Raport zgodności

Przykładowy Operator sp. z o.o. · Podmiot kluczowy · stan na 2.08.2026

Narzędzie samooceny ITORO. Dokument nie stanowi audytu w rozumieniu art. 15 ustawy o KSC ani opinii prawnej.

Podsumowanie dla zarządu

STATUS PODMIOTU

Podmiot kluczowy

ustawa o KSC | art. 5 ust. 1 pkt 2 ustawy o KSC (przedsiębiorca komunikacji elektronicznej co najmniej spełniający wymogi dla średniego przedsiębiorcy) | s. 4

STOPIEŃ PRZYGOTOWANIA

61%

Dojrzałość 2.4 przy poziomie docelowym 4

OBOWIĄZKI FORMALNE

52/105

15 niewykonanych, 38 w toku

Najbliższe terminy ustawowe

- **3.10.2026** (za 62 dni) — Wniosek o wpis do wykazu podmiotów kluczowych i ważnych
- **3.04.2027** (za 244 dni) — Wdrożenie obowiązków rozdziału 3 ustawy o KSC
- **3.04.2027** (za 244 dni) — Rozpoczęcie korzystania z Systemu S46

Największe luki

1. 7. Polityki i procedury służące ocenie skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie — dojrzałość 2.0 wobec docelowej 4, priorytet krytyczny
2. 1. Polityka bezpieczeństwa sieci i systemów informatycznych — dojrzałość 2.1 wobec docelowej 4, priorytet wysoki
3. Bezpieczeństwo fizyczne i środowiskowe — dojrzałość 2.3 wobec docelowej 4, priorytet wysoki
4. Monitorowanie w trybie ciągłym — dojrzałość 2.3 wobec docelowej 4, priorytet wysoki
5. Edukacja personelu i cyberhigiena — dojrzałość 2.3 wobec docelowej 4, priorytet wysoki

Organy uzyskują uprawnienie do nakładania kar pieniężnych od **3.04.2028** (nowelizacja KSC | art. 35 ustawy nowelizującej | s. 79). Do tego czasu ryzyko finansowe nie jest jeszcze wymagalne, natomiast obowiązki wdrożeniowe biegną już teraz — termin realizacji obowiązków rozdziału 3 upływa 3 kwietnia 2027 r.

Odpowiedzialność finansowa

Podmiot

Jak powstaje ten pułap — dwa różne kroki

1. **Pułap wyznacza ustawa, nie organ**
   Porównuje się dwie wartości: sztywną kwotę w euro oraz procent przychodu z poprzedniego roku obrotowego. Wyższa z nich staje się górną granicą. Organ nie wybiera między nimi — wynika to wprost z przepisu.
   ustawa o KSC | art. 73 ust. 3 ustawy o KSC | s. 31
2. **Kwotę w granicach pułapu ustala organ**
   Dopiero tutaj jest uznanie. Organ bierze pod uwagę wagę i czas naruszenia, wcześniejsze naruszenia oraz wysokość przychodu i możliwości finansowe. Może też odstąpić od kary przy znikomej wadze naruszenia.
   ustawa o KSC | art. 76a ust. 1 ustawy o KSC | nowelizacja KSC s. 70,
   ustawa o KSC | art. 53 ust. 12 ustawy o KSC | s. 26

Pułap może wielokrotnie przewyższać roczny przychód — tak samo jak w RODO. Nie znaczy to, że taka kara zostanie nałożona: to górna granica, a nie kwota oczekiwana.

Ustawowy pułap kary pieniężnej wynosi **43 000 000 zł**. Przeważa limit kwotowy: równowartość 10 mln EUR jest wyższa niż 2 % przychodu.

- Wariant procentowy: 480 000 zł
- Wariant kwotowy: 43 000 000 zł (kurs 4.3 zł/EUR)
- Ustawowe minimum: 20 000 zł

Ustawowy pułap przewyższa roczny przychód podmiotu 1.8-krotnie. Kara w tej wysokości byłaby nie do pogodzenia z art. 76a ust. 1, który nakazuje organowi uwzględnić wysokość przychodu i możliwości finansowe podmiotu. To górna granica ustawowa, a nie kara oczekiwana.

Miarkowanie kary — ustawa o KSC | art. 76a ust. 1 ustawy o KSC | nowelizacja KSC s. 70

Organ właściwy, podejmując decyzję o nałożeniu kary pieniężnej i ustalając jej wysokość, uwzględnia odpowiednio kryteria określone w art. 53 ust. 12 oraz wysokość przychodu uzyskanego z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary pieniężnej i możliwości finansowe podmiotu.

Kryteria z art. 53 ust. 12:

- waga naruszenia i znaczenie naruszonych przepisów — za poważne uznaje się m.in. naruszenie powtarzające się, niezgłoszenie lub nieobsłużenie incydentu poważnego, nieusunięcie uchybień wbrew nakazowi, utrudnianie audytu lub monitorowania, podawanie nieprawdziwych informacji
- czas trwania naruszenia
- wcześniejsze poważne naruszenia ze strony podmiotu

- spowodowane szkody majątkowe i niemajątkowe, wpływ na inne usługi i liczbę użytkowników
- umyślny lub nieumyślny charakter czynu
- środki zastosowane, aby zapobiec szkodom lub je ograniczyć
- stopień współpracy z organem właściwym

Przy znikomej wadze naruszenia oraz zaprzestaniu naruszania lub naprawieniu szkody organ może odstąpić od nałożenia kary (art. 76a ust. 9).

- Kara okresowa za zwłokę w wykonaniu decyzji: od 500 zł do 100 000 zł za każdy dzień (ustawa o KSC art. 76b ust. 1 ustawy o KSC nowelizacja KSC s. 71)
- Przypadek kwalifikowany: do 100 000 000 zł (ustawa o KSC art. 73 ust. 5 ustawy o KSC s. 31)

Kierownik podmiotu

Akt prawny	Podstawa	Organ	Pułap
Ustawa o KSC	ustawa o KSC art. 73a ust. 4 nowelizacja KSC s. 68	Organ właściwy do spraw cyberbezpieczeństwa	**66 000 zł**
Prawo komunikacji elektronicznej	PKE art. 444 ust. 4 PKE s. 168	Prezes UKE (a w sprawach danych osobowych — Prezes UODO)	**66 000 zł**
Łącznie z obu ustaw			**132 000 zł**

- Kara jest niezależna od kary nałożonej na podmiot (art. 73a ust. 3).
- Może zostać nałożona także przy zaniechaniu o charakterze jednorazowym (art. 73a ust. 2).
- Powierzenie obowiązków innej osobie nie wyłącza odpowiedzialności kierownika (art. 8c ust. 3).
- Przy organie wieloosobowym bez wskazania osoby odpowiedzialnej odpowiadają wszyscy członkowie organu (art. 8c ust. 2).
- Przesłanką jest czas, zakres lub charakter naruszenia (art. 73a ust. 1).

Podmiot prowadzi działalność telekomunikacyjną, więc osoba zarządzająca odpowiada **równolegle na podstawie dwóch ustaw** — ustawy o KSC przed organem właściwym oraz Prawa komunikacji elektronicznej przed Prezesem UKE. Są to kary odrębne, niezależne od siebie i od kary nałożonej na przedsiębiorcę.

Organy uzyskują uprawnienie do nakładania kar pieniężnych od **3.04.2028** (nowelizacja KSC art. 35 ustawy nowelizującej s. 79). Obowiązki wdrożeniowe biegną jednak już teraz — termin realizacji obowiązków rozdziału 3 upływa 3 kwietnia 2027 r.

2.4
Rozwijany
DOJRZAŁOŚĆ OGÓLNA

61%
Cel: poziom 4
STOPIEŃ ZGODNOŚCI

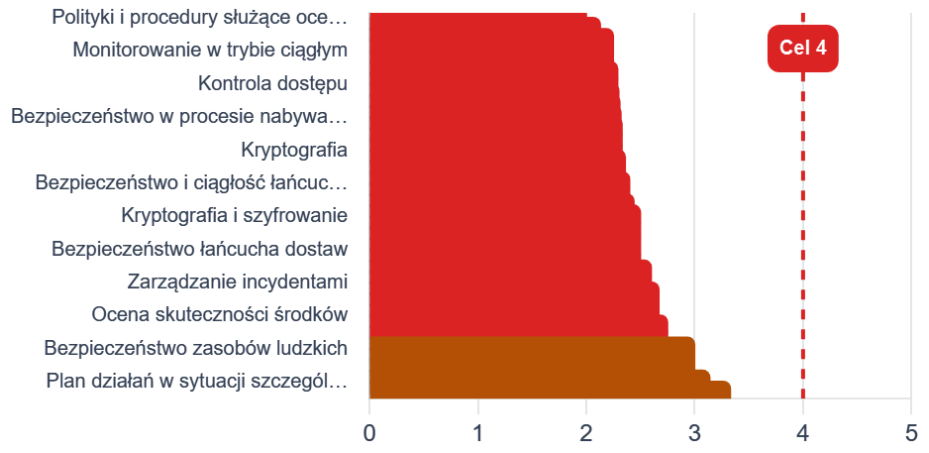
1.6
do poziomu docelowego
ŚREDNIA LUKA

349/349
100% wypełnione
ODPOWIEDZI

Profil dojrzałości

12 obszarów z największą luką z 35

Dojrzałość wg obszarów



Wypełnienie wg aktów prawnych

Akt prawny	Wypełnione	Dojrzałość
Obowiązki Ustawa o KSC — obowiązki formalne	49/49	—
KSC Ustawa o KSC — art. 8	68/68	2.5
PKE Prawo komunikacji elektronicznej	71/71	3.1
2024/2690 Rozporządzenie (UE) 2024/2690	161/161	2.3

Analiza luk

Obszar	Obecnie	Cel	Luka	Priorytet	Wypełnienie
7. Polityki i procedury służące ocenie skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie rozp. 2024/2690 Załącznik do rozporządzenia (UE) 2024/2690 rozp. 2024/2690 sekcja 7	2.0	4	2.0	Krytyczny	3/3
1. Polityka bezpieczeństwa sieci i systemów informatycznych rozp. 2024/2690 Załącznik do rozporządzenia (UE) 2024/2690 rozp. 2024/2690 sekcja 1	2.1	4	1.9	Wysoki	8/8
Bezpieczeństwo fizyczne i środowiskowe ustawa o KSC art. 8 ust. 1 pkt 2 lit. c s. 5	2.3	4	1.8	Wysoki	4/4
Monitorowanie w trybie ciągłym ustawa o KSC art. 8 ust. 1 pkt 2 lit. g s. 5	2.3	4	1.8	Wysoki	4/4
Edukacja personelu i cyberhigiena ustawa o KSC art. 8 ust. 1 pkt 2 lit. i oraz j s. 5	2.3	4	1.8	Wysoki	4/4
4. Ciągłość działania i zarządzanie kryzysowe rozp. 2024/2690 Załącznik do rozporządzenia (UE) 2024/2690 rozp. 2024/2690 sekcja 4	2.3	4	1.7	Wysoki	14/14
11. Kontrola dostępu rozp. 2024/2690 Załącznik do rozporządzenia (UE) 2024/2690 rozp. 2024/2690 sekcja 11	2.3	4	1.7	Wysoki	21/21
10. Bezpieczeństwo zasobów ludzkich rozp. 2024/2690 Załącznik do rozporządzenia (UE) 2024/2690 rozp. 2024/2690 sekcja 10	2.3	4	1.7	Wysoki	10/10
12. Zarządzanie aktywami rozp. 2024/2690 Załącznik do rozporządzenia (UE) 2024/2690 rozp. 2024/2690 sekcja 12	2.3	4	1.7	Wysoki	13/13
6. Bezpieczeństwo w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych rozp. 2024/2690 Załącznik do rozporządzenia (UE) 2024/2690 rozp. 2024/2690 sekcja 6	2.3	4	1.7	Wysoki	31/31
Polityki bezpieczeństwa ustawa o KSC art. 8 ust. 1 pkt 2 lit. a s. 5	2.3	4	1.7	Wysoki	3/3
Zarządzanie aktywami ustawa o KSC art. 8 ust. 1 pkt 2 lit. m s. 5	2.3	4	1.7	Wysoki	3/3

Obszar	Obecnie	Cel	Luka	Priorytet	Wypełnienie
9. Kryptografia rozp. 2024/2690 Załącznik do rozporządzenia (UE) 2024/2690 rozp. 2024/2690 sekcja 9	2.3	4	1.7	Wysoki	3/3
2. Polityka zarządzania ryzykiem rozp. 2024/2690 Załącznik do rozporządzenia (UE) 2024/2690 rozp. 2024/2690 sekcja 2	2.4	4	1.6	Wysoki	11/11
3. Obsługa incydentów rozp. 2024/2690 Załącznik do rozporządzenia (UE) 2024/2690 rozp. 2024/2690 sekcja 3	2.4	4	1.6	Wysoki	22/22
Bezpieczeństwo i ciągłość łańcucha dostaw ustawa o KSC art. 8 ust. 1 pkt 2 lit. e oraz ust. 2 s. 5	2.4	4	1.6	Wysoki	5/5
Kontrola dostępu ustawa o KSC art. 8 ust. 1 pkt 2 lit. n s. 5	2.4	4	1.6	Wysoki	5/5
13. Bezpieczeństwo środowiskowe i fizyczne rozp. 2024/2690 Załącznik do rozporządzenia (UE) 2024/2690 rozp. 2024/2690 sekcja 13	2.4	4	1.6	Wysoki	9/9
Kryptografia i szyfrowanie ustawa o KSC art. 8 ust. 1 pkt 2 lit. k s. 5	2.5	4	1.5	Wysoki	4/4
Środki zapobiegające i ograniczające wpływ incydentów ustawa o KSC art. 8 ust. 1 pkt 5 s. 5	2.5	4	1.5	Wysoki	6/6
Status regulacyjny i rejestr przedsiębiorców telekomunikacyjnych PKE art. 1, 2, 5–20 PKE s. 2	2.5	4	1.5	Wysoki	7/7
5. Bezpieczeństwo łańcucha dostaw rozp. 2024/2690 Załącznik do rozporządzenia (UE) 2024/2690 rozp. 2024/2690 sekcja 5	2.5	4	1.5	Wysoki	8/8
8. Podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa rozp. 2024/2690 Załącznik do rozporządzenia (UE) 2024/2690 rozp. 2024/2690 sekcja 8	2.5	4	1.5	Wysoki	8/8
Ciągłość działania i odtwarzanie ustawa o KSC art. 8 ust. 1 pkt 2 lit. f s. 5	2.6	4	1.4	Średni	5/5
Zarządzanie incydentami ustawa o KSC art. 8 ust. 1 pkt 4 s. 5	2.6	4	1.4	Średni	5/5

Obszar	Obecnie	Cel	Luka	Priorytet	Wypełnienie
Szacowanie ryzyka i zarządzanie ryzykiem ustawa o KSC art. 8 ust. 1 pkt 1 s. 5	2.7	4	1.3	Średni	3/3
Bezpieczeństwo w nabywaniu, rozwoju, utrzymaniu i eksploatacji ustawa o KSC art. 8 ust. 1 pkt 2 lit. b s. 5	2.7	4	1.3	Średni	3/3
Ocena skuteczności środków ustawa o KSC art. 8 ust. 1 pkt 2 lit. h s. 5	2.7	4	1.3	Średni	3/3
Bezpieczna komunikacja i uwierzytelnianie wieloskładnikowe ustawa o KSC art. 8 ust. 1 pkt 2 lit. l s. 5	2.8	4	1.3	Średni	4/4
Zbieranie informacji o cyberzagrożeniach i podatnościach ustawa o KSC art. 8 ust. 1 pkt 3 s. 5	2.8	4	1.3	Średni	4/4
Bezpieczeństwo zasobów ludzkich ustawa o KSC art. 8 ust. 1 pkt 2 lit. d s. 5	3.0	4	1.0	Średni	3/3
Ochrona danych osobowych i tajemnica komunikacji elektronicznej PKE art. 393, 399, 401–405 PKE s. 148	3.0	4	1.0	Średni	8/8
Ciągłość, jakość usług i numery alarmowe PKE art. 171, 285, 312, 316, 336–339 PKE s. 75	3.0	4	1.0	Średni	8/8
Plan działań w sytuacji szczególnego zagrożenia PKE art. 39 PKE s. 25	3.1	4	0.9	Średni	16/16
Obowiązki wobec uprawnionych podmiotów, retencja danych i punkt kontaktowy PKE art. 43–54 PKE s. 29	3.3	4	0.7	Średni	19/19

Rejestr ryzyka prawnego — obowiązki niewykonane

Obowiązek	Podstawa	Termin	Zagrożenie karą
Czy istnieje proces zapewniający złożenie wniosku o zmianę wpisu w terminie 14 dni od dnia zmiany danych? Wykaz podmiotów kluczowych i ważnych	ustawa o KSC art. 7c ust. 3 nowelizacja KSC s. 10	14 dni od zmiany danych	art. 73a ust. 1
Czy kierownik podmiotu formalnie zatwierdził system zarządzania bezpieczeństwem informacji i podejmuje decyzje dotyczące jego przeglądu i nadzoru? Obowiązki kierownika podmiotu	ustawa o KSC art. 8d pkt 1 nowelizacja KSC s. 16	—	art. 73a ust. 1
Czy powołano wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo albo zawarto umowę z dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa? Osoby kontaktowe i struktury	ustawa o KSC art. 14 s. 8	—	art. 73a ust. 1
Czy podmiot ma zdolność do przekazania zgłoszenia incydentu poważnego nie później niż w ciągu 72 godzin od wykrycia, z pełnym zakresem informacji z art. 12 ust. 3? Zgłaszanie incydentów poważnych	ustawa o KSC art. 11 ust. 1 pkt 4a s. 7	72 godziny od wykrycia	art. 73 ust. 1 pkt 7
Czy podmiot jest przygotowany na kontrolę organu właściwego, w tym doraźną i zdalną, oraz na przekazanie żądanych informacji i dowodów? Gotowość na czynności nadzorcze	ustawa o KSC art. 53 ust. 2 s. 26	—	art. 73 ust. 1 pkt 14–16

Kalendarz ustawowy

Data	Zdarzenie	Podstawa	Pozostało
3.04.2026	**Wejście w życie nowelizacji ustawy o KSC** Operatorzy usług kluczowych stają się z mocy prawa podmiotami kluczowymi.	nowelizacja KSC: art. 49 ustawy z 23.01.2026 o zmianie ustawy o KSC, s. 86 nowelizacja KSC: art. 22 ust. 1 ustawy z 23.01.2026 o zmianie ustawy o KSC, s. 78	obowiązuje
13.04.2026	**Uruchomienie Wykazu podmiotów kluczowych i ważnych** Wykaz KSC dostępny pod adresem wykaz-ksc.gov.pl, w Systemie S46. Do 6 maja 2026 r. trwały wpisy z urzędu — samodzielne składanie wniosków było w tym czasie niedostępne.	ustawa o KSC: art. 7c ustawy o KSC, komunikat Ministerstwa Cyfryzacji — nowelizacja KSC s. 10	obowiązuje
7.05.2026	**Otwarcie samorejestracji w wykazie** Od tego dnia podmioty nieobjęte wpisem z urzędu mogą samodzielnie składać wnioski o wpis. Realne okno na wniosek jest więc krótsze niż ustawowe 6 miesięcy.	komunikat Ministerstwa Cyfryzacji	obowiązuje
12.06.2026	**Udostępnienie Systemu S46 nowym podmiotom** Od tej daty podmioty mogą rozpocząć korzystanie z Systemu S46, w tym zgłaszanie incydentów i komunikację z organami.	ustawa o KSC: art. 46 ust. 1 ustawy o KSC, komunikat Ministerstwa Cyfryzacji, s. 24	obowiązuje
3.10.2026	**Wniosek o wpis do wykazu podmiotów kluczowych i ważnych** Dla podmiotów spełniających przesłanki w dniu wejścia w życie nowelizacji.	nowelizacja KSC: art. 33 ust. 3 ustawy z 23.01.2026 o zmianie ustawy o KSC, s. 79 ustawa o KSC: art. 7c ust. 1 ustawy o KSC — nowelizacja KSC s. 10	62 dni
3.04.2027	**Wdrożenie obowiązków rozdziału 3 ustawy o KSC** Rozdział 3 „Obowiązki podmiotów kluczowych i podmiotów ważnych”: system zarządzania bezpieczeństwem informacji, dokumentacja, procedury oraz korzystanie z systemu teleinformatycznego z art. 46 ust. 1 ustawy o KSC.	nowelizacja KSC: art. 33 ust. 1 ustawy z 23.01.2026 o zmianie ustawy o KSC, s. 79 ustawa o KSC: art. 16 pkt 1 ustawy o KSC, s. 10 ustawa o KSC: art. 46 ust. 4 ustawy o KSC, s. 24	244 dni

Data	Zdarzenie	Podstawa	Pozostało
3.04.2027	**Rozpoczęcie korzystania z Systemu S46** Obowiązek korzystania z systemu teleinformatycznego, przez który zgłasza się incydenty poważne i prowadzi wymianę informacji z organami. Termin 12 miesięcy od spełnienia przesłanek.	ustawa o KSC art. 46 ust. 1 ustawy o KSC s. 24, ustawa o KSC art. 16 pkt 1 ustawy o KSC s. 10	244 dni
3.10.2027	**Ustanowienie CSIRT sektorowych przez organy właściwe** Do czasu ogłoszenia komunikatu o zdolności operacyjnej CSIRT sektorowego zgłoszenia incydentów kieruje się do CSIRT NASK, CSIRT GOV albo CSIRT MON.	ustawa o KSC art. 42 ust. 1 ustawy o KSC s. 21, nowelizacja KSC art. 44 ustawy z 23.01.2026 o zmianie ustawy o KSC s. 81	427 dni
3.04.2028	**Pierwsza możliwa kara pieniężna** Organy uzyskują uprawnienie do nakładania kar pieniężnych z art. 73 ust. 1–4, art. 73a–73c i art. 76b ustawy o KSC. Odroczenie nie obejmuje kary nadzwyczajnej do 100 mln zł za naruszenie powodujące bezpośrednie i poważne cyberzagrożenie — ta może zostać nałożona wcześniej.	nowelizacja KSC art. 35 ustawy z 23.01.2026 o zmianie ustawy o KSC s. 79	610 dni
3.04.2028	**Pierwszy audyt bezpieczeństwa podmiotu kluczowego** Termin przeprowadzenia pierwszego audytu bezpieczeństwa systemu informacyjnego.	nowelizacja KSC art. 33 ust. 2 ustawy z 23.01.2026 o zmianie ustawy o KSC s. 79, ustawa o KSC art. 16 pkt 2 ustawy o KSC s. 10, ustawa o KSC art. 15 ust. 1 ustawy o KSC s. 9	610 dni

Progi uznania incydentu za poważny

Dla poniższych ról progi wynikają wprost z rozporządzenia (UE) 2024/2690 i obowiązują od 7 listopada 2024 r.

Dostawcy usługi ośrodka przetwarzania danych (art. 8)

Najostrzejszy zestaw progów w całym rozporządzeniu. Dla centrów przetwarzania danych NIE MA progu 30 minut ani progu 5 % / 1 mln użytkowników — każda pełna niedostępność usługi oraz każde naruszenie dostępu fizycznego stanowi incydent poważny.

- **a)** Usługa ośrodka przetwarzania danych jest całkowicie niedostępna — BEZ progu czasowego.
- **b)** Dostępność usługi jest ograniczona przez okres dłuższy niż 1 godzina — BEZ progu procentowego ani progu liczby użytkowników.
- **c)** Naruszono integralność, poufność lub autentyczność danych w wyniku podejrzewanego działania złośliwego.
- **d)** Naruszono dostęp fizyczny do ośrodka przetwarzania danych obsługiwanego przez dostawcę.

Kryteria horyzontalne (art. 3 ust. 1) — wystarczy spełnienie jednego

- **a)** Strata finansowa — Strata finansowa poniesiona lub możliwa przekracza 500 000 EUR albo 5 % całkowitego rocznego obrotu podmiotu w poprzednim roku obrotowym — w zależności od tego, która wartość jest niższa.
- **b)** Wyciek tajemnic przedsiębiorstwa — Incydent spowodował lub może spowodować wyciek tajemnic przedsiębiorstwa w rozumieniu art. 2 pkt 1 dyrektywy (UE) 2016/943.
- **c)** Śmierć osoby fizycznej — Incydent spowodował lub może spowodować śmierć osoby fizycznej.
- **d)** Znaczny uszczerbek na zdrowiu — Incydent spowodował lub może spowodować znaczny uszczerbek na zdrowiu osoby fizycznej.
- **e)** Nieuprawniony dostęp — Miał miejsce skuteczny, prawdopodobnie złośliwy i nieuprawniony dostęp do sieci i systemów informatycznych, który może spowodować poważne zakłócenia operacyjne.
- **f)** Incydenty powtarzające się — Incydent spełnia kryteria z art. 4: wystąpił co najmniej dwa razy w ciągu sześciu miesięcy, incydenty mają tę samą widoczną podstawową przyczynę i łącznie spełniają kryterium straty finansowej z art. 3 ust. 1 lit. a). Uznaje się je łącznie za jeden poważny incydent.
- **g)** Kryterium sektorowe — Incydent spełnia co najmniej jedno z kryteriów sektorowych określonych w art. 5–14 rozporządzenia.

Działalność telekomunikacyjna — stan otwarty. Rozporządzenie (UE) 2024/2690 nie ma zastosowania do przedsiębiorców komunikacji elektronicznej, a progi krajowe określi dopiero rozporządzenie Rady Ministrów wydane na podstawie art. 11 ust. 4 ustawy o KSC. Do czasu jego wydania obowiązują dotychczasowe przepisy wykonawcze. Narzędzie nie podaje tu wartości liczbowych, ponieważ nie zostały jeszcze ustalone.

Historia i postęp

Nie zapisano jeszcze żadnej migawki. Migawka zamraża bieżący stan oceny wraz z datą, dzięki czemu kolejne raporty pokazują postęp.

Zapisz pierwszą migawkę

Ocena zgodności z ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (KSC), wdrażającą dyrektywę (UE) 2022/2555 (NIS 2), z rozporządzeniem wykonawczym Komisji (UE) 2024/2690 oraz z ustawą z dnia 12 lipca 2024 r. — Prawo komunikacji elektronicznej (PKE).

Nie stanowi opinii prawnej; wszystkie dane pozostają w tej przeglądarce lub lokalnie na Twoim komputerze.

Wersja 1.0.2 · 2 sierpnia 2026 · **lista zmian**