Clifford Chance

BRIEFING

Polska: Spóźniona implementacja Dyrektywy NIS II

3 marca 2026 r.

Dnia 19 lutego 2026 r. Prezydent Karol Nawrocki podpisał nowelizację ustawy o Krajowym Systemie Cyberbezpieczeństwa (odpowiednio, "Nowelizacja" i „Ustawa o KSC"). Celem Nowelizacji jest wdrożenie Dyrektywy NIS II[1] i wejdzie ona w życie 2 kwietnia 2026 roku.

Jednocześnie Prezydent skierował Nowelizację do Trybunału Konstytucyjnego w trybie kontroli następczej w zakresie m.in. przepisów regulujących zasady uznawania podmiotów za dostawców wysokiego ryzyka, poleceń zabezpieczających oraz kar administracyjnych. W przypadku skutecznego stwierdzenia niekonstytucyjności tych przepisów, przestaną one obowiązywać.

Poszerzenie katalogu podmiotów objętych Ustawą o KSC

Dotychczasowe pojęcia operatorów usług kluczowych oraz dostawców usług cyfrowych zastąpiono nowymi kategoriami: podmiotów ważnych i podmiotów kluczowych. Jednocześnie rozszerzono zakres sektorów objętych Ustawą o KSC.

Wcześniej obejmowała ona sektor:

- Energetyki
- Transportu
- bankowości i infrastruktury rynków finansowych
- ochrony zdrowia
- zaopatrzenia w wodę pitną i jej dystrybucji oraz
- infrastruktury cyfrowej.

[1] Dyrektywa 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, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2).

Po Nowelizacji Ustawa o KSC obejmie dwie kategorie sektorów:

- sektory kluczowe:
  - energia
  - transport
  - bankowość i infrastruktura rynków finansowych
  - ochrona zdrowia
  - zaopatrzenie w wodę pitną i jej dystrybucja
  - zbiorowe odprowadzanie ścieków
  - infrastruktura cyfrowa
  - zarządzanie usługami ICT
  - przestrzeń kosmiczna
  - podmioty publiczne

  („**Sektory Kluczowe**"),
- sektory ważne:
  - usługi pocztowe
  - inwestycje energetyki jądrowej
  - gospodarowanie odpadami
  - produkcja, wytwarzanie i dystrybucja chemikaliów
  - produkcja, przetwarzanie i dystrybucja żywności
  - produkcja
  - dostawcy usług cyfrowych
  - badania naukowe
  - podmioty publiczne, w tym samorządowe jednostki i zakłady budżetowe

  („**Sektory Ważne**").

Różni regulatorzy i CSIRT dla poszczególnych sektorów

Zachowano dotychczasową zasadę podziału uprawnień regulacyjnych pomiędzy regulatorów dla poszczególnych sektorów - w zależności od sektora regulatorami będą właściwi ministrowie, Komisja Nadzoru Finansowego lub Prezes Urzędu Komunikacji Elektronicznej.

Obok dotychczasowych Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego (ang. Computer Security Incident Response Team – CSIRT), powstać mają dodatkowe CSIRT-y sektorowe, które usprawnią system reagowania na cyberzagrożenia oraz pozwolą zbudować bazę wiedzy o zagrożeniach i podatnościach danego sektora. Już w październiku pojawiły się komunikaty Ministerstwa Cyfryzacji o tworzeniu CSIRT-u Cyfra – sektorowego zespołu reagowania na incydenty bezpieczeństwa komputerowego dla sektora infrastruktury cyfrowej.

Przesłanki uznania za podmiot kluczowy i ważny

Za podmioty kluczowe uznaje się:

- podmioty działające w Sektorach Kluczowych, które zatrudniają co najmniej 250 pracowników, ich roczny obrót przekracza równowartość 50 milionów euro lub ich roczna suma bilansowa przekracza równowartość 43 milionów euro,

- przedsiębiorców komunikacji elektronicznej, którzy zatrudniają co najmniej 50 pracowników lub ich roczny obrót albo bilans roczny przekracza równowartość 10 milionów euro,
- dostawców usług zarządzanych w zakresie cyberbezpieczeństwa, którzy zatrudniają co najmniej 10 pracowników i ich roczny obrót albo całkowity bilans roczny przekracza równowartość 2 milionów euro,
- niektóre inne podmioty niezależnie od ich wielkości, m.in. podmioty będące operatorami obiektu energetyki jądrowej, dostawcy usług DNS, podmioty świadczące usługi rejestracji nazw domen czy podmioty krytyczne.

Za podmioty ważne uznaje się m.in.:

- podmioty działające w Sektorach Kluczowych, które zatrudniają co najmniej 50, lecz nie więcej niż 249 pracowników lub ich roczny obrót nie przekracza 50 milionów euro albo całkowity bilans roczny przekracza równowartość 10 milionów euro, ale wynosi nie więcej niż równowartość 43 milionów euro,
- podmioty działające w Sektorach Ważnych, które zatrudniają co najmniej 50 pracowników lub ich roczny obrót albo bilans roczny przekracza równowartość 10 milionów euro.

Procedura wpisu do Wykazu – obowiązek samoidentyfikacji:

Każdy podmiot musi sam zidentyfikować czy spełnia kryteria uznania go za podmiot kluczowy lub podmiot ważny, a jeśli tak – samodzielnie dokonać elektronicznego zgłoszenia do wykazu podmiotów kluczowych i podmiotów ważnych („**Wykaz**"),

Wykaz powinien zostać utworzony przez ministra właściwego do spraw informatyzacji (obecnie: Minister Cyfryzacji) w ciągu miesiąca od wejścia w życie Nowelizacji.

Minister wpisze do Wykazu z urzędu podmioty wpisane do dotychczasowego rejestru operatorów usług kluczowych oraz ogłosi harmonogram złożenia wniosków o wpis do Wykazu przez podmioty, które w dniu wejścia Nowelizacji będą spełniać przesłanki do bycia uznanym za podmiot kluczowy lub ważny oraz rozpoczęcia korzystania przez te podmioty z systemu teleinformatycznego (S46).

Docelowo wnioski o wpis do Wykazu powinny być składane w terminie 6 miesięcy od zaistnienia ustawowych przesłanek uznania za podmiot kluczowy lub ważny, a w wnioski o zmianę wpisu w ciągu 14 dni od dnia zaistnienia zmiany.

Regulator właściwy dla danego sektora będzie mógł też wydać decyzję o uznaniu danego podmiotu za podmiot ważny lub kluczowy i wpisać do Wykazu podmioty ważne lub kluczowe, które się w nim nie zarejestrują.

Najważniejsze obowiązki

Poza wymogiem złożenia wniosku o wpis do Wykazu, podmioty kluczowe oraz ważne będą musiały realizować szereg dodatkowych obowiązków.

W ramach prowadzenia systemu zarządzania bezpieczeństwem informacji wprowadzono m.in. wymogi:

- wdrożenia zaawansowanych środków cyberbezpieczeństwa,
- wprowadzenia polityki szacowania ryzyka,

- zapewnienia bezpieczeństwa łańcucha dostaw produktów, usług i procesów ICT,
- ciągłego monitorowania systemu,
- przeszkolenia pracowników w zakresie cyberbezpieczeństwa,
- identyfikacji cyberzagrożeń,
- analizy zasobów,
- przeglądu dotychczas obowiązujących procedur,
- wprowadzenia skutecznych procedur reagowania na incydenty.

Szczegóły obowiązków różnią się w zależności od sektora działalności. Zakres ich realizacji powinien być dostosowany do wielkości podmiotu oraz poziomu jego narażenia na ryzyka.

Wprowadzono także obowiązki:

- wyznaczenia co najmniej dwóch osób odpowiedzialnych za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa,
- zapewnienie użytkownikom możliwości zgłoszenia cyberzagrożenia lub incydentu związanego ze świadczoną usługą,
- poszerzenia zakresu dokumentacji dotyczącej bezpieczeństwa systemu informacyjnego,
- zmiany procedury zgłaszania incydentów poważnych (tj. zdarzeń powodujących lub mogących spowodować istotne zakłócenie działania usług, poważną szkodę materialną lub niematerialną albo znaczące straty finansowe).

Zgłaszanie incydentów

Wprowadzono także wieloetapowy model zgłaszania incydentów poważnych (tj. zdarzeń, które poważnie zakłócają albo mogą zakłócić ciągłość świadczenia usługi, mogą spowodować straty finansowe lub poważną szkodę dla użytkowników) poprzez system teleinformatyczny (S46):

- **wczesne ostrzeżenie**: niezwłocznie, nie później niż 24h od wykrycia, zgłaszane do odpowiedniego CSIRTu sektorowego
- **zgłoszenie incydentu poważnego**: niezwłocznie, nie później niż 72h od wykrycia, zgłaszane do właściwego CSIRTu sektorowego

W przypadku incydentu poważnego, w ciągu miesiąca od chwili zgłoszenia należy także, poprzez system S46 złożyć sprawozdanie końcowe z jego obsługi, zawierające m.in. opis incydentu, podjęte środki, analizę skutków, w tym transgraniczne skutki (jeśli wystąpiły) i ocenę przyczyn jego wystąpienia. W szczególnych przypadkach, właściwy CSIRT może także żądać złożenia okresowego sprawozdania z obsługi incydentu poważnego.

Podmioty kluczowe i ważne mają 6 miesięcy od dnia wejścia w życie Ustawy o KSC na dostosowanie procesu zgłaszania incydentów poważnych do nowych przepisów.

Okres przejściowy dla realizacji obowiązków

Podmioty kluczowe lub ważne:

Podmioty, które z dniem wejścia w życie Nowelizacji spełniają przesłanki uznania ich za podmioty kluczowe lub ważne rozpoczynają realizację

wymogów Ustawy o KSC, w tym wdrożenia systemu zarządzania bezpieczeństwem informacji, dokumentacji, procedur incydentowych, struktur cyberbezpieczeństwa oraz wyznaczenia osób kontaktowych - w terminie 12 miesięcy od dnia wejścia w życie Nowelizacji.

Dodatkowo podmioty kluczowe są także zobowiązane do przeprowadzenia pierwszego audytu cyberbezpieczeństwa w ciągu 24 miesięcy i następnie cyklicznego ich prowadzenia, nie rzadziej niż raz na 3 lata (dotychczas audyty były prowadzone co 2 lata).

Dotychczasowi operatorzy usług kluczowych

Dotychczasowi operatorzy usług kluczowych - przez 6 miesięcy od wejścia w życie Nowelizacji zgłaszają incydenty poważne zgodnie z dotychczasową procedura.

Przedsiębiorcy telekomunikacyjni:

Do czasu wdrożenia obowiązków wynikających z Nowelizacji przedsiębiorcy telekomunikacyjni kontynuują realizację swoich dotychczasowych obowiązków zgodnie z ustawą prawo telekomunikacyjne.

Podmioty uznane decyzją administracyjną za kluczowe lub ważne:

W przypadku podmiotów, które zostaną uznane za podmiot kluczowy lub podmiot ważny w drodze decyzji administracyjnej właściwego regulatora, terminy - odpowiednio: 12 miesięcy na wdrożenie obowiązków określonych w Nowelizacji oraz 24 miesiące na przeprowadzenie pierwszego audytu, są liczone od dnia doręczenia decyzji.

Kary administracyjne oraz okres przejściowy dla nich

Karom pieniężnym będą podlegać podmioty kluczowe lub ważne za niewykonywanie określonych obowiązków z zakresu cyberbezpieczeństwa.

Wysokość kar będzie zależna od statusu podmiotu.

- **Dla podmiotu kluczowego**: maksymalny wymiar kary to 10 000 000 euro lub 2% przychodów osiągniętych w poprzednim roku obrotowym z działalności gospodarczej, jednak nie mniej niż 20 000 zł.
- **Dla podmiotu ważnego**: maksymalny wymiar kary to 7 000 000 euro lub 1,4% przychodów osiągniętych w poprzednim roku obrotowym z działalności gospodarczej, jednak nie mniej niż 15 000 zł.

W przypadku najpoważniejszych naruszeń powodujących bezpośrednie i poważne cyberzagrożenie dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi, lub zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług kara może wynieść do 100 000 000 zł, niezależnie od statusu podmiotu.

Odpowiedzialność osobista kierownictwa

Dodatkowo, w przypadku naruszenia niektórych obowiązków, Nowelizacja przewiduje osobistą odpowiedzialność kierownika podmiotu kluczowego – m.in. osoby fizycznej wchodzącej w skład organu zarządzającego, wspólnika spółki osobowej prowadzącego jej sprawy, likwidatora, syndyka lub zarządcę w postępowaniu restrukturyzacyjnym lub zarządcę sukcesyjnego.

Dotyczy to naruszeń m.in. w zakresie:

- wpisu do Wykazu i ewentualnych aktualizacji;
- podejmowania decyzji dotyczących przygotowania, wdrażania, stosowania, przeglądu i nadzoru systemu zarządzania bezpieczeństwem informacji w podmiocie;
- planowania adekwatnych środków finansowych na realizację obowiązków z zakresu cyberbezpieczeństwa;
- przydzielania zadań z zakresu cyberbezpieczeństwa oraz nadzoru nad ich wykonaniem;
- zapewniania świadomości personelu w zakresie obowiązków cyberbezpieczeństwa oraz znajomości wewnętrznych regulacji;
- zapewniania zgodności działań podmiotu z przepisami prawa, w tym Nowelizacją Ustawy o KSC i wewnętrznymi regulacjami;
- corocznego obowiązkowego szkolenia kierownika i osoby, której powierzono obowiązki kierownika w zakresie cyberbezpieczeństwa;
- obsługi incydentów.

Kary mogą wynosić:

- do 300% wynagrodzenia kierownika podmiotu kluczowego lub ważnego obliczanego według zasad obowiązujących przy ustalaniu ekwiwalentu urlopowego, lub
- w przypadku podmiotów publicznych będzie do 100% wynagrodzenia obliczanego w ten sposób.

Co gdy kierowników jest wielu?

Jeśli kierownikiem podmiotu kluczowego lub ważnego jest organ wieloosobowy (np. zarząd), wówczas odpowiedzialność ponoszą wszyscy członkowie organu, chyba że wskazano konkretną osobę, która ponosi odpowiedzialność za dany obszar obowiązków wynikających z Ustawy o KSC.

Zawieszenia nakładania kar

Kary (inne niż kary za najpoważniejsze naruszenia zagrożone karą do 100 000 000 złotych) mogą być po raz pierwszy nałożone po upływie 2 lat od wejścia w życie Nowelizacji.

Oznacza to, że w sprawach, w których decyzje stwierdzające naruszenia zapadną wcześniej, kary nie będą wymierzane. Przepis nie wyklucza jednak nałożenia kar za wcześniejsze naruszenia.

Nie jest więc jasne, choć jest możliwe, że okres najbliższych 2 lat będzie interpretowany jako okres przejściowy, w którym brak dostosowania się do nowych wymogów skutkujący naruszeniem nie będzie penalizowany, o ile przedsiębiorcy usuną ewentualne naruszenia przed upływem dwóch lat od wejścia w życie Nowelizacji.

Wprowadzenie procedury uznawania za dostawcę wysokiego ryzyka

Postępowanie w sprawie uznania dostawcy za dostawcę wysokiego ryzyka realizować będzie postulat bezpieczeństwa łańcucha dostaw - pomoże w niedopuszczeniu do obrotu gospodarczego sprzętu i usług, które nie spełniają standardów cyberbezpieczeństwa. Decyzje w tym zakresie będzie podejmował Minister Cyfryzacji po uzyskaniu opinii Kolegium do Spraw Cyberbezpieczeństwa. Dostawcom, którzy nie zgodzą się z decyzją, będzie przysługiwać skarga do sądu administracyjnego.

- Podmioty istotne dla funkcjonowania państwa nie będą mogły wprowadzać do swoich systemów produktów pochodzących od dostawcy wysokiego ryzyka, a jeżeli już korzystają z takowych, będą zobowiązane do ich wycofania w terminie 7 lat od ogłoszenia decyzji.
- Dostawca spoza UE i NATO nie będzie automatycznie uznawany za dostawcę wysokiego ryzyka, a podmiotom, które korzystają ze sprzętu lub oprogramowania dostarczanego przez takie podmioty, nie będzie grozić zawieszenie działalności w związku z obowiązkiem ich wycofania.
- Decyzja Ministra Cyfryzacji będzie dotyczyć wyłącznie konkretnego sprzętu lub oprogramowania wskazanego w decyzji, nie zaś wszystkich produktów danego dostawcy i tylko co do tego sprzętu lub oprogramowania powstanie obowiązek wycofania.

Nowe kompetencje organów ds. cyberbezpieczeństwa

Nowelizacja rozszerza zakres kompetencji organów odpowiedzialnych za cyberbezpieczeństwo, co pozwoli na sprawniejsze i skuteczniejsze reagowanie na zagrożenia. Organy właściwe do spraw cyberbezpieczeństwa w poszczególnych sektorach (np. ministrowie, KNF, Prezes UKE) będą mogły m.in. wydawać ostrzeżenia, wyznaczać urzędników monitorujących oraz nakazywać przeprowadzenie audytów i ocen bezpieczeństwa, w szczególności:

- Minister Cyfryzacji uzyska nowe uprawnienia do wydawania poleceń zabezpieczających w przypadku incydentów krytycznych oraz prowadzenia działań edukacyjnych w zakresie cyberbezpieczeństwa,
- Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa będzie mógł wydawać rekomendacje, żądać informacji od organów administracji oraz zlecać niezbędne badania, a także nabywać oprogramowanie dla uczestników Połączonego Centrum Operacyjnego Cyberbezpieczeństwa,
- CSIRT-y szczebla krajowego, w tym CSIRT NASK - będą posiadały nowe kompetencje związane ze wsparciem rosnącej liczby podmiotów kluczowych i ważnych w reagowaniu na incydenty. Połączone Centrum Operacyjne Cyberbezpieczeństwa zostanie wprowadzone do Ustawy jako centralny punkt wymiany informacji o cyberzagrożeniach, incydentach i podatnościach.

Usprawnienie procedury zgłaszania incydentów

Informacje o zgłoszonych incydentach będą przekazywane bezpośrednio do zespołów CSIRT, z którymi bezpośrednią komunikację umożliwi nowy system S46, zrealizowany przez Państwowy Instytut Badawczy (NASK-PIB) na zlecenie Ministra Cyfryzacji, jako właściciela systemu. Dostęp do S46 podmioty otrzymają po wpisie do Wykazu.

Włączenie przedstawiciela Prezydenta do tworzenia planu reagowania na incydenty

Uwzględniono udział przedstawiciela Prezydenta w pracach nad Krajowym planem reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie, co ma wzmocnić współpracę kluczowych instytucji państwa. Krajowy plan, opracowywany przez Ministra Cyfryzacji we współpracy m.in. z RCB i pełnomocnikiem Prezydenta, zostanie przyjęty przez Radę Ministrów.

Podsumowanie

Nowelizacja znacząco rozszerza krąg podmiotów objętych regulacją oraz nakłada nowe, wymagające obowiązki w obszarze cyberbezpieczeństwa – od kompleksowych procedur zarządzania ryzykiem i bezpieczeństwem IT po nowe zasady raportowania incydentów oraz weryfikację dostawców wysokiego ryzyka. Nowelizacja wzmacnia również kompetencje organów nadzorczych i przewiduje surowe sankcje, w tym osobistą odpowiedzialność kierownictwa, co sprawia, że szybkie dostosowanie procesów do nowych wymogów stanie się kluczowe zarówno dla bezpieczeństwa operacyjnego, jak i minimalizacji ryzyk regulacyjnych.

Zakres Nowelizacji wykracza poza minimalne wymogi wynikające z dyrektywy NIS-2. Daleko idące obowiązki nałożone na przedsiębiorców i szeroki zakres uprawnień i dyskrecji regulatorów spotykają się z krytyką ze strony niektórych środowisk biznesowych.

Dla pełnej oceny skutków Nowelizacji dla przedsiębiorców konieczne będzie monitorowanie wydania i wejścia w życie przepisów wykonawczych oraz praktyki stosowania Ustawy o KSC przez regulatorów.

Agnieszka Janicka
Partner, Warsaw

E:agnieszka.janicka@clifffordchance.com
T: +48 22 627 11 77

Krzysztof Hajdamowicz
Counsel, Warsaw

E:krzysztof.hajdamowicz@cliffordchance.com
T: +48 22 627 11 77

Martyna Sieczka
Aplikantka adwokacka, Warsaw

E:martyna.sieczka@cliffordchance.com
T: +48 22 627 11 77

cliffordchance.com

ul. Lwowska 19, 00-660 Warsaw, Poland

Akta rejestrowe przechowuje Sąd Rejonowy dla m.st. Warszawy w Warszawie XII Wydział Gospodarczy Krajowego Rejestru Sądowego KRS: 0000053301 NIP: 5262579191