsługi incydentów w sposób adekwatny, zgodny z minimalnymi wymogami oraz odpowiedni w stosunku do krajobrazu cyberzagrożeń. Wydłużenie czasu z perspektywy operacyjnej oraz strategicznej, niezależnie od tego kiedy ustawa wejdzie w życie, pozwala na lepsze rozplanowanie ewentualnych kosztów czy działań w sferze organizacyjnej (np. zatrudnienie nowych pracowników, podpisanie umów lub porozumień, ustalenia z organami właściwymi tam gdzie to niezbędne) związanych z dostosowaniem się do wymagań ustawowych.

Dodatkowo wprowadzenie okresu karencji w nakładaniu kar pieniężnych na 2 lata eliminuje ryzyko, że w okresie najbardziej newralgicznym pod względem uzyskania zgodności z ustawą i dostosowania do nowych warunków będą podlegać potencjalnie dotkliwym sankcjom. Należy jednak podkreślić, że w systemie kar przewidzianym w KSC 2.0 za ewentualne naruszenia jest przewidziany szereg środków nadzoru, a kary pieniężne są najbardziej dotkliwymi środkami, stosowanymi w przypadku najpoważniejszych lub niejednokrotnych naruszeń. Z tego względu nawet w pierwotnym projekcie ich nałożenie nie byłoby pierwszym zastosowanym środkiem. Natomiast odsunięcie w czasie tej możliwości niweluje ryzyko nałożenia kar pieniężnych w ciągu 2 lat do zera.

Innym ułatwieniem dla podmiotów jest kwestia audytów bezpieczeństwa. Wersja przyjęta przez Senat zawiera zwolnienie podmiotów ważnych z obligatoryjnych, cyklicznych audytów oraz wydłużenie czasu na pierwszy audyt dla podmiotów kluczowych do 2 lat. Jest to kolejna kwestia, dająca więcej czasu na dostosowanie się do nowych, rozbudowanych obowiązków. Umożliwi to w pierwszej kolejności zaadresowanie przez podmioty kwestii wdrożenia SZBI, a następnie przekierowanie sił i środków na rzecz utrzymania zdolności na odpowiednim poziomie.

Podsumowując można stwierdzić, że przepisy przyjęte przez Senat po pracach w parlamencie wydłużają swoistą „mapę drogową” dla podmiotów do zrealizowania wymogów nakładanych ustawą, co powinno w efekcie przyczynić się do jeszcze lepszej i realnej niż pierwotnie zakładanej implementacji wymogów. Tym samym oznacza to większe szanse na zbudowanie bardziej trwałego i odpornego na cyberzagrożenia krajowego systemu cyberbezpieczeństwa.