NIS2 i KSC w praktyce

Przewodnik wdrożeniowy dla organizacji

Wojciech Ciemski, Bartłomiej Wieczorek

Helion

Redaktor prowadzący: Małgorzata Kulik

Projekt okładki: Studio Gravite/Olsztyn
Obarek, Pokoński, Pazdrijowski, Zaprucki

Grafika na okładce została wykorzystana za zgodą AdobeStock.com.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
helion.pl/user/opinie/nis2pr
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-289-3286-9

Printed in Poland.

Spis treści

Rozdział 3.

Identyfikacja Twojej organizacji w kontekście NIS2 i KSC

KRYTERIA SEKTOROWE (RODZAJ PROWADZONEJ DZIAŁALNOŚCI)

Pierwszym krokiem jest sprawdzenie, czy organizacja prowadzi działalność wskazaną w załączniku nr 1 albo nr 2 do ustawy o KSC. To właśnie te załączniki decydują w polskim porządku prawnym o tym, które rodzaje działalności wchodzą do zakresu regulacji. Ustawa rozróżnia w tym zakresie **sektory kluczowe** i **sektory ważne**, a analiza dotyczy nie tylko przedsiębiorców, ale również wskazanych w ustawie **podmiotów publicznych** oraz innych jednostek niebędących przedsiębiorcami.

- **Sektory kluczowe (załącznik nr 1 do ustawy).** Ich zakłócenie może mieć szczególnie istotny wpływ na funkcjonowanie państwa, gospodarki i bezpieczeństwo publiczne. Zaliczamy do nich m.in.:
  - Energię — w tym działalność w obszarze wydobywania kopalin, energii elektrycznej, ciepła, ropy i paliw, gazu oraz wodoru.
  - Transport — w szczególności transport lotniczy, kolejowy, wodny i drogowy.
  - Bankowość i infrastrukturę rynków finansowych.
  - Zdrowie.
  - Zaopatrzenie w wodę pitną.
  - Infrastrukturę cyfrową — m.in.: dostawców usług DNS, rejestry nazw domen najwyższego poziomu (TLD), podmioty świadczące usługi rejestracji nazw domen, dostawców chmury obliczeniowej, dostawców usług centrum przetwarzania danych, dostawców sieci dostarczania treści oraz dostawców usług zaufania.

  - Łączność elektroniczną — tj. przedsiębiorców komunikacji elektronicznej.
  - Zarządzanie usługami ICT — w szczególności dostawców usług zarządzanych oraz dostawców usług zarządzanych w zakresie cyberbezpieczeństwa.
  - Podmioty publiczne — ale wyłącznie te wskazane literalnie w załączniku nr 1 do ustawy.
  - Przestrzeń kosmiczną.
- **Sektory ważne (załącznik nr 2 do ustawy).** Są to sektory istotne z punktu widzenia funkcjonowania państwa i gospodarki, lecz objęte w ustawie kategorią **podmiotów ważnych**. Należą do nich m.in.:
  - Usługi pocztowe.
  - Inwestycje energetyki jądrowej.
  - Gospodarowanie odpadami.
  - Produkcja, wytwarzanie i dystrybucja chemikaliów.
  - Produkcja, przetwarzanie i dystrybucja żywności.
  - Produkcja wyrobów medycznych i wyrobów medycznych do diagnostyki *in vitro*.
  - Określone rodzaje produkcji przemysłowej wskazane w załączniku nr 2 do ustawy.
  - Dostawcy usług cyfrowych — ale w węższym znaczeniu ustawowym: internetowe platformy handlowe, wyszukiwarki internetowe oraz platformy sieci usług społecznościowych. Usługi chmurowe, centra danych, sieci dostarczania treści czy usługi zarządzane nie należą do tej grupy, ponieważ w ustawie zostały przypisane do sektorów kluczowych.
  - Badania naukowe — w szczególności organizacje badawcze oraz określone podmioty systemu szkolnictwa wyższego i nauki.
  - Podmioty publiczne wskazane w załączniku nr 2 do ustawy.

Jeśli żaden z sektorów lub rodzajów działalności z załącznika nr 1 czy nr 2 nie dotyczy danej organizacji, to co do zasady nie będzie ona objęta obowiązkami KSC. Jeżeli jednak organizacja działa w choć jednym z wymienionych obszarów, należy przejść do kolejnych kryteriów, aby określić status jako **podmiot kluczowy** lub **ważny**.

KRYTERIA WIELKOŚCIOWE (ROZMIAR PRZEDSIĘBIORSTWA)

Drugim krokiem identyfikacji jest ocena wielkości organizacji. Ustawa o KSC odwołuje się tutaj do definicji przedsiębiorstwa z załącznika I do rozporządzenia 651/2014/UE. Co do zasady:

- podmiot wskazany w załączniku nr 1 do ustawy, który przewyższa wymogi dla średniego przedsiębiorcy, jest podmiotem kluczowym;
- podmiot wskazany w załączniku nr 1 do ustawy, który spełnia wymogi dla średniego przedsiębiorcy, jest podmiotem ważnym, o ile ustawa nie zalicza go do kategorii kluczowej na podstawie reguły szczególnej;
- podmiot wskazany w załączniku nr 2 do ustawy, który spełnia wymogi dla średniego przedsiębiorcy lub je przewyższa, jest podmiotem ważnym.

Dla potrzeb praktycznej samooceny można przyjąć następujący podział:

- **Duże przedsiębiorstwo** — podmiot przewyższający wymogi dla średniego przedsiębiorcy w rozumieniu załącznika I do rozporządzenia 651/2014/UE.
- **Średnie przedsiębiorstwo** — podmiot spełniający wymogi dla średniego przedsiębiorcy w rozumieniu tego załącznika.
- **Małe przedsiębiorstwo** — podmiot spełniający wymogi dla małego przedsiębiorcy w rozumieniu tego załącznika.
- **Mikroprzedsiębiorstwo** — podmiot spełniający wymogi dla mikroprzedsiębiorcy w rozumieniu tego załącznika.

Trzeba przy tym pamiętać, że sama wielkość nie rozstrzyga wszystkiego. W KSC istnieje kilka kategorii, które są objęte ustawą niezależnie od wielkości albo według odrębnych reguł. Jeżeli status podmiotu zależy od wielkości, przesłanki uznania bada się według stanu na dzień sporządzenia sprawozdania finansowego. Ustawa przewiduje również wyjątek dla podmiotów, które spełniają kryteria wielkości wyłącznie ze względu na przedsiębiorstwa powiązane lub partnerskie, ale ich system informacyjny jest niezależny od systemów tych przedsiębiorstw albo nie świadczą usług wspólnie z nimi.

Podsumowując kryterium wielkości: jeśli Twoja organizacja działa w sektorze wskazanym w załączniku nr 1 albo nr 2, wielkość będzie bardzo często jednym z głównych kryteriów kwalifikacji, ale nie zawsze będzie kryterium wyłącznym. Dlatego przed końcowym wnioskiem trzeba jeszcze sprawdzić wyjątki i szczególne przypadki przewidziane w samej ustawie.

WYJĄTKI I SZCZEGÓLNE PRZYPADKI (ZNACZENIE ŚWIADCZONYCH USŁUG)

Od powyższych zasad istnieją wyjątki i reguły szczególne, które trzeba przeanalizować osobno, bo w praktyce to one najczęściej przesądzają o błędnej samoocenie:

- **Kwalifikowani dostawcy usług zaufania, dostawcy usług DNS, rejestry nazw domen najwyższego poziomu (TLD) oraz podmioty świadczące usługi rejestracji nazw domen** są podmiotami kluczowymi niezależnie od wielkości. Oznacza to, że nawet niewielki podmiot z tej kategorii nie wypada poza zakres ustawy tylko dlatego, że nie spełnia klasycznych progów wielkościowych.
- **Niekwalifikowani dostawcy usług zaufania** są podmiotami ważnymi, jeżeli są mikroprzedsiębiorcami, małymi przedsiębiorcami lub średnimi przedsiębiorcami. W praktyce nie można więc traktować wszystkich dostawców usług zaufania jednakowo: znaczenie ma to, czy mamy do czynienia z dostawcą kwalifikowanym, czy niekwalifikowanym.
- **Przedsiębiorcy komunikacji elektronicznej.** Co najmniej średni przedsiębiorca komunikacji elektronicznej jest podmiotem kluczowym, a mikroprzedsiębiorca lub mały przedsiębiorca komunikacji elektronicznej jest podmiotem ważnym. To bardzo istotna różnica względem uproszczonego podejścia, w którym mały operator bywa błędnie uznawany za podmiot znajdujący się poza zakresem ustawy.
- **Dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa.** Podmioty co najmniej małe są podmiotami kluczowymi. Nie można więc traktować MSSP (*Managed Security Service Provider*) wyłącznie jako zwykłego dostawcy usług cyfrowych lub zwykłej firmy IT. Z kolei dostawcy usług zarządzanych innych niż usługi zarządzane w zakresie cyberbezpieczeństwa podlegają ogólnym regułom dla działalności wskazanej w załączniku nr 1.
- **Podmioty lecznicze, które nie są przedsiębiorcami**, są podmiotami ważnymi, jeżeli zatrudniają od 50 do 249 osób, a podmiotami kluczowymi, jeżeli zatrudniają co najmniej 250 osób. W sektorze zdrowia nie można więc ograniczać analizy wyłącznie do statusu przedsiębiorcy.
- **Podmioty publiczne.** O ich statusie nie decyduje ogólna ocena ryzyka ani samo zakwalifikowanie organizacji do „administracji publicznej", lecz literalne wskazanie w załączniku nr 1 albo nr 2. W przypadku podmiotu publicznego pojęcie usługi oznacza także zadanie publiczne realizowane przez ten podmiot. Po stronie samorządu załącznik nr 1 obejmuje m.in. starostwa powiatowe oraz urzędy gmin zatrudniające co najmniej 50 osób, a załącznik nr 2 obejmuje samorządowe jednostki budżetowe, samorządowe zakłady budżetowe, samorządowe instytucje kultury oraz spółki wykonujące zadania o charakterze użyteczności publicznej, jeżeli realizują zadanie publiczne z wykorzystaniem systemów informacyjnych.
- **Podmioty krytyczne** są podmiotami kluczowymi niezależnie od wielkości.
- **Małe podmioty albo mikropodmioty o szczególnym znaczeniu.** Organ właściwy do spraw cyberbezpieczeństwa może, w drodze decyzji, uznać osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej za podmiot kluczowy lub ważny mimo niespełnienia standardowych przesłanek wielkościowych, jeżeli podmiot ten jest wskazany w załączniku nr 1 albo nr 2 i spełnia jedną z przesłanek

z art. 7l. Dotyczy to sytuacji, gdy podmiot jako jedyny świadczy usługę o kluczowym znaczeniu, zakłócenie jego usługi spowodowałoby poważne zagrożenie dla bezpieczeństwa państwa, porządku publicznego, obronności lub zdrowia publicznego, wywoływałoby ryzyko systemowe zaprzestania świadczenia usług przez inne podmioty kluczowe lub ważne albo usługa ma istotne znaczenie na poziomie wojewódzkim lub krajowym, lub dla co najmniej dwóch sektorów.

- **Państwowe osoby prawne.** Minister właściwy do spraw informatyzacji może uznać je, w drodze decyzji, za podmioty kluczowe w sektorze podmiotów publicznych, jeżeli realizują za pomocą systemu informacyjnego zadanie publiczne, którego zakłócenie powodowałoby poważne zagrożenie albo które ma istotne znaczenie na poziomie krajowym.
- **Dostawcy usług IT dla podmiotów regulowanych.** Firma technologiczna podlega ustawie tylko wtedy, gdy mieści się w jednym z ustawowych rodzajów podmiotów, np. jako dostawca chmury obliczeniowej, usługi centrum przetwarzania danych, sieci dostarczania treści, usług zarządzanych, usług zarządzanych w zakresie cyberbezpieczeństwa, internetowej platformy handlowej, wyszukiwarki internetowej albo platformy sieci usług społecznościowych. Sama rola dostawcy oprogramowania lub sprzętu nie wystarcza jeszcze do objęcia ustawą.
- **Podmioty wcześniej uznane za OUK.** Przedsiębiorstwa, które były operatorami usług kluczowych na gruncie dotychczasowej ustawy, stają się podmiotami kluczowymi z dniem wejścia w życie nowelizacji. Nie jest to jedynie prawdopodobieństwo ani domniemanie, lecz skutek wynikający wprost z przepisów przejściowych.

LISTA KONTROLNA — SAMOOCENA STATUSU NIS2/KSC

Poniżej przedstawiamy szczegółową listę kontrolną, która krok po kroku pozwoli ocenić, do której kategorii kwalifikuje się dana organizacja. Odpowiadając na pytania i zaznaczając spełnione kryteria, czytelnik może zdiagnozować swój status jako **podmiot kluczowy**, **podmiot ważny** lub **podmiot nieobjęty obowiązkami**.

SEKTOR DZIAŁALNOŚCI

Czy Twoja organizacja działa w którymś z następujących sektorów lub świadczy wymienione rodzaje usług? Zaznacz wszystkie pasujące opcje.

- Energia.
- Transport.
- Bankowość i infrastruktura rynków finansowych.
- Zdrowie.
- Zaopatrzenie w wodę pitną.
- Zbiorowe odprowadzanie ścieków.
- Infrastruktura cyfrowa (np.: DNS, TLD, rejestracja domen, chmura, centra danych, CDN, usługi zaufania).
- Łączność elektroniczna (przedsiębiorca komunikacji elektronicznej).
- Zarządzanie usługami ICT (usługi zarządzane, usługi zarządzane w zakresie cyberbezpieczeństwa).
- Podmioty publiczne.
- Przestrzeń kosmiczna.
- Usługi pocztowe.
- Inwestycje energetyki jądrowej.
- Gospodarowanie odpadami.
- Chemikalia.
- Żywność.
- Produkcja wyrobów medycznych i wyrobów medycznych do diagnostyki *in vitro*.
- Produkcja określona w załączniku nr 2 do ustawy.
- Dostawcy usług cyfrowych (internetowa platforma handlowa, wyszukiwarka internetowa, platforma sieci usług społecznościowych).
- Badania naukowe.
- Żadne z powyższych.

Interpretacja: jeśli żaden sektor nie został zaznaczony, to co do zasady Twoja organizacja nie podlega KSC. W przeciwnym razie przejdź do pytania 2. Pamiętaj przy tym, że polska ustawa posługuje się własnymi załącznikami, dlatego warto porównywać swój model działania właśnie z rodzajem podmiotu opisanym w załączniku nr 1 albo nr 2, a nie tylko z ogólnym opisem sektora.

WIELKOŚĆ ORGANIZACJI

Który z poniższych opisów najlepiej odpowiada wielkości Twojej organizacji?

- Podmiot przewyższa wymogi dla średniego przedsiębiorcy w rozumieniu załącznika I do rozporządzenia 651/2014/UE.
- Podmiot spełnia wymogi dla średniego przedsiębiorcy w rozumieniu załącznika I do rozporządzenia 651/2014/UE.
- Podmiot spełnia wymogi dla małego przedsiębiorcy w rozumieniu załącznika I do rozporządzenia 651/2014/UE.
- Podmiot spełnia wymogi dla mikroprzedsiębiorcy w rozumieniu załącznika I do rozporządzenia 651/2014/UE.

Interpretacja: jeżeli organizacja jest średnia albo większa i działa w sektorze z załącznika nr 1 lub nr 2, istnieje duże prawdopodobieństwo objęcia ustawą. Jeżeli jest mała albo mikro, nie oznacza to jeszcze automatycznie wyłączenia — trzeba sprawdzić pytanie 3, ponieważ ustawa przewiduje liczne wyjątki. Jeżeli organizacja nie jest przedsiębiorcą, także nie wolno poprzestać na tym kroku, bo w niektórych przypadkach ustawa wprowadza odrębne reguły, np. dla podmiotów leczniczych niebędących przedsiębiorcami i dla podmiotów publicznych.

SZCZEGÓLNE PRZYPADKI (ZNACZENIE USŁUG)

Sprawdź, czy dotyczą Cię dodatkowe warunki, które mogą wpływać na kwalifikację Twojej organizacji.

- Świadczysz kwalifikowane usługi zaufania, usługi DNS, prowadzisz rejestr nazw domen najwyższego poziomu (TLD) albo świadczysz usługi rejestracji nazw domen.
- Świadczysz niekwalifikowane usługi zaufania.
- Jesteś przedsiębiorcą komunikacji elektronicznej.
- Jesteś dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa.
- Jesteś podmiotem leczniczym, który nie jest przedsiębiorcą.
- Jesteś podmiotem krytycznym.
- Jesteś podmiotem publicznym wskazanym w załączniku nr 1 albo nr 2 do ustawy.
- Twoja organizacja była przed wejściem w życie nowelizacji operatorem usług kluczowych.

- Jesteś podmiotem z załącznika nr 1 albo nr 2, którego usługa ma szczególne znaczenie i może zostać objęta decyzją organu właściwego do spraw cyberbezpieczeństwa na podstawie art. 7l.
- Jesteś państwową osobą prawną realizującą zadanie publiczne o istotnym znaczeniu krajowym.

Interpretacja: każdy zaznaczony punkt ma istotne znaczenie dla końcowej kwalifikacji. Niektóre z tych okoliczności powodują objęcie ustawą niezależnie od wielkości, inne przesuwają podmiot z kategorii ważnej do kluczowej, a jeszcze inne wprowadzają odrębną ścieżkę kwalifikacji decyzją właściwego organu.

KWALIFIKACJA KOŃCOWA

Na podstawie powyższych odpowiedzi określ status swojej organizacji.

- **Podmiot kluczowy** — jeżeli prowadzisz działalność określoną w załączniku nr 1 i przewyższasz wymogi dla średniego przedsiębiorcy. Do tej kategorii należą też — niezależnie od wielkości albo na podstawie przepisów szczególnych — kwalifikowani dostawcy usług zaufania, dostawcy usług DNS, rejestry nazw domen najwyższego poziomu (TLD), podmioty świadczące usługi rejestracji nazw domen, podmioty krytyczne, podmioty publiczne wskazane w załączniku nr 1, przedsiębiorcy komunikacji elektronicznej co najmniej średni, dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa co najmniej mali, podmioty lecznicze niebędące przedsiębiorcami zatrudniające co najmniej 250 osób, operatorzy obiektów energetyki jądrowej, państwowe osoby prawne uznane decyzją na podstawie art. 7m, podmioty uznane decyzją organu właściwego do spraw cyberbezpieczeństwa na podstawie art. 7l za prowadzące działalność z załącznika nr 1 oraz podmioty będące wcześniej operatorami usług kluczowych. Wniosek: podmiot kluczowy to nie tylko „duża firma z sektora krytycznego", lecz również szereg kategorii objętych ustawą z mocy szczególnej reguły.
- **Podmiot ważny** — jeżeli prowadzisz działalność określoną w załączniku nr 1 i spełniasz wymogi dla średniego przedsiębiorcy, ale nie wchodzisz do kategorii kluczowej na podstawie przepisu szczególnego, albo jeżeli prowadzisz działalność z załącznika nr 2 i spełniasz wymogi dla średniego przedsiębiorcy lub je przewyższasz. Do tej kategorii należą także niekwalifikowani dostawcy usług zaufania będący mikroprzedsiębiorcami, małymi przedsiębiorcami lub średnimi przedsiębiorcami, przedsiębiorcy komunikacji elektronicznej będący mikroprzedsiębiorcami lub małymi przedsiębiorcami, podmioty lecznicze niebędące przedsiębiorcami zatrudniające od 50 do 249 osób, podmioty publiczne wskazane w załączniku nr 2, określone podmioty niebędące przedsiębiorcami wskazane w załączniku nr 2, inwestorzy obiektów energetyki jądrowej, którzy uzyskali decyzję zasadniczą, oraz podmioty uznane decyzją organu właściwego

do spraw cyberbezpieczeństwa na podstawie art. 7l za prowadzące działalność z załącznika nr 2. Wniosek: podmiot ważny to nie tylko „średnia firma z sektora istotnego", ale także część podmiotów z załącznika nr 1 oraz szereg kategorii objętych przepisami szczególnymi.

- **Podmiot poza zakresem NIS2/KSC** — jeżeli Twoja organizacja nie prowadzi działalności określonej w załączniku nr 1 ani nr 2, nie podpada pod żadną z reguł szczególnych i nie została objęta decyzją organu właściwego do spraw cyberbezpieczeństwa. Poza ogólnym mechanizmem kwalifikacji pozostają też służby specjalne, a w przypadku podmiotów podległych ministrowi obrony narodowej lub nadzorowanych przez ministra obrony narodowej status wynika z odrębnych reguł i decyzji tego ministra. Wniosek: jeżeli nie mieścisz się w żadnym z ustawowych rodzajów podmiotu, nie ciąży na Tobie reżim ustawowy, choć nadal warto stosować adekwatne środki bezpieczeństwa.

UWAGI KOŃCOWE: SAMOOCENA STATUSU I DALSZE KROKI

Zgodnie z nowymi przepisami samoidentyfikacja nie kończy się na wewnętrznym ustaleniu, że organizacja „raczej podpada pod ustawę". Jeżeli organizacja spełnia przesłanki uznania za **podmiot kluczowy** albo **ważny**, musi przejść do dalszych działań wynikających już wprost z ustawy.

- **Dokumentuj wyniki analizy.** Jeżeli Twoja organizacja uzna, że jest podmiotem kluczowym lub ważnym, powinna zachować dokumentację tej oceny — w szczególności opis działalności, przyjętą kwalifikację sektorową, ocenę wielkości i wskazanie ewentualnych wyjątków ustawowych. Taka dokumentacja będzie przydatna przy wpisie do wykazu, aktualizacji danych lub w razie kontroli.
- **Zadbaj o wpis do wykazu.** Co do zasady podmiot kluczowy lub podmiot ważny składa wniosek o wpis do wykazu w terminie 6 miesięcy od dnia spełnienia przesłanek uznania za taki podmiot. Zmianę danych objętych wpisem zgłasza się w terminie 14 dni od dnia ich przekształcenia. Trzeba jednak pamiętać, że część kategorii jest wpisywana do wykazu z urzędu — dotyczy to w szczególności przedsiębiorców komunikacji elektronicznej, dostawców usług zaufania, podmiotów publicznych, podmiotów krytycznych oraz dotychczasowych operatorów usług kluczowych.
- **Sprawdź terminy przejściowe.** Podmioty, które spełniają przesłanki już w dniu wejścia w życie nowelizacji, realizują obowiązki z rozdziału 3 w terminie 12 miesięcy od dnia wejścia w życie ustawy, a podmioty kluczowe przeprowadzają pierwszy audyt w terminie 24 miesięcy od tego dnia. Wniosek o wpis do wykazu dla tych podmiotów składa się zgodnie z harmonogramem ogłoszonym przez ministra właściwego do spraw informatyzacji. Podmioty, które przed nowelizacją były operatorami usług kluczowych,

stają się podmiotami kluczowymi z dniem wejścia w życie ustawy, są wpisywane do wykazu z urzędu, a obowiązek zgłaszania incydentów poważnych według nowych zasad wdrażają w terminie 6 miesięcy od wejścia w życie ustawy.

- **Przygotuj się na realne obowiązki.** Ustalenie statusu to dopiero początek. Podmiot kluczowy lub ważny będzie musiał wdrożyć **system zarządzania bezpieczeństwem informacji** w systemach informacyjnych wykorzystywanych w procesach wpływających na świadczenie usługi, prowadzić wymaganą dokumentację, wyznaczyć osoby do kontaktu, zapewnić obsługę incydentów oraz przygotować się na odpowiedzialność kierownika podmiotu. **Kierownik podmiotu kluczowego lub ważnego** odpowiada za wykonywanie obowiązków z zakresu cyberbezpieczeństwa, podejmuje decyzje dotyczące systemu zarządzania bezpieczeństwem informacji, planuje środki finansowe, nadzoruje wykonanie zadań i przechodzi coroczne szkolenie. Osoby realizujące zadania z art. 8 i art. 11 muszą spełniać wymogi niekaralności za przestępstwa przeciwko ochronie informacji. Co do zasady obsługa **incydentu poważnego** obejmuje wczesne ostrzeżenie w terminie 24 godzin, zgłoszenie incydentu w terminie 72 godzin oraz sprawozdanie końcowe w terminie miesiąca, przekazywane do właściwego CSIRT sektorowego, ale ustawa przewiduje tu wyjątki — w szczególności dla podmiotu ważnego będącego podmiotem publicznym, dla dostawców usług zaufania oraz dla sektora bankowości i infrastruktury rynków finansowych. **Podmiot kluczowy** przeprowadza **audyt bezpieczeństwa** co najmniej raz na 3 lata, natomiast wobec podmiotu ważnego audyt zewnętrzny może zostać nakazany decyzją właściwego organu.
- **Pamiętaj o różnicach sektorowych.** Nie wszystkie obowiązki będą wyglądały identycznie w każdym sektorze. Podmiot ważny będący podmiotem publicznym nie stosuje pełnego modelu z art. 8 ust. 1, lecz system zarządzania bezpieczeństwem informacji zgodny z załącznikiem nr 4 do ustawy. Z kolei sektor bankowości i infrastruktury rynków finansowych podlega ustawie z istotnymi modyfikacjami, więc nie wolno automatycznie przenosić na niego wszystkich ogólnych reguł dotyczących systemu zarządzania bezpieczeństwem informacji i zgłaszania incydentów.

Ta lista kontrolna i opis kryteriów mają charakter instruktażowy i praktyczny. Pozwalają zorientować się, czy Twoja organizacja znajduje się w zakresie **KSC 2026** oraz czy bliżej jej do kategorii **podmiotu kluczowego**, **podmiotu ważnego** czy **podmiotu pozostającego poza zakresem regulacji**. Kluczowe jest jednak to, aby punktem odniesienia była przede wszystkim ustawa o KSC i jej załączniki, bo to one — wraz z przepisami szczególnymi art. 5, art. 7l i art. 7m — rozstrzygają o statusie podmiotu. Dzięki temu można podjąć odpowiednie działania przygotowawcze oparte na rzeczywistych, krajowych wymogach prawnych, a nie na uproszczonych analogiach do samej dyrektywy.

Nie taka dyrektywa straszna, jak ją malują — o ile ma się dostęp do odpowiedniej wiedzy

Dyrektywa NIS2 to regulacja unijna, która została wdrożona do polskiego prawa w 2026 roku nowelizacją ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC). Celem jest zwiększenie poziomu cyberbezpieczeństwa państw należących do Unii Europejskiej. W praktyce sektory, które są objęte dyrektywą, to nie tylko podmioty związane z władzami lub administracją publiczną, ale też wiele firm prywatnych i instytucji. Wiąże się to między innymi z koniecznością uporządkowania odpowiedzialności, przejrzenia modelu zarządzania ryzykiem, zaktualizowania dokumentacji, stworzenia skutecznego procesu obsługi incydentów, uporządkowania relacji z dostawcami i przygotowania kierownictwa do realnej odpowiedzialności za obszar cyberbezpieczeństwa.

Jeśli jesteś osobą odpowiedzialną za zastosowanie dyrektywy NIS2 w firmie, a także zrozumienie, uporządkowanie i wdrożenie wymagań wynikających z nowych regulacji w ramach KSC — ten poradnik powstał właśnie dla Ciebie. Został pomyślany tak, by móc z niego korzystać roboczo, zadaniowo i w odniesieniu do konkretnego problemu.

Ta książka pozwoli Ci:

- **Uporządkować wiedzę o tym, kogo dotyczą nowe przepisy i jak rozpoznać status organizacji**
- **Szybko wrócić do kluczowych zagadnień**
- **Bez problemu znaleźć praktyczne wyjaśnienie obowiązków związanych z ryzykiem, incydentami, dokumentacją, dostawcami, monitoringiem i audytem**
- **W prosty sposób odszukać najważniejsze terminy, wyjątki i punkty krytyczne, które najczęściej decydują o powodzeniu albo niepowodzeniu wdrożenia**
- **Uzyskać solidne merytoryczne wsparcie w rozmowie z kierownictwem, działem IT, działem prawnym, audytem i dostawcami**
- **Mieć stały dostęp do przykładowych wzorów dokumentów, których można użyć jako podstawy do przygotowania własnej dokumentacji**

Helion

helion.pl

HELION S.A.
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl

KOD KORZYŚCI
Sięgnij po więcej!

ISBN 978-83-289-3286-9

9 788328 932869

Cena: 89,00 zł