

**DOŁĄCZ
DO NAS**

7 października 2026 r.
szkolenie on - line

CYBERBEZPIECZEŃSTWO W ENERGETYCE - NIS2 DLA DZIAŁÓW PRAWNYCH I COMPLIANCE

Praktyczna realizacja obowiązków
wynikających z NIS2 i ustawy o KSC
– odpowiedzialność, dokumentacja
i zarządzanie zgodnością



Cyberbezpieczeństwo w energetyce - NIS2 dla działów prawnych i compliance

Rosnąca liczba cyberzagrożeń oraz nowe obowiązki wynikające z Dyrektywy NIS2 i ustawy o krajowym systemie cyberbezpieczeństwa (KSC) sprawiają, że zapewnienie zgodności z przepisami staje się jednym z najważniejszych wyzwań dla przedsiębiorstw sektora energetycznego. Szczególną rolę w tym procesie odgrywają działy prawne i compliance, które wspierają organizację w prawidłowej interpretacji przepisów, przygotowaniu procesów oraz realizacji obowiązków związanych z cyberbezpieczeństwem.

Szkolenie „**Cyberbezpieczeństwo w energetyce - NIS2 dla działów prawnych i compliance**” zostało przygotowane z myślą o osobach odpowiedzialnych za kwestie prawne i zgodność z przepisami w przedsiębiorstwach energetycznych. Program koncentruje się na praktycznych zagadnieniach związanych z kwalifikacją podmiotów, realizacją obowiązków wynikających z Dyrektywy NIS2 i ustawy o KSC, rejestracją podmiotów kluczowych i ważnych, a także obowiązkami dotyczącymi dokumentacji, raportowania oraz współpracy z właściwymi organami.

Podczas szkolenia omówione zostaną najczęstsze problemy interpretacyjne i organizacyjne związane ze stosowaniem przepisów dotyczących cyberbezpieczeństwa w przedsiębiorstwach energetycznych. Uczestnicy przeanalizują również studia przypadków (case study) dotyczące odpowiedzialności kontraktowej oraz ustalania odpowiedzialności za incydenty i naruszenia bezpieczeństwa informacji, co pozwoli lepiej zrozumieć praktyczne aspekty realizacji obowiązków wynikających z obowiązujących przepisów.

Zapraszam do rezerwacji miejsc!

Anna Chmielewska
Project Director
a.chmielewska@langas.pl | tel. 512 773 769

KORZYŚCI

- Poznasz najważniejsze obowiązki wynikające z Dyrektywy NIS2 oraz zmian w ustawie o KSC, istotne z perspektywy przedsiębiorstw energetycznych oraz działów prawnych i Compliance.
- Dowiesz się, jak prawidłowo identyfikować obowiązki w zakresie cyberbezpieczeństwa w zależności od rodzaju prowadzonej działalności oraz statusu przedsiębiorstwa.
- Zrozumiesz zasady rejestracji podmiotów kluczowych i ważnych, raportowania incydentów oraz współpracy z właściwymi organami i CSIRT.
- Poznasz praktyczne zagadnienia związane z zapewnieniem zgodności w relacjach z dostawcami ICT, przygotowywaniem zapisów umownych oraz zarządzaniem ryzykiem w łańcuchu dostaw.
- Dowiesz się, jakie obowiązki i obszary odpowiedzialności spoczywają na zarządzie, działach prawnych i compliance oraz osobach pełniących funkcje związane z cyberbezpieczeństwem, a także poznasz praktyczne problemy omawiane na przykładach (case study).

PROGRAM

9.15 – Logowanie do platformy

9.30 – Rozpoczęcie szkolenia

JAK PRAWIDŁOWO USTALIĆ WYMOGI CYBERBEZPIECZEŃSTWA W PRZEDSIĘBIORSTWACH ENERGETYCZNYCH Z UWZGLĘDNIENIEM NOWYCH WYMOGÓW PRAWNYCH?

- Pułapki multikwalifikacji statusów w sektorze energetycznym między innymi sektorami oraz ich wpływ na realizację obowiązków dotyczących cyberbezpieczeństwa.
- Wpływ zmian w prowadzonej działalności na status z NIS2.
- Zasady warstwowania środków bezpieczeństwa – różnice między spółkami obrotu, wytwórcami, dystrybutorami i przedsiębiorstwami przesyłowymi.
- Ramy systemu zarządzania bezpieczeństwem i typy dokumentacji, której nie trzeba dublować w spółkach należących do infrastruktury krytycznej.
- Digitalizacja dokumentacji cyberbezpieczeństwa – wyzwania i ograniczenia.
- Zapewnienie zgodności w oparciu o różne standardy bezpieczeństwa – jakie warunki muszą być spełnione, żeby skutecznie zadeklarować zgodność z przepisami w oparciu o ISO czy IEC.

REJESTRACJA W WYKAZIE PODMIOTÓW KLUCZOWYCH I WAŻNYCH, KORZYSTANIE Z SYSTEMU S46

- Różnice między procedurą samogłoszenia a wpisem z urzędu, powiązania między przepisami NIS2 i CER.
- Zasady korygowania i aktualizacji treści wpisu, organy realizujące czynności.
- Terminy, wymogi formalne, osoby uprawnione do reprezentacji i ich odpowiedzialność za składane oświadczenia – w okresie przejściowym i po uruchomieniu s46.
- Co robić w razie awarii s46 – kwestia biegu terminów i odpowiedzialności za realizację obowiązków.
- Zakres informacji, które trzeba pozyskać do wniosków z działów technicznych – jak nie pomylić się przy wypełnianiu formularzy.
- Proces raportowania zdarzeń do właściwego CSIRT.

CYBERBEZPIECZEŃSTWO W RELACJACH Z KONTRAHENTAMI

- Problemy dotyczące analizy ryzyka związanego z dostawcami ICT.
- Rodzaje zapisów dotyczących wymogów cyberbezpieczeństwa niezbędne w umowach.
- Problem dostawcy wysokiego ryzyka z punktu widzenia zakupów realizowanych w trybie zamówień publicznych.
- Obsługa incydentów w łańcuchu dostaw.

CASE STUDY:

- Zapisy umowne dotyczące odpowiedzialności kontrahenta za włamanie do systemu ERP

WYZWANIA ZWIĄZANE Z FUNKCJONOWANIEM WEWNĘTRZNYCH STRUKTUR CYBERBEZPIECZEŃSTWA

- Obowiązki, za które odpowiada bezpośrednio zarząd i zakres działań, za które organizacja można skutecznie delegować na inne osoby.
- Umowa o pracę i współpraca B2B z punktu widzenia odpowiedzialności dyscyplinarnej.
- Wymogi dotyczące osób wyznaczonych do kontaktu z krajowym systemem cyberbezpieczeństwa – kwestie korporacyjne i związane z prawem pracy a przepisy Ustawy o KSC.
- Problemy związane z łączeniem funkcji wynikających z Ustawy o KSC czy RODO i innych ról w organizacji.
- Obowiązek przetwarzania danych osobowych o niekaralności z punktu widzenia aktualizacji rejestru czynności przetwarzania i ponownego wykonania obowiązku informacyjnego.
- Wymogi dotyczące wyposażenia i parametrów pomieszczeń struktur cyberbezpieczeństwa przed i po NIS2.

CASE STUDY

- Przebieg czynności związanych z ustaleniem odpowiedzialności za wyciek danych.

15.30 – Zakończenie szkolenia



Ekspertka: **dr Monika Bogdał**

Radca prawny, audytor wiodący ISO 2700, doświadczona ekspertka w obszarze cyberbezpieczeństwa oraz regulacji dotyczących nowych technologii.

Doktorat z ekonomii zdobyła na Uniwersytecie Ekonomicznym w Poznaniu. Ukończyła też studia podyplomowe z zakresu zarządzania technologiami wysokich lotów na Jyväskylä University of Applied Sciences. Uzyskała też tytuł magistra prawa na Uniwersytecie im. Adama Mickiewicza w Poznaniu.

Specjalizuje się w takich dziedzinach jak cyberbezpieczeństwo, governance, compliance, ciągłość działania, zarządzanie kryzysowe, a także w regulacjach związanych z NIS2 oraz Ustawą o Krajowym Systemie Cyberbezpieczeństwa (KSC). Dodatkowo zajmuje się zagadnieniami ochrony środowiska oraz oceną zgodności produktów z wymogami CE.

Od 2025 roku prowadzi własną kancelarię radcy prawnego, świadcząc doradztwo prawne i biznesowe dla przedsiębiorstw działających w sektorze technologii pod marką.

Wcześniej, w latach 2014–2024, pełniła funkcję współnika i kierownika zespołu ds. nowych technologii w Kancelarii Prawnej Piszcz i Wspólnicy, gdzie odpowiadała za rozwój usług prawnych dedykowanych branży IT i technologicznej, zarządzanie zespołem specjalistów oraz doradztwo w zakresie zarządzania ryzykiem, budowy procesów i dokumentacji związanej z bezpieczeństwem informacji.

W ramach swoich obowiązków wspierała klientów w sytuacjach incydentów cyberbezpieczeństwa oraz reprezentowała ich podczas negocjacji kontraktów oraz przed organami administracyjnymi i regulacyjnymi. Jej doświadczenie obejmuje również doradztwo w sprawach środowiskowych i odpadowych oraz wsparcie branż przemysłowych i infrastruktury krytycznej.

Monika Bogdał posiada wieloletnie doświadczenie trenerskie, zdobyte jako wykładowca akademicki na Uniwersytecie Ekonomicznym w Poznaniu oraz trener szkoleń dedykowanych sektorowi energetycznemu i branży odpadowej.

Prowadzi liczne szkolenia i warsztaty z zakresu praktycznego stosowania wymogów NIS2, governance i compliance w sektorze energetycznym, zarządzania ryzykiem, procedur reklamacyjnych, a także zagadnień związanych z rozliczeniami prosumentów oraz rynkiem bilansującym energii.

Jest autorką wielu publikacji naukowych i branżowych, które poruszają tematykę cyberbezpieczeństwa, regulacji prawnych i innowacji technologicznych w sektorze energetycznym i ochronie środowiska. Posiada uprawnienia audytora wiodącego ISO 27001 i regularnie uczestniczy jako prelegentka w krajowych oraz międzynarodowych konferencjach branżowych.



LANGAS REGTECH SP. Z O.O.
MARSZAŁKOWSKA 58/15
00545 WARSZAWA
NIP: 7010991220

+48 22 50 60 850 | SZKOLENIA@LANGAS.PL

Cyberbezpieczeństwo w energetyce - NIS2 dla działów prawnych i compliance

7 października 2026r.,
szkolenie on-line

LICZBA MIEJSC OGRANICZONA

☐ do 16.09.2026 - 1570 pln + 23% VAT

☐ od 17.09.2026 - 1870 pln + 23% VAT

CENA ZAWIERA

Uczestnictwo w szkoleniu, materiały, certyfikat

SPOSÓB PŁATNOŚCI

Przelewem w terminie 7 dni od daty otrzymania faktury proforma
na konto Langas Regtech Sp. z o.o. NIP 7010991220

POTWIERDZENIE ZGŁOSZENIA

Po otrzymaniu formularza zgłoszeniowego prześlemy Państwu
potwierdzenia przyjęcia zgłoszenia na adres e-mail podany
w formularzu. Na ok. 10 dni przed rozpoczęciem wydarzenia
otrzymają Państwo szczegółowe informacje organizacyjne.

FIRMA

Adres

Imię i nazwisko (1)

Stanowisko

E-mail

Imię i nazwisko (2)

Stanowisko

E-mail

Imię i nazwisko (3)

Stanowisko

E-mail

Osoba do kontaktu

(przed szkoleniem otrzyma na adres
e-mail informacje o szkoleniu)

Stanowisko

E-mail

Telefon/Fax

☐

Wyrażam zgodę na przetwarzanie moich danych osobowych przez Langas Regtech Sp. z o.o., ul. Marszałkowska 10k.15, 00-545 Warszawa, NIP: 7010991220 w celu dostarczania informacji handlowych drogą elektroniczną, w tym pocztą elektroniczną oraz telefonicznie, z art. 6 ust. 1 lit. a rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO) oraz ustawę z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. 2017 poz. 1219 z późn. zm.). Wyrażenie zgody jest dobrowolne i może być w każdym czasie cofnięte.

☐

Wyrażam zgodę na inicjowanie telefonicznych połączeń przychodzących z wykorzystaniem przez Langas Regtech Sp. z o.o., ul. Marszałkowska 10k.15, 00-545 Warszawa, NIP: 7010991220 w celach handlowych i marketingowych zgodnie z art. 6 ust. 1 lit. a rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO) oraz z art. 172 ustawy prawo telekomunikacyjne (Dz. U. Dz. U. 2016. 1489 z późn. zm.). Wyrażenie zgody jest dobrowolne i może być w każdym czasie cofnięte.

FAKTURA

☐

Oświadczamy, że jesteśmy płatnikami VAT nasz nr NIP:

Upoważniamy firmę Langas Regtech Sp. z o.o. do wystawienia faktury VAT bez naszego podpisu.

☐

Oświadczamy, że nie jesteśmy płatnikami VAT

J. Oświadczam, że zapoznałem się z ogólnymi warunkami uczestnictwa w projektach edukacyjnych realizowanych przez Langas Regtech <https://langas.pl/wp-content/uploads/2020/09/Og%C3%B3lne-warunki-uczestnictwa-w-projektach-edukacyjnych-realizowanych-przez-Langas-Group.pdf>

☐

Oświadczam, że jestem upoważniony (-na) przez firmę do podpisania formularza.

Langas Group – Level up!

podpis

data

pieczęć