SOŁTYSIŃSKI KAWECKI SZLĘZAK

Prawne standardy cyberbezpieczeństwa – nadchodzą poważne zmiany

W najbliższych dniach wejdą w życie polskie przepisy nakładające szereg obowiązków w obszarze cyberbezpieczeństwa. **Nowe przepisy rozszerzą zarówno krąg podmiotów objętych obowiązkami w obszarze cyberbezpieczeństwa, jak i zakres tych obowiązków.**

Dotychczasowe rozwiązania w tym zakresie okazały się niewystarczające. Na poziomie Unii Europejskiej uchwalono Dyrektywę NIS-2[1], która doprowadziła nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa.

Nowe przepisy mają być ruchem w stronę bezpieczeństwa cyfrowego zarówno sektora prywatnego, jak i publicznego. To oznacza inwestycję, która będzie wiązała się z dodatkowymi nakładami finansowymi oraz obowiązkami. Kto w organizacji powinien zająć się zagadnieniem cyberbezpieczeństwa? Kiedy nowe przepisy wejdą w życie? Kto zostanie nimi objęty? Jakie obowiązki i sankcje wprowadzą? Czy należy się przygotować, a jeśli tak to od czego zacząć? Odpowiedzi na te oraz inne pytania znajdziesz w tym tekście.

---

[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 uchylając dyrektywę (UE) 2014/1148 (Dyrektywa NIS 2)

[2] Podstawy prawno-instytucjonalne dla systemu cyberbezpieczeństwa w Polsce reguluje obecnie Ustawa o KSC , która jest implementacją unijnej Dyrektywy NIS-1.

Zarząd będzie odpowiadał za obowiązki w zakresie cyberbezpieczeństwa

Odpowiedzialność za realizację obowiązków w zakresie cyberbezpieczeństwa została nałożona na kierowników podmiotów objętych ustawą (ustawa przewiduje dwie kategorie podmiotów – kluczowe i ważne – przeczytasz o tym dalej). W przypadku, gdy podmiotem kluczowym lub ważnym zarządza organ wieloosobowy, to odpowiedzialność będą ponosić wszyscy członkowie tego organu, chyba, że została wyznaczona konkretna osoba.

WAŻNE: Kierownik podmiotu kluczowego lub podmiotu ważnego będzie ponosił odpowiedzialność także wtedy, gdy niektóre z obowiązków albo wszystkie obowiązki delegowane innej osobie. W uzasadnieniu ustawy wyraźnie podkreślono: celem tych rozwiązań jest to, aby kierownictwo podmiotu poważnie podchodziło do zapewnienia cyberbezpieczeństwa podmiotu.

Kierownicy podmiotów kluczowych i ważnych będą odpowiedzialni za realizację konkretnych obowiązków: m.in. podejmowania decyzji w zakresie przygotowania, wdrażania, stosowania i przeglądu systemu zarządzania bezpieczeństwem informacji w podmiocie, a także zapewnienia zaplanowanie adekwatnych środków finansowych oraz ludzkich do realizacji obowiązków z zakresu cyberbezpieczeństwa. Dodatkowo wprowadzony zostaje obowiązek odbycia szkolenie z zakresu cyberbezpieczeństwa raz w roku.

UWAGA: W przypadku niedopełnienia obowiązków ustawowych, organ będzie miał możliwość ukarania kierownika podmiotu karą pieniężną maksymalnie do 3-krotności wynagrodzenia, a nawet zakazać pełnienia funkcji kierowniczej do czasu zaprzestania naruszeń.

Kierownik, czyli kto?

- członkowie zarządu lub innego organu zarządzającego,
- wspólnicy prowadzących sprawy spółki w przypadku spółki jawnej oraz cywilnej,
- wspólnicy prowadzących sprawy spółki albo zarząd w przypadku spółki partnerskiej,
- komplementariusze prowadzących sprawy spółki w przypadku spółki komandytowej i spółki komandytowo-akcyjnej – komplementariusze prowadzących sprawy spółki,
- osoby fizyczne prowadzące działalność gospodarczą.

Kluczowe daty

- **n –** data publikacji w Dzienniku Ustaw
- **n + 1 miesiąc** – wejście w życie ustawy
- **n + 7 miesięcy** – termin na dokonanie samorejestracji przez podmioty ważne i kluczowe
- **n + 13 miesięcy –** termin na dostosowanie się do wymogów ustawy
- **n + 25 miesięcy** – termin przeprowadzenia pierwszego audytu dla nowych podmiotów kluczowych
- **n + 25 miesięcy** – okres w którym organ nie będzie nakładał kar za niektóre uchybienia w realizacji obowiązków

Kto zostanie objęty nowymi przepisami?

Nowe przepisy wprowadzają podział podmiotów objętych ustawą na podmioty kluczowe i ważne.

To na podmiotach objętych ustawą spoczywa obowiązek weryfikacji czy kwalifikują się do którejś z tych kategorii. Decydujące są dwa kryteria: wielkościowe (co do zasady status co najmniej średniego przedsiębiorstwa) oraz zakres prowadzonej działalności.

Kryterium zakresu prowadzonej działalności

Załącznik do ustawy zawiera opis zakresów prowadzonej działalności, które mogą powodować, ze dany podmiot będzie podmiotem ważnym lub kluczowym.

WAŻNE: Analiza wymaga uwzględnienia wszystkich rodzajów działalności realizowanych przez dany podmiot. Niekiedy działalność poboczna lub pomijalna z perspektywy przychodów będzie decydować o tym, że podmiot będzie musiał dostosować się do wymogów ustawy.

SEKTOR KLUCZOWY

- ENERGETYKA
- TRANSPORT
- BANKOWOŚĆ
- INFRASTRUKTURA RYNKÓW FINANSOWYCH
- OPIEKA ZDROWOTNA
- ZAOPATRZENIE W WODĘ PITNĄ I JEJ DYSTRYBUCJA
- ODPROWADZANIE ŚCIEKÓW
- INFRASTRUKTURA CYFROWA
- ZARZĄDZANIE USŁUGAMI ICT
- PODMIOTY ADMINISTRACJI PUBLICZNEJ
- PRZESTRZEŃ KOSMICZNA

SEKTOR WAŻNY

- USŁUGI POCZTOWE
- GOSPODAROWANIE ODPADAMI
- PRODUKCJA, WYTWARZENIE I DYSTRYBUCJA CHEMIKALIÓW
- PRODUKCJA, PRZETWARZENIE I DYSTRYBUCJA ŻYWNOŚCI
- PRODUKCJA WYBRANYCH URZĄDZEŃ, MASZYN I POJAZDÓW
- DOSTAWCY USŁUG CYFROWYCH
- BADANIA NAUKOWE
- INWESTYCJE ENERGETYKI JĄDROWEJ
- PODMIOTY ADMINISTRACJI PUBLICZNEJ – NA SZCZEBLU SAMORZĄDOWYM

Kryterium wielkościowe

Nowymi przepisami będą objęci co do zasady wszyscy **średni przedsiębiorcy** prowadzący działalność w sektorach wymieniowych w załączniku do ustawy, **a w niektórych przypadkach również przedsiębiorcy niezależnie od wielkości podmiotu**.

Przy obliczaniu wielkości przedsiębiorstwa należy co do zasady wziąć pod uwagę także przedsiębiorstwa powiązane (tj. grupę kapitałową) i partnerskie (co najmniej 25% udziałów). Przepisy przewidują jednak wyjątki od tej zasady.

Polskie przepisy co do zasady znajdują zastosowanie do podmiotów, które mają siedzibę w Polsce, ale też takich które prowadzą działalność jako oddział przedsiębiorcy zagranicznego, czy też prowadzą działalność transgraniczną na terytorium Polski.

W odniesieniu do pewnej kategorii podmiotów, obowiązek dostosowanie się do polskich przepisów będzie uzależniony od tego czy Polska jest głównym miejscem prowadzenia działalność, a przepisy przewidują sposób weryfikacji tego kryterium. Przepisy te dotyczą np. dostawców DNS, rejestratorów nazw domen, dostawców chmury obliczeniowej, dostawców sieci dostarczania treści, dostawców usług zarządzanych (MSP), dostawców usług zarządzanych w zakresie cyberbezpieczeństwa (MSSP), dostawców platform handlowych, dostawców wyszukiwarek internetowych oraz dostawców platform sieci społecznościowych.

Podmiot kluczowy lub podmiot ważny musi złożyć wniosek o wpis do wykazu w ciągu 6 miesięcy od dnia, w którym zaczyna spełniać przesłanki uznania za taki podmiot. Oznacza to konieczność bieżącego monitorowania, realizacji kryteriów, spóźnienie może zostać uznane za naruszenie obowiązków.

⚠ **UWAGA:** Według szacunków Ministerstwa Cyfryzacji ponad **10 000 podmiotów** zostanie objętych obowiązkiem wpisu do wykazu. Według niektórych innych szacunków, może to być **nawet do 40 000 podmiotów.**

O obowiązkach

Obowiązki podmiotów kluczowych i ważnych są w zasadniczej części identyczne.

Podstawowym obowiązkiem wynikającym z ustawy jest **wdrożenie systemu zarządzania bezpieczeństwem informacji (SZBI)** w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot. Co do samego systemu przewidziano szereg warunków oraz elementów, które powinien obejmować, m.in.:

- prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem,
- wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy oraz tzw. kontekst danego podmiotu,

WAŻNE: Środki techniczne i organizacyjne powinny obejmować m.in.: polityki szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego, bezpieczeństwo zasobów ludzkich, bezpieczeństwo fizyczne i środowiskowe, zapewnienie ciągłości działania, monitorowanie systemu informacyjnego, ocena skuteczności wdrażanych środków technicznych i organizacyjnych, edukację z zakresu cyberbezpieczeństwa dla personelu podmiotu, podstawowe zasady cyberhigieny, bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, zarządzanie aktywami, polityki kontroli dostępu.

- zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi,
- zarządzanie incydentami, a także stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego.

WAŻNE: Ustawodawca sugeruje opracowanie polityki zarządzania incydentami, wprowadzenie narzędzia do zgłaszania incydentów wewnątrz podmiotu, a także wprowadzenie procedury obsługi incydentów.

Raportowanie incydentów

Do szczególnej kategorii należy zaliczyć obowiązki związane z raportowaniem incydentów do właściwego CSIRT sektorowego. Podmioty kluczowe oraz ważne objęte nowymi regulacjami będą obowiązane co do zasady do:

- zgłoszenia wczesnego ostrzeżenia o incydencie poważnym niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia incydentu poważnego,
- zgłoszenia incydentu poważnego w ciągu 72 godzin wraz z dodatkowymi informacjami o tym incydencie, m.in. opis wpływu incydentu na świadczone usługi, opis przyczyn incydentu, a także informacje o podjętych dzianiach,
- przekazania sprawozdania okresowego z obsługi tego incydentu na wniosek CSIRT sektorowego,
- przekazania sprawozdania końcowego z obsługi incydentu poważnego nie później niż w ciągu miesiąca od dnia zgłoszenia incydentu.

Co może organ?

Organy nadzoru w stosunku do podmiotów nadzorowanych będzie miał uprawnienie do działania, jeśli uzyskają uzasadnione podejrzenie o niestosowaniu się przez dany podmiot do przepisów ustawy. W ramach nadzoru organ może m.in.:

- przeprowadzić kontrolę;
- zobowiązać podmiot do przeprowadzenia audytu;
- wystąpić do podmiotu o udostępnienie dokumentacji.

UWAGA: W przypadku stwierdzenia naruszenia ustawy, organ może wydać wiążące zalecenia lub decyzję w której określi zachowanie mające na celu zaprzestanie naruszeń. Niespełnienie obowiązków wnikających z decyzji organu może wiązać się z dalszymi konsekwencjami np.: z wstrzymaniem koncesji.

Jakie sankcje?

Niespełnienie nowych wymogów w zakresie cyberbezpieczeństwa będzie mogło spowodować nałożenie administracyjnych kar pieniężnych.

	PODMIOT KLUCZOWY	PODMIOT WAŻNY
Kara minimalna	20 000 zł	15 000 zł
Kara maksymalna	Równowartość 10.000.000 euro LUB 2 % przychodów osiągniętych w roku obrotowym poprzedzającym wymierzenie kary (górny próg określa kara wyższa)	Równowartość 7.000.000 euro LUB 1,4 % przychodów osiągniętych w roku obrotowym poprzedzającym wymierzenie kary (górny próg określa kara wyższa)

WAŻNE: Organ właściwy będzie mógł nałożyć karę **nawet do 100.000.000 zł**, jeżeli podmiot kluczowy albo podmiot ważny naruszając przepisy ustawy spowoduje bezpośrednie i poważne zagrożenie cyberbezpieczeństwa 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.

Ustawa przewiduje, że wybrane administracyjne kary pieniężne będzie można nałożyć dopiero po upływie 2 lat od wejścia w życie ustawy. Dotyczą one m.in. naruszeń takich jak brak wpisu lub aktualizacji danych w wykazie, niewdrożenie wymaganych środków bezpieczeństwa (w tym SZBI), niewykonanie obowiązków zgłaszania incydentów, brak audytu oraz niewykonanie decyzji/nakazów organu (w tym kar za zwłokę).

Za niewykonywanie obowiązków określonych w ustawie karze pieniężnej może podlegać także kierownik podmiotu kluczowego lub podmiotu ważnego. Kara będzie mogła może zostać nałożona niezależnie od tego czy została nałożona na podmiot kluczowy lub podmiot ważny.

	KIEROWNIK PODMIOTU KLUCZOWEGO LUB WAŻNEGO	
Kara maksymalna	300% otrzymywanego przez ukaranego wynagrodzenia	Tymczasowy zakaz zajmowania kierowniczego stanowiska lub tymczasowy zakazu pełnienia funkcji zarządczych do czasu usunięcia uchybień lub zaprzestania naruszeń.

Czy to już? Od czego zacząć?

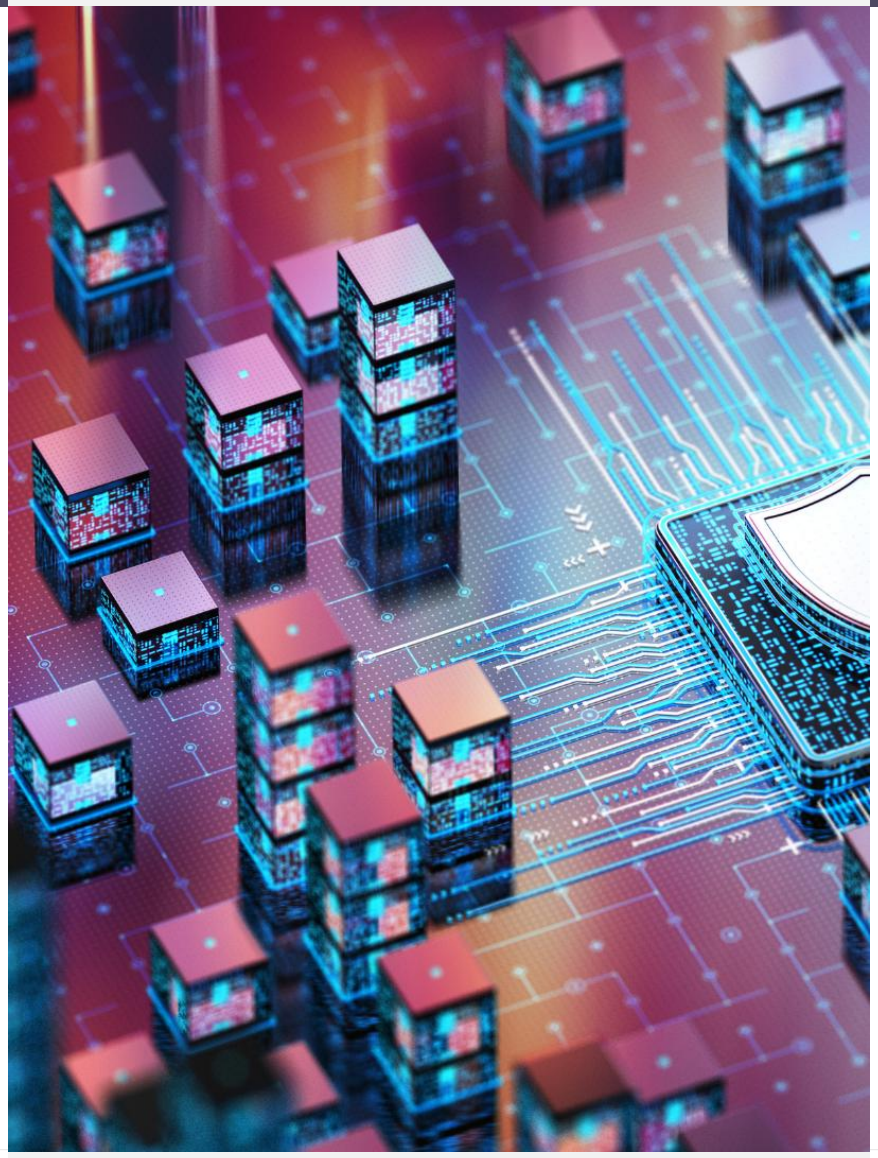
Nowe przepisy zaczną niebawem obowiązywać.

Krótki czas vacatio legis oraz termin na wprowadzenie nowych regulacji wymaga rozpoczęcia prac nad wdrożeniem postanowień ustawy w organizacji już od samego momentu jej ogłoszenia, jest to ostatni dzwonek na dostosowanie się do nowych wymogów. Niektóre podmioty już dzisiaj dbają o wysoką świadomość w obszarze cyberbezpieczeństwa w swoich organizacjach i są przygotowane na nowe regulacje. Inne będą tą świadomość dopiero budować.

Niezależnie od miejsca w jakim znajduje się obecnie Twoja organizacja, istotnym jest, aby wystrzec się szukania na szybko nieprzemyślanych rozwiązań. Przyjmowane środki powinny być **odpowiednie** dla danej organizacji i **proporcjonalne** do możliwości oraz realnych zagrożeń. **Dostosowanie się do wymogów nie zawsze musi oznaczać zakup drogich i zaawansowanych rozwiązań**.

Uważamy, że **punktem wyjścia jest dokonanie rzetelnej samoidentyfikacji**. Zachęcamy, aby zacząć od skorzystania z naszego KWESTIONARIUSZA. Wynik ankiety może być pierwszą wskazówką, która pozwoli na dokonanie właściwej oceny rzeczywistości w jakiej znajduje się Twoja organizacja.

Przejdź do kwestionariusza



Jak możemy pomóc?

Kancelaria SK&S oferuje profesjonalne wsparcie prawne w procesie samoidentyfikacji, dostosowania organizacji do nadchodzących wymogów prawnych oraz wsparcia prawnego w procesie obsługi incydentów. Służymy również pomocą w weryfikacji oraz tworzeniu wewnętrznych procedur czy postanowień umownych ze szczególnym uwzględnieniem dbałości o bezpieczeństwo łańcucha dostaw.

Chętnie odpowiemy na dodatkowe pytania oraz pomożemy zidentyfikować obszary, których dotkną nowe regulacje.

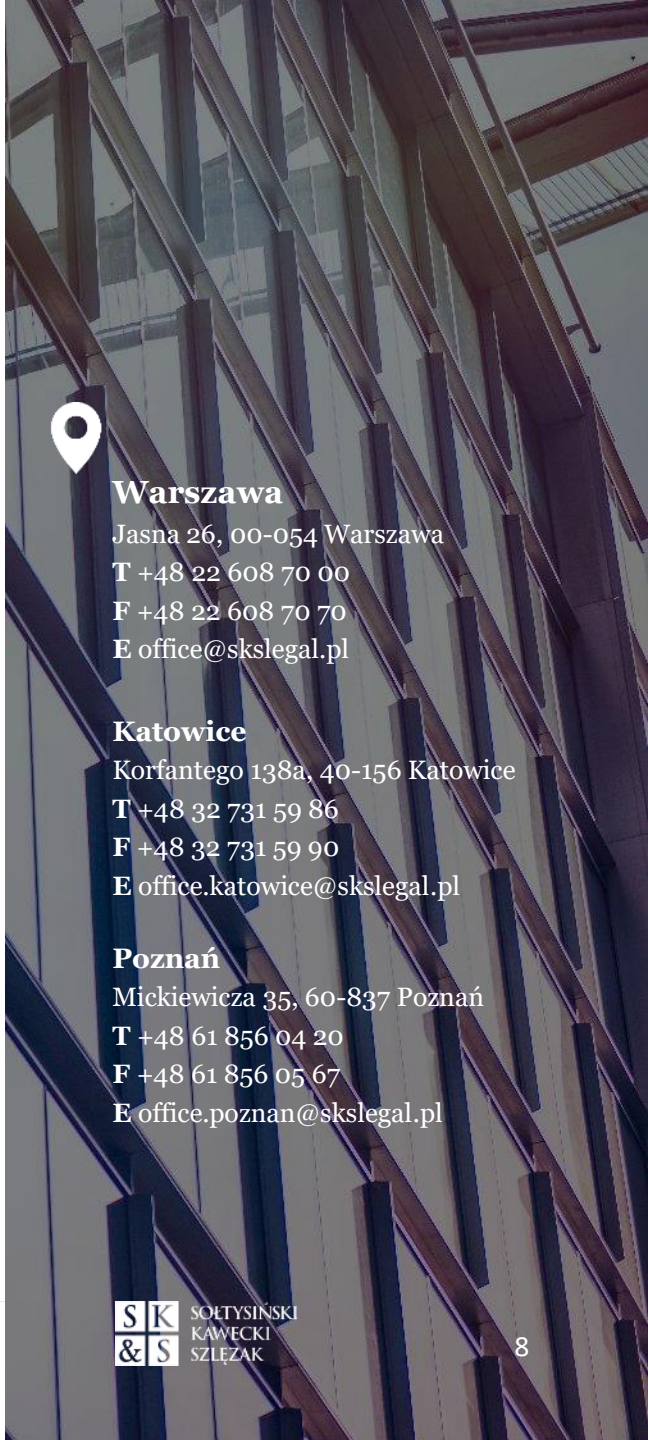
- Doradztwo w zakresie wdrożenia
- Pomoc w samoidentyfikacji
- Polityki i procedury
- Klauzule umowne (bezpieczeństwo łańcucha dostaw)
- Ubezpieczenia „cyber”
- Zabezpieczenie interesów kierowników podmiotów
- Wsparcie w obsłudze i zgłaszaniu incydentów
- Wsparcie DD przy transakcjach
- Tabletop exercise
- Bezpieczeństwo zasobów ludzkich

Napisz do nas:

Michał Opala
Senior Counsel, adwokat
✆ +48 602 402 617
✉ michal.opala@skslegal.pl

Mikołaj Sowiński
Partner, radca prawny
✉ mikolaj.sowinski@skslegal.pl

Tomasz Konopka
Partner, adwokat
✆ +48 604 243 699
✉ tomasz.konopka@skslegal.pl



Warszawa
Jasna 26, 00-054 Warszawa
T +48 22 608 70 00
F +48 22 608 70 70
E office@skslegal.pl

Katowice
Korfantego 138a, 40-156 Katowice
T +48 32 731 59 86
F +48 32 731 59 90
E office.katowice@skslegal.pl

Poznań
Mickiewicza 35, 60-837 Poznań
T +48 61 856 04 20
F +48 61 856 05 67
E office.poznan@skslegal.pl

SOŁTYSIŃSKI KAWECKI SZLĘZAK