NIS2 i ustawa o krajowym systemie cyberbezpieczeństwa (UKSC)

Miesiąc Prawa EY Law

The better the question.
The better the answer.
The better the world works.

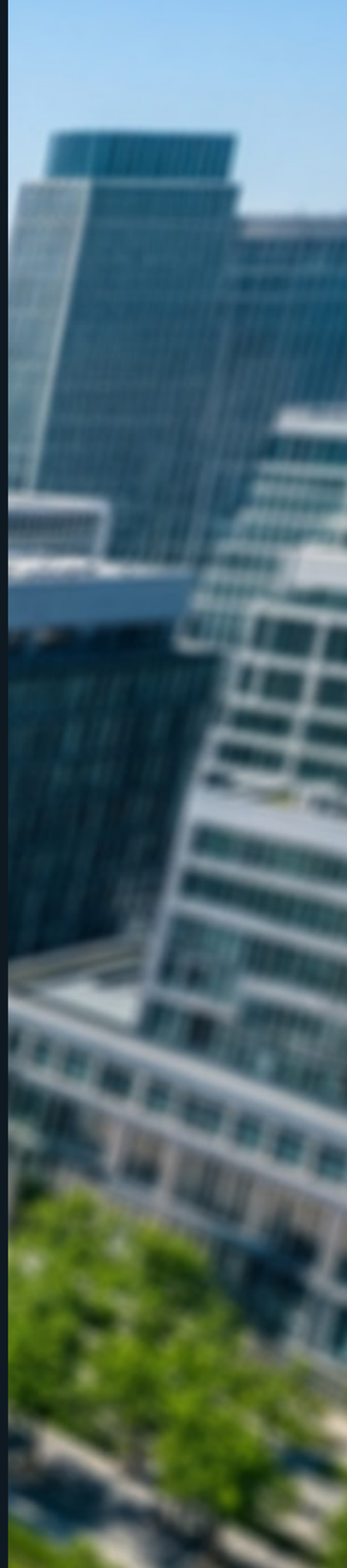
EY
Shape the future with confidence

Czy Twoja organizacja jest gotowa na obowiązki z zakresu cyberbezpieczeństwa?

3 października 2026 r. mija termin samorejestracji podmiotów objętych ustawą o krajowym systemie cyberbezpieczeństwa.

Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (UKSC), wdrażająca dyrektywę NIS2, znacząco rozszerzyła katalog podmiotów objętych obowiązkami cyberbezpieczeństwa. W praktyce przepisy obowiązujące od 3 kwietnia 2026 roku dotyczą nie tylko sektorów w przeszłości uznawanych za infrastrukturę krytyczną, lecz także wielu przedsiębiorstw produkcyjnych, technologicznych, logistycznych, spożywczych, chemicznych oraz usługowych.

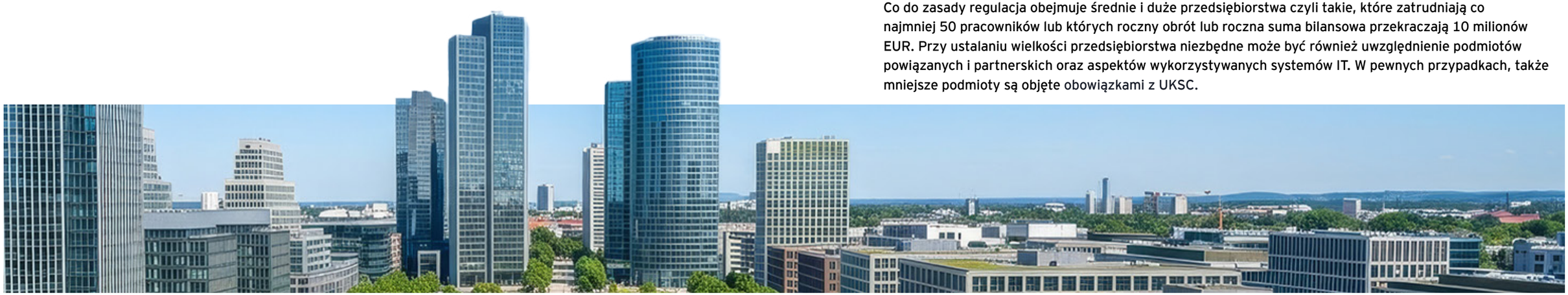
Brak działań może oznaczać nie tylko ryzyko sankcji administracyjnych, ale również osobistą odpowiedzialność członków kierownictwa za niewypełnienie obowiązków wynikających z UKSC.



1 NIS2 i UKSC w 60 sekund

Jeżeli Twoja organizacja podlega przepisom UKSC, może być zobowiązana do:

1. Przeprowadzenia samoidentyfikacji i rejestracji w wykazie KSC
2. Wdrożenia środków zarządzania ryzykiem cyberbezpieczeństwa
3. Raportowania określonych incydentów cyberbezpieczeństwa
4. Zarządzania ryzykiem związanym z dostawcami ICT
5. Zapewnienia ciągłości działania i odtwarzania po awarii
6. Prowadzenia wymaganej dokumentacji bezpieczeństwa
7. Szkolenia kierownictwa i pracowników
8. Przeprowadzania audytów bezpieczeństwa



2 Kogo dotyczą nowe przepisy?

Objęcie organizacji wymogami UKSC zależy przede wszystkim od:

Rodzaju prowadzonej działalności.	Sektora, w którym działa przedsiębiorstwo.	Wielkości przedsiębiorstwa.	W niektórych przypadkach także relacji grupowych, powiązań kapitałowych oraz wspólnych systemów IT w grupie.

Przepisy UKSC obejmują podmioty działające m.in. w sektorach:

- Energetycznym
- Transportowym
- Finansowym
- Ochrony zdrowia
- Infrastruktury cyfrowej
- Usług cyfrowych
- Usług pocztowych i kurierskich
- Gospodarowania odpadami
- Produkcji żywności
- Produkcji chemicznej
- Produkcji farmaceutycznej
- Produkcji urządzeń i wyrobów przemysłowych

Co do zasady regulacja obejmuje średnie i duże przedsiębiorstwa czyli takie, które zatrudniają co najmniej 50 pracowników lub których roczny obrót lub roczna suma bilansowa przekraczają 10 milionów EUR. Przy ustalaniu wielkości przedsiębiorstwa niezbędne może być również uwzględnienie podmiotów powiązanych i partnerskich oraz aspektów wykorzystywanych systemów IT. W pewnych przypadkach, także mniejsze podmioty są objęte obowiązkami z UKSC.

3 Najważniejsze terminy

3 kwietnia 2028 r.

Termin na przeprowadzenie pierwszego obowiązkowego audytu dla podmiotów kluczowych

3 kwietnia 2027 r.

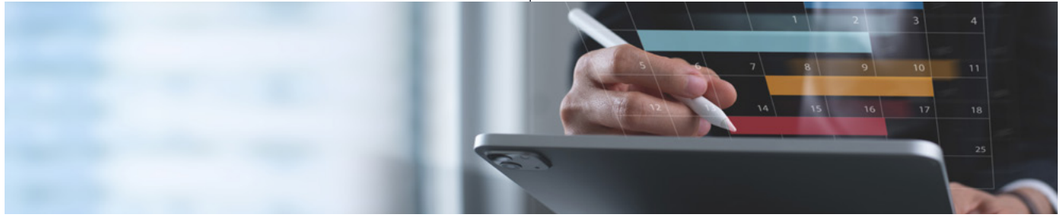
Termin wdrożenia wymaganych środków zarządzania ryzykiem oraz rozpoczęcia pełnego korzystania z systemu S46 przez podmioty kluczowe i ważne

3 października 2026 r.

Termin dokonania samoidentyfikacji oraz rejestracji organizacji objętych regulacją – podmioty kluczowe i ważne powinny do tej daty zgłosić się do wykazu KSC

3 kwietnia 2026 r.

Wdrożenie NIS2 w Polsce - wejście w życie nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa



4 Najczęstsze pytania przedsiębiorców

Czy NIS2 dotyczy wyłącznie infrastruktury krytycznej?	Nie. Zakres podmiotów objętych przepisami został znacząco rozszerzony. W praktyce regulacja może dotyczyć także wielu przedsiębiorstw prywatnych działających w sektorach produkcyjnych, logistycznych, cyfrowych, spożywczych czy chemicznych, a także w branży IT.
Czy przedsiębiorca musi sam ustalić, czy podlega przepisom?	Tak. Co do zasady organizacja samodzielnie dokonuje kwalifikacji swojego statusu oraz rejestracji do wykazu KSC.
Czy przynależność do grupy kapitałowej ma znaczenie?	Tak. W wielu przypadkach przy ocenie wielkości przedsiębiorstwa należy uwzględnić także podmioty powiązane i partnerskie, co może wpływać na objęcie przepisami UKSC. Istotne może okazać się także wspólne korzystanie z systemów teleinformatycznych w ramach grupy kapitałowej.
Czy certyfikat ISO 27001 oznacza zgodność z UKSC?	Nie. Certyfikacja może wspierać spełnienie części wymagań, jednak nie zastępuje analizy obowiązków wynikających bezpośrednio z UKSC.
Czy odpowiedzialność spoczywa wyłącznie na dziale IT?	Nie. UKSC przewiduje bezpośrednią i osobistą odpowiedzialność kierownictwa za nadzór nad wykonywaniem obowiązków cyberbezpieczeństwa. Zarząd powinien aktywnie uczestniczyć w zarządzaniu ryzykiem oraz nadzorować wdrożenie odpowiednich środków bezpieczeństwa, a także zapewnić alokację dostatecznych środków na wdrożenie zabezpieczeń.
Czy można korzystać z usług zewnętrznych dostawców cyberbezpieczeństwa?	Tak. Część obowiązków może być wykonywana przy wsparciu podmiotów zewnętrznych, jednak odpowiedzialność za zgodność z regulacją pozostaje po stronie przedsiębiorcy.
Czy wystarczy, że działalność objęta UKSC jest prowadzona na niewielką skalę, aby uniknąć kwalifikacji jako podmiot kluczowy lub podmiot ważny?	Nie zawsze. W wielu sektorach sama skala działalności nie ma znaczenia – pomimo marginalnego charakteru prowadzonej działalności dla przedsiębiorstwa, będzie to działalność podlegająca pod UKSC. Przykładowo, przedsiębiorstwo posiadające koncesję na dystrybucję energii lub gazu może podlegać UKSC nawet wtedy, gdy działalność ta odpowiada za mniej niż 1% przychodów spółki lub jest działalnością poboczną względem podstawowego biznesu.
Czy działalność pomocnicza lub uboczna może powodować podleganie pod UKSC?	Tak. W odniesieniu do wielu sektorów przepisy UKSC nie rozróżniają działalności głównej i pomocniczej. Jeżeli działalność wskazana w ustawie jest faktycznie wykonywana, może ona stanowić podstawę objęcia organizacji reżimem UKSC, nawet gdy jest pobocznym elementem działalności przedsiębiorstwa.

Administruję systemami IT lub bazami danych dla spółki z mojej grupy kapitałowej. Czy UKSC może mnie dotyczyć?	Tak. Przepisy nie przewidują ogólnego wyłączenia dla usług świadczonych wewnątrz grupy kapitałowej. Jeżeli spółka wykonuje aktywną administrację systemami informacyjnymi, bazami danych, kopiami zapasowymi lub innymi systemami ICT na rzecz innego podmiotu z grupy, może zostać uznana za dostawcę usług zarządzanych objętego UKSC.
Czy brak klientów oznacza automatycznie brak podlegania UKSC?	Niekoniecznie. Znaczenie może mieć nie tylko faktyczne wykonywanie działalności, ale również posiadane zezwolenia, koncesje lub sposób organizacji działalności. W niektórych przypadkach zaprzestanie wykonywania działalności oraz odpowiednie działania formalne mogą ograniczać ryzyko kwalifikacji, jednak wymaga to indywidualnej analizy.
Czy fakt, że działam wyłącznie w modelu B2B, wyłącza mnie spod UKSC?	Co do zasady - nie. Przepisy nie różnicują sytuacji przedsiębiorców świadczących usługi dla konsumentów i dla innych przedsiębiorców. Relacja B2B nie stanowi podstawy wyłączenia z zakresu stosowania UKSC.

5 Dlaczego warto działać już teraz?

W praktyce największym wyzwaniem jest nie samo wdrożenie wymagań technicznych, ale:

- ustalenie statusu regulacyjnego organizacji;
- analiza grupy kapitałowej i powiązań;
- identyfikacja systemów objętych obowiązkami;
- określenie dostawców krytycznych z perspektywy cyberbezpieczeństwa;
- przygotowanie kumentacji;
- zaplanowanie budżetu i odpowiedzialności po stronie zarządu.

Im później organizacja rozpocznie działania, tym większe ryzyko problemów z dochowaniem ustawowych terminów.

Compliance checklist

Krok 1. Ustal status swojej organizacji

- ☐ przeprowadź kwalifikację podmiotu;
- ☐ przeanalizuj powiązania grupowe i kapitałowe;
- ☐ ustal właściwy organ nadzoru;
- ☐ dokonaj rejestracji w wykazie KSC;
- ☐ przygotuj procedurę aktualizowania zgłoszeń.

Krok 2. Zbuduj model zarządzania cyberbezpieczeństwem

- ☐ wdróż system zarządzania bezpieczeństwem informacji;
- ☐ określ role i odpowiedzialności;
- ☐ wyznacz osoby odpowiedzialne za kontakty z organami;
- ☐ określ proces zarządzania ryzykiem;
- ☐ zaangażuj zarząd w proces nadzoru.

Krok 3. Zapewnij gotowość operacyjną

- ☐ wdróż procedury zarządzania incydentami;
- ☐ przygotuj proces raportowania przez S46;
- ☐ opracuj plany BCP i DRP;
- ☐ zweryfikuj proces tworzenia kopii zapasowych;
- ☐ wdróż MFA i odpowiednie mechanizmy kontroli dostępu.

Krok 4. Zarządzaj ryzykiem dostawców

- ☐ zinwentaryzuj dostawców ICT;
- ☐ określ dostawców krytycznych;
- ☐ przeprowadź ocenę ryzyka dostawców;
- ☐ zaktualizuj umowy i procedury zakupowe.

Krok 5. Audyty i szkolenia

- ☐ przeszkol zarząd;
- ☐ przeprowadź szkolenia pracowników;
- ☐ opracuj harmonogram audytów;
- ☐ przygotuj plan testowania bezpieczeństwa.

6 Jak możemy pomóc?

Wspieramy klientów na każdym etapie przygotowań do UKSC:

Nasze doświadczenie obejmuje projekty realizowane dla podmiotów z sektorów energetycznego, produkcyjnego, gospodarowania odpadami, usług cyfrowych oraz organizacji działających w międzynarodowych grupach kapitałowych.

Zapraszam do kontaktu!

Joanna Ostrowska

Partner | Leader of Digital, Cyber & Data Team, EY Law

joanna.ostrowska@pl.ey.com

Gabriela Sacha

Manager | Digital, Cyber & Data Team, EY Law

gabriela.sacha@pl.ey.com

Agata Wilska

Project Manager | Digital, Cyber & Data Team, EY Law

agata.wilska@pl.ey.com

Zobacz nasz webcast o kwalifikacji podmiotów na gruncie NIS2 i UKSC:

20 minut o NIS2: Kwalifikacja na gruncie NIS2 i UKSC | EY - Polska

EY | Building a better working world

Celem działalności EY jest budowanie lepiej funkcjonującego świata poprzez wspieranie klientów, pracowników, społeczeństwa i planety w tworzeniu trwałych wartości oraz budowanie zaufania na rynkach kapitałowych.

Korzystając z danych, sztucznej inteligencji oraz zaawansowanych technologii, zespoły EY pomagają klientom odważnie kształtować przyszłość i znajdować odpowiedzi na obecne i przyszłe wyzwania.

EY świadczy kompleksowe usługi w zakresie audytu, doradztwa, podatków, strategii i transakcji. Dzięki wiedzy sektorowej, globalnie połączonym, multidyscyplinarnym zespołom i różnorodnym partnerstwom EY może świadczyć usługi w ponad 150 krajach.

EY w Polsce to prawie 4000 specjalistów pracujących w 8 miastach: Warszawie, Gdańsku, Katowicach, Krakowie, Łodzi, Poznaniu, Wrocławiu i Rzeszowie. Działając na polskim rynku, co roku EY doradza tysiącom firm, zarówno małym i średnim przedsiębiorstwom, jak i największym korporacjom. Tworzy unikatowe analizy, dzieli się wiedzą, integruje środowisko przedsiębiorców oraz angażuje się społecznie.

Wszystko po to, aby z odwagą kształtować przyszłość.

ey.com/pl

Designed by EY Creative Services Warsaw, Poland.