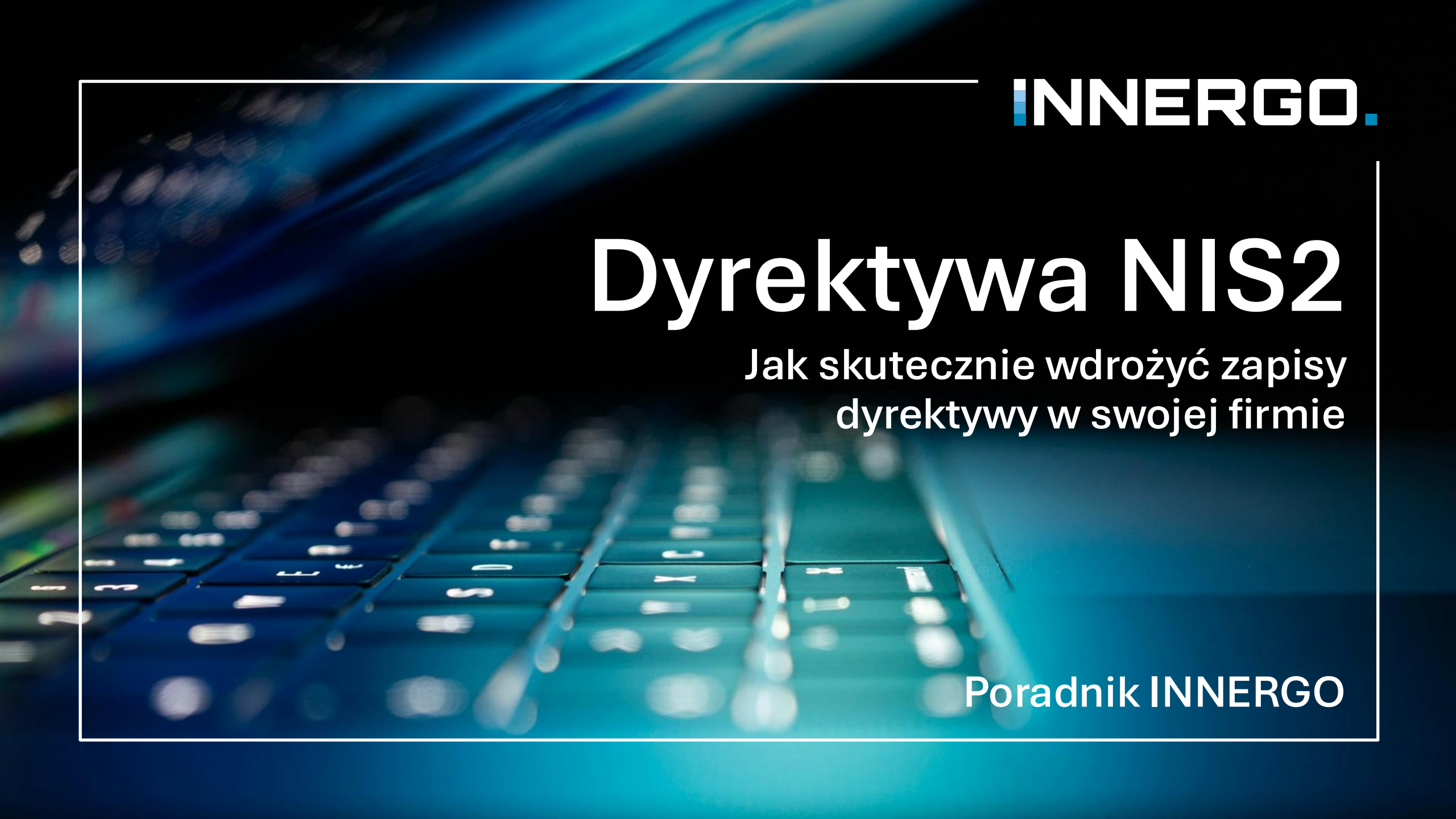


INNERGO.

Dyrektywa NIS2

Jak skutecznie wdrożyć zapisy dyrektywy w swojej firmie

Poradnik INNERGO

Krajobraz legislacyjny w Unii Europejskiej

Od kilku lat ekosystem regulacyjny cyberbezpieczeństwa w Polsce, podobnie jak w pozostałych krajach Unii Europejskiej, jest kształtowany przez dyrektywy i rozporządzenia unijne. Proces ten rozpoczął się w 2016 roku od przyjęcia rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO) oraz dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (NIS).

W kolejnych latach Komisja Europejska wraz z Parlamentem Europejskim i Radą przeprowadziły tzw. "sztorm legislacyjny", który uzupełnił system prawny o:

- Dyrektywę w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii (Dyrektywa NIS 2) – rok 2022,
- Dyrektywę w sprawie odporności podmiotów krytycznych (Dyrektywa CER) – rok 2022,
- Rozporządzenie w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych (Cybersecurity Act) – rok 2019,
- Rozporządzenie w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA) – rok 2022.

W kolejce do publikacji czeka jeszcze rozporządzenie w sprawie horyzontalnych wymogów bezpieczeństwa cybernetycznego dla produktów z elementami cyfrowymi (rozporządzenie CRA), a całość uzupełni rozporządzenie o sztucznej inteligencji (AI Act).

Dlaczego wymieniamy wszystkie te regulacje, mimo że większość mediów skupia się na Dyrektywie NIS2?

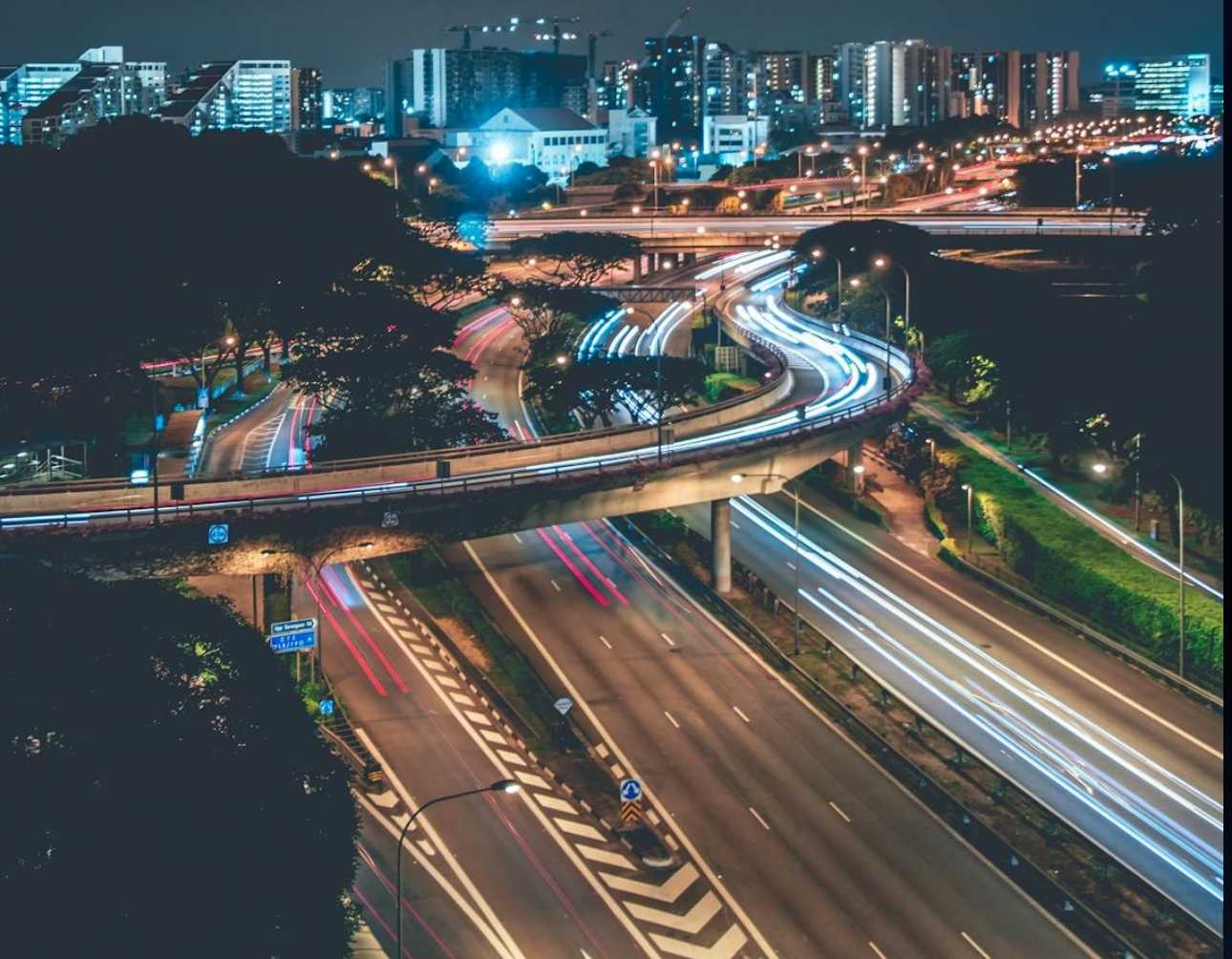
> *Rozsądne ekonomicznie wdrażanie regulacji wymaga od przedsiębiorców, aby podejmowali świadome i zintegrowane działania w zakresie implementacji przepisów prawnych, minimalizując jednocześnie koszty. Oznacza to, że wdrożenie NIS2 nie powinno być zupełnie odrębnym projektem, ale kontynuacją wdrożenia RODO”*

A co jeśli przedsiębiorca posiada wdrożoną normę ISO 27001?

> *Wtedy wdrożenie NIS2 powinno być jedynie kontynuacją tego procesu, a nie oddzielną aktywnością. Procedury związane z NIS2 oraz związane z tym wydatki powinny być elementem całego ekosystemu cyberbezpieczeństwa przedsiębiorstwa, a nie oddzielnym wysiłkiem realizowanym dodatkowo*

mówi **dr inż. Andrzej Bartosiewicz, Prezes Fundacji CISO #Poland,** skupiającej szefów cyberbezpieczeństwa w Polsce.

Dyrektywa NIS2 a Ustawa o Krajowym Systemie Cyberbezpieczeństwa



Dyrektywa NIS2 z 2022 roku jest transponowana do systemu prawnego każdego z krajów UE, w tym także Polski.

Nowe przepisy dotyczą cyberbezpieczeństwa firm działających w kluczowych i ważnych sektorach gospodarki. Ich celem jest zwiększenie odporności państwa i przedsiębiorstw na cyberzagrożenia oraz zapewnienie ciągłości działania usług.

Podstawą zmian jest dyrektywa NIS2, czyli unijne prawo, które nakłada obowiązki w zakresie zarządzania ryzykiem, zgłaszania incydentów i organizacji bezpieczeństwa IT.

W Polsce przepisy te zostały wdrożone przez nowelizację ustawy o Krajowym Systemie Cyberbezpieczeństwa (ustawa o KSC).

Nowe przepisy obowiązują od **3 kwietnia 2026 roku**, ale obowiązki wdrażasz etapami.

Sprawdź, czy ustawa o KSC dotyczy twojej firmy - ustal, czy twoja firma :

- jest podmiotem kluczowym lub ważnym
- działa w sektorze objętym ustawą o KSC.

Zarejestruj się w wykazie podmiotów kluczowych i ważnych

- Od momentu, gdy spełnisz kryteria uznania za podmiot kluczowy lub ważny, masz 6 miesięcy na zgłoszenie do wykazu podmiotów kluczowych i ważnych.
- Jeśli twoja firma spełniała kryteria dla podmiotu kluczowego lub ważnego to **termin na zgłoszenie do wykazu upływa 3 października 2026** roku.

Jeśli jesteś podmiotem kluczowym najpóźniej w ciągu 24 miesięcy od spełnienia przesłanek uznania za podmiot kluczowy musisz:

przeprowadzić audyt zgodności z przepisami, aby potwierdzić spełnienie obowiązków i przygotować się na kontrole organów

- sprawdzić, czy wdrożone środki działają prawidłowo.
- po tym czasie organy nadzorcze mogą już nakładać kary za naruszenie przepisów.

Kto podlega dyrektywie NIS2?

- Dyrektywa NIS2 **obejmuje długą listę podmiotów, szacowaną na ok. 2.000.000 podmiotów w UE, z tego 100.000 w Polsce,** a najważniejszą grupę stanowią podmioty kluczowe i ważne.

- Podmioty kluczowe obejmują:
- podmioty o których mowa w załączniku I dyrektywy, przekraczające pułapy dla średnich przedsiębiorstw*,
- podmioty które zostały wskazane przez państwo członkowskie jako podmioty kluczowe,
- podmioty wskazane jako podmioty krytyczne na podstawie dyrektywy CER.

** przedsiębiorstwo zatrudniające mniej niż 250 osób, którego obroty roczne nie przekraczają 50 mln EUR i/lub roczna suma bilansowa nie przekracza 43 mln EUR.*

- Podmioty ważne obejmują:

podmioty o których mowa w załączniku I lub II dyrektywy, które nie kwalifikują się jako podmioty kluczowe, ale zatrudniają więcej niż 50 osób, a ich obroty roczne przekraczają 10 mln EUR.

Zakres stosowania NIS2

INNERGO.

Podmioty Kluczowe

- Energetyka
- Transport
- Bankowość i infrastruktura rynków finansowych
- Ochrona zdrowia
- Woda pitna
- Ścieki
- Infrastruktura cyfrowa
- Zarządzanie usługami ICT
- Podmioty administracji publicznej
- Przestrzeń kosmiczna

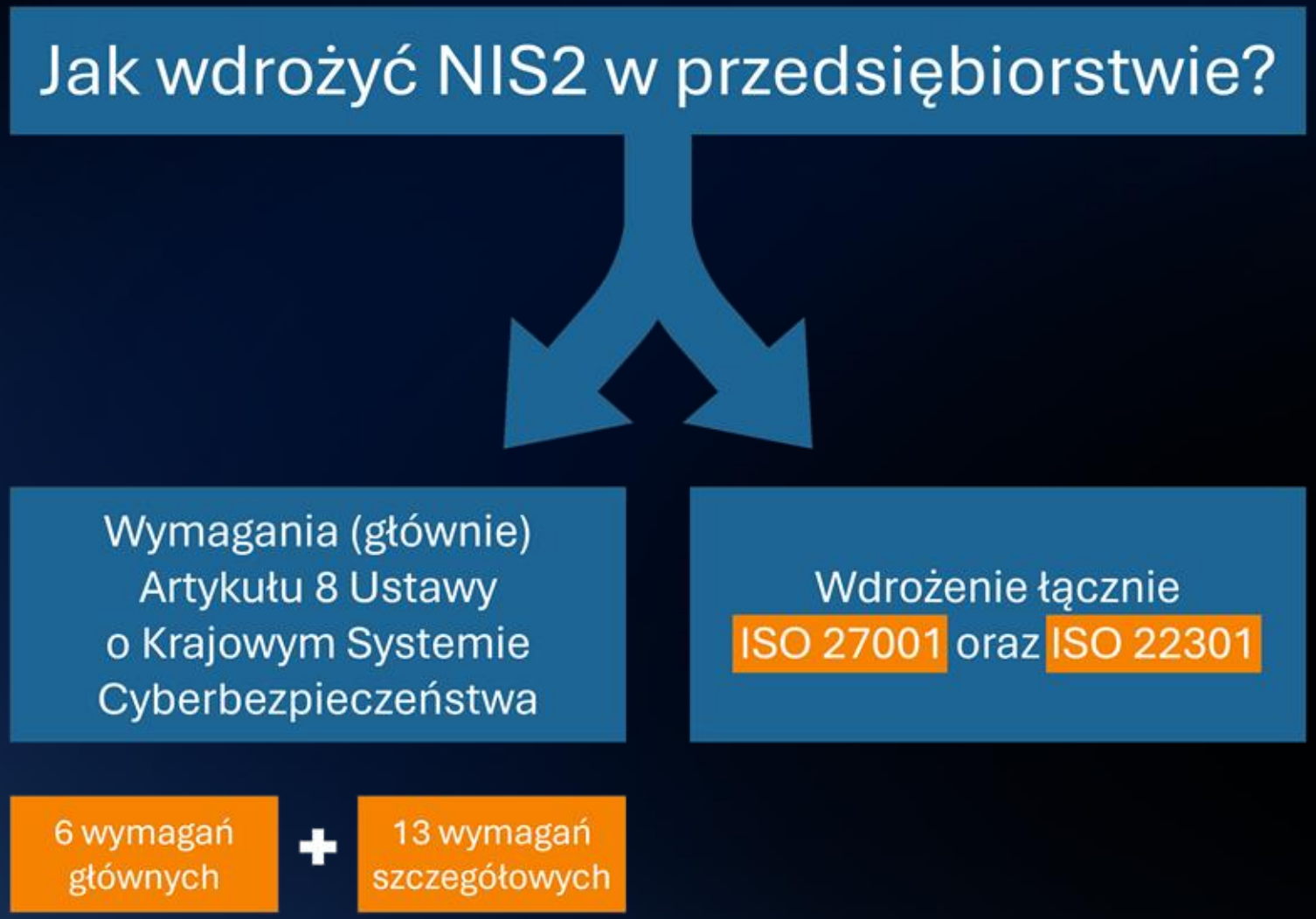
Podmioty Ważne

- Usługi pocztowe i kurierskie
- Gospodarowania odpadami
- Produkcja, przetwarzania i dystrybucja chemikaliów
- Produkcja, przetwarzania i dystrybucji żywności
- Produkcja (szeroko rozumiana)
- Dostawcy usług cyfrowych
- Badania naukowe

Podmioty średnie lub duże
zatrudniające ponad 50 pracowników i których roczny obrót i/lub roczna suma bilansowa przekracza 10 mln euro

Podmioty z Art. 2 ust. 2 punkty 2 do 5

dostawcy publicznych sieci łączności elektronicznej lub dostawcy publicznie dostępnych usług łączności elektronicznej	dostawcy usług zaufania	rejestry nazw domen najwyższego poziomu
podmiot jest jedynym dostawcą usługi, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej	zakłócenie usługi świadczonej przez podmiot mogłoby mieć znaczący wpływ na porządek publiczny, bezpieczeństwo publiczne lub zdrowie publiczne	zakłócenie usługi mogłoby prowadzić do powstania poważnego ryzyka systemowego, w szczególności w sektorach, w których takie zakłócenie mogłoby mieć wpływ transgraniczny
podmiot ma charakter krytyczny ze względu na jego szczególne znaczenie na poziomie krajowym lub regionalnym dla konkretnego sektora	podmiot administracji publicznej na poziomie rządu centralnego lub na poziomie regionalnym, świadczący usługi których zakłócenie mogłoby mieć znaczący wpływ na krytyczną działalność społeczną lub gospodarczą	



Dwa sposoby zapewnienia zgodności z NIS2

- Przedsiębiorca może wybrać jeden z dwóch sposobów wdrożenia wymagań:

1. spełnienie wymagań zawartych głównie w Artykule 8 Ustawy,
2. wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji zgodnego łącznie z ISO 27001 oraz ISO 22301.

Warto podkreślić, że **nie jest wymagana certyfikacja na zgodność z normą, a jedynie deklaracja takiej zgodności.**

Podstawowe wymagania zgodności 1/2

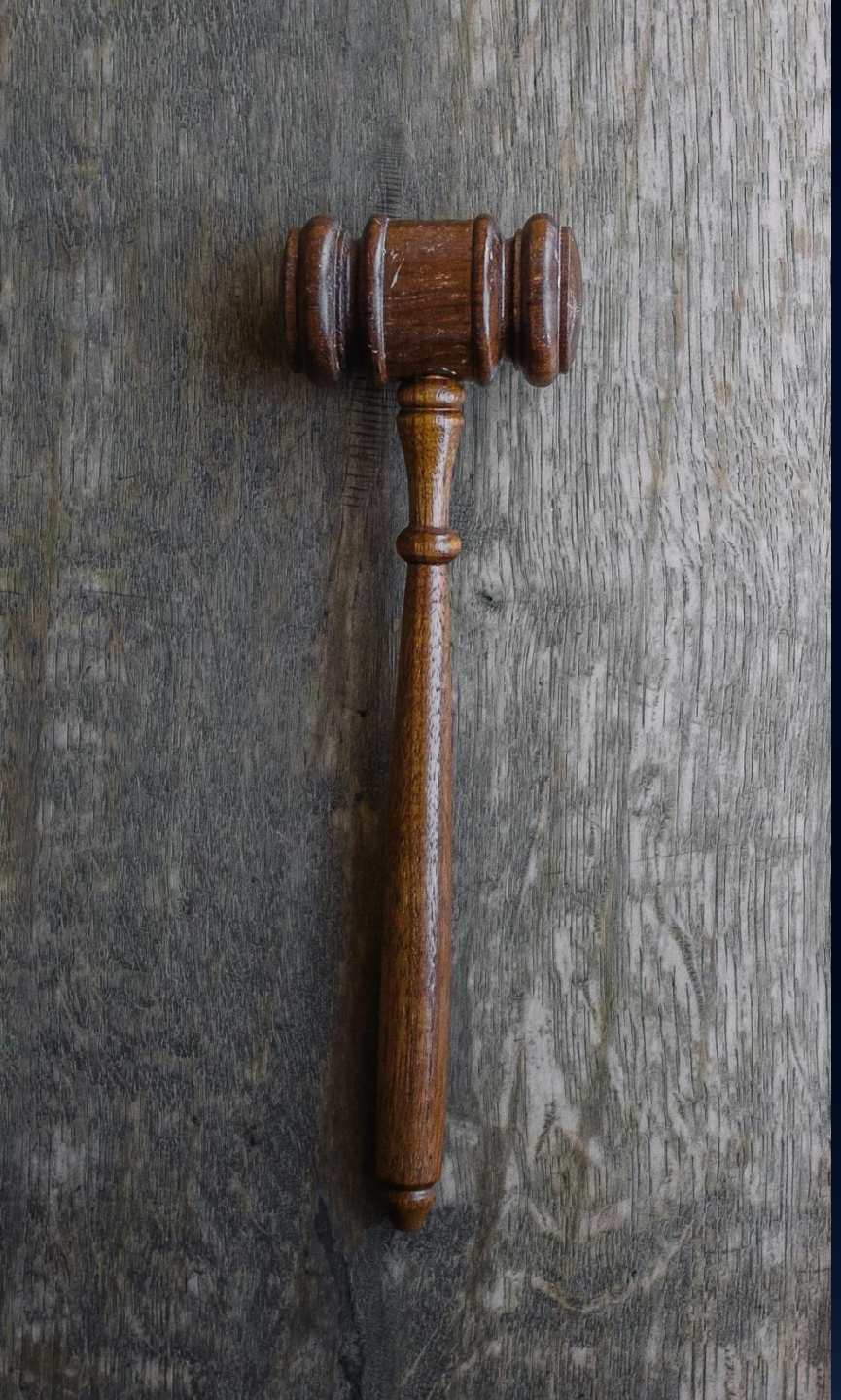
Zgodnie z treścią projektu Ustawy KSC, przedsiębiorca powinien zapewnić:

- ❑ 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, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, w szczególności:
  - *polityki szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego, w tym polityki tematyczne;*
  - *utrzymanie i bezpieczną eksploatację systemu informacyjnego,*
  - *bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu,*
  - *bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi z uwzględnieniem związków pomiędzy dostawcą sprzętu lub oprogramowania a podmiotem kluczowym lub podmiotem ważnym,*
  - *wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi oraz zapewniających poufność, integralność, dostępność i autentyczność informacji oraz planów awaryjnych umożliwiających odtworzenie systemu informacyjnego po katastrofie,*
  - *objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie ciągłym;*
  - *polityki i procedury oceny skuteczności środków technicznych i organizacyjnych*
  - *edukację z zakresu cyberbezpieczeństwa dla personelu podmiotu, w tym podstawowe zasady cyberhigieny,*
  - *polityki i procedury stosowania kryptografii, w tym szyfrowania,*

Podstawowe wymagania zgodności 2/2

Zgodnie z treścią projektu Ustawy KSC, przedsiębiorca powinien zapewnić (c.d.):

- ❑ zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi;
- ❑ zarządzanie incydentami;
- ❑ stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi, w tym:
  - *stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym,*
  - *regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi oraz poziomu krytyczności poszczególnych aktualizacji,*
  - *ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym,*
  - *niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub cyberzagrożeń;*
- ❑ stosowanie bezpiecznych środków komunikacji elektronicznej w ramach krajowego systemu cyberbezpieczeństwa uwzględniających uwierzytelnianie wieloskładnikowe.



Kary pieniężne

NIS2, podobnie jak RODO oraz DORA, przewiduje administracyjne kary pieniężne za niewłaściwe stosowanie przepisów.

Podmioty kluczowe

Administracyjne kary pieniężne w maksymalnej wysokości co najmniej **10 000 000 EUR** lub co najmniej **2 % łącznego rocznego światowego obrotu** w poprzednim roku obrotowym przedsiębiorstwa, do którego należy podmiot kluczowy, przy czym zastosowanie ma kwota wyższa.

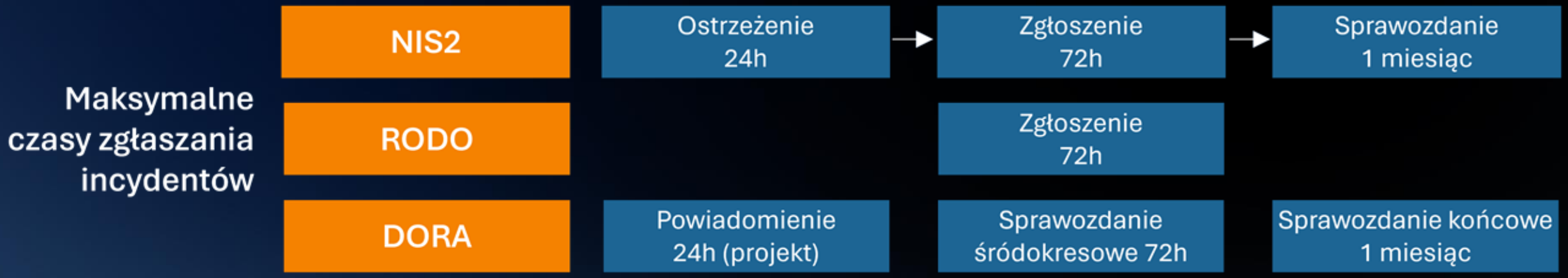
Podmioty ważne

Administracyjne kary pieniężne w maksymalnej wysokości co najmniej **7 000 000 EUR** lub **1,4 % łącznego rocznego światowego obrotu** w poprzednim roku obrotowym przedsiębiorstwa, do którego należy podmiot ważny, przy czym zastosowanie ma kwota wyższa.

Zarządzanie incydentami – jedno z kluczowych wymagań NIS2

Jednym z kluczowych wymagań NIS2, podobnie jak w RODO, jest wdrożenie procesu zarządzania incydentami poważnymi obejmującego zapobieganie, wykrywanie oraz reagowanie na incydenty. Proces ten powinien obejmować m.in. posiadanie udokumentowanego planu reagowania na incydenty bezpieczeństwa, który pozwoli na spełnienie wymagań określonych w Ustawie:

- zgłoszenie **wczesnego ostrzeżenia** o incydencie poważnym niezwłocznie, **nie później niż w ciągu 24 godzin** od momentu jego wykrycia, do właściwego CSIRT sektorowego;
- zgłoszenie incydentu niezwłocznie, **nie później niż w ciągu 72 godzin** od momentu jego wykrycia, do właściwego CSIRT sektorowego;
- przekazanie na wniosek CSIRT sektorowego, **sprawozdania okresowego** z obsługi incydentu poważnego;
- przekazanie właściwemu zespołowi CSIRT sektorowemu **sprawozdania końcowego** z obsługi incydentu poważnego, nie później niż **w ciągu miesiąca od dnia zgłoszenia**.



Co się składa na zgodność z NIS2?

NIS2 podobnie jak RODO można wdrożyć albo dobrze albo źle. Przykłady złego sposobu wdrożenia znane z RODO, a które odnoszą się także do NIS2, zazwyczaj sprowadzają się do dwóch skrajnych przypadków:

- **opracowanie procedur i instrukcji,** przyjęcie ich przez Zarząd oraz odłożenie na półkę;
- **zakup drogich technologii bezpieczeństwa** jako odpowiedzi na wymagania regulacyjne.

Oba wymienione podejścia są nieprawidłowe.

NIS2 podobnie jak RODO, DORA czy inne regulacje na pierwszym miejscu stawiają poprawnie wdrożony proces zarządzania ryzykiem.

To **zarządzanie ryzykiem ma być podstawą podejmowania dalszych decyzji** np. o zakupie zabezpieczeń technicznych. Dlatego też **pierwszym krokiem powinno być wdrożenie skutecznego systemu zarządzania ryzykiem** – który będzie spójny dla wszystkich regulacji – **RODO, NIS2, DORA oraz CER**.

Na tym fundamencie należy zbudować trzy filary:

- ✓ **odpowiednie procesy** (polityki, procedury, instrukcje – udokumentowane, wdrożone i testowane),
- ✓ **załoga** (odpowiednio dobrana, wyszkolona, dokształcana, zmotywowana),
- ✓ **technologia** (zapory, monitorowanie, kopie zapasowe, MFA, ZTNA i wiele innych).

INNERGO jest integratorem rozwiązań cyfrowej transformacji, działającym na rynku od 2009 roku. Współpracujemy z takimi dostawcami rozwiązań z obszaru IT, jak Apple, Ascom, Alcatel Lucent Enterprise Cisco, Dell, HPE, HPE Aruba Networking, Lenovo, Nokia, Nokia, Fortinet, Check Point, Samsung, Yubico.

Dlaczego warto skorzystać z usług INNERGO przy wdrażaniu NIS2?

Posiadamy odpowiednią wiedzę i doświadczenie we wdrażaniu i utrzymaniu zaawansowanych technologicznie systemów IT, przy instalacji i utrzymaniu których zawracamy istotną uwagę aby korzystanie z nich jak najmniej narażało organizację na zewnętrzne zagrożenia.

Sami jako firma dbamy o odpowiedni poziom kompetencji naszych pracowników. Mamy wdrożone ISO 27001. Bezpieczeństwo firmy jest kluczowe w naszej działalności. Szczególnie, że prowadzimy również tzw. projekty specjalne. Nasze urządzenia zarządzane są poprzez system Mobile Device Management. Zresztą jesteśmy autoryzowanym partnerem takich firm jak Jamf, Kandji czy VMWare Workspace One.

Mirosław Musiał, Członek Zarządu INNERGO.

- ❑ Nie wiesz w jakim stopniu Twoja organizacja jest już przygotowana do NIS2?
- ❑ Uważasz, że wyzwaniem jest przygotowanie Twojej organizacji do NIS2, bo nie masz odpowiednich zasobów?
- ❑ Zmagasz się ze spełnieniem rygorystycznych wymagań dotyczących cyberbezpieczeństwa?
- ❑ Potrzebujesz zweryfikować swoje systemy informatyczne pod kątem zgodności z NIS2?
- ❑ Nie wiesz jak odpowiednio przeszkolić pracowników i zweryfikować ich wiedzę?
- ❑ Czy masz procedurę bezpiecznego wdrożenia i pożegnania pracownika (onboarding i offboarding)?
- ❑ Masz rozwiązania zapewniające bezpieczny dostęp do komputerów i telefonów, tylko upoważniony pracownikom?
- ❑ Nie wiesz na ile Twoja organizacja jest przygotowana na niedostępność lub awarie krytyczne rozwiązań, z których korzystacie?

Możemy Cię w tym wesprzeć.
Jesteśmy integratorem rozwiązań cyfrowej transformacji z ponad 15 letnim doświadczeniem w obszarze cyberbezpieczeństwa i sieci, posiadamy wiedzę i rozwiązania, które pomogą Ci spełnić wymagania NIS2.
Wesprzemy cię w przeprowadzeniu analizy ryzyk oraz identyfikacji tych krytycznych dla Twojej organizacji a także przedstawiamy odpowiednie rozwiązania

Skontaktuj się z nami pisząc na odkrywaj@innergo.pl
Ekspert INNERGO skontaktuje się z Tobą aby indywidualnie dopasować najlepsze rozwiązanie dla Twojej organizacji.

Ty wiesz czego potrzebujesz, my wiemy jak to zrealizować.
INNERGO odpowiedzialny partner Twojej cyfrowej transformacji.

INNERGO.

Potrzebujesz wsparcia przy wdrożeniu NIS2?

Zapraszamy do współpracy.

Napisz do nas na odkrywaj@innergo.pl

INNERGO.

polski kapitał	100%
rok założenia	2009
pracownicy	160 +
zespół techniczny	60+

1	własny magazyn centralny w Krośnie
3	lokalizacje serwisowe + stoki u klientów
200+	umowy serwisowe i utrzymaniowe
24/7 8/5	usługi serwisowe

INNERGO.

GŁÓWNE OBSZARY SPECJALIZACJI

Centra danych

Pełne modernizacje serwerowni i obiektów Data Center

Projektowanie i budowa chmury hybrydowej

Wsparcie w utrzymaniu

Nowoczesne miejsce pracy

Rozwiązania sprzętowo-aplikacyjne dopasowane do pracy hybrydowej

Rozwiązania klasy Mobile Device Management

Device as a Service z zapewnieniem SLA

Wydajne sieci IT

Budowa niezawodnych sieci IT do transmisji danych krytycznych oraz komunikacji głosowej

Sieci dedykowane do monitoringu

Systemy medyczne

Rozwiązania i oprogramowanie healthcare klasy CIS dla bloków operacyjnych oraz Oddziałów Intensywnej Terapii

Systemy przyzywowe

Prywatne sieci 5G

Wdrażanie prywatnych sieci mobilnych 5G, zapewniających szybką, niezawodną i bezpieczną komunikację na potrzeby wewnętrzne i przemysłu 4.0

INNERGO.

PARTNERZY, Z KTÓRYMI REALIZUJEMY PROJEKTY DLA NASZYCH KLIENTÓW

Premium Business Partner

NOKIA

Alcatel·Lucent Enterprise

HPE

HPE aruba networking

ascom

FORTINET

CISCO

NUTANIX

DELL

yubico

SAMSUNG

jamf

Rynek i partnerzy nas doceniają

HPE Networking Solution Provider of the Year 2025

HPE Storage Partner Roku 2025

Best Project Alcatel-Lucent Enterprise na Connex 24

Partner Roku HPE Aruba Networking

Diamentowa Tarcza KBP 2026

INNERGO.

ODPOWIEDZIALNY PARTNER TWOJEJ CYFROWEJ TRANSFORMACJI

ZAUFANIE

Zaufanie to fundament
każdej trwałej relacji

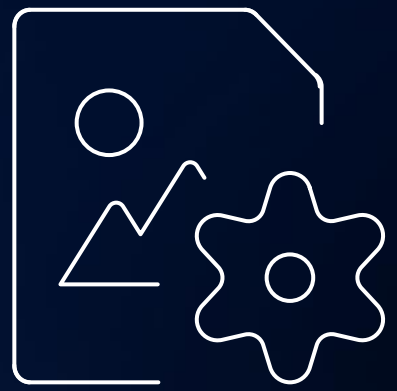
ODPOWIEDZIALNOŚĆ

Jesteśmy odpowiedzialni
za to, co robimy i jak to robimy

WSPÓŁPRACA

Współpraca oparta na zaufaniu
buduje trwałe relacje

INNERGO.



Ty wiesz, czego potrzebujesz,
my wiemy, jak to zrealizować

#odkrywajINNERGO