# Kompleksowa obsługa prawna w zakresie cyberbezpieczeństwa

Dyrektywa NIS 2 (UE 2022/2555) i wdrażająca ją polska ustawa o zmianie ustawy o krajowym systemie cyberbezpieczeństwa zasadniczo zmieniają krajobraz prawny w obszarze cyberbezpieczeństwa. Dwa najważniejsze fakty dla Państwa firmy:

## Kogo dotyczą nowe przepisy i jakie grożą sankcje?

### Kto podlega nowym przepisom?

Podmioty z **18 sektorów gospodarki** – od energetyki i transportu, przez ochronę zdrowia i bankowość, po produkcję żywności, chemikalia, usługi pocztowe i platformy cyfrowe. Kryterium to nie tylko branża, ale również wielkość firmy: co do zasady objęte są **średnie i duże przedsiębiorstwa**.

### Co grozi za brak wdrożenia?

Kary administracyjne sięgające **10 mln EUR lub 2% globalnego obrotu** (podmioty kluczowe) oraz **7 mln EUR lub 1,4% obrotu** (podmioty ważne). W przypadku bezpośredniego zagrożenia bezpieczeństwa państwa – do **100 mln PLN**. Możliwa **osobista odpowiedzialność członków zarządu**.

Organy właściwe ds. cyberbezpieczeństwa zyskują szerokie uprawnienia nadzorcze: mogą prowadzić kontrole na miejscu, zlecać audyty bezpieczeństwa i skanowanie podatności. W stosunku do podmiotów kluczowych nadzór ma charakter **proaktywny** – nie czeka na zdarzenie, lecz weryfikuje stan zgodności z wyprzedzeniem. Dla podmiotów ważnych nadzór uruchamiany jest reaktywnie, jednak po wszczęciu postępowania prawa organu są takie same.

# Najważniejsze terminy

Poniżej przedstawiamy kluczowe daty i działania, które każda firma objęta nową regulacją powinna uwzględnić w swoim harmonogramie wdrożenia.

| Termin | Działanie |
|---|---|
| 19 lutego 2026 | Podpisanie ustawy przez Prezydenta RP |
| 1 miesiąc od ogłoszenia w Dzienniku Ustaw | Wejście w życie ustawy |
| Do 6 miesięcy od wejścia w życie | Termin na złożenie wniosku o wpis do wykazu podmiotów kluczowych / ważnych |
| Do 12 miesięcy od wejścia w życie | Termin na wdrożenie systemu zarządzania bezpieczeństwem informacji (SZBI) |
| Do 12 miesięcy od wejścia w życie | Termin na uruchomienie procedur zgłaszania incydentów (system S46) |

GWW
LEGAL & TAX

# Co oferujemy

Nasze usługi obejmują **pełne spektrum wsparcia prawnego** – od pierwszego kroku (ustalenie statusu prawnego firmy), przez kompleksowe wdrożenie, aż po obronę w postępowaniach nadzorczych i sankcyjnych.

01

## Kwalifikacja prawna i analiza obowiązków

Ustalenie, czy i w jakiej kategorii firma podlega nowej ustawie.

02

## Postępowanie rejestrowe – wpis do wykazu

Przygotowanie dokumentacji i reprezentacja wobec organu właściwego.

03

## Wdrożenie SZBI

Ocena stanu obecnego, dokumentacja i szkolenia dla organów zarządzających.

04

## Bezpieczeństwo łańcucha dostaw

Przegląd umów z dostawcami ICT i opracowanie klauzul bezpieczeństwa.

05

## Procedury zgłaszania incydentów

Opracowanie procedur klasyfikacji zdarzeń i obsługa kryzysowa.

06

## Nadzór, kontrole i postępowania sankcyjne

Audyt prawny, przygotowanie do kontroli i reprezentacja przed organami.

07

## Szkolenia z zakresu cyberbezpieczeństwa

Dedykowane szkolenia zamknięte dla zarządu, działu prawnego i compliance.

GWW
LEGAL & TAX

# Usługa 1–2: Kwalifikacja prawna i rejestracja

USŁUGA 1

## Kwalifikacja prawna i analiza obowiązków

Punktem wyjścia jest ustalenie, czy i w jakiej kategorii Państwa firma podlega nowej ustawie. Bez tej analizy nie można ocenić, jakie obowiązki i w jakim terminie należy wypełnić.

**Zakres naszych działań:**

- Analiza struktury prawnej i operacyjnej firmy pod kątem kryteriów podmiotowych i sektorowych
- Określenie kategorii (podmiot kluczowy / podmiot ważny) lub potwierdzenie braku obowiązków
- Identyfikacja przypadków szczególnych – jedyny dostawca usługi, powiązania w grupie kapitałowej
- Pisemna opinia prawna z rekomendacją dalszego postępowania

**Dla kogo:** wszystkie firmy, które nie mają pewności co do swojego statusu pod nową ustawą

USŁUGA 2

## Postępowanie rejestrowe – wpis do wykazu

Podmioty kluczowe i ważne mają obowiązek zgłoszenia się do wykazu prowadzonego przez organ właściwy. Termin: **6 miesięcy od wejścia ustawy w życie**. Błędy lub opóźnienia w rejestracji mogą prowadzić do sankcji.

**Zakres naszych działań:**

- Doradztwo w zakresie procedury i terminarza rejestracji
- Przygotowanie dokumentacji i wniosku o wpis
- Reprezentacja wobec organu właściwego w toku postępowania
- Obsługa ewentualnych wpisów z urzędu i aktualizacji danych

**Dla kogo:** wszystkie podmioty objęte nową regulacją

GWW LEGAL & TAX

# Usługa 3: Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

Ustawa nakłada obowiązek wdrożenia środków zarządzania ryzykiem w cyberbezpieczeństwie. Termin: **12 miesięcy od wejścia ustawy w życie**. Organy zarządzające (zarządy, rady nadzorcze) są zobowiązane osobiście zatwierdzić ten system i ponoszą odpowiedzialność za jego brak.

### Gap Analysis

Ocena stanu obecnego – identyfikacja luk formalnych i dokumentacyjnych

### Polityka ryzyka

Opracowanie lub weryfikacja polityki zarządzania ryzykiem w cyberbezpieczeństwie

### Dokumentacja SZBI

Polityki bezpieczeństwa, procedury obsługi incydentów, plan ciągłości działania, polityka bezpieczeństwa łańcucha dostaw, zasady kontroli dostępu, procedury zarządzania podatnościami

### Szkolenia zarządu

Szkolenia dla członków organów zarządzających z zakresu obowiązków wynikających z KSC

** W zależności od stopnia złożoności infrastruktury technicznej klienta, realizacja powyższego zakresu prac może wymagać zaangażowania zewnętrznych ekspertów ds. cyberbezpieczeństwa. W takim przypadku koordynujemy współpracę z audytorami i specjalistami technicznymi, zapewniając spójność działań prawnych i technicznych.*

**Dla kogo:** podmioty kluczowe i ważne; szczególnie firmy wdrażające SZBI po raz pierwszy

GWW LEGAL & TAX

# Usługa 4–5: Łańcuch dostaw i procedury incydentów

USŁUGA 4

## Bezpieczeństwo łańcucha dostaw – umowy z dostawcami ICT

Nowe przepisy wymagają, aby podmioty objęte ustawą uwzględniały ryzyka cyberbezpieczeństwa w relacjach z dostawcami usług i produktów ICT. Brak odpowiednich klauzul w umowach z podwykonawcami może prowadzić do naruszenia obowiązków ustawowych.

**Zakres naszych działań:**

- Przegląd i weryfikacja umów z dostawcami ICT pod kątem wymogów bezpieczeństwa
- Opracowanie standardowych klauzul bezpieczeństwa do stosowania w kontraktach z podwykonawcami
- Doradztwo przy ocenie ryzyka dostawców (vendor risk assessment) – aspekty prawne
- Przygotowanie wewnętrznej polityki zarządzania ryzykiem w łańcuchu dostaw

**Dla kogo:** podmioty z rozbudowanym łańcuchem dostawców ICT (energetyka, transport, infrastruktura cyfrowa, zdrowie)

USŁUGA 5

## Procedury zgłaszania incydentów

Poważny incydent cyberbezpieczeństwa musi zostać zgłoszony organom w ściśle określonych terminach: **wczesne ostrzeżenie – 24 godziny, pełne zgłoszenie – 72 godziny, sprawozdanie końcowe – 1 miesiąc**. Brak procedur lub opóźnione zgłoszenie stanowi samodzielną przesłankę nałożenia kary.

**Zakres naszych działań:**

- Opracowanie wewnętrznych procedur klasyfikacji zdarzeń i eskalacji
- Przygotowanie szablonów zgłoszeń (wczesne ostrzeżenie, zgłoszenie incydentu, sprawozdanie końcowe)
- Integracja procedur KSC z procedurami zgłaszania naruszeń danych osobowych (RODO)
- Doradztwo prawne w toku trwającego incydentu – obsługa kryzysowa
- Nadzór nad komunikacją z organami i CSIRT podczas incydentu

**Dla kogo:** wszystkie podmioty objęte ustawą; obsługa kryzysowa dostępna ad hoc dla każdego klienta

** W zależności od stopnia złożoności infrastruktury technicznej klienta, realizacja powyższego zakresu prac może wymagać zaangażowania zewnętrznych ekspertów ds. cyberbezpieczeństwa. W takim przypadku koordynujemy współpracę z audytorami i specjalistami technicznymi, zapewniając spójność działań prawnych i technicznych.*

GWW LEGAL & TAX

# Usługa 6: Nadzór, kontrole i postępowania sankcyjne

Organy właściwe ds. cyberbezpieczeństwa dysponują szerokim zakresem środków: kontrole na miejscu, audyty bezpieczeństwa, skanowanie podatności, a w razie stwierdzenia naruszeń – decyzje administracyjne i kary finansowe. Pomagamy zarówno przygotować się do kontroli, jak i skutecznie bronić się w postępowaniu.

### Audyt prawny zgodności

Wewnętrzny audyt prawny zgodności z KSC (legal compliance review)

### Przygotowanie do kontroli

Przygotowanie firmy do kontroli organu właściwego – przegląd dokumentacji

### Plany naprawcze

Opracowanie planów naprawczych w odpowiedzi na zalecenia organów

### Reprezentacja przed organami

Reprezentacja klienta przed organami właściwymi w postępowaniach nadzorczych i sankcyjnych

### Odwołania od decyzji

Sporządzanie odwołań od decyzji administracyjnych nakładających kary

### Odpowiedzialność zarządu

Doradztwo w zakresie osobistej odpowiedzialności członków zarządu

** W zależności od stopnia złożoności infrastruktury technicznej klienta, realizacja powyższego zakresu prac może wymagać zaangażowania zewnętrznych ekspertów ds. cyberbezpieczeństwa. W takim przypadku koordynujemy współpracę z audytorami i specjalistami technicznymi, zapewniając spójność działań prawnych i technicznych.*

**Dla kogo:** przede wszystkim podmioty kluczowe; dla podmiotów ważnych – po sygnale o wszczęciu postępowania

GWW LEGAL & TAX

# Usługa 7: Szkolenia z zakresu cyberbezpieczeństwa i obowiązków prawnych KSC

Ustawa o KSC nakłada obowiązek regularnego szkolenia kadry zarządzającej oraz pracowników odpowiedzialnych za bezpieczeństwo informacji. Szkolenie to nie jest formalnym warunkiem wypełnienia obowiązków ustawowych sam w sobie – jest jednak jednym ze środków zarządzania ryzykiem, które organ nadzorczy może sprawdzić w toku kontroli. Oferujemy **dedykowane szkolenia zamknięte**, przeprowadzane stacjonarnie w siedzibie klienta lub w formule online, dostosowane do potrzeb trzech grup odbiorców.

PROGRAM A

## Szkolenie dla zarządu i rady nadzorczej

- Zakres regulacji NIS 2 i ustawy o KSC – co zmieniło się względem poprzedniego stanu prawnego
- Osobista odpowiedzialność członków zarządu i rady nadzorczej – podstawy prawne, zakres, ryzyko zakazu pełnienia funkcji
- Obowiązek zatwierdzania i nadzorowania systemu zarządzania bezpieczeństwem informacji (SZBI) przez organ zarządzający
- System sankcji – kary administracyjne, skalowanie kary, czynniki łagodzące
- Praktyczne pytania i scenariusze: co muszę zatwierdzić, czego pilnować, kiedy poinformować organ

PROGRAM B

## Szkolenie dla działu prawnego i compliance

- Szczegółowa analiza obowiązków wynikających z ustawy o KSC – katalog środków zarządzania ryzykiem, wymogi dokumentacyjne, terminy
- Procedura zgłaszania incydentów – terminy (24h / 72h / 1 miesiąc), schematy decyzyjne, integracja z RODO
- Bezpieczeństwo łańcucha dostaw – wymogi prawne wobec dostawców ICT, klauzule umowne, ocena ryzyka
- Postępowania nadzorcze i sankcyjne – przebieg kontroli, prawa podmiotu, argumentacja obronna

**Dla kogo:** wszystkie podmioty objęte nową regulacją; szkolenia realizowane jako zamknięte – dedykowane wyłącznie Państwa firmie, stacjonarnie lub online

GWW LEGAL & TAX

# Dlaczego warto działać już teraz?

Dyrektywa NIS 2 i polska ustawa o KSC wyznaczają ścisłe terminy – od rejestracji po wdrożenie pełnego systemu zarządzania bezpieczeństwem. Każdy miesiąc zwłoki skraca czas na przygotowanie i zwiększa ryzyko sankcji.

### Pełne spektrum

Od kwalifikacji prawnej, przez wdrożenie SZBI, aż po obronę w postępowaniach sankcyjnych

### Spójność prawna i techniczna

Koordynujemy współpracę z audytorami i specjalistami technicznymi, zapewniając spójność działań

### Dedykowane podejście

Każde działanie dostosowane do specyfiki Państwa firmy, sektora i stopnia złożoności infrastruktury

### Obsługa kryzysowa

Wsparcie ad hoc w toku trwającego incydentu – dostępne dla każdego klienta

GWW Ladziński, Cmoch
i Wspólnicy sp. k.
ul. Książęca 4
00-498 Warszawa
NIP: 7010313649
gww@gww.pl

gww.pl