



Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa po nowelizacji

PYTANIA I ODPOWIEDZI





Szanowni Państwo,

otaczająca nas technologia umożliwia funkcjonowanie społeczeństwa i gospodarki. Jednocześnie istnieje również szereg zagrożeń, które mogą mieć negatywny wpływ na funkcjonowanie polskich przedsiębiorstw i obywateli. W 2025 r. zespoły CSIRT otrzymały zgłoszenia 272 941 incydentów. Liczba ta pokazuje jak ważne jest zapewnienie cyberbezpieczeństwa Państwa.

W tym celu uchwalona została nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa. Przebudowuje ona krajowy system cyberbezpieczeństwa, aby skutecznie reagować na cyberzagrożenia i incydenty.

Zdaję sobie jednak sprawę, że jej wdrożenie będzie wyzwaniem przede wszystkim w nowych podmiotach kluczowych i podmiotach ważnych.

Nie chcemy pozostawiać tych podmiotów samym sobie. Dlatego przygotowaliśmy zestaw pytań i odpowiedzi, który ma na celu ułatwić podmiotom kluczowym i podmiotom ważnym stosowanie znowelizowanej ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Zestaw pytań będzie aktualizowany i uzupełniany stosownie do potrzeb podmiotów kluczowych i podmiotów ważnych.

Niniejszy dokument nie ma mocy prawnej i nie jest dokumentem wiążącym. Jest on jednak przydatny przy dokonywaniu wykładni przepisów ustawy.

Ufam, że dokument będzie efektywnym wsparciem we wdrożeniu ustawy o krajowym systemie cyberbezpieczeństwa.

**Wiceprezes Rady Ministrów
Minister Cyfryzacji
Krzysztof Gawkowski**



Spis treści

1. Identyfikacja podmiotów kluczowych i podmiotów ważnych 16

1.1. Co musi zrobić przedsiębiorca, który nie wie czy podlega pod krajowy system cyberbezpieczeństwa?	16
1.2. Kto jest podmiotem kluczowym?.....	16
1.3. Kto jest podmiotem ważnym?	17
1.4. Jakie sektory są objęte ustawą?.....	17
1.5. Jak określić wielkość przedsiębiorstwa?	19
1.6. Czy przy ustalaniu wielkości przedsiębiorstwa podmiot musi uwzględnić przedsiębiorstwa partnerskie i powiązane, jeżeli nie świadczy z nimi wspólnie usług?	20
1.7. Jakie podmioty są podmiotami kluczowymi niezależnie od ich wielkości? ..	21
1.8. Czy wszystkie podmioty publiczne podlegają pod ustawę o krajowym systemie cyberbezpieczeństwa?	21
1.9. Czy wszyscy przedsiębiorcy telekomunikacyjni podlegają pod ustawę o krajowym systemie cyberbezpieczeństwa?.....	22
1.10. Co w przypadku, gdy podmiot spełnia kryteria zarówno dla podmiotu kluczowego jak i podmiotu ważnego?	22
1.11. Czym się różni podmiot kluczowy od podmiotu ważnego?	22
1.12. Czy podmiot kluczowy lub podmiot ważny otrzymują decyzję administracyjną o ich kwalifikacji?.....	23
1.13. Czy organ właściwy do spraw cyberbezpieczeństwa może skierować zapytanie do podmiotu w sprawie ustalenia czy jest podmiotem kluczowym lub podmiotem ważnym?	23
1.14. Kiedy podmiot kluczowy lub podmiot ważny podlega pod właściwość polskich organów?	24
1.15. Jakie są wyjątki od jurysdykcji polskiej?	24
1.16. Czy szkoły (podstawowe), przedszkola również są podmiotami KSC?	24
1.17. Kiedy uczelnia staje się organizacją badawczą w rozumieniu ustawy?	25
1.18. Czy przedsiębiorca komunikacji elektronicznej w świetle ustawy może być dostawcą sieci dostarczania treści (Content Delivery Network)?.....	25
1.19. Czy mały przedsiębiorca komunikacji elektronicznej będący jednocześnie dostawcą usługi dostępu do Internetu oraz świadczący usługę DNS będzie podmiotem kluczowym czy podmiotem ważnym?	25
1.20. Co, jeśli przedsiębiorca dokona nieprawidłowej samoidentyfikacji?	26



1.21. Czy spółka IT realizująca zadania z zakresu cyberbezpieczeństwa tylko dla własnej grupy kapitałowej podlega znowelizowanej KSC?.....	26
1.22. Kim jest dostawca usług chmurowych?	26
1.23. Czy w zakres definicji dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa wchodzi dostawca oprogramowania?	27
1.24. Czy objęcie podmiotów publicznych – podmiotów ważnych wspólną obsługą przez jednostkę wyznaczoną do realizacji z zakresu cyberbezpieczeństwa powoduje automatyczne podniesienie statusu podmiotu ważnego do podmiotu kluczowego? [NOWE – aktualizacja czerwiec 2026 r.]	27
1.25. Jakie podmioty publiczne będą podmiotami kluczowymi? [NOWE - aktualizacja czerwiec 2026 r.]	27
1.26. Czy wszystkie wojewódzkie jednostki budżetowe oraz wojewódzkie zakłady budżetowe są podmiotami kluczowymi? [NOWE - aktualizacja czerwiec 2026 r.]	30
1.27. Które przedsiębiorstwa spożywcze są podmiotami ważnymi w sektorze „produkcja, przetwarzanie i dystrybucja żywności”? [NOWE - aktualizacja czerwiec 2026 r.]	31
2. Wykaz podmiotów kluczowych i podmiotów ważnych	35
2.1. Kiedy należy zarejestrować się w wykazie podmiotów kluczowych i podmiotów ważnych?	35
2.2. W jaki sposób należy złożyć wniosek o wpis do wykazu podmiotów kluczowych i podmiotów ważnych?	35
2.3. Które podmioty zostaną wpisane do wykazu z urzędu?	35
2.4. Czy organ właściwy do spraw cyberbezpieczeństwa może wpisać z urzędu podmiot do wykazu podmiotów kluczowych i podmiotów ważnych?	36
2.5. Czy spółka uznana za operatora usługi kluczowej musi wpisać się do wykazu podmiotów kluczowych i podmiotów ważnych?	36
2.6. Czy wszystkie urzędy gmin stają się automatycznie podmiotem ważnym lub kluczowym? Czy urząd otrzyma decyzję o ujęciu w rejestrze jako podmiot kluczowy lub ważny?.....	36
2.7. Czy wpisowi do wykazu podmiotów kluczowych i podmiotów ważnych podlega działalność faktyczna czy ta wykazana w rejestrach publicznych?	37
2.8. Co z przedsiębiorstwem, którego główna działalność nie kwalifikuje się do wpisania do rejestru podmiotów ważnych i kluczowych, ale poboczna tak. Czy powinien złożyć wniosek o wpis?.....	37
2.9. Czy spółki zależne od operatora usługi kluczowej też powinny zostać zgłoszone do wykazu podmiotów kluczowych i podmiotów ważnych?.....	37



2.10. Jakie dane będą znajdowały się w wykazie podmiotów kluczowych i podmiotów ważnych?	37
2.11. Co, jeżeli podmiot powinien zostać wpisany do Wykazu z urzędu, jednak wciąż nie otrzymał zawiadomienia o wpisie oraz wezwania do uzupełnienia brakujących danych? [NOWE – aktualizacja czerwiec 2026 r.]	39
2.12. Dlaczego w wezwaniu do uzupełnienia wpisu w Wykazie podmiotów kluczowych i podmiotów ważnych wskazano, że jestem podmiotem ważnym, mimo że – zgodnie z moją oceną – powinienem zostać zakwalifikowany jako podmiot kluczowy? [NOWE – aktualizacja czerwiec 2026 r.]	39
2.13. Gdzie mogę zweryfikować, po dokonaniu wpisu lub uzupełnieniu wpisu, czy mój podmiot został zaklasyfikowany jako podmiot ważny czy jako podmiot kluczowy? [NOWE – aktualizacja czerwiec 2026 r.]	40
2.14. Co zrobić, jeżeli zostałem błędnie wpisany do Wykazu KSC? [NOWE – aktualizacja czerwiec 2026 r.]	40
2.15. Kiedy otrzymam dostęp do Systemu S46 Cyber Hub? [NOWE – aktualizacja czerwiec 2026 r.]	41
2.16. Czy forma prawna podmiotu ma wpływ na stosowanie ustawy o KSC? [NOWE – aktualizacja czerwiec 2026 r.]	41
2.17. Czy termin na wpis do wykazu liczony jest od wejścia ustawy w życie czy od spełnienia przesłanek? [NOWE – aktualizacja czerwiec 2026 r.]	41
2.18. Co, jeżeli podmiot dokonuje wpisu do wykazu przez pełnomocnika? [NOWE – aktualizacja czerwiec 2026 r.]	42
2.19. Czy możliwa jest korekta danych po wpisie do Wykazu KSC? Kto powinien dokonać zgłoszenia zmiany danych podmiotu? W jakim terminie należy aktualizować dane? [NOWE – aktualizacja czerwiec 2026 r.]	42
2.20. Jeżeli podmiot nie podlega pod wpis z urzędu i złożył wniosek o wpis do Wykazu KSC, to czy otrzyma formalne potwierdzenie? [NOWE – aktualizacja czerwiec 2026 r.]	42
2.21. Kto ma dostęp do danych podmiotu wpisanego do Wykazu KSC? [NOWE – aktualizacja czerwiec 2026 r.]	43
2.22. Jak wygląda procedura wykreślenia podmiotu z Wykazu KSC? [NOWE – aktualizacja czerwiec 2026 r.]	43
2.23. Gdzie publikowane są komunikaty dotyczące Wykazu KSC? [NOWE – aktualizacja czerwiec 2026 r.]	43
2.24. Czy dział IT może złożyć wniosek o wpis do Wykazu KSC, a dyrektor lub prezes może go potem podpisać? [NOWE – aktualizacja czerwiec 2026 r.]	44
2.25. Czy wpis do Wykazu KSC następuje automatycznie po wysłaniu formularza? [NOWE – aktualizacja czerwiec 2026 r.]	44



- 2.26. Czy korekta danych w Wykazie KSC wymaga ponownego złożenia i podpisania wniosku? [NOWE – aktualizacja czerwiec 2026 r.] 44
- 2.27. Czy konieczna jest aktualizacja wpisu w Wykazie KSC po każdej zmianie domeny lub IP? [NOWE – aktualizacja czerwiec 2026 r.]..... 44
- 2.28. Czy likwidacja spółki powoduje automatyczne wykreślenie z Wykazu KSC? [NOWE – aktualizacja czerwiec 2026 r.]..... 44
- 2.29. Jakie podmioty powinny wskazać przedstawiciela zgodnie z art. 5a ust. 7-9 ustawy o KSC? Kto może nim zostać? [NOWE – aktualizacja czerwiec 2026 r.].. 45
- 2.30. Jeżeli podmiot operuje na wielu adresach opartych o jedną domenę główną – czy wystarczy wskazanie w Wykazie KSC tej domeny głównej z dodatkowym wyjaśnieniem, że wszystkie inne na niej bazują, czy też konieczne jest wymienienie każdej z wykorzystywanych domen z osobna? [NOWE – aktualizacja czerwiec 2026 r.]..... 46
- 2.31. Czy jeśli będę czekał z dokonaniem wpisu do Wykazu KSC do października br. to nie muszę wykonywać obowiązków lub będę miał więcej czasu na dostosowanie? [NOWE – aktualizacja czerwiec 2026 r.]..... 46
- 2.32. Co musi zrobić podmiot, który zacznie spełniać przesłanki uznania za podmiot kluczowy lub podmiot ważny po 3 października 2026 r., tj. po zakończeniu samorejestracji podmiotów w wykazie podmiotów kluczowych i podmiotów ważnych, wskazanej w harmonogramie opublikowanym przez Ministra Cyfryzacji? [NOWE – aktualizacja czerwiec 2026 r.] 46
- 2.33. Od kiedy podmioty mogą składać wnioski o wpis do wykazu podmiotów kluczowych i podmiotów ważnych? [NOWE – aktualizacja czerwiec 2026 r.]..... 47
- 2.34. Kiedy podmioty objęte wpisem z urzędu do wykazu podmiotów kluczowych i podmiotów ważnych otrzymają zawiadomienie o wpisie z urzędu wraz z wezwaniem do uzupełnienia brakujących danych? [NOWE – aktualizacja czerwiec 2026 r.]..... 47
- 2.35. Jak złożyć wniosek o wpis do wykazu podmiotów kluczowych i podmiotów ważnych? [NOWE – aktualizacja czerwiec 2026 r.] 47
- 2.36. W jakim czasie mam uzupełnić dane w Wykazie KSC po otrzymaniu zawiadomienia o wpisie z urzędu wraz z wezwaniem do uzupełnienia brakujących danych? [NOWE – aktualizacja czerwiec 2026 r.]..... 48
- 2.37. Czy podmioty krytyczne są obecnie wpisywane z urzędu do Wykazu KSC, skoro nowelizacja ustawy o zarządzaniu kryzysowym nie weszła jeszcze w życie? [NOWE – aktualizacja czerwiec 2026 r.]..... 48
- 2.38. Kiedy w wykazie zostanie wskazana informacja o uznaniu podmiotu kluczowego lub podmiotu ważnego za podmiot krytyczny? [NOWE – aktualizacja czerwiec 2026 r.] 48



2.39. Czy Wykaz KSC może być uzupełniany bez wskazania osób do kontaktu, skoro ustawa o KSC przewiduje okres przejściowy na wdrożenie części obowiązków? [NOWE – aktualizacja czerwiec 2026 r.] 49

3. Obowiązki podmiotów kluczowych i ważnych 50

3.1. Jakie są istotne terminy wdrożenia dla podmiotów kluczowych i podmiotów ważnych? 50

3.2. Co musi zrobić podmiot, żeby dostosować się do wymogów ustawy? 50

3.3. Jakie są podstawowe obowiązki dla podmiotu kluczowego i podmiotu ważnego w zakresie systemu zarządzania bezpieczeństwem informacji? 52

3.4. Jak zidentyfikować systemy informacyjne, w których należy wdrożyć system zarządzania bezpieczeństwem informacji (SZBI)? 57

3.5. Co powinna zawierać dokumentacja systemu zarządzania bezpieczeństwem informacji (SZBI)? 58

3.6. Czy muszę tworzyć nową odrębną dokumentację systemu zarządzania bezpieczeństwem informacji (SZBI)? 60

3.7. Kupiłem dokumentację zgodną z NIS2. Czy jestem zgodny z ustawą o KSC? 60

3.8. Czy należy zapewnić szkolenia z zakresu cyberbezpieczeństwa dla personelu podmiotu kluczowego lub podmiotu ważnego? 61

3.9. Jakie są obowiązki w zakresie zarządzania bezpieczeństwem łańcucha dostaw? 61

3.10. Czy personel podmiotu kluczowego lub podmiotu ważnego podlega weryfikacji? 62

3.11. Czy osoba, która posiada poświadczenie bezpieczeństwa również podlega obowiązkowej weryfikacji niekaralności? 63

3.12. Czy zaświadczenie o niekaralności obowiązuje również pracowników jednostek samorządowych? [NOWE - aktualizacja czerwiec 2026 r.] 63

3.13. Czy przedsiębiorcy świadczący usługi obsługi incydentów mają dodatkowe obowiązki? 63

3.14. Jakie są obowiązki z zakresu cyberbezpieczeństwa dla samorządowych podmiotów publicznych? 63

3.15. Czy jednostka samorządowa musi przeprowadzać szacowanie ryzyka? [NOWE - aktualizacja czerwiec 2026 r.] 67

3.16. Czy muszę mieć Security Operations Center (SOC)? 68

3.17. Jakie są obowiązki podmiotów kluczowych i podmiotów ważnych w zakresie kontaktów z innymi podmiotami oraz użytkownikami? 68

3.18. Kto może być osobą kontaktową z podmiotami krajowego systemu cyberbezpieczeństwa? 69



3.19. Czy obowiązki z zakresu cyberbezpieczeństwa muszą realizować w ramach swojej struktury organizacyjnej?	69
3.20. Czy samodzielny publiczny zakład opieki zdrowotnej zatrudniający poniżej 50 pracowników podlega pod ustawę o KSC? [NOWE – aktualizacja czerwiec 2026 r.]	69
3.21. Czy istnieje rejestr dostawców usług zaufania? [NOWE – aktualizacja czerwiec 2026 r.]	69
3.22. Czy istnieje rejestr bezpiecznych dostawców sprzętu i oprogramowania dla podmiotów kluczowych i podmiotów ważnych? [NOWE – aktualizacja czerwiec 2026 r.]	70
3.23. Jak należy określić wielkość podmiotu leczniczego, który nie jest przedsiębiorcą? [NOWE – aktualizacja czerwiec 2026 r.]	71
3.24. Czy urząd gminy posiadający w swoich strukturach Zakład Obsługi Komunalnej świadczący usługi dostarczania wody oraz odbioru ścieków będzie należał do podmiotów kluczowych czy też do podmiotów ważnych publicznych? [NOWE – aktualizacja czerwiec 2026 r.]	71
3.25. Czy związki jednostek samorządu terytorialnego podlegają pod ustawę o KSC? [NOWE – aktualizacja czerwiec 2026 r.]	72
3.26. Czy jeśli uczelnia wyższa prowadzi również badania aplikacyjne oraz prace rozwojowe lecz nie jest to jej podstawowa działalność (zajmuje się nią jedna z jednostek uczelni), to czy w zakresie działalności tej jednostki uczelnia jest zobowiązana wdrożyć SZBI zgodnie z art. 8 ustawy o KSC, czy też cały podmiot (uczelnia) podlega pod obowiązki określone w załączniku nr 4 do ustawy? [NOWE – aktualizacja czerwiec 2026 r.]	72
3.27. Czy jeśli podstawową działalnością uczelni jest prowadzenie badań aplikacyjnych i prac rozwojowych, a pozostałą działalnością jest działalność edukacyjna, to czy cała uczelnia podlega pod SZBI z art. 8 ustawy o KSC, czy też w zakresie w jakim uczelnia prowadzi działalność edukacyjną wystarczające jest wdrożenie obowiązków wskazanych w załączniku nr 4 do ustawy? [NOWE – aktualizacja czerwiec 2026 r.]	72
3.28. Czy podmioty kluczowe i podmioty ważne są uprawnione w okresie dostosowawczym do gromadzenia danych o niekaralności w aktualnie otwartych procesach rekrutacji? [NOWE – aktualizacja czerwiec 2026 r.]	73
3.29. Czy weryfikacja niekaralności personelu dotyczy również obecnego czy tylko przyszłego personelu? [NOWE – aktualizacja czerwiec 2026 r.]	73
3.30. Kto ponosi odpowiedzialność za realizację obowiązków z zakresu cyberbezpieczeństwa w przypadku jednostki wyznaczonej? [NOWE – aktualizacja czerwiec 2026 r.]	73
3.31. Czy system zarządzania bezpieczeństwem informacji dla kilku systemów informacyjnych wykorzystywanych przez podmiot może być opracowany w jednym dokumencie? [NOWE – aktualizacja czerwiec 2026 r.]	73



3.32. Czy termin realizacji obowiązków z zakresu wdrożenia systemu zarządzania bezpieczeństwem informacji należy liczyć się od daty wpisu do Wykazu KSC? [NOWE – aktualizacja czerwiec 2026 r.].....	73
3.33. Czy termin realizacji obowiązków dotyczących uzupełnienia danych w Wykazie KSC liczy się od daty wpisu do wykazu? [NOWE – aktualizacja czerwiec 2026 r.].....	74
3.34. Czy jeżeli spółka świadczy usługi zarządzane z zakresu cyberbezpieczeństwa tylko dla innych spółek w ramach grupy kapitałowej to czy podlega pod ustawę o KSC? [NOWE – aktualizacja czerwiec 2026 r.]	74
3.35. Czy jednostka wyznaczona z województwa może obsługiwać gminy i powiaty? [NOWE – aktualizacja czerwiec 2026 r.]	74
3.36. Czy Gminny Ośrodek Pomocy Społecznej jest podmiotem krajowego systemu cyberbezpieczeństwa? [NOWE – aktualizacja czerwiec 2026 r.].....	75
3.37. Czym są samorządowe podmioty publiczne? [NOWE – aktualizacja czerwiec 2026 r.].....	75
3.38. Czy ustalając wielkość podmiotów zgodnie z unijnymi kryteriami należy wziąć pod uwagę dane finansowe związane tylko z działalnością podmiotu wskazaną w załączniku do ustawy o KSC czy dane finansowe całego podmiotu? [NOWE – aktualizacja czerwiec 2026 r.].....	75
3.39. Czy podmioty kluczowe mają obowiązek stosowania Załącznika nr 4 do ustawy o KSC? [NOWE – aktualizacja czerwiec 2026 r.].....	75
3.40. Które elementy Załącznika nr 4 do ustawy o KSC mają charakter obowiązkowy, a które fakultatywny? [NOWE – aktualizacja czerwiec 2026 r.] ...	75
3.41. Jak rozumieć wykonywanie zapasowych kopii danych odseparowanych logicznie i fizycznie od danych przetwarzanych w systemach informacyjnych dla realizacji zadania publicznego wskazane w Załączniku nr 4. Czy muszą one być przechowywane w innym budynku czy wystarczy w innym pomieszczeniu? [NOWE – aktualizacja czerwiec 2026 r.].....	76
4. Obowiązki kierownika podmiotu	77
4.1. Jakie są podstawowe obowiązki kierownika podmiotu kluczowego lub podmiotu ważnego?	77
4.2. Kim jest kierownik podmiotu kluczowego lub podmiotu ważnego?	77
4.3. Czy kierownik podmiotu kluczowego lub podmiotu ważnego podlega obowiązkowym szkoleniom?	78
4.4. Za co ponosi odpowiedzialność kierownik podmiotu kluczowego lub ważnego?.....	78
4.5. Czy w przypadku samorządowej jednostki budżetowej, innej niż urząd, starostwo itd., przez kierownika urzędu należy rozumieć dyrektora tej jednostki? [NOWE – aktualizacja czerwiec 2026 r.].....	79



4.6. Kto odpowiada za niewykonanie obowiązków przez podmiot publiczny które nie współpracuje z jednostką wyznaczoną do realizacji zadań z zakresu cyberbezpieczeństwa? [NOWE – aktualizacja czerwiec 2026 r.]..... 79

5. Zespoły Reagowania na Incydynty Bezpieczeństwa Komputerowego (CSIRT)..... 80

5.1. Jakie są rodzaje zespołów CSIRT? 80

5.2. Jakie są dane kontaktowe do zespołów CSIRT poziomu krajowego? 80

5.3. Czym jest CSIRT sektorowy? 80

6. Zgłaszanie incydentów 81

6.1. Czym jest incydent?..... 81

6.2. Jakie są rodzaje incydentów? 81

6.3. Czy muszę zgłaszać wszystkie incydynty?..... 82

6.4. Jakie są obowiązki z zakresu obsługi incydentów? 82

6.5. Jak określić moment wykrycia incydyntu?..... 82

6.6. Czy incydynty związane z automatyką przemysłową są także zgłaszane do zespołów CSIRT sektorowych?..... 83

6.7. Czy mogę dobrowolnie zgłaszać informacje o incydyntach do zespołów CSIRT? 83

6.8. Co to jest potencjalne zdarzenie dla cyberbezpieczeństwa? Czy muszę je zgłaszać? 83

6.9. Czym jest poważne cyberzagrożenie? Czy wiążą się z nim obowiązki informacyjne? 84

6.10. Czym jest incydent poważny? 86

6.11. Co zawiera wczesne ostrzeżenie o incydencie poważnym?..... 86

6.12. Czy małe samorządowe jednostki budżetowe muszą zgłaszać wczesne ostrzeżenie o incydencie poważnym? 87

6.13. W jaki sposób zgłasza się incydynty poważne?..... 87

6.14. Co zawiera zgłoszenie incydyntu poważnego?..... 88

6.15. Nie mam wszystkich danych w chwili zgłoszenia incydyntu poważnego – co muszę zrobić? 89

6.16. Kiedy muszę poinformować swoich użytkowników o incydencie poważnym? 89

6.17. W jaki sposób zachować się w sytuacji, gdy jeden incydent (np. ten sam atak) ma bezpośredni wpływ na usługi świadczone w ramach różnych sektorów przez tego samego przedsiębiorcę? Czy należy dokonać zgłoszenia przez system



S46 do każdego CSIRT sektorowego, który jest właściwy dla dotkniętych usług?	89
6.18. Czy istnieją przepisy unijne określające progi incydentu poważnego dla niektórych podmiotów kluczowych i podmiotów ważnych?	89
6.19. Gdzie będą określone progi incydentu poważnego?	90
6.20. Niektóre dane wymagane przez ustawę przy zgłaszaniu incydentu stanowią tajemnicę przedsiębiorstwa – czy mam je zgłaszać?	90
6.21. W jaki sposób mam zgłosić informacje niejawne, które dotyczą zgłoszenia incydentu poważnego?	90
6.22. Czy zespoły CSIRT mogą opublikować informację o wystąpieniu incydentu poważnego?	90
6.23. Jakie sprawozdania związane z incydemem poważnym zgłasza podmiot kluczowy lub podmiot ważny?	91
7. System S46	92
7.1. Czym jest system S46?	92
7.2. Do czego służy system S46?	92
7.3. W jaki sposób zarejestrować się w systemie S46?	93
7.4. W jaki sposób podmioty uwierzytelniają się w systemie S46?	93
7.5. Jakie są minimalne wymagania techniczne i funkcjonalne korzystania z systemu teleinformatycznego S46?	93
7.6. Czy podmiot publiczny wpisany z urzędu do wykazu podmiotów kluczowych lub ważnych nadal samodzielnie musi rejestrować się w systemie S46? [NOWE – aktualizacja czerwiec 2026 r.]	93
8. Wymiana informacji z zakresu cyberbezpieczeństwa	94
8.1. Kto może wymieniać się informacjami z zakresu cyberbezpieczeństwa?	94
8.2. Jakie informacje z zakresu cyberbezpieczeństwa mogą wymieniać między sobą podmioty kluczowe i podmioty ważne?	94
8.3. Kiedy wymiana informacji o cyberbezpieczeństwie jest dopuszczalna?	95
8.4. W jaki sposób podmioty kluczowe i podmioty ważne wymieniają się informacjami z zakresu cyberbezpieczeństwa?	96
8.5. Czy w ustawie uregulowano działalność podmiotów typu Information Sharing and Analysis Center (ISAC)?	96
9. Audyty bezpieczeństwa systemu informacyjnego	97
9.1. Kto musi przeprowadzić cykliczny audyt?	97
9.2. Kto może przeprowadzić audyt w podmiocie?	97
9.3. Jakie certyfikaty uprawniają do przeprowadzenia audytu?	97



9.4. Czy audyt może być przeprowadzony przez osobę, która wcześniej w tym samym podmiocie realizowała zadania z zakresu SZBI?	98
9.5. Kiedy dotychczasowi operatorzy usług kluczowych mają obowiązek przeprowadzić audyt?	98
9.6. Kiedy dotychczasowi operatorzy usług kluczowych przeprowadzają pierwszy audyt bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej? [NOWE – aktualizacja czerwiec 2026 r.].....	99
10. Szczególne działania na rzecz zapewnienia cyberbezpieczeństwa	100
10.1. Czym jest polecenie zabezpieczające? Czy Minister Cyfryzacji będzie cenzurował internet w Polsce lub nawet wyłączy Internet w Polsce za pomocą polecenia zabezpieczającego?	100
10.2. Kto może być adresatem polecenia zabezpieczającego?.....	100
10.3. Jakie działania mogą być nakazane w ramach polecenia zabezpieczającego?	100
10.4. Na czym polega ocena bezpieczeństwa?	101
10.5. Kto może przeprowadzać ocenę bezpieczeństwa?	101
10.6. Jakie są gwarancje dla podmiotu krajowego systemu cyberbezpieczeństwa przy przeprowadzaniu oceny bezpieczeństwa?.....	102
10.7. Czy Pełnomocnik Rządu do spraw Cyberbezpieczeństwa może wydawać rekomendacje?	102
10.8. Czy Minister Cyfryzacji zaraz po wejściu w życie ustawy o KSC opublikuje listę Dostawców Wysokiego Ryzyka?	103
11. Nadzór nad podmiotami kluczowymi i ważnymi	104
11.1. Kim są organy właściwe do spraw cyberbezpieczeństwa?.....	104
11.2. Co w przypadku gdy ten sam podmiot będzie podlegał pod kilka organów właściwych do spraw cyberbezpieczeństwa?	105
11.3. Kto jest organem właściwym do spraw cyberbezpieczeństwa dla podmiotów publicznych?	105
11.4. Jakie są środki nadzoru nad podmiotami kluczowymi?	106
11.5. Jakie są środki nadzoru nad podmiotami ważnymi?	106
11.6. Czym są dowody realizacji wymogów SZBI?.....	107
12. Kary pieniężne.....	108
12.1. Czy kary pieniężne będą nakładane od razu po wejściu w życie ustawy? .	108
12.2. Kto nakłada kary pieniężne?	108



12.3. Jakie kary może nałożyć organ właściwy do spraw cyberbezpieczeństwa?	108
12.4. Jak wysokie mogą być kary pieniężne?	108
12.5. Czym jest kara okresowa?	109
12.6. Czym jest kara ekstraordynaryjna?.....	109
12.7. Czy organ właściwy do spraw cyberbezpieczeństwa ostrzega podmiot przed nałożeniem kary?	109
12.8. Czy organ właściwy do spraw cyberbezpieczeństwa informuje o wstępnych ustaleniach?	110
12.9. Jakie są przesłanki nałożenia kary pieniężnej?.....	110
12.10. Jakie są przesłanki nałożenia kary pieniężnej na kierownika podmiotu?	111
12.11. Jakie są kryteria analizy przed nałożeniem kary pieniężnej?	112
12.12. Czy organ właściwy do spraw cyberbezpieczeństwa może odstąpić od nałożenia kary pieniężnej?	112
12.13. Czy postępowanie nakładania kary może zostać umorzone?	112
12.14. Jakie są elementy poważnego naruszenia?	112
13. Obowiązki rejestratorów nazw domen	
[NOWE – aktualizacja czerwiec 2026 r.]	113
13.1. Czy należy podać swoje dane, aby być abonentem nazwy domeny internetowej? [NOWE – aktualizacja czerwiec 2026 r.].....	113
13.2. Jakie dane musi podać abonent nazwy domeny? [NOWE – aktualizacja czerwiec 2026 r.].....	113
13.3. Kto gromadzi i przechowuje dane podawane przez abonentów nazw domeny? [NOWE – aktualizacja czerwiec 2026 r.]	113
13.4. Czy relacje prawne abonentów nazw domeny z rejestrarami nazw domen najwyższego poziomu (TLD) i podmiotami świadczącymi usługi rejestracji nazw domen są ustanawiane na podstawie ustawy o KSC? [NOWE – aktualizacja czerwiec 2026 r.].....	114
13.5. Gdzie będą publikowane dane dotyczące rejestracji nazwy domeny? [NOWE – aktualizacja czerwiec 2026 r.].....	114
13.6. Czy dane osobowe dotyczące abonentów nazw domen podlegają publikacji? [NOWE – aktualizacja czerwiec 2026 r.].....	114
13.7. Czy numer telefonu i adres e-mail abonenta nazwy domeny podlegają publikacji? [NOWE – aktualizacja czerwiec 2026 r.].....	114
13.8. Czy abonent nazwy domeny może wskazać adres e-mail rejestratora zamiast swojego adresu e-mail? [NOWE – aktualizacja czerwiec 2026 r.]	115



13.9. Czy rejestrator to punkt kontaktowy zarządzający nazwą domeny? [NOWE – aktualizacja czerwiec 2026 r.].....	115
13.10. Czy abonent nazwy domeny musi brać udział w weryfikacji danych dotyczących rejestracji nazwy domeny i czemu ona służy? [NOWE – aktualizacja czerwiec 2026 r.].....	115
13.11. Jakie dane podlegają weryfikacji? [NOWE – aktualizacja czerwiec 2026 r.]	116
13.12. Jakie są terminy związane z przekazywaniem i weryfikacją danych dotyczących abonenta nazwy domeny? [NOWE – aktualizacja czerwiec 2026 r.]	116
13.13. Jakie mogą być skutki niepodania danych przez abonenta nazwy domeny lub zaniedbania udziału w procedurach weryfikacyjnych? [NOWE – aktualizacja czerwiec 2026 r.].....	116
13.14. Czy abonent nazwy domeny powinien brać udział w dostosowaniu bazy danych dotyczących rejestracji nazw domen do nowych regulacji? [NOWE – aktualizacja czerwiec 2026 r.].....	117
13.15. Kto jest podmiotem świadczącym usługi rejestracji nazw domen? [NOWE – aktualizacja czerwiec 2026 r.].....	117
13.16. Do kiedy należy wdrożyć obowiązki wynikające z art. 16 b ustawy o KSC? [NOWE – aktualizacja czerwiec 2026 r.]	118
13.17. Kto może żądać udostępnienia danych o domenie? [NOWE – aktualizacja czerwiec 2026 r.]	118
13.18. Czy przy udostępnianiu danych trzeba przestrzegać ochrony danych osobowych? [NOWE – aktualizacja czerwiec 2026 r.]	118
13.19. W jakiej formie składa się żądanie udostępnienia danych? [NOWE – aktualizacja czerwiec 2026 r.]	118
13.20. W jakim terminie należy odpowiedzieć na żądanie? [NOWE – aktualizacja czerwiec 2026 r.]	119
14. Inne	120
14.1. Czy istnieją dodatkowe przepisy unijne określające wymagania cyberbezpieczeństwa dla niektórych podmiotów kluczowych i podmiotów ważnych?	120
14.2. Jaka jest relacja pomiędzy ustawą o KSC a rozporządzeniem DORA?	120
14.3. Czy podleganie pod Rozporządzenie (WE) nr 1907/2006 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2006 r. w sprawie rejestracji, oceny, udzielania zezwoleń i stosowanych ograniczeń w zakresie chemikaliów i utworzenia Europejskiej Agencji Chemikaliów (REACH) oznacza automatyczne objęcie ustawą o KSC?.....	121



- 14.4. Czy podmiot należący do sektora „Produkcja, wytwarzanie i dystrybucja chemikaliów” jest objęty także obowiązkami wynikającymi z rozporządzenia REACH? 122
- 14.5. Czy sformułowanie „Przedsiębiorstwa zajmujące się wytwarzaniem (...) mieszanin chemicznych”, użyte w załączniku nr 2 do ustawy o KSC, należy interpretować szerzej niż definicję „producenta” REACH? 122
- 14.6. Czy przedsiębiorstwa zajmujące się produkcją lub dystrybucją substancji lub mieszanin obejmują też dalszych użytkowników? 122
- 14.7. Czy pojęcie systemu informacyjnego należy odnosić do całego środowiska teleinformatycznego organizacji czy do każdego systemu oddzielnie? [NOWE – aktualizacja czerwiec 2026 r.] 122
- 14.8. Czy urządzenia autonomiczne i rozwiązania smart city mieszczą się w definicji systemu informacyjnego nawet jak nie łączą się z siecią telekomunikacyjną? [NOWE – aktualizacja czerwiec 2026 r.] 123
- 14.9. Czy informacje o podatnościach i incydentach JST mogą zostać wyłączone z udostępnienia jako informacje związane z bezpieczeństwem publicznym lub bezpieczeństwem państwa, o którym mowa w art. 37 i 38 ustawy o KSC? [NOWE – aktualizacja czerwiec 2026 r.] 123
- 14.10. Jak należy rozumieć pojęcie usługi na gruncie ustawy o KSC? 124
- 14.11. Czy Ministerstwo zapewnia materiały wspierające wdrożenie ustawy o KSC? 124
- 14.12. Czy podmioty publiczne mają obowiązek stosować wymogi cyberbezpieczeństwa zawarte w rozporządzeniu w sprawie Krajowych Ram Interoperacyjności? [NOWE – aktualizacja czerwiec 2026 r.] 124



1. Identyfikacja podmiotów kluczowych i podmiotów ważnych

1.1. Co musi zrobić przedsiębiorca, który nie wie czy podlega pod krajowy system cyberbezpieczeństwa?

Przede wszystkim taki przedsiębiorca musi zorientować się jaka jest jego wielkość oraz jakie działalności prowadzi. Dane finansowe przedsiębiorstwa są wskazane w sprawozdaniu finansowym (przesłanki uznania za podmiot kluczowy lub podmiot ważny bada się według stanu na dzień sporządzenia sprawozdania finansowego). Konieczne będzie również ustalenie liczby zatrudnionego personelu. Działalność należy określić w oparciu o prawidłowo zadeklarowane kody Polskiej Klasyfikacji Działalności (PKD) oraz dokumenty urzędowe takie jak koncesje, zezwolenia, wpisy z rejestrów działalności regulowanej. Następnie należy przeanalizować art. 5 ustawy - gdzie wskazano jakie podmioty są podmiotami kluczowymi albo podmiotami ważnymi oraz przeanalizować rodzaje działalności wskazane w załączniku nr 1 i nr 2 do ustawy o KSC.

1.2. Kto jest podmiotem kluczowym?

Podmiotem kluczowym jest:

- 1) osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej wskazana w załączniku nr 1 do ustawy o KSC, która jest dużym przedsiębiorstwem;
- 2) przedsiębiorca komunikacji elektronicznej, który jest średnim lub dużym przedsiębiorstwem;
- 3) dostawca usług zarządzanych w zakresie cyberbezpieczeństwa, który jest małym, średnim lub dużym przedsiębiorstwem;
- 4) niezależnie od wielkości podmiotu:
 - a) dostawca usług DNS,
 - b) kwalifikowany dostawca usług zaufania,
 - c) podmiot krytyczny – w rozumieniu dyrektywy CER,
 - d) podmiot publiczny wskazany w załączniku nr 1 do ustawy o KSC w sektorze podmioty publiczne,
 - e) podmiot zidentyfikowany jako podmiot kluczowy przez organ właściwy do spraw cyberbezpieczeństwa,
 - f) państwowa osoba prawna zidentyfikowana jako podmiot kluczowy w sektorze podmiotów publicznych,



- g) podmiot, który nie jest przedsiębiorcą, a jest wskazany w załączniku nr 1 do ustawy o KSC z nazwy albo poprzez określenie jego rodzaju,
- h) operator obiektu energetyki jądrowej,
- i) rejestr nazw domen najwyższego poziomu (TLD),
- j) podmiot świadczący usługi rejestracji nazw domen.

1.3. Kto jest podmiotem ważnym?

Podmiotem ważnym jest:

- 1) osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej wskazana w załączniku nr 1 do ustawy o KSC, która jest średnim przedsiębiorstwem;
- 2) osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej wskazana w załączniku nr 2 do ustawy o KSC, która jest średnim lub dużym przedsiębiorstwem;
- 3) niekwalifikowany dostawca usług zaufania będący mikro-, małym lub średnim przedsiębiorstwem;
- 4) przedsiębiorca komunikacji elektronicznej będący mikro-, lub małym przedsiębiorstwem;
- 5) inwestor obiektu energetyki jądrowej – niezależnie od jego wielkości;
- 6) podmiot zidentyfikowany jako podmiot ważny przez organ właściwy do spraw cyberbezpieczeństwa;
- 7) podmiot określony w załączniku nr 2 do ustawy o KSC nazwą rodzajową, a który nie jest przedsiębiorcą;
- 8) podmiot publiczny, który nie jest podmiotem kluczowym oraz jest samorządową jednostką budżetową, samorządowym zakładem budżetowym, samorządową instytucją kultury albo spółką prawa handlowego wykonującą zadania o charakterze użyteczności publicznej jeżeli realizuje zadanie publiczne z wykorzystaniem systemów informacyjnych.

1.4. Jakie sektory są objęte ustawą?

Sektory gospodarki objęte ustawą zostały ujęte w załączniku nr 1 i nr 2 do ustawy o KSC.

Sektory kluczowe

- 1) Energia
 - ✓ Wydobywanie kopalin



- ✓ Energia elektryczna
 - ✓ Gaz
 - ✓ Energetyka jądrowa
 - ✓ Wodór
- 2) Transport
- ✓ Transport lotniczy
 - ✓ Transport kolejowy
 - ✓ Transport wodny
 - ✓ Transport drogowy
- 3) Bankowość i infrastruktura rynków finansowych
- 4) Ochrona zdrowia
- ✓ Udzielanie świadczeń zdrowotnych i zdrowie publiczne
 - ✓ Produkcja i dystrybucja substancji czynnych, produktów leczniczych i wyrobów medycznych
- 5) Zaopatrzenie w wodę pitną i jej dystrybucja
- 6) Zbiorowe odprowadzanie ścieków
- 7) Infrastruktura cyfrowa
- ✓ Infrastruktura cyfrowa z wyłączeniem komunikacji elektronicznej
 - ✓ Komunikacja elektroniczna
- 8) Zarządzanie usługami ICT
- 9) Przestrzeń kosmiczna
- 10) Podmioty publiczne

Sektory ważne

- 1) Usługi pocztowe
- 2) Inwestycje energetyki jądrowej
- 3) Gospodarowanie odpadami
- ✓ Zbieranie odpadów
 - ✓ Transport odpadów
 - ✓ Przetwarzanie odpadów, w tym sortowanie, wraz z nadzorem nad wymienionymi działaniami, a także późniejsze postępowanie z miejscami unieszkodliwiania odpadów



- ✓ Działania wykonywane w charakterze sprzedawcy odpadów lub pośrednika w obrocie odpadami
- 4) Produkcja, wytwarzanie i dystrybucja chemikaliów
- 5) Produkcja, przetwarzanie i dystrybucja żywności
- 6) Produkcja
 - ✓ Produkcja wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro
 - ✓ Produkcja komputerów, wyrobów elektronicznych i optycznych
 - ✓ Produkcja urządzeń elektrycznych
 - ✓ Produkcja maszyn i urządzeń, gdzie indziej niesklasyfikowana
 - ✓ Produkcja pojazdów samochodowych, przyczep i naczep
 - ✓ Produkcja pozostałego sprzętu transportowego
- 7) Dostawcy usług cyfrowych
- 8) Badania naukowe
- 9) Podmioty publiczne

1.5. Jak określić wielkość przedsiębiorstwa?

Należy wziąć pod uwagę progi mikro, małych i średnich przedsiębiorstw. Przy obliczaniu wielkości przedsiębiorstwa uwzględnia się również przedsiębiorstwa powiązane oraz przedsiębiorstwa partnerskie.

Rodzaj	liczba zatrudnionych	dane finansowe
Mikroprzedsiębiorstwo	mniej niż 10	roczny obrót lub roczna suma bilansowa nie przekracza 2 mln EUR
Małe przedsiębiorstwo	mniej niż 50	roczny obrót lub roczna suma bilansowa nie przekracza 10 mln EUR
Średnie przedsiębiorstwo	mniej niż 250	roczny obrót nie przekracza 50 mln EUR lub roczna suma bilansowa nie przekracza 43 mln EUR

Do personelu zatrudnionego w podmiocie wlicza się:

- pracowników,



- osoby pracujące dla przedsiębiorstwa, podlegające mu i uważane za pracowników na mocy prawa krajowego,
 - osobę wykonującą pracę na podstawie umowy agencyjnej, umowy zlecenia lub innej umowy o świadczenie usług, do której zgodnie z Kodeksem cywilnym stosuje się przepisy dotyczące zlecenia, albo umowy o dzieło,
- właściciele-kierowników,
- partnerów prowadzących regularną działalność w przedsiębiorstwie i czerpiący z niego korzyści finansowe.

Przy określaniu wielkości podmiotu przydatny będzie Kwalifikator MŚP przygotowany przez Polską Agencję Rozwoju Przedsiębiorczości dostępny pod adresem <https://kwalifikator.parp.gov.pl/>.

1.6. Czy przy ustalaniu wielkości przedsiębiorstwa podmiot musi uwzględnić przedsiębiorstwa partnerskie i powiązane, jeżeli nie świadczy z nimi wspólnie usług?

Przy badaniu statusu mikro-, małych i średnich przedsiębiorstw bierze się pod uwagę przedsiębiorstwa powiązane i przedsiębiorstwa partnerskie – ich przychody, sumę bilansową i liczbę pracowników dolicza się przy ustalaniu wielkości podmiotu. To mogłoby oznaczać, że dany podmiot staje się średnim przedsiębiorcą, wliczając jego przedsiębiorstwa powiązane i partnerskie – i jest wtedy podmiotem ważnym. Ale jego systemy informacyjne, służące świadczeniu usług, mogą mieć charakter niezależny od systemów podmiotów partnerskich i powiązanych. Nie ma więc powodów, aby uznawać ten podmiot za podmiot ważny.

Niezależność systemu informacyjnego zachodzi m.in. wtedy, gdy do świadczenia usług przez podmiot nie jest konieczne działanie podmiotu powiązanego czy partnerskiego. Niezależność może przejawiać się również pod względem zastępowalności sieci i systemów informatycznych, tj. jeżeli w akceptowalnym przez podmiot czasie oraz po akceptowalnych kosztach można zastąpić posiadane rozwiązanie jednego podmiotu rozwiązaniami innych, o nie gorszych właściwościach funkcjonalno-technicznych.

Ponadto, jeżeli podmiot wraz ze swoim przedsiębiorstwem partnerskim lub przedsiębiorstwem powiązanym nie świadczy tej samej usługi (nominalnie podlegającej pod krajowy system cyberbezpieczeństwa) to danych przedsiębiorstwa partnerskiego lub powiązanego nie powinno się ujmować przy ustalaniu wielkości przedsiębiorstwa. Świadczenie tej samej usługi może polegać na tym, że podmioty podzielą między sobą zakres obowiązków związanych z tą usługą. Powinno to być należycie udokumentowane.



1.7. Jakie podmioty są podmiotami kluczowymi niezależnie od ich wielkości?

Podmiotami kluczowymi niezależnie od ich wielkości są:

- dostawca usług DNS,
- kwalifikowany dostawca usług zaufania,
- podmiot krytyczny,
- podmiot publiczny wskazany w załączniku nr 1 do ustawy o KSC w sektorze podmioty publiczne,
- podmiot zidentyfikowany jako podmiot kluczowy w drodze decyzji administracyjnej organu właściwego do spraw cyberbezpieczeństwa,
- państwowa osoba prawna zidentyfikowana jako podmiot kluczowy w drodze decyzji administracyjnej Ministra Cyfryzacji,
- podmiot, który nie jest przedsiębiorcą, a jest wskazany w załączniku nr 1 do ustawy o KSC z nazwy albo przez określenie jego rodzaju,
- podmiot będący operatorem obiektu energetyki jądrowej,
- rejestr nazw domen najwyższego poziomu (TLD),
- podmiot świadczący usługi rejestracji nazw domen.

1.8. Czy wszystkie podmioty publiczne podlegają pod ustawę o krajowym systemie cyberbezpieczeństwa?

Ustawę stosuje się do podmiotów publicznych wskazanych w załączniku nr 1 i 2 do ustawy o KSC.

Podmioty wskazane w załączniku nr 1 do ustawy o KSC w sektorze „podmioty publiczne” są podmiotami kluczowymi niezależnie od wielkości podmiotu.

Podmioty wskazane w załączniku nr 2 do ustawy o KSC w sektorze „podmioty publiczne” są podmiotami ważnymi niezależnie od wielkości podmiotu.

Oznacza to, że podlegają obowiązkowi wpisu do wykazu. **Nie robią tego jednak samodzielnie.** Wpisanie podmiotów publicznych do wykazu następuje **z urzędu**, a podmiot zostaje o tym **zawiadomiony**. Takiego wpisu dokonuje minister właściwy do spraw informatyzacji na podstawie:

- Danych zawartych w rejestrach publicznych
- Danych zawartych w bazie adresów elektronicznych
- Danych przekazanych przez właściwe organy nadzorcze

Jeżeli minister właściwy do spraw informatyzacji stwierdzi brak danych, które wymagane są do dokonania wpisu do wykazu, zwróci się do takiego podmiotu z wezwaniem do uzupełnienia danych, w terminie 6 w miesięcy od dnia doręczenia wezwania.



Przykładowe podmioty publiczne będące podmiotami kluczowymi to: starostwa powiatowe, instytuty badawcze, państwowe instytucje kultury, wojewódzkie fundusze ochrony środowiska i gospodarki wodnej.

Urząd gminy jest podmiotem kluczowym i podlega wpisowi do wykazu jako ten podmiot **tylko jeżeli** zatrudnia na dzień 1 stycznia danego roku w przeliczeniu na pełny etat czasu pracy na podstawie umowy o pracę co najmniej 50 osób. Pozostałe urzędy gminy będące samorządowymi jednostkami budżetowymi są podmiotami ważnymi.

1.9. Czy wszyscy przedsiębiorcy telekomunikacyjni podlegają pod ustawę o krajowym systemie cyberbezpieczeństwa?

Wszyscy przedsiębiorcy telekomunikacyjni niezależnie od ich wielkości podlegają pod ustawę. Status podmiotu będzie się jednak różnił od wielkości.

Przedsiębiorca telekomunikacyjny	
Wielkość	Rodzaj
Duży przedsiębiorca	podmiot kluczowy
Średni przedsiębiorca	podmiot kluczowy
Mały przedsiębiorca	podmiot ważny
Mikroprzedsiębiorca	podmiot ważny

1.10. Co w przypadku, gdy podmiot spełnia kryteria zarówno dla podmiotu kluczowego jak i podmiotu ważnego?

Podmiot spełniający kryteria dla podmiotu kluczowego oraz podmiotu ważnego jest podmiotem kluczowym i tak go należy traktować.

1.11. Czym się różni podmiot kluczowy od podmiotu ważnego?

Upraszczając, co do zasady podmiotem kluczowym jest duży przedsiębiorca wskazany w załączniku nr 1 do ustawy. Podmiotem ważnym jest średni przedsiębiorca wskazany w załączniku nr 1 do ustawy o KSC oraz duży i średni przedsiębiorca prowadzący działalność określoną w załączniku nr 2 do ustawy. Jednakże istnieje od tego szereg wyjątków.

Merytoryczne obowiązki podmiotu kluczowego i podmiotu ważnego są takie same. Różnica sprowadza się do zakresu czynności nadzorczych, które mogą prowadzić organy właściwe do spraw cyberbezpieczeństwa. Nadzór nad podmiotami kluczowymi ma charakter ex ante, a nadzór nad podmiotami ważnymi ex post. Podmioty kluczowe mają obowiązek przeprowadzić audyt co 3 lata oraz na żądanie organu właściwego do spraw cyberbezpieczeństwa. Podmioty ważne



przeprowadzają audyt wyłącznie na żądanie organu właściwego do spraw cyberbezpieczeństwa.

1.12. Czy podmiot kluczowy lub podmiot ważny otrzymują decyzję administracyjną o ich kwalifikacji?

Nie – każdy podmiot prowadzący działalność wskazaną w załącznikach nr 1 i 2 do ustawy o KSC musi przeanalizować czy jest podmiotem kluczowym lub podmiotem ważnym.

Istnieje od tego wyjątek – organy właściwe do spraw cyberbezpieczeństwa mogą uznać za podmiot kluczowy lub ważny podmiot, który co do zasady nie spełnia wymogów ustawowych, ale spełnia jedną z następujących przesłanek:

- 1) jako jedyny świadczy usługę, która ma kluczowe znaczenie dla krytycznej działalności społecznej lub gospodarczej,
- 2) zakłócenie świadczenia usługi przez niego spowoduje poważne zagrożenie dla bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub obronności,
- 3) zakłócenie świadczenia usługi przez niego spowoduje ryzyko systemowe zaprzestania świadczenia usług przez podmioty kluczowe lub podmioty ważne lub
- 4) świadczenie przez niego usług ma istotne znaczenie na poziomie krajowym lub województwa lub ma znaczenie dla dwóch lub więcej sektorów określonych w załączniku nr 1 lub 2 do ustawy.

Przepis ten ma zagwarantować, że w krajowym systemie cyberbezpieczeństwa znajdują się wszystkie podmioty prowadzące szczególnie istotną dla państwa i społeczeństwa działalność. Jak wykazały doświadczenia pandemii w wielu przypadkach zaprzestanie działalności przez stosunkowo mały podmiot może mieć bardzo szerokie skutki dla innej działalności, np. w sektorze energetyki czy przemyśle. Tego rodzaju podmioty muszą znaleźć się w krajowym systemie cyberbezpieczeństwa.

1.13. Czy organ właściwy do spraw cyberbezpieczeństwa może skierować zapytanie do podmiotu w sprawie ustalenia czy jest podmiotem kluczowym lub podmiotem ważnym?

Tak, organ właściwy do spraw cyberbezpieczeństwa może odpytać każdy podmiot i żądać przedstawienia informacji umożliwiających identyfikację podmiotu jako podmiot kluczowy lub podmiot ważny.



1.14. Kiedy podmiot kluczowy lub podmiot ważny podlega pod właściwość polskich organów?

Jeżeli podmioty kluczowe lub podmioty ważne mają miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej lub prowadzą działalność na terytorium Rzeczypospolitej Polskiej przez swoje siedziby, oddziały lub w ramach działalności transgranicznej to podlegają pod właściwość polskich organów.

Przedsiębiorcy komunikacji elektronicznej podlegają pod właściwość polskich organów, jeżeli świadczą swoje usługi na terytorium Rzeczypospolitej Polskiej.

Ustawę o KSC stosuje się do podmiotów publicznych niezależnie od miejsca ich siedziby – obejmie więc ona polskie placówki dyplomatyczne i konsularne.

1.15. Jakie są wyjątki od jurysdykcji polskiej?

Wyjątki dotyczą niektórych podmiotów z sektorów infrastruktury cyfrowej, zarządzania usługami ICT oraz dostawców usług cyfrowych. Jeśli te podmioty świadczą usługi na terenie Polski, to podlegają ustawie jeśli Polska jest głównym miejscem prowadzenia działalności przez ten podmiot. Kryterium to jest ustalone w sposób schodkowy:

- 1) Głównym miejscem prowadzenia działalności jest państwo członkowskie Unii Europejskiej, w którym ma siedzibę kierownik podmiotu podejmujący decyzje w sprawie systemu zarządzania bezpieczeństwem informacji.
- 2) Jeżeli tej informacji nie można ustalić, to głównym miejscem prowadzenia działalności jest państwo członkowskie Unii Europejskiej, w którym są realizowane zadania związane z systemem zarządzania bezpieczeństwem informacji.
- 3) Jeżeli i tej informacji nie można ustalić to głównym miejscem prowadzenia działalności jest państwo członkowskie UE.

1.16. Czy szkoły (podstawowe), przedszkola również są podmiotami KSC?

Podmiotami krajowego systemu cyberbezpieczeństwa są m.in. jednostki budżetowe - szkoły publiczne czy przedszkola są jednostkami budżetowymi. Jednocześnie ustawa przewiduje dla tego typu mniejszych jednostek uproszczone wymagania cyberbezpieczeństwa, określone w załączniku nr 4 do ustawy oraz możliwość tworzenia, np. przez gminę, wspólnych jednostek obsługowych z zakresu cyberbezpieczeństwa.



1.17. Kiedy uczelnia staje się organizacją badawczą w rozumieniu ustawy?

Jeżeli uczelnia w ramach swojej podstawowej działalności prowadzi badania aplikacyjne lub prace rozwojowe za pomocą systemów informacyjnych to taka uczelnia będzie organizacją badawczą - podmiotem ważnym zobligowanym do wdrożenia systemu zarządzania bezpieczeństwem informacji wskazanego w art. 8 ust. 1 ustawy.

Przy czym sformułowanie "za pomocą systemów informacyjnych" należy rozumieć w ten sposób, że bez systemu informacyjnego przeprowadzenie badań naukowych lub prac rozwojowych jest niemożliwe. Nie chodzi tutaj o tylko zwykłe udokumentowanie tego rodzaju działań, a faktyczne prowadzenie badań naukowych lub prac rozwojowych np. poprzez prowadzenie symulacji, obliczenia, przetwarzanie dużej ilości danych itd.

1.18. Czy przedsiębiorca komunikacji elektronicznej w świetle ustawy może być dostawcą sieci dostarczania treści (Content Delivery Network)?

Ustawa rozgraniczyła te definicje, wyraźnie wskazując, że za dostawcę sieci dostarczania treści nie uznaje się przedsiębiorcy komunikacji elektronicznej. Przedsiębiorcy komunikacji elektronicznej i świadczone przez nich usługi podlegają reżimowi ustawy – ich usługi CDN też będą podlegać pod reżim ustawy jako usługi komunikacji elektronicznej.

1.19. Czy mały przedsiębiorca komunikacji elektronicznej będący jednocześnie dostawcą usługi dostępu do Internetu oraz świadczący usługę DNS będzie podmiotem kluczowym czy podmiotem ważnym?

Taki podmiot będzie podmiotem ważnym.

Dostawca usługi DNS jest podmiotem kluczowym niezależnie od wielkości podmiotu. Jednakże definicja wskazuje, że jest to podmiot, który świadczy **dostępne publicznie** rekurencyjne usługi rozpoznawania nazw domen **na rzecz ogółu użytkowników końcowych Internetu** lub autorytatywne usługi rozpoznawania nazw domen **do użytku ogółu użytkowników końcowych Internetu**, z wyjątkiem głównych serwerów nazw. Definicja wskazuje, że chodzi o usługi świadczone publicznie dla ogółu użytkowników Internetu a nie tylko dla własnych użytkowników.

Po drugie wyjaśnienia Organu Europejskich Regulatorów Łączności Elektronicznej (BEREC) wskazują, że serwery DNS udostępniane przez dostawcę usług internetowych w ramach usługi dostępu do Internetu stanowią w praktyce część



tej usługi, ponieważ są one instalowane automatycznie w momencie uruchomienia połączenia, a bez nich usługa dostępu do internetu byłaby praktycznie bezużyteczna dla przeciętnego użytkownika końcowego. Są więc one elementem usługi dostępu do Internetu a nie samodzielną usługą.

W konsekwencji nie należy traktować małego dostawcy usługi dostępu do Internetu jako dostawcę usługi DNS, ponieważ ta usługa nie jest usługą samodzielną, a jedynie elementem usługi dostępu do internetu.

BEREC Guidelines on the Implementation of the Open Internet Regulation
https://www.berec.europa.eu/sites/default/files/files/document_register_store/2022/6/BoR_%2822%29_81_Update_to_the_BEREC_Guidelines_on_the_Implementation_of_the_Open_Internet_Regulation.pdf

1.20. Co, jeśli przedsiębiorca dokona nieprawidłowej samoidentyfikacji?

Firmy, które nie zarejestrują się w wykazie będą wpisywane z urzędu przez organy właściwe do spraw cyberbezpieczeństwa. Konsekwencją takiego działania mogą być jednak czynności nadzorcze nad podmiotem lub w dalszej perspektywie nałożenie administracyjnej kary pieniężnej.

Natomiast podmiot wpisany do wykazu podmiotów kluczowych i podmiotów ważnych, który nie podlega pod ustawę, będzie mógł być wykreślony z wykazu przez organ właściwy do spraw cyberbezpieczeństwa.

1.21. Czy spółka IT realizująca zadania z zakresu cyberbezpieczeństwa tylko dla własnej grupy kapitałowej podlega znowelizowanej KSC?

Tak, jeżeli jest co najmniej małym przedsiębiorstwem. Skoro tego typu podmioty świadczą usługi np. obsługi incydentów, przetwarzając przy tym wrażliwe dane swoich klientów, to powinny spełniać wymogi z zakresu cyberbezpieczeństwa.

1.22. Kim jest dostawca usług chmurowych?

Dostawca usług chmurowych jest to podmiot świadczący usługi przetwarzania danych w modelu chmury obliczeniowej, zapewniając użytkownikowi na żądanie zdalny dostęp do skalowalnych oraz elastycznych zasobów IT - m.in. mocy obliczeniowej, pamięci, oprogramowania lub platform. Obejmuje to w szczególności usługi w modelu infrastruktura jako usługa (IaaS), platforma jako usługa (PaaS) oraz oprogramowanie jako usługa (SaaS). Usługi te mogą być świadczone w różnych modelach wdrożeń, np. chmurze prywatnej, publicznej, hybrydowej, czy wspólnotowej.

Przy identyfikacji, czy dany dostawca jest dostawcą usług chmurowych należy przede wszystkim zwrócić uwagę na cel i funkcjonalność usługi, tj. czy usługa



zapewnia użytkownikowi bezpośredni dostęp do skalowalnej i elastycznej puli zasobów obliczeniowych. W niektórych sytuacjach, w modelu SaaS, dostawca może być jedynie dostawcą oprogramowania, a nie dostawcą chmury obliczeniowej. Może to mieć miejsce w sytuacji, w której dostawca oprogramowania korzysta jedynie z chmury obliczeniowej, ale nie jest jej dostawcą, a dane oprogramowanie uruchamiane jest u odbiorcy na zasadzie on-premise.

1.23. Czy w zakres definicji dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa wchodzi dostawca oprogramowania?

Nie, nie wchodzi. Dostawcy oprogramowania co do zasady są regulowani przez Cyber Resilience Act.

1.24. Czy objęcie podmiotów publicznych – podmiotów ważnych wspólną obsługą przez jednostkę wyznaczoną do realizacji z zakresu cyberbezpieczeństwa powoduje automatyczne podniesienie statusu podmiotu ważnego do podmiotu kluczowego?

[NOWE – aktualizacja czerwiec 2026 r.]

Status podmiotu publicznego jako podmiotu kluczowego lub podmiotu ważnego nie zależy od tego czy jest on obsługiwany przez jednostkę wyznaczoną. Jednostka ta realizuje zadania z zakresu cyberbezpieczeństwa dla obsługiwanych podmiotów publicznych - podmiotów ważnych zgodnie z załącznikiem nr 4 do ustawy. Może przy tym wdrożyć dodatkowe środki techniczne i organizacyjne, jeżeli jest to konieczne dla zapewnienia odpowiedniego poziomu bezpieczeństwa systemów informacyjnych.

1.25. Jakie podmioty publiczne będą podmiotami kluczowymi? **[NOWE - aktualizacja czerwiec 2026 r.]**

Podmiotami kluczowymi będą następujące podmioty publiczne:

- 1) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, oraz urzędy je obsługujące;
 - a. organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały;
 - b. Przykłady: Ministrowie i ministerstwa, wojewodowie i urzędy wojewódzkie, sądy powszechne, urzędy centralne, np. Prezes



Urzędu Komunikacji Elektronicznej wraz z Urzędem Komunikacji Elektronicznej, Służba Ochrony Państwa;

- 2) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 3, 5–6, 8 i 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych;
 - a. jednostki budżetowe;
 - i. Jednostkami budżetowymi są jednostki organizacyjne sektora finansów publicznych nieposiadające osobowości prawnej, które pokrywają swoje wydatki bezpośrednio z budżetu, a pobrane dochody odprowadzają na rachunek odpowiednio dochodów budżetu państwa albo budżetu jednostki samorządu terytorialnego;
 - b. agencje wykonawcze;
 - i. Polska Agencja Kosmiczna – wskazana w sektorze kosmicznym;
 - ii. Narodowy Instytut Wolności – Centrum Rozwoju Społeczeństwa Obywatelskiego;
 - iii. Polska Agencja Rozwoju Przedsiębiorczości;
 - iv. Narodowe Centrum Badań i Rozwoju;
 - v. Narodowe Centrum Nauki;
 - vi. Agencja Mienia Wojskowego;
 - vii. Agencja Restrukturyzacji i Modernizacji Rolnictwa;
 - viii. Krajowy Ośrodek Wsparcia Rolnictwa;
 - ix. Centralny Ośrodek Badań Odmian Roślin Uprawnych;
 - x. Rządowa Agencja Rezerw Strategicznych wskazana w sektorze energetycznym;
 - c. instytucje gospodarki budżetowej;
 - i. Centrum Obsługi Kancelarii Prezydenta RP;
 - ii. Centrum Zakupów dla Sądownictwa Instytucja Gospodarki Budżetowej;
 - iii. Centrum Obsługi Administracji Rządowej;
 - iv. Centralny Ośrodek Informatyki;
 - v. Centrum Usług Logistycznych;
 - vi. Centralny Ośrodek Sportu;
 - vii. Zakład Inwestycji Organizacji Traktatu Północnoatlantyckiego;
 - viii. Profilaktyczny Dom Zdrowia w Juracie;
 - ix. Krajowy Instytut Mediów w likwidacji;
 - d. Zakład Ubezpieczeń Społecznych i zarządzane przez niego fundusze;
 - e. Kasa Rolniczego Ubezpieczenia Społecznego i fundusze zarządzane przez Prezesa Kasy Rolniczego Ubezpieczenia Społecznego;
 - f. Narodowy Fundusz Zdrowia;
- 3) państwowe instytucje kultury;



- a. Ministrowie oraz kierownicy urzędów centralnych organizują działalność kulturalną, tworząc państwowe instytucje kultury, dla których prowadzenie takiej działalności jest podstawowym celem statutowym;
- 4) instytuty badawcze;
 - a. Instytuty badawcze są tworzone przez Radę Ministrów w drodze rozporządzenia;
- 5) Narodowy Bank Polski;
- 6) Bank Gospodarstwa Krajowego;
- 7) Urząd Dozoru Technicznego;
- 8) Polska Agencja Żeglugi Powietrznej;
- 9) Polskie Centrum Akredytacji;
- 10) Urząd Komisji Nadzoru Finansowego;
- 11) Polska Agencja Prasowa;
- 12) Państwowe Gospodarstwo Wodne Wody Polskie;
- 13) Polski Fundusz Rozwoju i inne instytucje rozwoju, o których mowa w art. 2 ust. 1 pkt 1 i 3–6 ustawy z dnia 4 lipca 2019 r. o systemie instytucji rozwoju;
 - a. Polski Fundusz Rozwoju;
 - b. Polska Agencja Rozwoju Przedsiębiorczości;
 - c. Korporacja Ubezpieczeń Kredytów Eksportowych Spółka Akcyjna;
 - d. Polska Agencja Inwestycji i Handlu Spółka Akcyjna;
 - e. Agencja Rozwoju Przemysłu Spółka Akcyjna;
- 14) Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej;
- 15) wojewódzkie fundusze ochrony środowiska i gospodarki wodnej;
- 16) Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych;
- 17) Zakład Unieszkodliwiania Odpadów Promieniotwórczych z siedzibą w Otwocku-Świerku;
- 18) państwowa osoba prawna, wobec której wydano decyzję, o której mowa w art. 7m;
- 19) spółka, o której mowa w art. 2 ust. 1 ustawy z dnia 29 kwietnia 2016 r. o szczególnych zasadach wykonywania niektórych zadań dotyczących informatyzacji w zakresie działań administracji rządowej budżet i finanse publiczne;
- 20) w odniesieniu do samorządu województwa: jednostki budżetowe oraz zakłady budżetowe z wyjątkami;
- 21) w odniesieniu do samorządu powiatu: starostwo powiatowe;
- 22) w odniesieniu do samorządu gminy: urząd gminy, jeżeli zatrudnia na dzień 1 stycznia danego roku w przeliczeniu na pełny wymiar czasu pracy na podstawie umowy o pracę co najmniej 50 osób.



1.26. Czy wszystkie wojewódzkie jednostki budżetowe oraz wojewódzkie zakłady budżetowe są podmiotami kluczowymi? [NOWE - aktualizacja czerwiec 2026 r.]

Nie. Podmiotami kluczowymi nie są wojewódzkie:

1. przedszkola;
3. szkoły;
4. placówki oświatowo-wychowawcze;
4. placówki kształcenia ustawicznego, centra kształcenia zawodowego oraz branżowe centra umiejętności, umożliwiające uzyskanie i uzupełnienie wiedzy, umiejętności i kwalifikacji zawodowych lub zmianę kwalifikacji zawodowych;
5. placówki artystyczne;
6. poradnie psychologiczno-pedagogiczne;
7. młodzieżowe ośrodki wychowawcze, młodzieżowe ośrodki socjoterapii, specjalne ośrodki szkolno-wychowawcze oraz specjalne ośrodki wychowawcze dla dzieci i młodzieży wymagających stosowania specjalnej organizacji nauki, metod pracy i wychowania, a także ośrodki rewalidacyjno-wychowawcze;
8. placówki zapewniające opiekę i wychowanie uczniom w okresie pobierania nauki poza miejscem stałego zamieszkania;
9. placówki doskonalenia nauczycieli;
10. biblioteki pedagogiczne;
11. kolegia pracowników służb społecznych;
12. jednostki organizacyjne województwa wykonujące zadania w zakresie wspierania rodziny i systemu pieczy zastępczej;
13. placówki wsparcia dziennego;
14. organizatorzy rodzinnej pieczy zastępczej;
15. placówki opiekuńczo-wychowawcze;
16. regionalne placówki opiekuńczo-terapeutyczne;
17. interwencyjne ośrodki preadopcyjne;
18. ośrodki adopcyjne;
19. jednostek organizacyjnych, o których mowa w art. 6 pkt 5 ustawy z dnia 12 marca 2004 r. o pomocy społecznej, oprócz regionalnych ośrodków polityki społecznej;
20. ośrodek pomocy społecznej;
21. centrum usług społecznych - w przypadku przekształcenia ośrodka pomocy społecznej w centrum usług społecznych na podstawie przepisów



ustawy z dnia 19 lipca 2019 r. o realizowaniu usług społecznych przez centrum usług społecznych (Dz.U. poz. 1818 oraz z 2025 r. poz. 620);

22. dom pomocy społecznej;
23. placówkę specjalistycznego poradnictwa, w tym rodzinnego;
24. ośrodek wsparcia i ośrodek interwencji kryzysowej;
25. wojewódzkie urzędy pracy;
26. parki krajobrazowe i ich zespoły;
27. jednostek obsługujących, o których mowa w art. 8d ustawy z dnia 5 czerwca 1998 r. o samorządzie województwa, w zakresie, w jakim prowadzą wspólną obsługę ww. jednostek.

1.27. Które przedsiębiorstwa spożywcze są podmiotami ważnymi w sektorze „produkcja, przetwarzanie i dystrybucja żywności”? [NOWE - aktualizacja czerwiec 2026 r.]

Przedsiębiorstwo spożywcze, będące co najmniej średnim przedsiębiorstwem będzie zaklasyfikowane jako podmiot ważny, o ile prowadzi jeden z typów działalności:

Dystrybucja hurtowa żywności – pomocne dla ustalenia tej działalności mogą być kody PKD 2025:

SEKCJA G		HANDEL HURTOWY I DETALICZNY		
Dział	Grupa	Klasa	Podklasa	Nazwa grupowania
46				Handel hurtowy
	46.1			Sprzedaż hurtowa realizowana na zlecenie
		46.17	46.17.Z	Działalność agentów zajmujących się sprzedażą hurtową żywności, napojów i wyrobów tytoniowych
	46.3			Sprzedaż hurtowa żywności, napojów i wyrobów tytoniowych
		46.31	46.31.Z	Sprzedaż hurtowa owoców i warzyw
		46.32	46.32.Z	Sprzedaż hurtowa mięsa i wyrobów z mięsa oraz ryb i wyrobów z ryb
		46.33	46.33.Z	Sprzedaż hurtowa mleka, wyrobów mleczarskich, jaj, olejów i tłuszczów jadalnych



		46.34		Sprzedaż hurtowa napojów alkoholowych i bezalkoholowych
			46.34.A	Sprzedaż hurtowa napojów alkoholowych
			46.34.B	Sprzedaż hurtowa napojów bezalkoholowych
		46.35	46.35.Z	Sprzedaż hurtowa wyrobów tytoniowych
		46.36	46.36.Z	Sprzedaż hurtowa cukru, czekolady i wyrobów cukierniczych
		46.37	46.37.Z	Sprzedaż hurtowa herbaty, kawy, kakao i przypraw
		46.38	46.38.Z	Sprzedaż hurtowa pozostałej żywności
		46.39	46.39.Z	Sprzedaż hurtowa niewyspecjalizowana żywności, napojów i wyrobów tytoniowych

Przemysłowa produkcja i przetwarzanie żywności

SEKCJA C		PRZETWÓRSTWO PRZEMYSŁOWE		
Dział	Grupa	Klasa	Podklasa	Nazwa grupowania
10				Produkcja artykułów spożywczych
	10.1			Przetwarzanie i konserwowanie mięsa oraz produkcja wyrobów z mięsa
		10.11	10.11.Z	Przetwarzanie i konserwowanie mięsa, z wyłączeniem mięsa z drobiu
		10.12	10.12.Z	Przetwarzanie i konserwowanie mięsa z drobiu
		10.13	10.13.Z	Produkcja wyrobów z mięsa, włączając wyroby z mięsa drobiowego
	10.2	10.20	10.20.Z	Przetwarzanie i konserwowanie ryb, skorupiaków i mięczaków
	10.3			Przetwarzanie i konserwowanie owoców i warzyw
		10.31	10.31.Z	Przetwarzanie i konserwowanie ziemniaków
		10.32	10.32.Z	Produkcja soków z owoców i warzyw



	10.39	10.39.Z	Pozostałe przetwarzanie i konserwowanie owoców i warzyw
10.4			Produkcja olejów i tłuszczów pochodzenia roślinnego i zwierzęcego
	10.41	10.41.Z	Produkcja olejów i pozostałych tłuszczów płynnych
	10.42	10.42.Z	Produkcja margaryny i podobnych tłuszczów jadalnych
10.5			Wytwarzanie wyrobów mleczarskich i lodów jadalnych
	10.51	10.51.Z	Wytwarzanie wyrobów mleczarskich
	10.52	10.52.Z	Produkcja lodów śmietankowych i pozostałych lodów jadalnych
10.6			Wytwarzanie produktów przemiału zbóż, skrobi i wyrobów skrobiowych
	10.61	10.61.Z	Wytwarzanie produktów przemiału zbóż
	10.62	10.62.Z	Wytwarzanie skrobi i wyrobów skrobiowych
10.7			Produkcja wyrobów piekarniczych i mącznych
	10.71	10.71.Z	Produkcja pieczywa; produkcja świeżych wyrobów ciastkarskich i ciastek
	10.72	10.72.Z	Produkcja sucharów, herbatników, konserwowanych wyrobów ciastkarskich i ciastek
	10.73	10.73.Z	Produkcja wyrobów mącznych
10.8			Produkcja pozostałych artykułów spożywczych
	10.81	10.81.Z	Produkcja cukru
	10.82	10.82.Z	Produkcja kakao, czekolady i wyrobów cukierniczych
	10.83	10.83.Z	Przetwórstwo herbaty i kawy



		10.84	10.84.Z	Produkcja przypraw
		10.85	10.85.Z	Wytwarzanie gotowych posiłków i dań
		10.86	10.86.Z	Produkcja artykułów spożywczych homogenizowanych i żywności dietetycznej
		10.89		Produkcja pozostałych artykułów spożywczych, gdzie indziej niesklasyfikowana
			10.89.A	Produkcja suplementów diety
			10.89.B	Produkcja substytutów mięsa
			10.89.C	Produkcja roślinnych substytutów dla jaj, nabiału i innych produktów mlecznych, z wyłączeniem napojów
			10.89.D	Produkcja pozostałych artykułów spożywczych, z wyłączeniem suplementów diety, substytutów mięsa, roślinnych substytutów dla jaj, nabiału i innych produktów mlecznych, gdzie indziej niesklasyfikowana
11	11.0			Produkcja napojów
		11.01	11.01.Z	Destylowanie, rektyfikowanie i mieszanie alkoholi
		11.02	11.02.Z	Produkcja win gronowych
		11.03	11.03.Z	Produkcja cydru i pozostałych owocowych napojów fermentowanych
		11.04	11.04.Z	Produkcja pozostałych niedestylowanych napojów fermentowanych
		11.05	11.05.Z	Produkcja piwa
		11.06	11.06.Z	Produkcja słodu
		11.07	11.07.Z	Produkcja napojów bezalkoholowych i wód butelkowanych
12	12.0	12.00	12.00.Z	Produkcja wyrobów tytoniowych



2. Wykaz podmiotów kluczowych i podmiotów ważnych

2.1. Kiedy należy zarejestrować się w wykazie podmiotów kluczowych i podmiotów ważnych?

Podmioty spełniające wymogi dla podmiotów kluczowych i podmiotów ważnych będą obowiązane do zarejestrowania się w tym rejestrze w terminie 6 miesięcy od dnia spełnienia przesłanek uznania za podmiot kluczowy albo podmiot ważny.



Pierwszą taką analizę należy przeprowadzić więc na moment wejścia w życie ustawy, czyli dzień **3 kwietnia 2026 r.**

Podmioty, które na dzień wejścia w życie ustawy, tj. 3 kwietnia 2026 r., spełniają warunki uznania za podmiot kluczowy lub podmiot ważny są obowiązane złożyć wnioski o wpis do wykazu do **3 października 2026 r.**

Wpisu dokonuje się za pomocą **systemu S46**.

2.2. W jaki sposób należy złożyć wniosek o wpis do wykazu podmiotów kluczowych i podmiotów ważnych?

Wnioski będą składane w systemie teleinformatycznym S46. Wniosek będzie mógł być podpisany kwalifikowanym podpisem elektronicznym, podpisem zaufanym, podpisem osobistym kierownika podmiotu kluczowego lub podmiotu ważnego albo osoby upoważnionej albo kwalifikowaną pieczęcią elektroniczną.

2.3. Które podmioty zostaną wpisane do wykazu z urzędu?

Minister właściwy do spraw informatyzacji dokona z urzędu wpisu do wykazu:

- przedsiębiorców telekomunikacyjnych,
- dostawców usług zaufania,
- podmiotów publicznych,
- dotychczasowych operatorów usług kluczowych.

Takiego wpisu dokonuje się na podstawie danych zawartych w rejestrach publicznych, danych zawartych w bazie adresów elektronicznych oraz danych przekazanych przez właściwe organy nadzorcze.

Jeżeli minister właściwy do spraw informatyzacji stwierdzi brak danych, które wymagane są do dokonania wpisu do wykazu, zwróci się do takiego podmiotu z wezwaniem do uzupełnienia danych, w terminie 6 w miesięcy od dnia doręczenia wezwania.

Doręczenie jest realizowane na adres do doręczeń elektronicznych lub z wykorzystaniem publicznej usługi hybrydowej, o których mowa w ustawie



o doręczeniach elektronicznych. W przypadku przedsiębiorców telekomunikacyjnych doręczenie może być realizowane za pomocą Platformy Usług Elektronicznych Urzędu Komunikacji Elektronicznej.

Wezwanie zawiera w szczególności:

- dane podmiotu wpisane do Wykazu KSC,
- wskazanie brakujących danych, które podmiot musi uzupełnić,
- dane pozwalające na zalogowanie się do aplikacji Wykaz KSC na konto podmiotu.

Podmiot wpisany z urzędu otrzyma zawiadomienie o tym fakcie.

Wobec tego konieczne jest aby jak najszybciej podmioty publiczne, które tego nie zrobiły, założyły i aktywowały adres do doręczeń elektronicznych.

2.4. Czy organ właściwy do spraw cyberbezpieczeństwa może wpisać z urzędu podmiot do wykazu podmiotów kluczowych i podmiotów ważnych?

Tak, organ właściwy do spraw cyberbezpieczeństwa będzie mógł również z urzędu wpisać dany podmiot do wykazu podmiotów kluczowych i podmiotów ważnych jeżeli podmiot spełnia kryteria podmiotu kluczowego lub podmiotu ważnego, a podmiot ten nie wpisał się do wykazu w terminie 6 miesięcy od spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny. To rozwiązanie gwarantuje, że nawet jeśli dany podmiot nie będzie chciał się wpisać do wykazu, będzie możliwe włączenie go do rejestru.

2.5. Czy spółka uznana za operatora usługi kluczowej musi wpisać się do wykazu podmiotów kluczowych i podmiotów ważnych?

Operatorzy usług kluczowych zostaną wpisani do wykazu podmiotów kluczowych i podmiotów ważnych z urzędu przez Ministra Cyfryzacji.

2.6. Czy wszystkie urzędy gmin stają się automatycznie podmiotem ważnym lub kluczowym? Czy urząd otrzyma decyzję o ujęciu w rejestrze jako podmiot kluczowy lub ważny?

Wszystkie urzędy gmin staną się podmiotami krajowego systemu cyberbezpieczeństwa. Urzędy gmin, które zatrudniają na dzień 1 stycznia danego roku w przeliczeniu na pełny wymiar czasu pracy na podstawie umowy o pracę co



najmniej 50 osób będą podmiotami kluczowymi. Pozostałe urzędy gmin będą co do zasady podmiotami ważnymi.

Minister Cyfryzacji wpisze z urzędu wszystkie urzędy gmin do wykazu podmiotów kluczowych i podmiotów ważnych - podmioty te otrzymają ewentualnie wezwanie do uzupełnienia brakujących danych.

2.7. Czy wpisowi do wykazu podmiotów kluczowych i podmiotów ważnych podlega działalność faktyczna czy ta wykazana w rejestrach publicznych?

Zarówno w wykazie podmiotów kluczowych i podmiotów ważnych jak i w pozostałych rejestrach publicznych należy wykazywać działalność faktycznie wykonywaną.

2.8. Co z przedsiębiorstwem, którego główna działalność nie kwalifikuje się do wpisania do rejestru podmiotów ważnych i kluczowych, ale poboczna tak. Czy powinien złożyć wniosek o wpis?

Ustawie KSC podlega działalność podmiotu wskazana w załącznikach do ustawy, niezależnie od tego, czy jest to działalność główna czy pomocnicza.

Wyjątki dotyczą kilku sektorów – sektora zaopatrzenia w wodę i jej dystrybucji, zbiorowego odprowadzania ścieków, gospodarowania odpadami, gdzie regulacje dotyczą wyłącznie działalności głównej. W tym przypadku istotna jest główna działalność podmiotu.

2.9. Czy spółki zależne od operatora usługi kluczowej też powinny zostać zgłoszone do wykazu podmiotów kluczowych i podmiotów ważnych?

Spółki zależne od operatora usług kluczowych powinny samodzielnie zarejestrować się w wykazie podmiotów kluczowych i podmiotów ważnych, jeżeli spełniają kryteria podmiotu kluczowego lub podmiotu ważnego.

2.10. Jakie dane będą znajdowały się w wykazie podmiotów kluczowych i podmiotów ważnych?

Wykaz będzie zawierał wszystkie informacje niezbędne do skutecznego nadzoru nad tymi podmiotami. Przede wszystkim będą to dane identyfikujące podmiot – nazwa (firma) podmiotu, sektor, podsektor i rodzaj lub rodzaje podmiotu, zgodnie z załącznikiem nr 1 lub 2 do ustawy o KSC, siedzibę i adres do korespondencji, adres do doręczeń elektronicznych, jeżeli został nadany, adres poczty



elektronicznej, numer identyfikacji podatkowej (NIP), numer w krajowym rejestrze urzędowym podmiotów gospodarki narodowej (REGON) oraz numer we właściwym rejestrze działalności regulowanej.

Oprócz samych danych identyfikujących będą w nim zawarte informacje takie jak:

- 1) zakres publicznych adresów IP wykorzystywanych przez podmiot wykorzystywanych w sposób ciągły;
- 2) zakres nazw domen wykorzystywane przez ten podmiot w sposób ciągły;
- 3) dane osób do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa zawierające imię i nazwisko, numer telefonu służbowego oraz adres służbowej poczty elektronicznej (w przypadku mikro i małych przedsiębiorców – jednej osoby);
- 4) w przypadku osoby która będzie pełnić rolę administratora konta podmiotu w systemie S46 dodatkowo numer PESEL lub niepowtarzalny identyfikator środka identyfikacji elektronicznej;
- 5) numer telefonu przyporządkowany do wykonywanej działalności;
- 6) deklarację podmiotu, czy spełnia kryteria mikroprzedsiębiorcy, małego przedsiębiorcy, średniego przedsiębiorcy lub przewyższa te progi;
- 7) informację określającą, w których państwach członkowskich Unii Europejskiej podmiot wykonuje działalność, wraz z określeniem wykonywanej działalności;
- 8) w przypadku dostawcy usług DNS, rejestru nazw domen najwyższego poziomu (TLD), podmiotu świadczącego usługi rejestracji nazw domen, dostawcy chmury obliczeniowej, dostawcy usługi centrum przetwarzania danych, dostawcy sieci dostarczania treści, dostawcy usług zarządzanych, dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa, dostawcy internetowej platformy handlowej, dostawcy wyszukiwarki internetowej oraz dostawcy platformy usług sieci społecznościowych – główne miejsce prowadzenia działalności;
- 9) informację o zawarciu umowy z dostawcą usług zarządzanych w zakresie bezpieczeństwa na realizację zadań z zakresu SZBI wraz z danymi tego podmiotu;
- 10) informację o ustanowieniu przedstawiciela podmiotu kluczowego lub podmiotu ważnego z sektora infrastruktury cyfrowej, który nie ma siedziby na terytorium;
- 11) informację w sprawie zawarcia porozumienia o wymianie informacji w zakresie cyberbezpieczeństwa.



2.11. Co, jeżeli podmiot powinien zostać wpisany do Wykazu z urzędu, jednak wciąż nie otrzymał zawiadomienia o wpisie oraz wezwania do uzupełnienia brakujących danych? [NOWE – aktualizacja czerwiec 2026 r.]

Minister Cyfryzacji dokonał wpisów z urzędu do wykazu dotychczas zidentyfikowanych podmiotów. Wysyłka zawiadomień o wpisie wraz z wezwaniami do uzupełnienia brakujących danych została już rozpoczęta i jest prowadzona sukcesywnie w maju i czerwcu 2026 r. Wysyłka realizowana jest przez NASK-PIB, któremu Minister Cyfryzacji powierzył realizację zadań związanych z prowadzeniem Systemu S46 i Wykazu KSC.

W przypadku, gdy podmiot powinien zostać wpisany do Wykazu z urzędu, jednak w najbliższych tygodniach nie otrzyma zawiadomienia o wpisie wraz z wezwaniem do uzupełnienia brakujących danych, powinien o powstałej sytuacji poinformować przesyłając wiadomość na adres S46-admin@nask.pl, a takie zgłoszenie zostanie zweryfikowane przez operatora Wykazu.

2.12. Dlaczego w wezwaniu do uzupełnienia wpisu w Wykazie podmiotów kluczowych i podmiotów ważnych wskazano, że jestem podmiotem ważnym, mimo że – zgodnie z moją oceną – powinienem zostać zakwalifikowany jako podmiot kluczowy? [NOWE – aktualizacja czerwiec 2026 r.]

Taka sytuacja może wystąpić, jeżeli instytucja kierująca wezwaniem do uzupełnienia wpisu nie dysponuje kompletem danych niezbędnych do prawidłowej klasyfikacji podmiotu. Dotyczy to w szczególności przypadków takich jak:

- brak informacji o wielkości zatrudnienia, lub
- brak danych potwierdzających spełnienie kryteriów dla mikro-, małego lub średniego przedsiębiorcy, określonych w art. 2 ust. 1 załącznika I do rozporządzenia Komisji (UE) nr 651/2014.

Po uzupełnieniu wpisu o wymagane informacje Wykaz KSC przypisze podmiotowi właściwy typ (podmiot kluczowy lub podmiot ważny) zgodnie z dostarczonymi danymi.



2.13. Gdzie mogę zweryfikować, po dokonaniu wpisu lub uzupełnieniu wpisu, czy mój podmiot został zaklasyfikowany jako podmiot ważny czy jako podmiot kluczowy? [NOWE – aktualizacja czerwiec 2026 r.]

Po dokonaniu wpisu lub uzupełnieniu wpisu informacja o klasyfikacji podmiotu jako kluczowy lub ważny jest dostępna w polu „Typ podmiotu”. Pole to znajduje się w zakładce „Szczegóły wpisu”, w sekcji „H. Przypisanie”.

2.14. Co zrobić, jeżeli zostałem błędnie wpisany do Wykazu KSC? [NOWE – aktualizacja czerwiec 2026 r.]

Minister właściwy do spraw informatyzacji lub organ właściwy do spraw cyberbezpieczeństwa posiadają uprawnienia do wpisania z urzędu podmiotu do Wykazu KSC. Dotyczy to w szczególności kilkudziesięciu tysięcy podmiotów publicznych w Polsce. Przy wpisach z urzędu, dane są czerpane przede wszystkim z dostępnych rejestrów publicznych, które mogą zawierać dane niepełne lub nieaktualne. Przy takiej liczbie podmiotów, niestety mogą pojawić się błędne wpisy w Wykazie KSC.

Jeżeli otrzymasz zawiadomienie o wpisie z urzędu z wezwaniem do uzupełnienia danych, a uważasz, że nie spełniasz przesłanek uznania za podmiot kluczowy lub podmiot ważny, złóż wniosek o wykreślenie z Wykazu KSC. Wniosek ten zostanie rozpatrzony w ciągu miesiąca przez organ właściwy do spraw cyberbezpieczeństwa. Jeżeli zgadzasz się z wpisem do Wykazu KSC, ale dane wpisane z urzędu są według Ciebie nieprawidłowe lub niepełne, złóż wniosek o zmianę wpisu i podaj w nim poprawne dane dotyczące np. nazwy podmiotu, adresu lub rodzaju prowadzonej działalności. Części pól we wpisie do wykazu nie możesz samodzielnie zmienić, np. przypisanego właściwego zespołu CSIRT. Jeżeli widzisz w nich nieprawidłowość, zgłoś to na adres S46-admin@nask.pl, a takie zgłoszenie zostanie zweryfikowane przez operatora Wykazu. W zgłoszeniu podaj swoje dane kontaktowe, jednoznaczne wskazanie, którego podmiotu dotyczy błędny wpis, które dane są według Ciebie nieprawidłowe, a jakie uznajesz za prawidłowe.



2.15. Kiedy otrzymam dostęp do Systemu S46 Cyber Hub? [NOWE – aktualizacja czerwiec 2026 r.]

Zgodnie z harmonogramem opublikowanym w Dzienniku Urzędowym Ministra Cyfryzacji <https://www.gov.pl/web/cyfryzacja/du-mc-poz-7>, podmioty kluczowe i podmioty ważne, które zostały wpisane do Wykazu KSC z urzędu lub na wniosek i uzupełniły w wykazie komplet niezbędnych danych, od 12 czerwca 2026 r. mogą rozpocząć korzystanie z Systemu S46 Cyber Hub. Na podany w Wykazie KSC adres poczty elektronicznej administratora konta podmiotu w Systemie S46, wysłane zostaną informacje, które pozwolą zalogować się do konta podmiotu. Dostęp do Systemu S46 Cyber Hub będzie przyznawany po tej dacie sukcesywnie dla podmiotów, które będą dokonywać wpisu na wniosek lub uzupełniać dane na wezwanie po wpisie z urzędu. Podmioty, które uzyskały dostęp do Systemu S46 Cyber Hub przed wejściem w życie nowelizacji ustawy o KSC, czyli przed 3 kwietnia 2026 r., zachowują przyznany dostęp do konta podmiotu. Jeżeli taki podmiot podlega wpisowi do Wykazu KSC, to podaje w nim dodatkową informację o kodzie przestrzeni w Systemie S46 Cyber Hub, co pozwala na powiązanie wpisu z istniejącą przestrzenią, zamiast tworzenia nowej.

2.16. Czy forma prawna podmiotu ma wpływ na stosowanie ustawy o KSC? [NOWE – aktualizacja czerwiec 2026 r.]

Sama forma prawna nie decyduje o objęciu ustawą o KSC. O obowiązkach wynikających z ustawy decyduje przede wszystkim rodzaj faktycznie wykonywanej działalności oraz spełnienie przesłanek uznania za podmiot kluczowy lub podmiot ważny (w szczególności wielkość podmiotu).

2.17. Czy termin na wpis do wykazu liczony jest od wejścia ustawy w życie czy od spełnienia przesłanek? [NOWE – aktualizacja czerwiec 2026 r.]

Co do zasady termin liczony jest od momentu spełnienia przesłanek uznania za podmiot kluczowy lub ważny. Dla podmiotów spełniających przesłanki już w dniu wejścia w życie ustawy, termin liczony jest od 3 kwietnia 2026 r.



2.18. Co, jeżeli podmiot dokonuje wpisu do wykazu przez pełnomocnika? [NOWE – aktualizacja czerwiec 2026 r.]

Jeżeli działasz przez pełnomocnika, do każdego wniosku o wpis, zmianę wpisu albo o wykreślenie z Wykazu dołącz pełnomocnictwo w postaci elektronicznej, podpisane:

- kwalifikowanym podpisem elektronicznym,
- podpisem zaufanym,
- podpisem osobistym,
- kwalifikowaną pieczęcią elektroniczną.

Pełnomocnictwa nie dołącza się w przypadku, gdy pełnomocnik podmiotu jest ujawniony w Centralnej Ewidencji i Informacji o Działalności Gospodarczej albo gdy prokurent jest ujawniony w Krajowym Rejestrze Sądowym.

Przypominamy, że w przypadku udzielenia pełnomocnictwa do reprezentowania podmiotu należy uiścić stosowną opłatę skarbową. Jednocześnie informujemy, że system nie gromadzi dowodów opłat skarbowych.

2.19. Czy możliwa jest korekta danych po wpisie do Wykazu KSC? Kto powinien dokonać zgłoszenia zmiany danych podmiotu? W jakim terminie należy aktualizować dane? [NOWE – aktualizacja czerwiec 2026 r.]

Dane w Wykazie KSC powinny być aktualne. Ich aktualizowanie możliwe jest poprzez złożenie wniosku o zmianę danych w wykazie. Zgłoszenia zmiany danych w wykazie dokonuje osoba upoważniona do dokonania wpisu, w tym pełnomocnik działający na podstawie udzielonego pełnomocnictwa. Podmiot ma 14 dni na aktualizację danych z art. 7 ust. 2 pkt 1-18 ustawy o KSC od dnia ich zmiany.

2.20. Jeżeli podmiot nie podlega pod wpis z urzędu i złożył wniosek o wpis do Wykazu KSC, to czy otrzyma formalne potwierdzenie? [NOWE – aktualizacja czerwiec 2026 r.]

Podmiot, który dokonał wpisu do wykazu, ma możliwość samodzielnego wygenerowania zaświadczenia o wpisie do Wykazu KSC na stronie <https://wykaz-ksc.gov.pl>. Może tego dokonać we wniosku, poprzez wybór



opcji “pobierz”, a następnie wybór typu zaświadczenia pn. “Zaświadczenie o wpisie do wykazu” lub “Zaświadczenie o zmianie wpisu w wykazie”.

2.21. Kto ma dostęp do danych podmiotu wpisanego do Wykazu KSC? [NOWE – aktualizacja czerwiec 2026 r.]

Bezpośredni dostęp do danych podmiotu wpisanego do wykazu posiada właściciel wpisu, organy właściwe do sprawy cyberbezpieczeństwa, pod które podlega podmiot, CSIRT sektorowy oraz krajowy, a także operator wykazu (Minister Cyfryzacji). Właściciel wpisu może również udzielić dostępu do wykazu innym osobom, poprzez zaproszenie e-mail. Zawiera ono jednorazowy kod dostępu do wpisu podmiotu.

2.22. Jak wygląda procedura wykreślenia podmiotu z Wykazu KSC? [NOWE – aktualizacja czerwiec 2026 r.]

Podmiot może zostać całkowicie usunięty z wykazu albo wykreślony tylko z tych sektorów, podsektorów lub rodzajów działalności, w których już nie prowadzi działalności.

W tym celu należy we wpisie w wykazie wybrać opcję „Utwórz nowy wniosek”, a następnie „Wniosek o wykreślenie podmiotu z Wykazu”. Dalej należy określić, z których sektorów lub działalności podmiot ma zostać wykreślony oraz podać uzasadnienie takiego wniosku, wskazując podstawę wykreślenia podmiotu.

Po sprawdzeniu poprawności danych w podsumowaniu osoba upoważniona podpisuje wniosek o wykreślenie. Organ właściwy w ciągu miesiąca rozpatruje wniosek, a następnie informuje podmiot o wykreśleniu albo odmowie wykreślenia z wykazu.

2.23. Gdzie publikowane są komunikaty dotyczące Wykazu KSC? [NOWE – aktualizacja czerwiec 2026 r.]

Komunikaty dotyczące wykazu publikowane są na następujących stronach internetowych:

- <https://cyber.gov.pl/>
- <https://www.gov.pl/web/cyfryzacja/>
- <https://cyberpolicy.nask.pl/aktualnosci/>



2.24. Czy dział IT może złożyć wniosek o wpis do Wykazu KSC, a dyrektor lub prezes może go potem podpisać? [NOWE – aktualizacja czerwiec 2026 r.]

Wniosek wypełnia i podpisuje osoba upoważniona do złożenia wniosku. Jeżeli osoba z działu IT posiada pełnomocnictwo do działania w imieniu podmiotu w zakresie wykazu, to może wypełnić, podpisać i złożyć wniosek.

2.25. Czy wpis do Wykazu KSC następuje automatycznie po wysłaniu formularza? [NOWE – aktualizacja czerwiec 2026 r.]

Po złożeniu wniosku system nadaje mu odpowiedni status. W przypadku statusu „Zatwierdzony” wpis do wykazu następuje automatycznie. W sytuacji konfliktu danych wniosek może wymagać dodatkowej weryfikacji. Więcej informacji dot. samorejestracji można znaleźć na stronie: [Samorejestracja \(wpis do Wykazu KSC\) - System S46 - Portal Gov.pl](#).

2.26. Czy korekta danych w Wykazie KSC wymaga ponownego złożenia i podpisania wniosku? [NOWE – aktualizacja czerwiec 2026 r.]

Tak, korekta danych podmiotu wymaga złożenia i podpisania wniosku o zmianę danych w wykazie.

2.27. Czy konieczna jest aktualizacja wpisu w Wykazie KSC po każdej zmianie domeny lub IP? [NOWE – aktualizacja czerwiec 2026 r.]

Tak. Dane w wykazie powinny być aktualne. Ich aktualizowanie możliwe jest poprzez złożenie wniosku o zmianę danych w Wykazie KSC.

2.28. Czy likwidacja spółki powoduje automatyczne wykreślenie z Wykazu KSC? [NOWE – aktualizacja czerwiec 2026 r.]

Po zakończeniu działań związanych z likwidacją podmiot/likwidatorzy (gdy są nimi członkowie zarządu) składają wniosek o wykreślenie podmiotu z wykazu. W innym przypadku, jeżeli podmiot nie złoży takiego wniosku,



organ właściwy wykreśli podmiot z wykazu dopiero po uzyskaniu informacji o wykreśleniu podmiotu z REGON, KRS lub CEIDG.

2.29. Jakie podmioty powinny wskazać przedstawiciela zgodnie z art. 5a ust. 7-9 ustawy o KSC? Kto może nim zostać? [NOWE – aktualizacja czerwiec 2026 r.]

Obowiązek wyznaczenia przedstawiciela dotyczy:

- dostawców usług DNS,
- rejestrów nazw domen najwyższego poziomu, czyli TLD,
- podmiotów świadczących usługi rejestracji nazw domen,
- dostawców chmury obliczeniowej,
- dostawców usługi centrum przetwarzania danych,
- dostawców sieci dostarczania treści,
- dostawców usług zarządzanych,
- dostawców usług zarządzanych w zakresie cyberbezpieczeństwa,
- dostawców internetowej platformy handlowej,
- dostawców wyszukiwarki internetowej,
- dostawców platformy usług sieci społecznościowych,

którzy nie posiadają jednostki organizacyjnej w żadnym państwie członkowskim Unii Europejskiej, ale oferują swoje usługi na terytorium Rzeczypospolitej Polskiej. Podmiot taki powinien wyznaczyć przedstawiciela posiadającego jednostkę organizacyjną w Polsce, chyba że wyznaczył już przedstawiciela w innym państwie członkowskim UE.

Należy podkreślić, że podmiot, który wyznaczy przedstawiciela w Polsce, podlega właściwości polskiego organu właściwego do spraw cyberbezpieczeństwa zgodnie z art. 5a ust. 9 ustawy o KSC.

Przedstawicielem może być osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej, ustanowiona na terytorium Rzeczypospolitej Polskiej albo innego państwa członkowskiego Unii Europejskiej. Przedstawiciel jest wyznaczany do występowania w imieniu podmiotu spoza UE w zakresie obowiązków wynikających z ustawy, w szczególności na potrzeby kontaktu z organem właściwym do spraw cyberbezpieczeństwa, CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowym.



2.30. Jeżeli podmiot operuje na wielu adresach opartych o jedną domenę główną – czy wystarczy wskazanie w Wykazie KSC tej domeny głównej z dodatkowym wyjaśnieniem, że wszystkie inne na niej bazują, czy też konieczne jest wymienienie każdej z wykorzystywanych domen z osobna? [NOWE – aktualizacja czerwiec 2026 r.]

W Wykazie KSC w sekcji domen internetowych należy wymienić wszystkie domeny, które aktywnie i w sposób ciągły wykorzystywane są przez podmiot. Wskazane domeny muszą należeć do podmiotu, nawet jeśli utrzymywane są u zewnętrznego dostawcy.

Nie należy wpisywać każdej subdomeny czy adresu technicznego (np. „logowanie.firma.pl”), lecz domeny główne wykorzystywane przez podmiot (np. „firma.pl”, „firma.com”, „marka.pl”).

2.31. Czy jeśli będę czekał z dokonaniem wpisu do Wykazu KSC do października br. to nie muszę wykonywać obowiązków lub będę miał więcej czasu na dostosowanie? [NOWE – aktualizacja czerwiec 2026 r.]

Nie. Termin do 3 października 2026 r. dotyczy wyłącznie wpisu do wykazu. Co do zasady termin na realizację obowiązków liczy się od momentu spełnienia przesłanek uznania za podmiot kluczowy lub ważny, a nie od dnia wpisu.

2.32. Co musi zrobić podmiot, który zacznie spełniać przesłanki uznania za podmiot kluczowy lub podmiot ważny po 3 października 2026 r., tj. po zakończeniu samorejestracji podmiotów w wykazie podmiotów kluczowych i podmiotów ważnych, wskazanej w harmonogramie opublikowanym przez Ministra Cyfryzacji? [NOWE – aktualizacja czerwiec 2026 r.]

Samorejestracja dostępna jest dla podmiotów przez cały czas. Podmiot, który zacznie spełniać przesłanki uznania za podmiot kluczowy lub podmiot ważny po 3 października 2026 r., również będzie zobowiązany do dokonania samodzielnej rejestracji w wykazie w terminie 6 miesięcy od spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny.



Termin 3 października 2026 r. jest ostatnim dniem rejestracji dla podmiotów, które spełniały przesłanki wpisu do wykazu na dzień wejścia w życie ustawy o KSC.

2.33. Od kiedy podmioty mogą składać wnioski o wpis do wykazu podmiotów kluczowych i podmiotów ważnych? [NOWE – aktualizacja czerwiec 2026 r.]

Zgodnie z *Komunikatem Ministra Cyfryzacji z dnia 8 kwietnia 2026 r. w sprawie harmonogramu złożenia wniosków o wpis do wykazu podmiotów kluczowych i podmiotów ważnych oraz rozpoczęcia korzystania z systemu teleinformatycznego przez podmioty kluczowe lub podmioty ważne od dnia 7 maja 2026 r.* podmioty, które spełniają przesłanki uznania za podmiot kluczowy lub ważny, nie należący do sektora administracji publicznej i nie zostały wpisane do wykazu z urzędu, mogą składać wnioski o wpis.

2.34. Kiedy podmioty objęte wpisem z urzędu do wykazu podmiotów kluczowych i podmiotów ważnych otrzymają zawiadomienie o wpisie z urzędu wraz z wezwaniem do uzupełnienia brakujących danych? [NOWE – aktualizacja czerwiec 2026 r.]

Przed uruchomieniem samorejestracji w dniu 7 maja 2026 r. Minister Cyfryzacji wpisał z urzędu do Wykazu KSC zidentyfikowane dotychczas podmioty.

W odniesieniu do podmiotów wpisanych do wykazu z urzędu do dnia 7 maja 2026 r., wysyłka zawiadomień o wpisie wraz z wezwaniami do uzupełnienia brakujących danych realizowana była do końca maja 2026 r.

Identyfikacja pozostałych podmiotów z sektora publicznego jest nadal prowadzona. W zakresie samorządowych instytucji kultury wpisy z urzędu i wysyłka zawiadomień i wezwań będą dokonywane w nadchodzących tygodniach.

2.35. Jak złożyć wniosek o wpis do wykazu podmiotów kluczowych i podmiotów ważnych? [NOWE – aktualizacja czerwiec 2026 r.]

1. W celu złożenia wniosku należy wejść na stronę <https://wykaz-ksc.gov.pl> i zalogować się przez Węzeł Krajowy.
2. Następnie należy zarejestrować konto użytkownika.



3. Potem należy kliknąć „Wpisz nowy podmiot” i wypełnić formularz.
4. Na końcu trzeba podpisać wniosek elektronicznie.

2.36. W jakim czasie mam uzupełnić dane w Wykazie KSC po otrzymaniu zawiadomienia o wpisie z urzędu wraz z wezwaniem do uzupełnienia brakujących danych? [NOWE – aktualizacja czerwiec 2026 r.]

Uzupełnienie brakujących danych musi nastąpić w terminie 6 miesięcy od dnia doręczenia wezwania (a nie od dnia wejścia w życie ustawy czy dnia wpisu do wykazu).

Zachęcamy jednocześnie do podejmowania działań związanych z uzupełnieniem brakujących danych z odpowiednim wyprzedzeniem i nieodkładania ich na koniec ustawowego terminu.

2.37. Czy podmioty krytyczne są obecnie wpisywane z urzędu do Wykazu KSC, skoro nowelizacja ustawy o zarządzaniu kryzysowym nie weszła jeszcze w życie? [NOWE – aktualizacja czerwiec 2026 r.]

Na obecnym etapie podmioty mogą podlegać wpisowi do Wykazu KSC jako podmioty kluczowe albo podmioty ważne, jeżeli spełniają przesłanki określone w ustawie o KSC. Przepisy ustawy o KSC przewidują obowiązek ujęcia w wykazie informacji o uznaniu danego podmiotu za podmiot krytyczny oraz wpisywania określonych danych dotyczących podmiotów krytycznych z urzędu. Jednak praktyczne zastosowanie tego mechanizmu wymaga uprzedniego formalnego ustalenia statusu podmiotu krytycznego na podstawie właściwych przepisów ustawy o zarządzaniu kryzysowym.

2.38. Kiedy w wykazie zostanie wskazana informacja o uznaniu podmiotu kluczowego lub podmiotu ważnego za podmiot krytyczny? [NOWE – aktualizacja czerwiec 2026 r.]

W dniu 15 maja 2026 r. Sejm uchwalił ustawę o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw. Ustawa ta przewiduje m.in. mechanizm identyfikacji podmiotów krytycznych. Organy do spraw podmiotów krytycznych po raz pierwszy zidentyfikują podmioty krytyczne i wpiszą je do wykazu podmiotów krytycznych w terminie 9 miesięcy od dnia wejścia w życie tej ustawy.

Rządowe Centrum Bezpieczeństwa prześle katalog zidentyfikowanych podmiotów krytycznych Ministrowi Cyfryzacji. Na podstawie tych informacji



Minister dokona wpisu do wykazu z urzędu nowych podmiotów uznanych za krytyczne.

W przypadku, kiedy podmioty już wpisane do wykazu KSC zostaną uznane za podmioty krytyczne, Minister Cyfryzacji zaktualizuje ich status zgodnie z przekazaną informacją.

Do czasu wejścia w życie nowelizacji ustawy o zarządzaniu kryzysowym oraz rozpoczęcia identyfikacji podmiotów krytycznych, sam fakt potencjalnego spełniania przyszłych kryteriów nie oznacza jeszcze automatycznego wpisu do Wykazu KSC jako podmiot krytyczny. Podmiot powinien sam ocenić, czy spełnia przesłanki uznania za podmiot kluczowy albo podmiot ważny na gruncie ustawy o KSC i – jeśli tak – dokonać wpisu do wykazu na zasadach określonych w tej ustawie.

2.39. Czy Wykaz KSC może być uzupełniany bez wskazania osób do kontaktu, skoro ustawa o KSC przewiduje okres przejściowy na wdrożenie części obowiązków? [NOWE – aktualizacja czerwiec 2026 r.]

Uzupełnienie danych w wykazie jest obowiązkiem podmiotu publicznego. Jednocześnie podmioty publiczne obowiązane są do stosowania ustawy w terminie 12 miesięcy od wejścia w życie ustawy. Od tego terminu podmiot publiczny musi spełnić wszystkie wymagania.

Przepisy dotyczące wykazu podmiotów kluczowych i podmiotów ważnych już obowiązują i zakres danych objętych wykazem wynika bezpośrednio z przepisów ustawy – w tym zakresie dane, które powinny zostać wskazane muszą być uzupełnione niezależnie od pozostałych działań. Okres przejściowy dotyczący obowiązków wskazanych w rozdziale 3 ustawy, czyli m. in. dotyczącym wdrożenia systemu zarządzania bezpieczeństwem informacji.



3. Obowiązki podmiotów kluczowych i ważnych

3.1. Jakie są istotne terminy wdrożenia dla podmiotów kluczowych i podmiotów ważnych?



Wpis do wykazu podmiotów kluczowych i ważnych – **6 miesięcy** od spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny.

- ✓ **3 października 2026 r.**

Podłączenie do systemu S46 – **12 miesięcy** od spełnienia przesłanek uznania za podmiot kluczowy lub ważny.

- ✓ **3 kwietnia 2027 r.**

Wdrożenie obowiązków z zakresu systemu zarządzania bezpieczeństwem informacji SZBI po raz pierwszy – **12 miesięcy** od spełnienia przesłanek uznania za podmiot kluczowy lub ważny.

- ✓ **3 kwietnia 2027 r.**

Pierwszy audyt podmiotu kluczowego – **24 miesiące** od spełnienia przesłanek uznania za podmiot kluczowy lub ważny.

- ✓ **3 kwietnia 2028 r.**

3.2. Co musi zrobić podmiot, żeby dostosować się do wymogów ustawy?

Przed wszystkim przedsiębiorca powinien przeanalizować swoją działalność i odpowiedzieć sobie na pytanie czy spełnia kryteria uznania za podmiot kluczowy lub podmiot ważny. Jeżeli tak, to kolejną czynnością będzie złożenie wniosku o wpis do wykazu podmiotów kluczowych lub podmiotów ważnych. We wniosku należy wskazać podstawowe informacje o podmiocie, adresy osób do kontaktu, administratora konta podmiotu w systemie S46, informacje o zakresach adresów IP i domenach wykorzystywanych przez podmiot.

Co podmiot musi zrobić żeby dostosować się do KSC:

1. Ustalenie czy podmiot kwalifikuje się jako podmiot kluczowy lub podmiot ważny (kryteria podmiotowe oraz kryteria wielkościowe)
2. Ustalenie czy podmiot podlega pod regulacje sektorowe w zakresie cyberbezpieczeństwa:
3. Podłączenie się do systemu S46
 - a. w tym zakresie współpraca z NASK-PIB,
 - b. ustalenie administratora konta podmiotu w systemie S46 i użytkowników systemu po stronie podmiotu



- c. wyznaczenie stałych dyżurów przy S46 – celem zgłaszania incydentów oraz uzyskiwania informacji zwrotnych z S46 o podatnościach, cyberzagrożeniach i dobrych praktykach
4. Przygotowanie i wdrożenie SZBI
 - a. Ustalenie kontekstu organizacji – jaką działalność prowadzi, jakie są wymagania regulacyjne, jakie są oczekiwania klientów i innych partnerów organizacji
 - b. Opracowanie polityki bezpieczeństwa
 - c. Przydzielenie ról w organizacji – kto ma odpowiadać za cyberbezpieczeństwo w organizacji oprócz zarządu
 - d. Wdrożenie zarządzania ryzykiem w podmiocie albo przegląd dotychczas stosowanych polityk i procedur w tym zakresie
 - e. Wdrożenie proporcjonalnych środków technicznych i organizacyjnych w podmiocie zapewniających poufność, integralność i dostępność informacji w szczególności:
 - ✓ Przegląd dotychczasowych polityk i procedur
 - ✓ Weryfikacja obecnego i przyszłego personelu pod kątem niekaralności, przegląd aktualnych procedur HR pod kątem bezpieczeństwa zasobów ludzkich
 - ✓ Przegląd uprawnień personelu do zasobów (aktywów) i aktualizacja tych aktywów; cofnięcie uprawnień dla personelu, który nie wykonuje już tych zadań
 - ✓ Przegląd dotychczasowych dostawców sprzętu i oprogramowania, przegląd umów zawartych z tymi dostawcami
 - ✓ Przegląd dotychczas stosowanych środków bezpieczeństwa w systemach informacyjnych i wdrożenie dodatkowych środków tam gdzie jest to konieczne
 - ✓ Wdrożenie stałe, automatyczne gdzie możliwe, monitoringu systemu informacyjnego pod kątem zdarzeń które mogą być incydentami, podatnościami cyberzagrozeniami
 - ✓ Przegląd planów ciągłości działania, planów awaryjnych systemu informacyjnego, planów odtworzenia ciągłości po katastrofie
 - ✓ Zarządzanie aktywami – identyfikacja aktywów
 - ✓ Zarządzanie aktualizacjami – wdrożenie polityk i procedur aktualizacji
 - ✓ Przegląd polityk i procedur w zakresie zarządzania incydentami



- f. Ustalenie wewnętrznych procedur oraz kanałów komunikacji z zespołami CSIRT
5. Nawiązanie współpracy roboczej z organami właściwymi do spraw cyberbezpieczeństwa
6. Stałe monitorowanie otoczenia regulacyjnego organizacji
7. Uwzględnienie w procedurach wewnętrznych skutków wydania rekomendacji Pełnomocnika Rządu ds. Cyberbezpieczeństwa, decyzji w sprawie uznania za dostawcę wysokiego ryzyka, polecenia zabezpieczającego – w tym procedur mających na celu sprawdzenie czy w podmiocie jest sprzęt lub oprogramowanie pochodzące od dostawcy wysokiego ryzyka.

3.3. Jakie są podstawowe obowiązki dla podmiotu kluczowego i podmiotu ważnego w zakresie systemu zarządzania bezpieczeństwem informacji?

Podstawowym obowiązkiem podmiotów kluczowych i podmiotów ważnych będzie wdrożenie systemu zarządzania bezpieczeństwem informacji (SZBI) w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot obejmującego:

- 1) **prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem** – należy regularnie szacować ryzyko (identyfikować, analizować, oceniać), a następnie podejmować decyzję o podejściu do tego ryzyka;
- 2) **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, skutki społeczne i gospodarcze, w szczególności:**

Każda z usług świadczona przez podmioty kluczowe lub podmioty ważne ma swoją specyfikę, dlatego wdrażając środki techniczne i organizacyjne podmiot powinien wybrać takie, które będą dopasowane (odpowiednie) do jego wielkości, charakteru świadczonych usług, możliwości finansowych, aktualnej wiedzy technicznej czy cyberzagrożeń, a zarazem żeby te środki były we właściwej harmonii (proporcjonalne) między sobą (przykład – rozbudowany dział cyberbezpieczeństwa, z politykami bezpieczeństwa i odpowiednim SIEM nie będzie efektywny, jeżeli jednocześnie zaniedbane będzie szkolenie personelu z cyberhigieny). Celem jest ograniczenie nadmiernych obowiązków nakładanych na podmiot i ich urealnienie przy stosowaniu. Można to sformułowanie traktować jako uelastyczenie przepisów.



Należy więc bardzo dobrze ustalić kontekst danej organizacji, jej charakterystykę, świadczone usługi, posiadane systemy, otoczenie regulacyjne, wymogi podmiotów trzecich.

a) polityki szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego, w tym polityki tematyczne,

Polityka szacowania ryzyka powinna opisać proces szacowania ryzyka w danej organizacji.

Należy ustanowić politykę bezpieczeństwa systemu informacyjnego wskazującą podejście podmiotu do zarządzania bezpieczeństwem informacji wraz z przypisaniem ról w tym procesie. Polityka ta powinna być adekwatna do danego podmiotu, wskazać cele bezpieczeństwa systemu informacyjnego, zobowiązanie do ciągłego rozwoju jak również przewidywać jej przegląd. Polityka powinna być zakomunikowana osobom zatrudnionym w podmiocie.

Polityki tematyczne – są to *topic specific policies*, o których mowa w normie ISO 27001. Założeniem tego przepisu jest to, aby tam gdzie to konieczne organizacja opracowała polityki tematyczne. Przykładowo, jeśli przyczyni się to do lepszej ochrony to organizacja może wprowadzić politykę bezpieczeństwa urządzeń mobilnych.

b) bezpieczeństwo w procesie nabywania, rozwoju, utrzymania i eksploatacji systemu informacyjnego, w tym testowanie systemu informacyjnego,

Należy opracować i wdrożyć procedury zarządzania konfiguracją urządzeń, procedury zarządzania zmianą w systemie informacyjnym, politykę i procedurę testowania systemu informacyjnego, procedury zarządzanie ryzykiem związanym z nabywaniem nowych produktów ICT, usług ICT i procesów ICT, segmentacja systemów na podstawie analizy ryzyka oraz zapewnienie ochrony przeciwko złośliwemu oprogramowaniu.

c) bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu,

Podmiot kluczowy lub podmiot ważny powinien monitorować dostęp fizyczny do elementów systemu informacyjnego, zapobiegać cyberzagrożeniom mającym charakter fizyczny, zapobiegać utracie, uszkodzeniu urządzeń wspierających funkcjonowaniu systemu informacyjnego (np. urządzenia elektryczne).

d) bezpieczeństwo zasobów ludzkich,

Należy dbać o zrozumienie wymogów bezpieczeństwa wśród personelu. Personel o szczególnym dostępie do aktywów powinien w szczególności sposób wykonywać swoje zadania w. Pamiętać należy o personelu zewnętrznego dostawcy – należy wprowadzić odpowiednie postanowienia umowne dotyczące bezpieczeństwa oraz zachowaniu w poufności



informacji. W procesie rekrutacji należy prowadzić weryfikację kandydatów (np. poprzez OSINT czy poprzez wymóg dostarczenia referencji czy zaświadczeń – przy czym należy pamiętać o wymogach RODO i poinformować kandydatów w ogłoszeniu, że takie czynności będą dokonywane i że wymagana jest ich zgoda); ponadto należy wprowadzić wewnętrzne reguły dyscyplinarne, jeśli nie wynikają z przepisów prawa powszechnie obowiązującego, dotyczące przypadków naruszenia obowiązków personelu w obszarze cyberbezpieczeństwa, wraz z możliwością wypowiedzenia umowy; w postanowieniach umownych z personelem należy zawrzeć zapisy dotyczące zachowania w poufności informacji związanych z organizacją także po zakończeniu umowy.

e) bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi z uwzględnieniem związków pomiędzy bezpośrednim dostawcą sprzętu lub oprogramowania a podmiotem kluczowym lub podmiotem ważnym,

Należy wprowadzić politykę łańcucha dostaw obejmującą relację z bezpośrednimi dostawcami. W polityce należy wskazać kryteria wyboru dostawców. W umowach z dostawcami należy zawierać postanowienia dotyczące cyberbezpieczeństwa m. in. obowiązek zachowania informacji w poufności, obowiązek zgłaszania incydentów do podmiotu, informowanie o podatnościach, wymogi dotyczące personelu podmiotu (np. co do certyfikacji osób) itd. Pamiętać przy tym należy, że duzi dostawcy sprzętu lub oprogramowania często mają wdrożoną certyfikację własnych systemów, osób lub produktów, usług z zakresu cyberbezpieczeństwa, co z jednej strony ułatwia zarządzanie bezpieczeństwem łańcuchów dostaw, z drugiej może potencjalnie utrudnić dodatkowe wymogi, zwłaszcza, jeżeli zamawiający jest zdecydowanie mniejszym podmiotem. Tutaj wchodzi więc zasada proporcjonalnych środków technicznych i organizacyjnych. Organizacja powinna mieć aktualny wykaz bezpośrednich dostawców z danymi kontaktowymi oraz wskazaniem jakie produkty ICT, usługi ICT czy procesy ICT dostarczają.

Należy identyfikować i oceniać potencjalne ryzyko wynikające z bezpośrednich dostawców sprzętu lub oprogramowania. Konieczne jest opracowanie aktualnej listy kontaktów z dostawcami oraz listy produktów ICT, usług ICT i procesów ICT, które ci dostawcy dostarczają.

f) wdrażanie, dokumentowanie, testowanie i utrzymywanie:

- planów ciągłości działania (*Business continuity plan – BCP*) umożliwiających ciągłe i niezakłócone świadczenie usługi oraz zapewniających poufność, integralność, dostępność i autentyczność informacji,
- planów awaryjnych (*Information System Contingency Plan – ISCP*), oraz



- planów odtworzenia działalności umożliwiających odtworzenie systemu informacyjnego po zdarzeniu, które spowodowało straty przekraczające zdolności podmiotu do odbudowy za pomocą własnych środków – (Disaster Recovery Plan – DRP),

g) objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie ciągłym,

System informacyjny powinien być monitorowany ciągle – chodzi o to, aby zapewnić rozliczalność działań podejmowanych w systemie i analizować zaistniałe zdarzenia. Niekoniecznie trzeba w tym celu zatrudniać dodatkową osobę, można skorzystać z narzędzi open-source typu SIEM i ustawić adekwatne reguły. W szczególności należy monitorować zdarzenia, które mogą być przyczyną lub skutkiem incydentu. Monitorowanie dotyczy w szczególności ruchu z i do podmiotu, dostępu do systemu, kont z uprzywilejowanym dostępem, krytyczne pliki konfiguracyjne i kopii zapasowej, logi z narzędzi cyberbezpieczeństwa (np. antywirusów, anti-spyware), zdarzenia środowiskowe, które mogą mieć wpływ na funkcjonowanie infrastruktury systemu (zalenie, pożar itd.).

h) polityki i procedury oceny skuteczności środków technicznych i organizacyjnych,

Należy ustalić, które aktywności w SZBI podmiotu będą monitorowane, jakie będą wskaźniki (KPI), kiedy, w jakich interwałach będą monitorowane, kto będzie to robił, czy nastąpi ich ewaluacja oraz kto za to będzie odpowiedzialny.

i) edukację z zakresu cyberbezpieczeństwa dla personelu podmiotu,

Podmiot powinien dbać o zrozumienie cyberzagrożeń wśród swojego personelu, niezależnie od roli personelu w organizacji.

j) podstawowe zasady cyberhigieny – jest to klauzula generalna, zmienna z uwagi na postęp technologiczny; podmiot kluczowy i podmiot ważny musi identyfikować te zasady w oparciu o aktualny poziom wiedzy technicznej,

k) polityki i procedury stosowania kryptografii, w tym w stosownych przypadkach szyfrowania,

Polityki i procedury stosowania kryptografii obejmują m. in. jakie protokoły i algorytmy, rozwiązania i praktyki są zatwierdzone do używania w podmiocie, kwestie zarządzania kluczami oraz kwestie identyfikowania poziomu ochrony i klasyfikacji aktywów oraz przypisania adekwatnych algorytmów.

l) stosowanie bezpiecznych środków komunikacji elektronicznej w ramach krajowego systemu cyberbezpieczeństwa oraz wewnątrz podmiotu,



uwzględniających uwierzytelnianie wieloskładnikowe w stosownych przypadkach,

Przykładowo uwierzytelnianie wieloskładnikowe powinno być stosowane przy zdalnym logowaniu, dostępie do wrażliwych informacji czy do kont administratorów oraz wszędzie tam gdzie podmiot uzna to za konieczne w świetle szacowania ryzyka.

m) zarządzanie aktywami,

Należy ustalić klasyfikację aktywów, polityki i procedury właściwego zarządzania aktywami, prowadzić inwentaryzację aktywów oraz dbać o zwrot aktywów po zakończeniu umowy z personelem. Przydatna będzie również polityka zarządzania nośnikami wymiennymi w organizacji.

n) polityki kontroli dostępu;

Należy ustalić politykę kontroli dostępu wskazującą kto może uzyskać dostęp fizyczny i logiczny do zasobów podmiotu. Należy zarządzać prawami dostępu i anulować dostęp dla osób, które już nie potrzebują dostępu do aktywów, w tym także personelu zewnętrznego dostawcy. Należy prowadzić rejestr udzielonych dostępu. Należy zarządzać tożsamościami użytkowników i systemów, które otrzymują dostęp do zasobów organizacji. Powinny być wdrożone bezpieczne procedury uwierzytelniania adekwatne do klasyfikacji aktywów.

3) zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi;

Zbieranie informacji o cyberzagrożeniach i podatnościach pozwala na rozwój własnego personelu, zwiększa dojrzałość organizacji, umożliwia prewencyjne usunięcie podatności w systemie lub zabezpieczenie się przed cyberzagrożeniem.

4) zarządzanie incydentami;

Warto opracować politykę zarządzania incydentami, wprowadzić narzędzie do zgłaszania incydentów wewnątrz podmiotu, wprowadzić procedurę obsługi incydentów.

5) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi, w tym:

a) stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym,

Podmiot kluczowy i podmiot ważny powinien przykładowo dokonywać kopii zapasowej.



- b) **regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi oraz poziomu krytyczności poszczególnych aktualizacji,**

Podmiot kluczowy i podmiot ważny ma systematycznie przeprowadzać aktualizacje oprogramowania. Przepis ma zapobiegać sytuacji, w której aktualizacje były dokonywane zbyt rzadko. Podejmując decyzję o aktualizacji, podmiot powinien dokonać analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi oraz ocenić poziom krytyczności poszczególnych aktualizacji. Celem tej analizy jest zabezpieczenie przed sytuacją, w której konkretna aktualizacja oprogramowania w istocie zagraża bezpieczeństwu świadczonej usługi. Podmiot kluczowy i podmiot ważny jest odpowiedzialny za bezpieczeństwo swoich systemów informacyjnych. Dlatego nie powinien bezrefleksyjnie kierować się zaleceniami producenta sprzętu, ale powinien samodzielnie oceniać wpływ aktualizacji na jego systemy.

- c) **ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym,**
- d) **niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub cyberzagrożeń, w tym również czasowe ograniczenie ruchu sieciowego przychodzącego do infrastruktury podmiotu kluczowego lub podmiotu ważnego, które może skutkować zakłóceniem usług świadczonych przez ten podmiot, mając na uwadze konieczność minimalizacji skutków ograniczenia dostępności tych usług, z uwagi na podjęte działania.**

Należy mieć przygotowane i wdrożone procedury uruchomienia planów ciągłości działania. Możliwe jest także czasowe „odcięcie” ruchu przychodzącego, aby uchronić się przed incydem.

Objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie ciągłym należy rozumieć w ten sposób, że podmiot powinien monitorować wszelkie zdarzenia, które zaistniały w systemie informacyjnym. Celem jest nie tylko zapewnienie rozliczalności, ale także umożliwienie odtworzenia co się stało w systemie informacyjnym w danym momencie.

3.4. Jak zidentyfikować systemy informacyjne, w których należy wdrożyć system zarządzania bezpieczeństwem informacji (SZBI)?

Należy przeanalizować procesy świadczenia usług (zadań publicznych) w organizacji oraz zidentyfikować systemy informacyjne, które są wykorzystywane w procesach mających wpływ na świadczenie tych usług.



Przy identyfikacji procesów należy nie tylko wziąć pod uwagę procesy techniczne czy organizacyjne, ale także te procesy które są związane z daną usługą i są wymagane przez przepisy prawa np. procesy służące realizacji uprawnień użytkownika, klienta, konsumenta czy abonenta.

Przy identyfikacji systemów należy zwrócić uwagę na to, czy dany system jest konieczny do świadczenia usługi, czy przetwarza dane oraz steruje procesami, od których zależy świadczenie usługi, a także czy zdarzenie w tym systemie może spowodować zaprzestanie świadczenia usługi. Każdorazowo należy wziąć pod uwagę charakter danego podmiotu. Systemy, które są w pełni odseparowane od świadczenia usługi i nie mają na nie wpływu nie podlegają obowiązkowi wdrożenia w nich systemu zarządzania bezpieczeństwem informacji. Jednocześnie może być tak, że systemy te są niezbędne w procesie świadczenia usługi, np. do zapewnienia realizacji świadczeń publicznych na rzecz obywateli niezbędne są systemy księgowo, bowiem bez nich podmiot publiczny nie będzie mógł tych świadczeń realizować. Wtedy należy również ująć te systemy w SZBI.

Obowiązkiem wdrożenia SZBI należy objąć systemy informacyjne związane z działalnością danego podmiotu zgodną z załącznikiem nr 1 lub nr 2 do ustawy.

3.5. Co powinna zawierać dokumentacja systemu zarządzania bezpieczeństwem informacji (SZBI)?

Dokumentacja dotyczy bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi i może być prowadzona w postaci elektronicznej lub w postaci papierowej.

Zakres dokumentacji podzielono na 2 części. Dokumentacja normatywna to ta część dokumentacji, która opisuje świadczoną usługę, systemy, infrastrukturę oraz funkcjonowanie bezpieczeństwa informacji w podmiocie. Dokumentacja operacyjna potwierdza wykonywanie czynności opisanych w dokumentacji normatywnej.



dokumentacja normatywna

- dokumentacja systemu zarządzania bezpieczeństwem informacji
- dokumentacja ochrony infrastruktury, z wykorzystaniem której świadczona jest usługa
- dokumentacja systemu zarządzania ciągłością działania
- dokumentacja techniczna systemu informacyjnego wykorzystywanego w procesie świadczenia usługi
- dokumentacja wynikająca ze specyfiki świadczonej usługi w danym sektorze lub podsektorze

dokumentacja operacyjna

- zapisy poświadczające wykonywanie czynności wymaganych przez postanowienia zawarte w dokumentacji normatywnej, w tym automatycznie generowane zapisy w dziennikach systemów informacyjnych (logi)

Zakres przedmiotowy dokumentacji ochrony infrastruktury

Dokumentacja ochrony infrastruktury obejmuje:

charakterystykę usługi oraz infrastruktury, w której świadczona jest usługa

ocenę aktualnego stanu ochrony infrastruktury

szacowanie ryzyka dla obiektów infrastruktury

plan postępowania z ryzykiem

opis zabezpieczeń technicznych obiektów infrastruktury

zasady organizacji i wykonywania ochrony fizycznej infrastruktury

dane o specjalistycznej uzbrojonej formacji ochronnej, o której mowa w art. 2 pkt 7 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia, chroniącej infrastrukturę

Może powstać z tego jeden dokument albo kilka. To należy już do decyzji podmiotu kluczowego i podmiotu ważnego. Istotne jest, aby zakres dokumentacji został zachowany.

Zakres dokumentacji operacyjnej powinien być adekwatny do danego systemu operacyjnego.



W dokumentacji SZBI powinny być ujęte wszystkie elementy wskazane w art. 8.

Ważne jest, aby podmiot dbał o bezpieczeństwo dokumentacji. Należy zapewnić dostępność dokumentacji dla uprawnionych osób (zasada *need to know*) w zakresie niezbędnym do realizacji zadań. Ograniczy to ryzyko ujawnienia informacji z dokumentacji osobom nieuprawnionym. Organizacja powinna ustalić kto i w jakim zakresie ma dostęp do dokumentacji – na żądanie kontroli należy przedstawić dowód przypisania dostępu do dokumentacji. Podmiot powinien także chronić dokumenty pod kątem fizycznym – ochrona przed uszkodzeniem (uszkodzenie papieru czy dysku), zniszczeniem, utratą, nieuprawnionym dostępem, niewłaściwym użyciem lub utratą integralności. Konieczne jest wskazanie kto odpowiada za dokumentację, kto ma ją chronić oraz jakie środki wdrożono, aby chronić dokumentację np. szkolenia, środki fizyczne (przechowywanie papierowej dokumentacji w zamkniętym pomieszczeniu czy szafie), środki techniczne np. szyfrowanie plików z dokumentacją. Pamiętać także należy o oznaczaniu kolejnych wersji dokumentów – ułatwi to identyfikację zmian i odnalezienie aktualnej wersji. Aby potwierdzić, że zniszczona dokumentacja w ogóle zaistniała, czynność zniszczenia potwierdza się protokołem brakowania. Te protokoły przechowuje się w sposób trwały, aby były dostępne dla kontrolerów.

3.6. Czy muszę tworzyć nową odrębną dokumentację systemu zarządzania bezpieczeństwem informacji (SZBI)?

Należy najpierw przejrzeć istniejące zasoby organizacji. Organizacje, które wdrożyły systemy zarządzania bezpieczeństwem informacji według jednych z dostępnych standardów mogą wykorzystać i dostosować już istniejącą dokumentację. Tak jak jednak wspomniano, sama dokumentacja to za mało, zapewnienie cyberbezpieczeństwa musi być realne, a nie papierowe.

3.7. Kupiłem dokumentację zgodną z NIS2. Czy jestem zgodny z ustawą o KSC?

Unijne i krajowe regulacje wymagają realnego zapewnienia cyberbezpieczeństwa. Organizacja musi być świadoma swoich aktywów, ryzyk, cyberzagrożeń i dopasować adekwatne środki techniczne i organizacyjne ograniczające ryzyko. Organizacja musi mieć wdrożone, przetestowane i stosowane w praktyce procedury zarządzania incydentami. Kupiona dokumentacja, podpisana przez zarząd i schowana w "szafie NIS2" nie zapewni realnego cyberbezpieczeństwa w organizacji.



3.8. Czy należy zapewnić szkolenia z zakresu cyberbezpieczeństwa dla personelu podmiotu kluczowego lub podmiotu ważnego?

Tak, podmiot musi edukować swój personel w obszarze cyberbezpieczeństwa. Edukacja ta powinna odbywać się na bieżąco, powinna uwzględniać obowiązki personelu podmiotu w ramach SZBI, istniejące procedury, a także cyberzagrożenia czy przykłady incydentów z jakimi mierzy się podmiot. Obowiązkowemu szkoleniu podlega także kierownik podmiotu kluczowego lub podmiotu ważnego.

3.9. Jakie są obowiązki w zakresie zarządzania bezpieczeństwem łańcucha dostaw?

Podmiot kluczowy oraz podmiot ważny jest obowiązany wdrożyć adekwatne i proporcjonalne środki techniczne i organizacyjne mające zapewnić bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, jak od których zależy świadczenie usługi, z uwzględnieniem związków pomiędzy bezpośrednim dostawcą sprzętu lub oprogramowania a podmiotem kluczowym lub podmiotem ważnym. W ramach tego procesu należy uwzględnić podatności związane z dostawcą sprzętu lub oprogramowania jak i ogólną jakość produktów ICT, usług ICT i procesów ICT pochodzących od dostawcy sprzętu lub oprogramowania, wyniki skoordynowanej oceny bezpieczeństwa przeprowadzonej przez Grupę Współpracy NIS oraz wyniki postępowania w sprawie uznania za dostawcę wysokiego ryzyka.

Wpisuje się to w proces zarządzania ryzykiem łańcuchów dostaw opisany w poradniku Agencji Unii Europejskiej do Spraw Cyberbezpieczeństwa³. Podmioty kluczowe i podmioty ważne powinny m.in.:

- znać swój łańcuch dostaw, w tym swoich dostawców oraz ryzyka związane z nimi,
- dbać o odpowiednie wymagania z zakresu cyberbezpieczeństwa w umowach, a w przypadku umów adhezyjnych z globalnymi dostawcami wybierać tych, którzy posiadają certyfikację z zakresu cyberbezpieczeństwa własnych produktów i usług,
- inwentaryzować swoje zasoby, monitorować podatności związane z wykorzystywanym sprzętem i oprogramowaniem, np. poprzez sprawdzanie na stronach internetowych baz podatności, mitygować zidentyfikowane podatności, np. poprzez aktualizację oprogramowania, jeśli jest dostępna.



3.10. Czy personel podmiotu kluczowego lub podmiotu ważnego podlega weryfikacji?

Ważną gwarancją prawidłowego wykonywania zadań z zakresu cyberbezpieczeństwa jest wskazanie, że zadań tych nie mogą wykonywać osoby skazane za przestępstwa przeciwko ochronie informacji, tj.: przestępstwa określone w rozdziale XXXIII Kodeksu karnego:

- art. 265 (ujawnienie informacji niejawnych),
- art. 266 (ujawnienie informacji służbowych),
- art. 267 (nielegalne uzyskanie informacji),
- art. 268 (niszczenie informacji),
- art. 268a (niszczenie danych w systemach),
- art. 269 (sabotaż komputerowy),
- art. 269a (zakłócanie sieci i systemów),
- art. 269b (bezprawne wykorzystanie programów i danych).

Daje to odpowiednią gwarancję, że zadania te będą wykonywały osoby dające rękojmię ich prawidłowej realizacji. Ograniczono się przy tym do przestępstw przeciwko ochronie informacji, ponieważ są one związane tematycznie z cyberbezpieczeństwem.

Osoba musi przedstawić zaświadczenie o niekaralności za ww. przestępstwa. Zaświadczenia w tym zakresie będą weryfikowane przez ich kierowników podmiotów kluczowych i podmiotów ważnych. Po otrzymaniu zaświadczenia kierownik dopuści taką osobę do realizacji zadań związanych z systemem zarządzania bezpieczeństwem informacji oraz zgłaszaniem incydentów. Podkreślić należy, że mogą tutaj wystąpić stosunek pracy, a także inne stosunki zatrudnienia, np. umowa zlecenia. Jest to istotne w kontekście przetwarzania danych osobowych, jako że dotyczy to danych o karalności w rozumieniu art. 10 RODO. Informacje o niekaralności będą przechowywane w dokumentacji pracowniczej albo w dokumentacji związanej z daną umową w przypadku innych stosunków zatrudnienia. Oczywiście, zgodnie z RODO, takie informacje będą musiały być należycie chronione.

Wprowadza się również uprawnienie podmiotu kluczowego i podmiotu ważnego do wezwania osoby do ponownego przedstawienia zaświadczenia o niekaralności za przestępstwa przeciwko ochronie informacji, jeżeli podmiot poweźmie uzasadnione podejrzenie, że osoba ta została skazana za przestępstwo przeciwko ochronie informacji. Podejrzenie to musi być uzasadnione, w jakimś mierze uprawdopodobnione. Przy czym sam anonim czy zgłoszenie od sygnalisty może być niewystarczające w tej mierze, trzeba wziąć pod uwagę, że takie zgłoszenie może być po prostu aktem szkalującym inną osobę. Również uzasadnionym działaniem podmiotu kluczowego i podmiotu ważnego nie będzie cykliczne wzywanie danej osoby do przedstawienia zaświadczenia o niekaralności.



3.11. Czy osoba, która posiada poświadczenie bezpieczeństwa również podlega obowiązkowej weryfikacji niekaralności?

Osoba, która posiada ważne poświadczenie bezpieczeństwa upoważniające w zakresie dostępu do informacji niejawnych o klauzuli „poufne” lub wyższej nie podlega weryfikacji niekaralności.

3.12. Czy zaświadczenie o niekaralności obowiązuje również pracowników jednostek samorządowych? [NOWE - aktualizacja czerwiec 2026 r.]

Tak, obowiązek przedstawienia zaświadczenia o niekaralności dotyczy również pracowników jednostek samorządowych realizujących zadania z zakresu systemu zarządzania bezpieczeństwem informacji oraz zgłaszania incydentów.

3.13. Czy przedsiębiorcy świadczący usługi obsługi incydentów mają dodatkowe obowiązki?

Tak. Nawiązując do powszechnej międzynarodowej praktyki (publikowanie informacji na podstawie wzoru zawartego w pkt. 3.3 dokumentu RFC 2350 <https://datatracker.ietf.org/doc/html/rfc2350>), nakłada się na dostawców usług zarządzanych z zakresu cyberbezpieczeństwa obowiązek udostępniania na stronie internetowej podstawowych informacji o swojej działalności. W celu zrealizowania tego obowiązku wystarczy zamieścić krótki plik tekstowy na stronie internetowej dostawcy usług zarządzanych z zakresu cyberbezpieczeństwa. Strona internetowa dostawcy powinna być w domenie, którą dostawca zgłosił do wykazu podmiotów kluczowych i podmiotów ważnych.

3.14. Jakie są obowiązki z zakresu cyberbezpieczeństwa dla samorządowych podmiotów publicznych?

Do katalogu tych podmiotów zaliczane będą również podmioty publiczne, w tym jednostki samorządu terytorialnego.

Podmioty publiczne będące podmiotami kluczowymi.	Podmioty publiczne będące podmiotami ważnymi
w odniesieniu do samorządu województwa: jednostki budżetowe oraz zakłady budżetowe z wyłączeniem a) jednostek organizacyjnych, o których mowa w art. 2 ustawy	wskazane w załączniku nr 2 w sektorze podmioty publiczne, tj. niewskazane w załączniku nr 1 Samorządowe jednostki budżetowe Samorządowe zakłady budżetowe



<p>z dnia 14 grudnia 2016 r. – Prawo oświatowe oraz ich zespołów,</p> <p>b) jednostek organizacyjnych wspierania rodziny i systemu pieczy zastępczej, o których mowa w art. 2 ust. 3 ustawy z dnia 9 czerwca 2011 r. o wspieraniu rodziny i systemie pieczy zastępczej</p> <p>c) jednostek organizacyjnych, o których mowa w art. 6 pkt 5 ustawy z dnia 12 marca 2004 r. o pomocy społecznej, oprócz regionalnych ośrodków polityki społecznej,</p> <p>d) wojewódzkich urzędów pracy,</p> <p>e) parków krajobrazowych i ich zespołów,</p> <p>f) jednostek obsługujących, o których mowa w art. 8d ustawy z dnia 5 czerwca 1998 r. o samorządzie województwa, w zakresie w jakim prowadzą wspólną obsługę jednostek, o których mowa w lit. a–e</p> <p>w odniesieniu do samorządu powiatu: starostwo powiatowe</p> <p>w odniesieniu do samorządu gminy: urząd gminy, jeżeli zatrudnia na dzień 1 stycznia danego roku w przeliczeniu na pełny wymiar czasu pracy na podstawie umowy o pracę co najmniej 50 osób.</p>	<p>Samorządowe instytucje kultury</p> <p>Spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy o gospodarce komunalnej.</p>
--	--

Każdorazowo należy przeanalizować status prawny danego podmiotu na gruncie ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.

W przypadku lokalnych wodociągów należałoby przeanalizować także podległość pod sektor:

<p>Zaopatrzenie w wodę pitną i jej dystrybucja</p>	<p>Podmiot dostarczający wodę przeznaczoną do spożycia przez ludzi, w tym przedsiębiorstwo wodociągowo-kanalizacyjne, o którym mowa w art. 2 pkt 4 ustawy z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków, z wyłączeniem podmiotów, dla których dostarczanie</p>
--	---



wody przeznaczonej do spożycia przez ludzi jest inną niż istotną częścią ich ogólnej działalności.

Samorządowe podmioty publiczne również prowadzą działalność jako przedsiębiorcy telekomunikacyjni, stąd mogą wchodzić pod podsektor komunikacji elektronicznej.

Wprowadzono uproszczone wymagania dla samorządowych podmiotów publicznych, które są podmiotami ważnymi. Mają one charakter listy kontrolnej minimalnych wymogów takich jak inwentaryzacja zasobów informatycznych, weryfikacja uprawnień personelu, stosowanie oprogramowania antywirusowego, czy stosowanie zasad cyberhigieny.

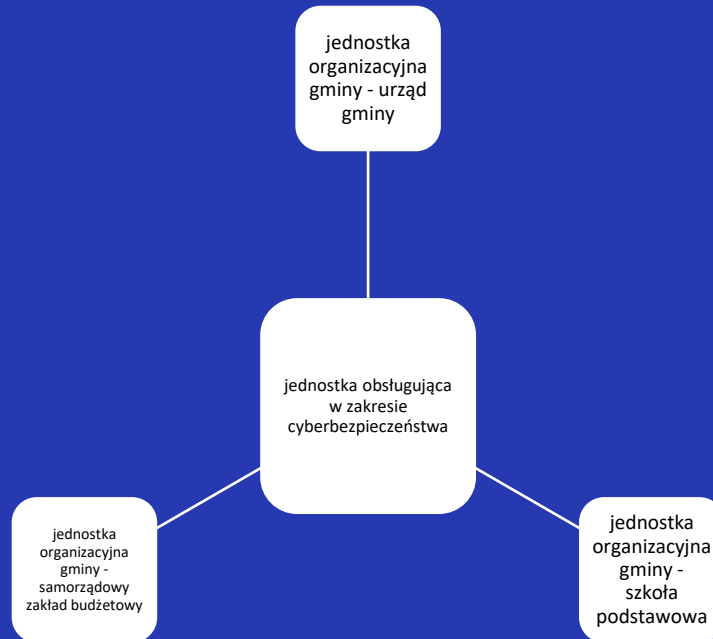
Zrezygnowano więc z podejścia opartego na ryzyku, ponieważ wymagałoby to najpierw posiadania odpowiedniego personelu przez mniejsze jednostki samorządowe, który potrafiłby przeprowadzić szacowanie ryzyka i na podstawie tego wprowadzić odpowiednie środki techniczne i organizacyjne. Mniejsze jednostki samorządowe nie posiadają takich zasobów osobowych, stąd obniżono wymagania z zakresu cyberbezpieczeństwa.

Przepisy te przewidują również **możliwość zawierania porozumień i wspólnego wykonywania zadań z zakresu cyberbezpieczeństwa**. Oznacza to, że możliwe będzie np. wyznaczenie jednostki odpowiedzialnej za realizację ustawowych obowiązków przez pozostałe jednostki samorządu terytorialnego oraz spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej. Mogą to być przypadki m.in. gdy jedna jednostka organizacyjna gminy będzie odpowiedzialna za obowiązki cyberbezpieczeństwa w pozostałych jednostkach organizacyjnych gminy.

Jednostka organizacyjna w jednej z JST może też odpowiadać za jednostki z innych JST, jeżeli zostanie zawarte stosowne porozumienie.

Jednostki obsługujące mogą być tworzone na poziomie gminy, powiatu lub województwa.

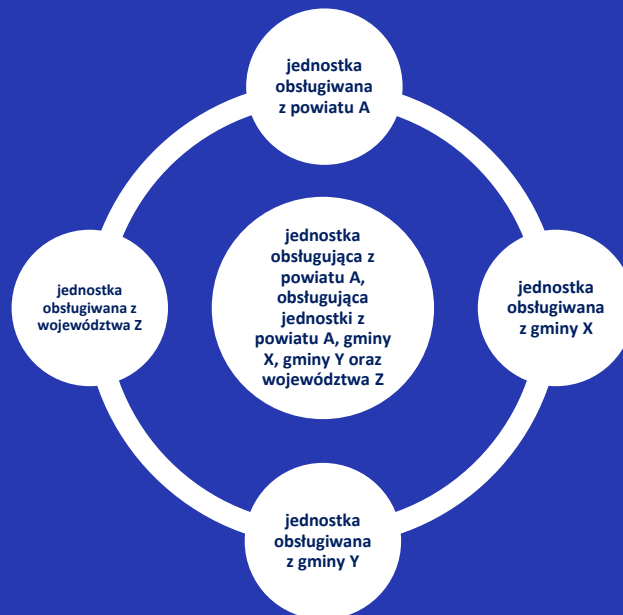
Przykładowy model jednostki obsługującej w obszarze cyberbezpieczeństwa w jednej gminie



Przykładowy model jednostki obsługującej w obszarze cyberbezpieczeństwa, gdy obsługuje jednostki z kilku gmin



Przykładowy schemat jednostki obsługującej w powiatu, która obsługuje jednostki z różnych JST



Przepisy ustawy umożliwią także docelowo **współpracę w zakresie cyberbezpieczeństwa pomiędzy gminami i powiatami**, tak aby zapewnić jeszcze większą skuteczność oraz prawidłową realizację obowiązków oraz zmitigować ich koszty. Proponowane przepisy w znacznym stopniu ułatwią wdrażanie i realizację obowiązków z zakresu cyberbezpieczeństwa, szczególnie w tych jednostkach samorządu terytorialnego, które zmagają się z problemami kadrowymi, czy niewystarczającymi środkami finansowymi.

Jednostce obsługowej mogą być powierzone wszystkie lub niektóre zadania wynikające z wdrożenia systemu zarządzania bezpieczeństwem informacji.

3.15. Czy jednostka samorządowa musi przeprowadzać szacowanie ryzyka? [NOWE - aktualizacja czerwiec 2026 r.]

Podmiot ważny będący podmiotem publicznym, stosujący załącznik nr 4 formalnie nie ma obowiązku przeprowadzania szacowania ryzyka. Jednakże należy podkreślić, że analiza ryzyka nie jest jakkolwiek zakazana – zgodnie z pkt II.9 załącznika nr 4 do ustawy o KSC, podmiot ważny będący podmiotem publicznym może stosować dodatkowe środki techniczne i organizacyjne, jeżeli jest to konieczne dla zapewnienia odpowiedniego poziomu bezpieczeństwa systemów informacyjnych.

Niezależnie od tego należy pamiętać o innych przepisach – jako przykład należy wskazać art. 32 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 i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zgodnie z którym „Uwzględniając stan



wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku (...)"'. Do prawidłowego zastosowania tego przepisu niezbędne jest przeprowadzenie analizy ryzyka. Przepis ten stosuje się także do podmiotów publicznych niezależnie od ich wielkości.

3.16. Czy muszę mieć Security Operations Center (SOC)?

Nie ma narzuconych rozwiązań technicznych czy organizacyjnych. To podmiot kluczowy lub podmiot ważny musi podjąć decyzję o tym, jakie rozwiązanie będzie adekwatne do jego sytuacji. Pamiętajmy, że ustawa obejmuje wiele bardzo zróżnicowanych podmiotów. Podmioty mogą zdecydować się na zewnętrzne, komercyjne usługi, lub postawić na budowanie własnych kompetencji, często w ramach grupy kapitałowej.

3.17. Jakie są obowiązki podmiotów kluczowych i podmiotów ważnych w zakresie kontaktów z innymi podmiotami oraz użytkownikami?

Podmioty kluczowe i podmioty ważne muszą również wyznaczyć dwie osoby do kontaktów z innymi podmiotami krajowego systemu cyberbezpieczeństwa.

Podmiot będący mikroprzedsiębiorcą lub małym przedsiębiorcą wyznaczy jedną osobę, ponieważ obowiązek wyznaczenia dwóch osób mógłby być zbyt dużym obciążeniem.

Podmioty te mają również obowiązek zapewniania użytkownikowi usługi dostępu do wiedzy pozwalającej na zrozumienie cyberzagrożeń i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczonymi usługami. Użytkownicy muszą posiadać aktualne informacje, aby być w stanie chronić się przed zagrożeniami.

Można wykonać ten obowiązek przez odesłanie do stron internetowych organu właściwego do spraw cyberbezpieczeństwa, CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowego.

Każdy podmiot kluczowy oraz podmiot ważny powinien zapewnić możliwość zgłaszania przez swoich użytkowników cyberzagrożeń, podatności czy incydentu związanego z usługą świadczoną przez podmiot. Forma zgłoszenia należy już do podmiotu – czy to będzie odrębny adres poczty elektronicznej, czat na stronie internetowej, adres do doręczeń elektronicznych w przypadku podmiotów zobowiązanych do stosowania ustawy o doręczeniach elektronicznych.



3.18. Kto może być osobą kontaktową z podmiotami krajowego systemu cyberbezpieczeństwa?

To może być każda osoba związana z podmiotem umową o pracę lub innym stosunkiem zatrudnienia. Nie jest wymagane określone wykształcenie, w tym związane z cyberbezpieczeństwem.

3.19. Czy obowiązki z zakresu cyberbezpieczeństwa muszą realizować w ramach swojej struktury organizacyjnej?

Podmiot kluczowy lub podmiot ważny realizuje zadania za pomocą wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo (np. komórka organizacyjna w danym podmiocie, niezależnie od jej nazwy, ale zajmująca się cyberbezpieczeństwem) lub zawiera umowę z dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa. Kluczowy jest tutaj spójnik „lub” – chodzi o możliwość outsourcingu tylko niektórych zadań. Decyzja o wyborze modelu realizacji zadań należy do podmiotu kluczowego lub podmiotu ważnego. Podkreślić jednak należy, że musi być ona rozsądna. Zadania z zakresu cyberbezpieczeństwa nie powinny być powierzane np. przeciętnemu działowi help-desk, ponieważ nie będą one realizowane efektywnie.

3.20. Czy samodzielny publiczny zakład opieki zdrowotnej zatrudniający poniżej 50 pracowników podlega pod ustawę o KSC? [NOWE – aktualizacja czerwiec 2026 r.]

Samodzielny publiczny zakład opieki zdrowotnej, który zatrudnia poniżej 50 pracowników nie podlega pod ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

3.21. Czy istnieje rejestr dostawców usług zaufania? [NOWE – aktualizacja czerwiec 2026 r.]

Rejestr dostawców usług zaufania jest dostępny pod adresem:
<https://www.nccert.pl/uslugi.htm> .

Zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (<https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32014R0910>) „usługa zaufania” oznacza usługę elektroniczną zazwyczaj świadczoną za wynagrodzeniem i obejmującą którąkolwiek z następujących czynności:



- wydawanie certyfikatów podpisów elektronicznych, certyfikatów pieczęci elektronicznych, certyfikatów uwierzytelniania witryn internetowych lub certyfikatów do celów świadczenia innych usług zaufania;
- walidację certyfikatów podpisów elektronicznych, certyfikatów pieczęci elektronicznych, certyfikatów uwierzytelniania witryn internetowych lub certyfikatów do celów świadczenia innych usług zaufania;
- tworzenie podpisów elektronicznych lub pieczęci elektronicznych;
- walidację podpisów elektronicznych lub pieczęci elektronicznych;
- konserwację podpisów elektronicznych, pieczęci elektronicznych, certyfikatów podpisów elektronicznych lub certyfikatów pieczęci elektronicznych;
- zarządzanie urządzeniami do składania podpisu elektronicznego na odległość lub urządzeniami do składania pieczęci elektronicznej na odległość;
- wydawanie elektronicznych poświadczeń atrybutów;
- walidację elektronicznych poświadczeń atrybutów;
- tworzenie elektronicznych znaczników czasu;
- walidację elektronicznych znaczników czasu;
- świadczenie usług rejestrowanego doręczenia elektronicznego;
- walidację danych przekazywanych za pośrednictwem usług rejestrowanego doręczenia elektronicznego i związanych z nimi dowodów;
- archiwizację elektroniczną danych elektronicznych i dokumentów elektronicznych;
- rejestrowanie danych elektronicznych w rejestrze elektronicznym.

3.22. Czy istnieje rejestr bezpiecznych dostawców sprzętu i oprogramowania dla podmiotów kluczowych i podmiotów ważnych? [NOWE – aktualizacja czerwiec 2026 r.]

Nie istnieje rejestr bezpiecznych, zweryfikowanych dostawców sprzętu i oprogramowania dla podmiotów kluczowych i podmiotów ważnych.

Podmioty kluczowe i podmioty ważne same muszą zarządzać ryzykiem związanym z łańcuchem dostaw i szacować ryzyko związane z danym dostawcą. Zamawiający, realizując obowiązki związane z zapewnieniem bezpieczeństwa teleinformatycznego oraz ciągłości działania, powinien każdorazowo dokonywać oceny nabywanych rozwiązań ICT z uwzględnieniem wiarygodności dostawcy, bezpieczeństwa oferowanego sprzętu, oprogramowania i usług, a także potencjalnych ryzyk związanych z łańcuchem dostaw.

Wybór sprzętu, oprogramowania oraz usług ICT powinien odbywać się w szczególności z uwzględnieniem, czy sprzęt, oprogramowanie lub usługa ICT pochodzą ze sprawdzonego i zaufanego źródła, od dostawców zapewniających odpowiedni poziom bezpieczeństwa i zgodność z obowiązującymi przepisami oraz standardami ochrony informacji.



Jednocześnie tacy dostawcy często sami będą podmiotami kluczowymi lub podmiotami ważnymi lub będą podlegać wymogom Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń (UE) nr 168/2013 i (UE) 2019/1020 i dyrektywy (UE) 2020/1828 (akt o cyberodporności) <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32024R2847>. Stąd też tacy dostawcy podlegają również wymogom z zakresu cyberbezpieczeństwa.

3.23. Jak należy określić wielkość podmiotu leczniczego, który nie jest przedsiębiorcą? [NOWE – aktualizacja czerwiec 2026 r.]

Podmiot leczniczy, który nie jest przedsiębiorcą:

- 1) jest podmiotem ważnym, jeżeli zatrudnia od 50 do 249 osób;
- 2) jest podmiotem kluczowym, jeżeli zatrudnia co najmniej 250 osób.

Przy ustalaniu statusu podmiotu należy wziąć pod uwagę wszystkie stosunki zatrudnienia jak zatrudnienie pracownicze, np. na umowę o pracę, oraz zatrudnienie niepracownicze, np. w oparciu o umowy cywilnoprawne. Ponadto nie rozróżnia on zatrudnienia w pełnym wymiarze czasu pracy jak i w niepełnym wymiarze.

Obowiązuje przy tym zasada, zgodnie z którą jeżeli status podmiotu kluczowego lub podmiotu ważnego zależy od wielkości podmiotu, to przesłanki uznania za podmiot kluczowy lub podmiot ważny bada się według stanu na dzień sporządzenia sprawozdania finansowego.

3.24. Czy urząd gminy posiadający w swoich strukturach Zakład Obsługi Komunalnej świadczący usługi dostarczania wody oraz odbioru ścieków będzie należał do podmiotów kluczowych czy też do podmiotów ważnych publicznych? [NOWE – aktualizacja czerwiec 2026 r.]

Urząd gminy, który ma w swojej strukturze komórkę organizacyjną zajmującą się dostarczaniem wody będzie podmiotem kluczowym. Zbiorowe zaopatrzenie w wodę i zbiorowe odprowadzanie ścieków jest zadaniem własnym gminy, stąd też jest to istotna część urzędu gminy, który zajmuje się dostarczaniem wody pitnej.



3.25. Czy związki jednostek samorządu terytorialnego podlegają pod ustawę o KSC? [NOWE – aktualizacja czerwiec 2026 r.]

Związki jednostek samorządu terytorialnego nie zostały wpisane do sektora podmiotów publicznych. Stąd też nie będą wpisane z urzędu przez Ministra Cyfryzacji do wykazu podmiotów kluczowych i podmiotów ważnych. Jednakże mogą znaleźć się w krajowym systemie cyberbezpieczeństwa, jeżeli spełniają kryteria dla innych sektorów, przykładowo zaopatrzenia w wodę pitną i jej dystrybucji lub zbiorowego odprowadzania ścieków.

3.26. Czy jeśli uczelnia wyższa prowadzi również badania aplikacyjne oraz prace rozwojowe lecz nie jest to jej podstawowa działalność (zajmuje się nią jedna z jednostek uczelni), to czy w zakresie działalności tej jednostki uczelnia jest zobowiązana wdrożyć SZBI zgodnie z art. 8 ustawy o KSC, czy też cały podmiot (uczelnia) podlega pod obowiązki określone w załączniku nr 4 do ustawy? [NOWE – aktualizacja czerwiec 2026 r.]

Uczelnia, która prowadzi badania aplikacyjne oraz prace rozwojowe przy pomocy systemu informacyjnego, ale nie jest to jej podstawowa działalność, nie jest organizacją badawczą. W tej sytuacji stosuje obowiązki wskazane w załączniku nr 4 do ustawy.

3.27. Czy jeśli podstawową działalnością uczelni jest prowadzenie badań aplikacyjnych i prac rozwojowych, a pozostałą działalnością jest działalność edukacyjna, to czy cała uczelnia podlega pod SZBI z art. 8 ustawy o KSC, czy też w zakresie w jakim uczelnia prowadzi działalność edukacyjną wystarczające jest wdrożenie obowiązków wskazanych w załączniku nr 4 do ustawy? [NOWE – aktualizacja czerwiec 2026 r.]

Jeżeli uczelnia jest organizacją badawczą to nie stosuje załącznika nr 4 do ustawy o KSC tylko wdraża pełny system zarządzania bezpieczeństwem informacji zgodny z art. 8 ust. 1 ustawy o KSC.



3.28. Czy podmioty kluczowe i podmioty ważne są uprawnione w okresie dostosowawczym do gromadzenia danych o niekaralności w aktualnie otwartych procesach rekrutacji? [NOWE – aktualizacja czerwiec 2026 r.]

W okresie dostosowawczym podmiot kluczowy i podmiot ważny jest uprawniony do podejmowania czynności mających na celu przystosowanie się do nowych obowiązków. Uprawnione jest wobec tego gromadzenie danych o niekaralności personelu, który będzie realizował te zadania także po zakończeniu okresu dostosowawczego.

3.29. Czy weryfikacja niekaralności personelu dotyczy również obecnego czy tylko przyszłego personelu? [NOWE – aktualizacja czerwiec 2026 r.]

Weryfikacja dotyczy obecnego i przyszłego personelu.

3.30. Kto ponosi odpowiedzialność za realizację obowiązków z zakresu cyberbezpieczeństwa w przypadku jednostki wyznaczonej? [NOWE – aktualizacja czerwiec 2026 r.]

Jeżeli wyznaczając jednostkę do realizacji obowiązków z zakresu cyberbezpieczeństwa organ wyznaczający wskazał, że będzie ona realizować również zadania kierownika podmiotu, to wtedy kierownik jednostki wyznaczonej ponosi odpowiedzialność za realizację zadań z zakresu cyberbezpieczeństwa.

3.31. Czy system zarządzania bezpieczeństwem informacji dla kilku systemów informacyjnych wykorzystywanych przez podmiot może być opracowany w jednym dokumencie? [NOWE – aktualizacja czerwiec 2026 r.]

Tak, ustawa nie wprowadza tutaj odrębnych wymogów.

3.32. Czy termin realizacji obowiązków z zakresu wdrożenia systemu zarządzania bezpieczeństwem informacji należy liczyć się od daty wpisu do Wykazu KSC? [NOWE – aktualizacja czerwiec 2026 r.]

Terminy dostosowawcze dla podmiotów kluczowych i podmiotów ważnych liczy się od dnia spełnienia przesłanek uznania za podmiot kluczowy lub podmiot



ważny, a nie od dnia wpisu w wykazie podmiotów kluczowych lub podmiotów ważnych.

3.33. Czy termin realizacji obowiązków dotyczących uzupełnienia danych w Wykazie KSC liczy się od daty wpisu do wykazu? [NOWE – aktualizacja czerwiec 2026 r.]

Obowiązek uzupełnienia danych liczony jest od dnia otrzymania wezwania do uzupełnienia danych w wykazie. Podmiot ma 6 miesięcy na zrealizowanie tego obowiązku.

3.34. Czy jeżeli spółka świadczy usługi zarządzane z zakresu cyberbezpieczeństwa tylko dla innych spółek w ramach grupy kapitałowej to czy podlega pod ustawę o KSC? [NOWE – aktualizacja czerwiec 2026 r.]

Tak, ponieważ jako odrębny podmiot świadczy usługi innemu podmiotowi.

3.35. Czy jednostka wyznaczona z województwa może obsługiwać gminy i powiaty? [NOWE – aktualizacja czerwiec 2026 r.]

Tak, wojewódzka jednostka wyznaczona do realizacji zadań z zakresu cyberbezpieczeństwa może obsługiwać jednostki gminne i powiatowe jeżeli województwo zawrze porozumienie z gminą lub z powiatem. Wynika to z brzmienia art. 16e ust. 6 ustawy o KSC, gdzie wskazano, że to jednostki samorządu terytorialnego - a więc gmina, powiat lub województwo mogą zawrzeć takie porozumienie.

Odpowiednie stosowanie art. 74 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym, które jest wskazane w ust. 9 należy rozumieć w ten sposób, jednostki samorządu terytorialnego mogą zawierać porozumienia w sprawie powierzenia jednej z nich określonych przez nie zadań z zakresu cyberbezpieczeństwa. Jednostka samorządu terytorialnego wykonująca zadania z zakresu cyberbezpieczeństwa objęte porozumieniem przejmując prawa i obowiązki pozostałych jednostek samorządu terytorialnego, związane z powierzonymi jej zadaniami, a jednostki te mają obowiązek udziału w kosztach realizacji powierzonego zadania.



3.36. Czy Gminny Ośrodek Pomocy Społecznej jest podmiotem krajowego systemu cyberbezpieczeństwa? [NOWE – aktualizacja czerwiec 2026 r.]

Gminne ośrodki pomocy społecznej jako samorządowe jednostki budżetowe podlegają pod ustawę o KSC. Będą one podmiotami ważnymi.

3.37. Czym są samorządowe podmioty publiczne? [NOWE – aktualizacja czerwiec 2026 r.]

Samorządowymi podmiotami publicznymi są:

- samorządowe jednostki budżetowe, w tym urzędy gmin, starostwa powiatowe;
- samorządowe zakłady budżetowe;
- samorządowe instytucje kultury;
- spółki wykonujące zadania o charakterze użyteczności publicznej, tzw. spółki komunalne.

3.38. Czy ustalając wielkość podmiotów zgodnie z unijnymi kryteriami należy wziąć pod uwagę dane finansowe związane tylko z działalnością podmiotu wskazaną w załączniku do ustawy o KSC czy dane finansowe całego podmiotu? [NOWE – aktualizacja czerwiec 2026 r.]

Należy wziąć pod uwagę dane finansowe obejmujące całą działalność podmiotu.

3.39. Czy podmioty kluczowe mają obowiązek stosowania Załącznika nr 4 do ustawy o KSC? [NOWE – aktualizacja czerwiec 2026 r.]

Załącznik nr 4 do ustawy był prezentowany jako uproszczony zestaw wymagań i przeznaczony jest dla podmiotów ważnych będących podmiotem publicznym. Podmioty kluczowe muszą realizować wszystkie obowiązki i pełny zakres wymagań SZBI określony w art. 8 ustawy o KSC.

3.40. Które elementy Załącznika nr 4 do ustawy o KSC mają charakter obowiązkowy, a które fakultatywny? [NOWE – aktualizacja czerwiec 2026 r.]

Załącznik nr 4 został podzielony na trzy części. Pierwsza część załącznika oznaczona numerem rzymskim I to część obowiązkowa, którą każdy podmiot



ważny będący podmiotem publicznym musi spełnić. Treść wskazana w części Załącznika nr 4 oznaczona rzymską cyfrą II to część fakultatywna, która zawiera elementy, których wdrożenie podmiot ważny będący podmiotem publicznym powinien rozważyć mając na uwadze potrzebę zapewnienia cyberbezpieczeństwa i jeżeli jego uwarunkowania organizacyjne, finansowe i osobowe na to pozwalają.

Część oznaczona rzymską cyfrą III jest to część obowiązkowa odnosząca się do aktualizacji i przeglądu spełniania obowiązków określonych w poprzednich częściach Załącznika nr 4.

3.41. Jak rozumieć wykonywania zapasowych kopii danych odseparowanych logicznie i fizycznie od danych przetwarzanych w systemach informacyjnych dla realizacji zadania publicznego wskazane w Załączniku nr 4. Czy muszą one być przechowywane w innym budynku czy wystarczy w innym pomieszczeniu? [NOWE – aktualizacja czerwiec 2026 r.]

Celem wymagania wskazanego w obowiązkowej części Załącznika nr 4 w pkt 10 jest, aby kopia zapasowa nie była narażona na te same ryzyka, które dotyczą danych w wersji produkcyjnej używanych do bieżącej realizacji zadań. Dlatego przepis zawiera wymóg odseparowania logicznego i fizycznego tych dwóch obszarów. Ustawa nie wskazuje na obowiązek przechowywania kopii zapasowych w innych budynkach. Z punktu widzenia celów ustawy minimalnym obowiązkiem jest przechowywanie kopii zapasowych w takim miejscu, aby zapewnić możliwość spełnienia jej celu lub funkcji.



4. Obowiązki kierownika podmiotu

4.1. Jakie są podstawowe obowiązki kierownika podmiotu kluczowego lub podmiotu ważnego?

Wskazano zadania kierownika podmiotu kluczowego lub podmiotu ważnego:

- 1) podejmuje decyzje w zakresie przygotowania, wdrażania, stosowania, przeglądu i nadzoru systemu zarządzania bezpieczeństwem informacji w podmiocie – co oznacza, że kierownik odpowiada za system zarządzania bezpieczeństwem informacji i jego rozwój zgodnie z cyklem Deminga;
- 2) planuje adekwatne środki finansowe na realizację obowiązków z zakresu cyberbezpieczeństwa – mając na uwadze, że cyberbezpieczeństwo wymaga nakładów i nie powinny one być pomijane w budżetach podmiotów kluczowych i podmiotów ważnych; z drugiej strony muszą być to adekwatne środki, czyli takie, które są też dostosowane do możliwości podmiotu;
- 3) przydziela zadania z zakresu cyberbezpieczeństwa w tym podmiocie i nadzoruje ich wykonanie – na przykład poprzez przyjęcie odpowiednich polityk, przydział obowiązków, wydanie upoważnień;
- 4) zapewnia, że personel podmiotu jest świadomy obowiązków z zakresu cyberbezpieczeństwa i zna wewnętrzne regulacje podmiotu w tym zakresie. System zarządzania bezpieczeństwem informacji wymaga, aby każdy pracownik organizacji miał przypisaną rolę i zadania do wykonania celem zachowania bezpieczeństwa informacji;
- 5) zapewnia zgodność działania tego podmiotu z przepisami prawa oraz z wewnętrznymi regulacjami podmiotu – tu chodzi o zapewnienie stosowalności w podmiocie nie tylko przepisów prawa powszechnie obowiązującego, ale również własnych regulacji, aby nie były pomijane w codziennej pracy.

4.2. Kim jest kierownik podmiotu kluczowego lub podmiotu ważnego?

Jest to członek zarządu lub innego organu zarządzającego, a jeżeli organ jest wieloosobowy – członków tego organu, z wyłączeniem pełnomocników ustanowionych przez jednostkę.

W przypadku spółki jawnej i spółki cywilnej za kierownika jednostki uważa się wspólników prowadzących sprawę spółki.

W przypadku spółki partnerskiej – wspólnicy prowadzący sprawę spółki albo zarząd.

W przypadku spółki komandytowej i spółki komandytowo-akcyjnej – komplementariusze prowadzący sprawę spółki.



W przypadku osoby fizycznej prowadzącej działalność gospodarczą za kierownika jednostki uważa się tę osobę.

Kierownikiem jest również likwidator, syndyk, zarządca ustanowiony w postępowaniu restrukturyzacyjnym oraz zarządca sukcesyjny oraz osoba, która dokonała zgłoszenia do naczelnika urzędu skarbowego o kontynuowaniu prowadzenia przedsiębiorstwa.

W przypadku podmiotu publicznego kierownikiem podmiotu jest kierownik jednostki sektora finansów publicznych.

4.3. Czy kierownik podmiotu kluczowego lub podmiotu ważnego podlega obowiązkowym szkoleniom?

Osoby kierujące podmiotami kluczowymi lub podmiotami ważnymi muszą również raz na rok przejść szkolenie z zakresu wykonywania zadań z zakresu cyberbezpieczeństwa. Dotyczy to zadań związanych z opracowaniem systemu zarządzania bezpieczeństwem informacji, zgłaszania incydentów, dokumentowania SZBI. Gwarantuje to, że będą posiadać aktualną wiedzę merytoryczną potrzebną do podejmowania decyzji w tym obszarze.

4.4. Za co ponosi odpowiedzialność kierownik podmiotu kluczowego lub ważnego?

Kierownik podmiotu kluczowego lub podmiotu ważnego ponosi odpowiedzialność za:

- dokonanie aktualnego wpisu do wykazu podmiotów kluczowych lub podmiotów ważnych,
- wdrożenie systemu zarządzania bezpieczeństwem informacji w podmiocie,
- realizację swoich zadań,
- weryfikację personelu realizującego zadania z zakresu systemu zarządzania bezpieczeństwem informacji i zgłaszania incydentów,
- przeszkolenie siebie z realizacji obowiązków,
- wyznaczenie osób kontaktowych,
- zapewnienie użytkownikowi usługi dostępu do wiedzy z zakresu cyberbezpieczeństwa,
- zapewnienie użytkownikowi usługi możliwości zgłoszenia cyberzagrożenia, incydentu lub podatności związanych ze świadczoną usługą,
- korzystanie z systemu S46,
- zgłaszanie incydentów,
- przeprowadzanie audytów.

Kierownik podmiotu kluczowego lub podmiotu ważnego ponosi odpowiedzialność także wtedy, gdy niektóre z obowiązków albo wszystkie obowiązki zostały powierzone innej osobie za jej zgodą.



4.5. Czy w przypadku samorządowej jednostki budżetowej, innej niż urząd, starostwo itd., przez kierownika urzędu należy rozumieć dyrektora tej jednostki? [NOWE – aktualizacja czerwiec 2026 r.]

Kierownik jednostki budżetowej jest kierownikiem podmiotu kluczowego lub podmiotu ważnego i odpowiada za realizację obowiązków z zakresu cyberbezpieczeństwa.

4.6. Kto odpowiada za niewykonanie obowiązków przez podmiot publiczny które nie współpracuje z jednostką wyznaczoną do realizacji zadań z zakresu cyberbezpieczeństwa? [NOWE – aktualizacja czerwiec 2026 r.]

Ustawa o KSC w art. 16e wskazuje, że podmiot publiczny wskazany w tym przepisie może wyznaczyć jednostkę odpowiedzialną za realizację obowiązków, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8c-8f, art. 9-12b lub art. 15. W takim zakresie jednostka wyznaczona przejmuje realizację tych zadań. Jest to więc jej zakres odpowiedzialności.

Jednocześnie ustawa o KSC wskazuje wyraźnie zakres obowiązków podmiotów publicznych w relacjach z ww. jednostką. Należy do nich obowiązek współpracy, np. w zakresie informacji o incydentach, udziału w szkoleniach, itp.

Brak realizacji tych obowiązków przez jednostki będzie podlegał ocenie w trakcie działań kontrolnych przez organy właściwe do spraw cyberbezpieczeństwa. Brak ich realizacji może być przedmiotem wystąpienia także do innych instytucji odpowiedzialnych za działanie tej jednostki.



5. Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT)

5.1. Jakie są rodzaje zespołów CSIRT?

Ustawa wprowadza pojęcia **CSIRT sektorowego** – jest to Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, działający na poziomie sektora lub podsektora, ustanowiony przez organ właściwy do spraw cyberbezpieczeństwa dla danego sektora lub podsektora.

Oprócz tego funkcjonują trzy zespoły **CSIRT poziomu krajowego**:

- 1) CSIRT GOV - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego;
- 2) CSIRT MON - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Ministra Obrony Narodowej;
- 3) CSIRT NASK - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy.

5.2. Jakie są dane kontaktowe do zespołów CSIRT poziomu krajowego?

CSIRT GOV

E-mail: csirt@csirt.gov.pl

Fax: +48 22 58 58 833

CSIRT MON

Tel.: +48 261 865 333

E-mail: csirt-mon@ron.mil.pl

CSIRT NASK

e-mail: info@cert.pl

5.3. Czym jest CSIRT sektorowy?

Jest to Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie sektora lub podsektora, ustanowiony przez organ właściwy do spraw cyberbezpieczeństwa dla danego sektora lub podsektora.



6. Zgłaszanie incydentów

6.1. Czym jest incydent?

Incydent jest to zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych.

Wyjaśnienia wymaga wskazanie w definicji, że incydent to zdarzenie „które ma lub może mieć” – ta fakultatywność jest obecna od 2018 r. i przede wszystkim związana jest z zapewnieniem, że zespoły CSIRT albo osoby odpowiedzialne za obsługę incydentów w podmiocie będą otrzymywały informację o zdarzeniu, które wystąpiło i nie można było mu zapobiec, a zagraża bezpieczeństwu systemów. Dzięki temu można już rozpocząć proces zarządzania incydem i na końcu wyciągnąć wnioski, które zapobiegną poważniejszym zdarzeniom w przyszłości. Takie podejście do incydemu pozwala zidentyfikować słabości organizacji, a także wdrożyć działania prewencyjne, poprawiające poziom bezpieczeństwa, jeszcze przed tym, zanim zdarzenie wywoła niekorzystne skutki.

Takie ukształtowanie przepisu jest zarazem zgodne z brzmieniem art. 3 rozporządzenia wykonawczego 2024/2690, w którym w kilku miejscach wskazano, że incydent uznaje się za incydent poważny (w przypadku podmiotów z sektora infrastruktury cyfrowej) jeśli „incydent spowodował lub może spowodować ...”.

6.2. Jakie są rodzaje incydentów?

Incydenty dzielą się na:

- 1) **incydent krytyczny** – incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV
- 2) **incydent poważny** - incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi przez podmiot kluczowy lub podmiot ważny, straty finansowe dla tego podmiotu lub wpływa na inne osoby fizyczne, osoby prawne, jednostki organizacyjne nieposiadające osobowości prawnej przez wywołanie poważnej szkody materialnej lub niematerialnej
- 3) **incydent w cyberbezpieczeństwie na dużą skalę** – incydent, którego skutki przekraczają możliwości reagowania państwa lub który ma poważny wpływ na inne państwo członkowskie Unii Europejskiej



6.3. Czy muszę zgłaszać wszystkie incydenty?

Każdy podmiot kluczowy lub podmiot ważny ma obowiązek zarządzania każdym incydentem. Jednakże obowiązkowemu zgłoszeniu podlegają jedynie incydenty poważne.

6.4. Jakie są obowiązki z zakresu obsługi incydentów?

Podmiot kluczowy lub podmiot ważny ma obowiązek zapewnić obsługę incydentu. Oznacza to m.in. obowiązek:

- zgłoszenia wczesnego ostrzeżenia o incydencie poważnym, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do właściwego CSIRT sektorowego,
- zgłoszenia incydentu poważnego niezwłocznie, nie później niż w ciągu 72 godzin od momentu jego wykrycia, do właściwego CSIRT sektorowego,
- zapewnienia dostępu do informacji o rejestrowanych incydentach właściwemu CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowemu, w zakresie niezbędnym do realizacji jego zadań,
- współdziałania podczas obsługi incydentu poważnego i incydentu krytycznego z właściwym CSIRT
- przekazania, na wniosek właściwego CSIRT sektorowego, sprawozdania okresowego z obsługi incydentu poważnego
- przekazania właściwemu CSIRT sektorowemu sprawozdania końcowego z obsługi incydentu poważnego, nie później niż w ciągu miesiąca od dnia zgłoszenia
- informowania użytkowników swoich usług o incydencie poważnym, jeżeli ma on niekorzystny wpływ na świadczenie tych usług
- podejmowania działań naprawczych.

W ramach obsługi incydentów podmiot krajowego systemu cyberbezpieczeństwa może w szczególności podejmować działania w celu wykrywania źródła lub dokonywania analizy aktywności, w tym ruchu sieciowego, powodujących wystąpienie incydentu zakłócającego świadczenie usług przez ten podmiot. Uprawnienia te są niezbędne dla zapewnienia skutecznej reakcji na incydent, a w praktyce sprawiają one problemy praktyczne. Wykrycie źródła ataku często jest niezbędne do jego powstrzymania i przywrócenia normalnego funkcjonowania systemów.

6.5. Jak określić moment wykrycia incydentu?

Jest to moment, w którym podmiot uzyskał informacje o zdarzeniu, które kwalifikuje się jako incydent. Informacje te może uzyskać monitorując własne systemy lub pozyskując informacje od dostawcy usługi. W umowach z



dostawcami należy zawrzeć obowiązek dostawcy o niezwłocznym informowaniu o incydencie związanym z usługą dostawcy.

6.6. Czy incydenty związane z automatyką przemysłową są także zgłaszane do zespołów CSIRT sektorowych?

Tak. Incydenty w systemach automatyki przemysłowej podlegają obowiązkowemu zgłoszeniu.

Incydentem jest zdarzenie które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych. Definicja systemu informacyjnego uwzględnia także systemy automatyki przemysłowej.

6.7. Czy mogę dobrowolnie zgłaszać informacje o incydentach do zespołów CSIRT?

Tak, istnieje możliwość dobrowolnego zgłoszenia do zespołów CSIRT poziomu krajowego jak również CSIRT sektorowego informacji o incydentach nie podlegających obowiązkowemu zgłoszeniu, o cyberzagrożeniach, wynikach szacowania ryzyka, podatnościach, potencjalnych zdarzeniach dla cyberbezpieczeństwa czy wykorzystywanych technologiach.

Zgłoszenia te są dokonywane za pomocą systemu teleinformatycznego S46. Umożliwia to dzielenie się informacjami z zespołami CSIRT, które mogą przeanalizować je i wyciągnąć wnioski, umożliwiając lepsze wspieranie podmiotów kluczowych i podmiotów ważnych.

Przykładowo informacje o podatnościach pozwolą na opracowanie sposobów ich mitygacji. Zapewniono przy tym możliwość ochrony informacji prawnie chronionych – w tym celu podmiot kluczowy i podmiot ważny ma obowiązek oznaczyć tego rodzaju informacje.

6.8. Co to jest potencjalne zdarzenie dla cyberbezpieczeństwa? Czy muszę je zgłaszać?

Jest to zdarzenie, które może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych. Zgłaszanie takich zdarzeń do zespołów CSIRT jest nieobowiązkowe. W samej możliwości zgłoszeń tego rodzaju zdarzeń chodzi o to, aby móc wyciągnąć informacje z tego rodzaju sytuacji, które nie doprowadziły do strat, ale wyciągnięte z nich wnioski mogą pozwolić na zabezpieczenie się przed innymi incydentami.



6.9. Czym jest poważne cyberzagrożenie? Czy wiążą się z nim obowiązki informacyjne?

Poważnym cyberzagrożeniem jest cyberzagrożenie, które przez swoje właściwości techniczne może mieć poważny wpływ na bezpieczeństwo systemów informacyjnych lub użytkowników tych systemów przez wywołanie poważnej szkody materialnej lub niematerialnej. Należy poinformować użytkowników podmiotu kluczowego lub podmiotu ważnego o możliwych środkach zapobiegawczych przed poważnym cyberzagrożeniem. Przydatny do realizacji tego obowiązku może być ten szablon:

1. Informacja o cyberzagrożeniu	
1.1. Nazwa	Ogólna nazwa zagrożenia
1.2. Data	Data
1.3. Opis	Krótki opis zagrożenia
1.4. Źródła	Źródło pozyskania informacji o cyberzagrożeniu
1.5. Charakter cyberzagrożenia	Np. awaria systemu, błąd ludzki, zjawiska naturalne, złośliwe działanie (malicious action), błędy po stronie osób trzecich
1.6. Prawdopodobny wpływ na systemy informacyjne i usługi	Opisać prawdopodobny wpływ na systemy i usługi na podstawie dostępnej wiedzy.
2. Kiedy komunikować?	
2.1. Właściwości techniczne cyberzagrożenia	Krótki opis szczegółów technicznych cyberzagrożenia
2.2. Czy cyberzagrożenie może mieć wpływ na bezpieczeństwo systemów informacyjnych?	Tak lub Nie
2.3. Czy cyberzagrożenie może mieć wpływ na użytkowników?	Tak lub Nie
2.4. Czy ten wpływ jest poważny?	Należy oszacować wpływ w oparciu o przyjętą w organizacji metodę szacowania ryzyka. Na pewno wpływ cyberzagrożenia będzie większy, jeśli nie jest to typowe



	lub generalnie występujące cyberzagrożenie.
<i>Jeśli na 2.2 lub 2.3 oraz 2.4 odpowiedź brzmi TAK</i>	
2.5.Czy może wywołać szkodę materialną – jaką?	Opisać krótko możliwe szkody materialne, które może wywołać cyberzagrożenie – wedle najlepszej dostępnej wiedzy – nie chodzi o wycenianie potencjalnej szkody materialnej, ale o jej świadomość np. cyberzagrożenie może spowodować przestoje w dostawach prądu, co uniemożliwi prowadzenie działalności gospodarczej.
2.6.Czy może wywołać szkodę niematerialną – jaką?	Opisać krótko możliwe szkody niematerialne, np. szkody wizerunkowe, szkody zdrowotne.
<i>Jeśli na 2.5 lub 2.6 odpowiedź brzmi TAK</i>	
2.7.Czy szkoda może być poważna?	Ocenić potencjalną szkodę.
2.8.Czy należy zakomunikować środki zaradcze?	Jeśli zidentyfikowano, że cyberzagrożenie może mieć poważny wpływ na bezpieczeństwo systemów informacyjnych lub użytkowników oraz może spowodować poważną szkodę – materialną lub niematerialną – należy zakomunikować środki zapobiegawcze użytkownikom.
3. Komunikacja	
3.1.Kanał komunikacji	Wybrać kanał komunikacji adekwatny do zagrożenia i użytkowników – wiadomość email, SMS, media społecznościowe, aplikacja mobilna, strona internetowa
3.2.Środki zapobiegawcze	W komunikacji wskazać środki, które użytkownicy mogą podjąć,



	aby zabezpieczyć się lub ograniczyć skutki poważnego cyberzagrożenia, np. rekomendacja instalacji oprogramowania antywirusowego, włączenie wieloskładnikowego uwierzytelnienia, edukacja z zakresu nowych zagrożeń.
3.3.Czy informować o samym poważnym cyberzagrożeniu?	Oszacować ryzyko dla komunikacji informacji o samym cyberzagrożeniu.
4. Ewaluacja – czy komunikacja była skuteczna?	
4.1.Czy komunikacja dotarła do użytkowników?	Przeanalizować dostępne logi z użytych kanałów komunikacji np. liczba unikalnych wejść na stronę.
4.2.Czy użytkownicy podjęli działania?	Przeanalizować dostępne informacje zwrotne od użytkowników np. reakcje w mediach społecznościowych.
4.3.Inne mierniki	Przeanalizować inne mierniki, jeśli są dostępne.

6.10. Czym jest incydent poważny?

Jest to incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi przez podmiot kluczowy lub podmiot ważny – a nie jak do tej pory świadczenia usługi kluczowej przez operatora usługi kluczowej. Ponadto incydemtem poważnym będzie też taki, który powoduje straty finansowe dla podmiotu kluczowego i podmiotu ważnego albo wpływa na inne podmioty – osoby fizyczne, osoby prawne i ułomne osoby prawne – w taki sposób, że wywołuje szkodę materialną albo niematerialną.

W praktyce istotne znaczenie dla zidentyfikowania incydentu poważnego będą miały progi incydentu poważnego ustalone w rozporządzeniu Rady Ministrów.

6.11. Co zawiera wczesne ostrzeżenie o incydencie poważnym?

Wczesne ostrzeżenie o incydencie poważnym jest zgłaszane w terminie 24 godzin od wykrycia incydentu. Zawiera m.in.



- 1) dane podmiotu zgłaszającego – w tym firmę przedsiębiorcy, numer z właściwego rejestru, siedzibę i adres – chodzi o konieczność zapewnienia identyfikacji podmiotu zgłaszającego wczesne ostrzeżenie;
- 2) imię i nazwisko, numer telefonu służbowego oraz służbowy adres poczty elektronicznej osoby dokonującej zgłoszenia;
- 3) imię i nazwisko, numer telefonu służbowego oraz adres służbowej poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji. W zależności od okoliczności osoba dokonująca zgłoszenia może być jednocześnie osobą uprawnioną do składania wyjaśnień. Może być też inaczej, stąd zasadne jest wyodrębnienie tych kategorii osób;
- 4) wskazanie momentu wystąpienia i wykrycia incydentu poważnego oraz czas jego trwania – jest to istotne dla CSIRT który może również dokonać korelacji tych danych z innymi dostępnymi informacjami o innych incydentach i np. zidentyfikować działania grup wrogich aktorów;
- 5) wskazanie, czy incydent poważny został wywołany działaniem bezprawnym lub działaniem w złej wierze, jeżeli możliwe jest dokonanie takiej oceny – dzięki tej informacji CSIRT będzie wiedział, czy konieczne jest zaangażowanie organów ścigania;
- 6) określenie, czy incydent dotyczy innych państw członkowskich Unii Europejskiej – jest to konieczne do określenia ewentualnego wpływu transgranicznego.

6.12. Czy małe samorządowe jednostki budżetowe muszą zgłaszać wczesne ostrzeżenie o incydencie poważnym?

Podmioty publiczne będące podmiotami ważnymi mają uproszczone obowiązki przy zgłaszaniu incydentów. Nie muszą zgłaszać wczesnego ostrzeżenia, sprawozdania okresowego, sprawozdania z postępu ani sprawozdania końcowego z obsługi incydentu. Zgłaszają wyłącznie zgłoszenie incydentu poważnego.

6.13. W jaki sposób zgłasza się incydenty poważne?

Incydenty poważne są zgłaszane do CSIRT sektorowych za pomocą systemu S46, który jest prowadzony przez Ministra Cyfryzacji.

Aby korzystać z systemu, najpierw należy uzyskać do niego dostęp. W tym celu należy wypełnić oświadczenie o dołączeniu do systemu i przekazać je za pośrednictwem formularza kontaktowego.

Instrukcja, oświadczenie oraz formularz kontaktowy znajdują się pod adresem: <https://www.gov.pl/web/system-s46/uzyskaj-dostep>.



Zespoły CSIRT sektorowe oraz CSIRT poziomu krajowego prześlą sobie zgłoszenie incydentu zgodnie z właściwością, jeżeli w danej sprawie nie są właściwi.

6.14. Co zawiera zgłoszenie incydentu poważnego?

W ciągu 72 godzin od wykrycia incydentu poważnego podmiot kluczowy i podmiot ważny zgłasza incydent poważny wraz z dodatkowymi informacjami o tym incydencie:

- 1) opis wpływu incydentu poważnego na świadczenie usługi, w tym:
 - a) wskazanie usługi zgłaszającego, na które incydent poważny miał wpływ.

Aby pomóc podmiotowi zgłaszającemu incydent CSIRT musi wiedzieć na świadczenie jakich usług wpływa incydent.
 - b) liczbę użytkowników usługi, na których incydent poważny miał wpływ.

Chodzi o szacunkowe określenie liczby użytkowników na których oddziałuje incydent.
 - c) zasięg geograficzny obszaru, którego dotyczy incydent poważny.

Chodzi o określenie obszaru na który wpływa incydent poważny, przykładowo ten obszar może obejmować niedostępność usług telekomunikacyjnych na terenie dwóch powiatów, albo brak prądu w mieście wojewódzkim spowodowany awarią systemów sterowania.
 - d) wpływ incydentu poważnego na świadczenie usługi przez inne podmioty.

Podmiot kluczowy i podmiot ważny powinien, w ramach analizy kontekstu organizacji ustalić podmioty z którymi współpracuje i którym świadczy usługi. Będzie więc mógł określić, czy incydent wpływa na te podmioty czy nie.
- 2) opis przyczyn tego incydentu, sposób jego przebiegu oraz prawdopodobne skutki oddziaływania na systemy informacyjne lub świadczone usługi.

Przykładowo należy wskazać oznaki naruszenia integralności systemu (indicators of compromise).
- 3) informacje o podjętych działaniach zapobiegawczych;
- 4) informacje o podjętych działaniach naprawczych;
- 5) aktualizację informacji przekazanych we wczesnym ostrzeżeniu, jeżeli nastąpiła ich zmiana.



6.15. Nie mam wszystkich danych w chwili zgłoszenia incydentu poważnego – co muszę zrobić?

Nie zawsze wszystkie informacje będą dostępne w trakcie zgłaszania incydentu poważnego, dlatego podmiot kluczowy lub podmiot ważny będzie obowiązany zgłosić te informacje, o których wie na moment zgłoszenia. Będzie przy tym zobligowany uzupełnić te informacje później w trakcie obsługi incydentu.

6.16. Kiedy muszę poinformować swoich użytkowników o incydencie poważnym?

Podmiot kluczowy lub podmiot ważny ma obowiązek poinformować użytkowników swoich usług o incydencie poważnym, jeżeli ma on niekorzystny wpływ na świadczenie usług.

Niekorzystny wpływ to taki, który przynosi straty dla użytkowników, np. tracą czas, pieniądze, czy w niektórych przypadkach zdrowie. Stąd też w takich sytuacjach należy ich informować o incydencie poważnym.

6.17. W jaki sposób zachować się w sytuacji, gdy jeden incydent (np. ten sam atak) ma bezpośredni wpływ na usługi świadczone w ramach różnych sektorów przez tego samego przedsiębiorcę? Czy należy dokonać zgłoszenia przez system S46 do każdego CSIRT sektorowego, który jest właściwy dla dotkniętych usług?

Wystarczy jedno zgłoszenie w systemie S46. CSIRT sektorowe mają obowiązek wzajemnego poinformowania się o incydencie

6.18. Czy istnieją przepisy unijne określające progi incydentu poważnego dla niektórych podmiotów kluczowych i podmiotów ważnych?

Tak. Zostały one określone w *Rozporządzeniu wykonawczym Komisji (UE) 2024/2690 odniesieniu do:*

- *dostawców usług DNS,*
- *rejestrów nazw TLD,*
- *dostawców usług chmurowych,*
- *dostawców usług ośrodka przetwarzania danych,*
- *dostawców sieci dostarczania treści,*
- *dostawców usług zarządzanych,*
- *dostawców usług zarządzanych w zakresie bezpieczeństwa,*



- dostawców internetowych platform handlowych,
- wyszukiwarek internetowych
- platform usług sieci społecznościowych
- dostawców usług zaufania

<https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32024R2690>.

6.19. Gdzie będą określone progi incydentu poważnego?

Progi uznania incydentu za incydent poważny zostaną określone w drodze rozporządzenia przez Radę Ministrów. Przy czym w tym rozporządzeniu nie będą określone progi incydentów dla podmiotów, dla których progi te ustaliła Komisja Europejska w bezpośrednio stosownym akcie wykonawczym wydanym na podstawie art. 23 ust. 11 dyrektywy NIS 2. Prawo krajowe nie może wkraczać w kwestie uregulowane bezpośrednio stosownym akcie prawa unijnego.

6.20. Niektóre dane wymagane przez ustawę przy zgłaszaniu incydentu stanowią tajemnicę przedsiębiorstwa – czy mam je zgłaszać?

Dane przekazywane w zgłoszeniu incydentu mogą stanowić tajemnice prawnie chronione w tym tajemnicę przedsiębiorstwa. Jednocześnie są one potrzebne aby zespół CSIRT był w stanie efektywnie pomóc podmiotowi. Dlatego podmiot kluczowy lub podmiot ważny zgłaszający incydent ma obowiązek przekazać we wczesnym ostrzeżeniu lub w zgłoszeniu incydentu informacje stanowiące tajemnice prawnie chronione. Jednocześnie zespoły CSIRT są obowiązane zachować te informacje w tajemnicy. Informacje te powinny być stosownie oznaczone we wczesnym ostrzeżeniu lub zgłoszeniu incydentu, aby CSIRT wiedział które informacje w szczególny sposób musi chronić.

6.21. W jaki sposób mam zgłosić informacje niejawne, które dotyczą zgłoszenia incydentu poważnego?

Informacje niejawne dotyczące incydentu poważnego są zgłaszane za pomocą systemu teleinformatycznego, który otrzymał akredytację bezpieczeństwa teleinformatycznego lub inną drogą przewidzianą w ustawie o ochronie informacji niejawnych.

6.22. Czy zespoły CSIRT mogą opublikować informację o wystąpieniu incydentu poważnego?

Tak, po konsultacji z podmiotem, w którym wystąpił incydent poważny gdy jest to niezbędne, aby zapobiec wystąpieniu incydentu albo zapewnić obsługę incydentu.



6.23. Jakie sprawozdania związane z incydem poważnym zgłasza podmiot kluczowy lub podmiot ważny?

Podmiot kluczowy lub podmiot ważny obowiązany jest złożyć sprawozdanie okresowe (na wniosek) i sprawozdanie końcowe.

Sprawozdanie okresowe dotyczy działań podjętych w trakcie obsługi incydem poważnego. Jest ono przekazywane na wniosek CSIRT sektorowego.

Sprawozdanie końcowe przekazuje się w ciągu miesiąca od dnia zgłoszenia incydem. Podsumowuje ono obsługę incydem poważnego. Zawiera ono:

- 1) szczegółowy opis incydem poważnego, w tym spowodowane zakłócenia i szkody;
- 2) rodzaj zagrożenia lub przyczynę, która prawdopodobnie była źródłem incydem;
- 3) zastosowane i wdrażane środki ograniczające ryzyko;
- 4) transgraniczne skutki incydem, jeżeli wystąpiły.

Podsumowując sprawozdanie końcowe opisuje co się stało, przyczynę, działania następcze oraz transgraniczne skutki incydem. Dzięki takiemu sprawozdaniu zarówno podmiot kluczowy i podmiot ważny jak i zespół CSIRT są w stanie wyciągnąć wnioski z incydem na przyszłość, ewentualnie wrócić do dokumentacji obsługi konkretnego incydem, jeżeli w przyszłości pojawi się inny podobny incydem. Świadomość tego jak postąpiło się z podobnym incydem pomoże przy obsłudze kolejnych tego typu zdarzeń.

Jeżeli jednak obsługa incydem poważnego nie zakończyła się w terminie miesiąca podmiot zgłaszający incydem poważny przesyła **sprawozdanie z postępu obsługi incydem**, a sprawozdanie końcowe w terminie miesiąca od zakończenia obsługi tego incydem.



7. System S46

7.1. Czym jest system S46?

System S46 Cyber Hub to kluczowa aplikacja stanowiąca fundament Krajowego Systemu Cyberbezpieczeństwa (KSC). Jest to rozwiązanie rozwijane przez NASK-PIB na zlecenie Ministra Cyfryzacji, które zostało oficjalnie uruchomione 1 stycznia 2021 r. System jest stale rozwijany, aby sprostać nowym wymogom prawnym określonym w nowelizacji ustawy o KSC wdrażającej dyrektywę NIS2.

7.2. Do czego służy system S46?

Głównym zadaniem systemu jest pełnienie roli scentralizowanego hubu, który umożliwi podmiotom KSC (podmioty kluczowe i podmioty ważne) realizację ustawowych obowiązków oraz budowanie wspólnej odporności cyfrowej. Jego funkcjonalność opiera się na kilku kluczowych obszarach:

- **System „jednego okienka” do obsługi incydentów:** Platforma pozwala na zgłaszanie incydentów w jednym miejscu, skąd informacja trafia do właściwego CSIRT poziomu krajowego (GOV, MON lub NASK) oraz docelowo będzie trafiać do odpowiedniego CSIRT sektorowego. Eliminuje to konieczność wielokrotnego raportowania tego samego zdarzenia.
- **Budowanie świadomości sytuacyjnej:** S46 agreguje i koreluje dane o podatnościach oraz incydentach z wielu różnych źródeł. Pozwala to Pełnomocnikowi Rządu ds. Cyberbezpieczeństwa na uzyskanie unikalnego, zagregowanego obrazu stanu cyberbezpieczeństwa państwa, a co najważniejsze wesprze podmioty w ochronie przed cyberzagrożeniami.
- **Wymiana informacji i ostrzeżenie:** System służy do dystrybucji ostrzeżeń o zagrożeniach, publikowania analiz merytorycznych oraz przekazywania rekomendacji technicznych.
- **Nowoczesne zarządzanie ryzykiem:** Docelowo S46 umożliwi użytkownikom monitorowanie własnej infrastruktury – po wprowadzeniu informacji o posiadanych rozwiązaniach, system będzie automatycznie generował alerty w przypadku wykrycia specyficznych podatności.
- **Zgłoszenia naruszenia ochrony danych:** Za pośrednictwem S46 możliwe będzie również dokonywanie zgłoszeń naruszeń ochrony danych osobowych bezpośrednio do Prezesa Urzędu Ochrony Danych Osobowych.



7.3. W jaki sposób zarejestrować się w systemie S46?

Aby korzystać z systemu, najpierw należy uzyskać do niego dostęp. W tym celu należy wypełnić oświadczenie o dołączeniu do systemu i przekazać je za pośrednictwem formularza kontaktowego.

Instrukcja, oświadczenie oraz formularz kontaktowy znajdują się pod adresem: <https://www.gov.pl/web/system-s46/uzyskaj-dostep>.

7.4. W jaki sposób podmioty uwierzytelniają się w systemie S46?

Uwierzytelnienie następuje za pomocą Węzła Krajowego – dostępne są następujące sposoby uwierzytelnienia:

- bankowość elektroniczną,
- profil zaufany,
- aplikację mObywatel,
- e-dowód,
- certyfikat kwalifikowany.

7.5. Jakie są minimalne wymagania techniczne i funkcjonalne korzystania z systemu teleinformatycznego S46?

Korzystanie z Systemu S46 przez Internet wymaga:

1. Korzystania ze stacji roboczej chronionej przed dostępem osób nieupoważnionych, wyposażonej w:
 - ochronę antywirusową,
 - ochronę antymalware.
2. Korzystania z przeglądarki internetowej wykorzystującej silnik Chromium (np. Chrome, Opera, Brave) w aktualnej wersji.

Stabilnego łącza internetowego o minimalnej przepustowości 10 Mb/s.

7.6. Czy podmiot publiczny wpisany z urzędu do wykazu podmiotów kluczowych lub ważnych nadal samodzielnie musi rejestrować się w systemie S46? [NOWE – aktualizacja czerwiec 2026 r.]

Podmiot publiczny musi samodzielnie zarejestrować się w systemie S46 w momencie, kiedy otrzyma informacje o wpisaniu do Wykazu KSC. Może to uczynić nawet jeżeli jeszcze nie uzupełnił wszystkich informacji wynikających z wezwania do uzupełnienia danych w wykazie.



8. Wymiana informacji z zakresu cyberbezpieczeństwa

8.1. Kto może wymieniać się informacjami z zakresu cyberbezpieczeństwa?

Informacjami z zakresu cyberbezpieczeństwa mogą wymieniać się:

- podmioty kluczowe,
- podmioty ważne,
- CSIRT MON,
- CSIRT NASK,
- CSIRT GOV,
- CSIRT sektorowy,
- dostawcy sprzętu lub oprogramowania dla tych podmiotów,
- organizacje społeczne zrzeszające podmioty kluczowe lub podmioty ważne.

8.2. Jakie informacje z zakresu cyberbezpieczeństwa mogą wymieniać między sobą podmioty kluczowe i podmioty ważne?

Dopuszczalna wymiana informacji w zakresie cyberbezpieczeństwa	
Rodzaj informacji	Opis informacji
<i>Cyberzagrożenia</i>	wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób
<i>potencjalnych zdarzeniach dla cyberbezpieczeństwa</i>	zdarzenie, które mogło mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych jednak nie wystąpiło lub, któremu udało się zapobiec
<i>Podatność</i>	właściwości produktu ICT lub usługi ICT, która mogą być wykorzystane przez cyberzagrożenie
<i>Techniki</i>	w tym kontekście - szczegółowy opis zachowania „actor” w kontekście jego



	taktyki – por. NIST-SP-800-150 https://csrc.nist.gov/pubs/sp/800/150/final
<i>Procedury</i>	drobiazgowy opis działania aktora w kontekście jego techniki – por. NIST-SP-800-150
<i>oznaki naruszenia integralności systemu informacyjnego</i>	ang. indicators of compromise - mogą to być artefakty lub zdarzenia wskazujące na naruszenie integralności systemu – por. NIST-SP-800-150
<i>wrogie taktyki</i>	generalny opis działania <i>actora</i> – por. NIST-SP-800-150
<i>grupy przestępcze</i>	grupy sponsorowane przez obce państwa działające agresywnie w cyberprzestrzeni grupy typu <i>Private Sector Offensive Actors</i> typowe grupy cyberprzestępców hacktywiści
<i>ostrzeżenia dotyczące cyberbezpieczeństwa</i>	porady, biuletyny, informacje o podatnościach, exploitach itd. przykładowo alerty amerykańskiej agencji CISA
<i>zalecenia dotyczące konfiguracji narzędzi bezpieczeństwa</i>	informacje o ustawieniu i skonfigurowaniu narzędzi służących automatycznemu zbieraniu, wymianie analizie i wykorzystaniu informacji o cyberzagrożeniach

8.3. Kiedy wymiana informacji o cyberbezpieczeństwie jest dopuszczalna?

Wymiana informacji, ostrzeżeń i zaleceń jest dopuszczalna, jeżeli:

- 1) ma na celu zapobieganie incydom, ich wykrywanie, reagowanie na nie, przywracanie normalnego działania po incydomach lub łagodzenie ich skutków lub
- 2) zwiększa poziom cyberbezpieczeństwa.



8.4. W jaki sposób podmioty kluczowe i podmioty ważne wymieniają się informacjami z zakresu cyberbezpieczeństwa?

Wymiana ta odbywa się za pomocą systemu S46, systemów teleinformatycznych zapewnianych przez organy właściwe do spraw cyberbezpieczeństwa lub w drodze porozumień między podmiotami kluczowymi, podmiotami ważnymi CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowy, dostawcami sprzętu lub oprogramowania dla tych podmiotów lub organizacjami społecznymi zrzeszającymi podmioty kluczowe lub podmioty ważne.

8.5. Czy w ustawie uregulowano działalność podmiotów typu Information Sharing and Analysis Center (ISAC)?

W Polsce coraz częściej pojawiają się Information Sharing and Analysis Center – ISAC. Wprowadzono możliwość zawierania porozumień pomiędzy podmiotami kluczowymi i podmiotami ważnymi w sprawie wymiany informacji o cyberbezpieczeństwie. W tych porozumieniach należy ustalić sposób wymiany informacji i zachowania informacji w poufności pomiędzy stronami porozumienia. Te porozumienia spełniają funkcję ISAC. Podmiot kluczowy lub podmiot ważny zgłasza w wykazie podmiotów kluczowych lub podmiotów ważnych informację o zawarciu takiego porozumienia.



9. Audyty bezpieczeństwa systemu informacyjnego

9.1. Kto musi przeprowadzić cykliczny audyt?

Podmioty kluczowe mają obowiązek zapewnić przeprowadzenie, na własny koszt, co najmniej raz na 3 lata, audytu bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi. Musi on być przeprowadzony przez podmiot posiadający odpowiednią akredytację, dwóch audytorów legitymujących się odpowiednimi certyfikatami i doświadczeniem lub przez CSIRT sektorowy. Audyty na zgodność należy rozumieć jako przeprowadzane na zgodność z przepisami ustawy. **Audyt może być audytem wewnętrznym lub zewnętrznym.** Audyt powinien dotyczyć całego systemu informacyjnego wykorzystywanego przez dany podmiot, a nie jedynie jego części związanych z konkretną usługą. Wynika to z tego, że dzięki powiązaniom między poszczególnymi systemami można poprzez inne elementy systemu wpłynąć na kluczową działalność danego podmiotu.

Podmioty ważne nie mają obowiązku przeprowadzenia cyklicznego audytu.

9.2. Kto może przeprowadzić audyt w podmiocie?

Audyt może być przeprowadzony przez:

- 1) jednostkę oceniającą zgodność, akredytowaną w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych;
- 2) co najmniej dwóch audytorów posiadających:
 - a) certyfikaty określone w rozporządzeniu Ministra Cyfryzacji lub
 - b) co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, lub
 - c) co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymujących się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych;
- 3) CSIRT sektorowy.

9.3. Jakie certyfikaty uprawniają do przeprowadzenia audytu?

Następujące certyfikaty uprawniają do przeprowadzenia audytu:

- 1 Certified Internal Auditor (CIA);



- 2 Certified Information System Auditor (CISA);
- 3 Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną, w zakresie certyfikacji osób;
- 4 Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;
- 5 Certified Information Security Manager (CISM);
- 6 Certified in Risk and Information Systems Control (CRISC);
- 7 Certified in the Governance of Enterprise IT (CGEIT);
- 8 Certified Information Systems Security Professional (CISSP);
- 9 Systems Security Certified Practitioner (SSCP);
- 10 Certified Reliability Professional;
- 11 Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

9.4. Czy audyt może być przeprowadzony przez osobę, która wcześniej w tym samym podmiocie realizowała zadania z zakresu SZBI?

Nie, audyt nie może być przeprowadzony przez osobę, która w tym samym podmiocie realizuje lub wcześniej realizowała zadania z zakresu SZBI oraz zgłaszania incydentów przez rok przed rozpoczęciem audytu.

9.5. Kiedy dotychczasowi operatorzy usług kluczowych mają obowiązek przeprowadzić audyt?

Dotychczasowi operatorzy usług kluczowych przeprowadzają audyt bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi zgodnie z zasadą określoną w art. 15 ust. 1, tj. co najmniej raz na 3 lata, licząc od dnia sporządzenia i podpisania raportu z ostatniego audytu.

Jednocześnie, zgodnie z przepisem przejściowym (art. 25), co do operatorów usług kluczowych, którzy wykonali audyt przed wejściem w życie nowelizacji ustawy, nie stosuje się obowiązku przeprowadzenia pierwszego audytu w terminie 24 miesięcy, o którym mowa w art. 16 pkt 2.

Oznacza to, że w ich przypadku zachowany zostaje dotychczasowy cykl audytowy. Przykładowo, jeżeli operator przeprowadził audyt w maju 2024 r., kolejny audyt powinien zostać przeprowadzony najpóźniej w maju 2027 r.



Jeżeli zgodnie z cyklem audytowym audyt wypada w trakcie okresu dostosowawczego to audyt obejmie realizację wymogów dotychczasowego systemu zarządzania bezpieczeństwem informacji – sprzed nowelizacji.

9.6. Kiedy dotychczasowi operatorzy usług kluczowych przeprowadzają pierwszy audyt bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej? [NOWE – aktualizacja czerwiec 2026 r.]

Dotychczasowi operatorzy usług kluczowych przeprowadzają pierwszy audyt w terminie 3 lat od dnia sporządzenia i podpisania ostatniego raportu z audytu.



10. Szczególne działania na rzecz zapewnienia cyberbezpieczeństwa

10.1. Czym jest polecenie zabezpieczające? Czy Minister Cyfryzacji będzie cenzurował internet w Polsce lub nawet wyłączy Internet w Polsce za pomocą polecenia zabezpieczającego?

Wprowadzenie do polskiego porządku prawnego polecenia zabezpieczającego jest konieczne dla zapewnienia bezpieczeństwa narodowego, ponieważ cyberataki są coraz częstsze i coraz bardziej niebezpieczne. Należy podkreślić, że są one dokonywane zarówno przez zwykłych przestępców jak i sprawców powiązanych z określonymi państwami, którzy dysponują znaczną wiedzą i zasobami. Państwo musi mieć odpowiednie prawne środki reakcji na incydenty krytyczne, aby bronić swojego społeczeństwa i gospodarki przed skutkami tych incydentów.

Polecenie zabezpieczające będzie skutecznym środkiem przeciwdziałania incydentom krytycznym. Będzie miało charakter proporcjonalny do cyberzagrożenia. Wpłynie ono wyłącznie w niezbędnym zakresie na swobodę działalności gospodarczej, aby uchronić kluczowe podmioty przed skutkami incydentu krytycznego, który jak wspomniano wyżej, w bardzo poważny sposób zagraża obywatelom, gospodarce, czy szerzej bezpieczeństwu narodowemu. Katalog zachowań możliwych do nałożenia w drodze polecenia zabezpieczającego zostanie ustawowo ograniczony. Ponadto minister będzie zobligowany wybrać zachowanie adekwatne do cyberzagrożenia, jakie stwarza incydent krytyczny. Przeciwdziałania to arbitralności władzy publicznej.

Polecenie zabezpieczające nie cenzuruje ani nie wyłącza internetu w Polsce. Umożliwia natomiast zablokowanie konkretnego ruchu sieciowego, który został zidentyfikowany przez zespoły CSIRT jako przyczyna incydentu krytycznego. Chodzi o przeciwdziałanie atakom typu DDoS.

10.2. Kto może być adresatem polecenia zabezpieczającego?

Adresatem polecenia zabezpieczającego mogą być podmioty kluczowe i podmioty ważne określone rodzajowo oraz podmioty finansowe.

10.3. Jakie działania mogą być nakazane w ramach polecenia zabezpieczającego?

W ramach polecenia zabezpieczającego mogą być nakazane podmiotom kluczowym i podmiotom ważnym następujące działania:



- 1) nakaz przeprowadzenia szacowania ryzyka związanego ze stosowaniem określonego produktu ICT, usługi ICT lub procesu ICT i wprowadzenie środków ochrony proporcjonalnych do zidentyfikowanych ryzyk;
- 2) nakaz przeglądu planów ciągłości działania, planów awaryjnych i planów odtworzenia działalności pod kątem ryzyka wystąpienia incydentu krytycznego związanego z daną podatnością;
- 3) nakaz zastosowania określonej poprawki bezpieczeństwa w produkcie ICT lub usłudze ICT posiadającym daną podatność;
- 4) nakaz szczególnej konfiguracji produktu ICT lub usługi ICT, zabezpieczającej przed wykorzystaniem określonej podatności;
- 5) nakaz wzmożonego monitorowania zachowania systemu informacyjnego;
- 6) zakaz korzystania z określonego produktu ICT lub usługi ICT, które posiada podatność, która przyczyniła się do zaistnienia incydentu krytycznego;
- 7) nakaz wprowadzenia ograniczenia ruchu sieciowego przychodzącego do infrastruktury podmiotu kluczowego lub podmiotu ważnego, który skutkując zakłóceniem usług świadczonych przez ten podmiot został sklasyfikowany przez CSIRT MON, CSIRT NASK lub CSIRT GOV jako przyczyna trwającego incydentu krytycznego;
- 8) nakaz wstrzymania dystrybucji lub zakaz instalacji określonej wersji oprogramowania;
- 9) nakaz zabezpieczenia określonych informacji, w tym dzienników systemowych;
- 10) nakaz wytworzenia obrazów stanu określonych urządzeń zainfekowanych złośliwym oprogramowaniem

10.4. Na czym polega ocena bezpieczeństwa?

Ocena bezpieczeństwa polega na przeprowadzeniu testów bezpieczeństwa systemu informacyjnego wykorzystywanego przez podmiot krajowego systemu cyberbezpieczeństwa w celu identyfikacji podatności tego systemu. Wyboru rodzaju testów bezpieczeństwa dokonuje się adekwatnie do systemu informacyjnego i świadczonej usługi z uwzględnieniem specyfiki sektora lub podsektora.

10.5. Kto może przeprowadzać ocenę bezpieczeństwa?

Ocenę bezpieczeństwa może przeprowadzić CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowy. Ocena odbywa się za zgodą podmiotu krajowego systemu cyberbezpieczeństwa wyrażoną w formie pisemnej lub formie elektronicznej pod rygorem nieważności albo na zlecenie organu właściwego do spraw cyberbezpieczeństwa. Zlecenie może dotyczyć tylko podmiotów kluczowych.



10.6. Jakie są gwarancje dla podmiotu krajowego systemu cyberbezpieczeństwa przy przeprowadzaniu oceny bezpieczeństwa?

Celem oceny bezpieczeństwa jest pomoc w identyfikacji podatności. Ma ona charakter prewencyjny. Jednakże prowadzenie tej oceny nie może zaszkodzić systemowi informacyjnemu, a szerzej podmiotowi, który korzysta z tego systemu i świadczy usługi dla swoich klientów. Dlatego wprowadza się zasadę, zgodnie z którą czynności przeprowadzane w ramach oceny bezpieczeństwa powinny w jak najmniejszym stopniu zakłócać funkcjonowanie tego systemu lub ograniczać jego dostępność. Tym bardziej nie jest dopuszczalne, aby działania te doprowadziły do nieodwracalnego zniszczenia danych w systemie poddanym ocenie. Przepis ten ma stanowić ogólną zasadę dla osób przeprowadzających ocenę bezpieczeństwa i stanowi gwarancję dla podmiotu krajowego systemu cyberbezpieczeństwa, wobec którego prowadzona jest ocena bezpieczeństwa. Dodatkowo wprowadzono katalog sytuacji w których ocena bezpieczeństwa nie może być przeprowadzona, a rozpoczętą przerywa się. Są to sytuacje, gdy:

- 1) podmiot krajowego systemu cyberbezpieczeństwa nie posiada kopii bezpieczeństwa badanego systemu;
- 2) istnieje zagrożenie nieodwracalnego zniszczenia danych przetwarzanych w systemie;
- 3) czas potrzebny na przywrócenie systemu z kopii bezpieczeństwa może w istotny sposób zakłócić pracę systemu lub ograniczyć jego dostępność;
- 4) czynności podejmowane podczas oceny bezpieczeństwa mogą doprowadzić do uszkodzenia produktów ICT wchodzących w skład tego systemu oraz innych systemów informacyjnych podmiotu kluczowego;
- 5) istnieje zagrożenie ograniczenia dostępności usług świadczonych przez podmiot krajowego systemu cyberbezpieczeństwa.

Ponadto informacje uzyskane w wyniku oceny stanowią tajemnicę prawnie chronioną. Zespół CSIRT nie będzie mógł wykorzystać ich do realizacji innych zadań ustawowych. Informacje te będą podlegały niezwłocznemu, komisijnemu i protokolarnemu zniszczeniu. Zniszczeniu nie podlegają informacje o czynnościach przeprowadzanych w ramach oceny bezpieczeństwa oraz o wykrytych podatnościach systemu informacyjnego.

10.7. Czy Pełnomocnik Rządu do spraw Cyberbezpieczeństwa może wydawać rekomendacje?

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa wydaje dwa rodzaje rekomendacji:



1. **Rekomendacje dotyczące stosowania produktów ICT lub usług ICT, w szczególności w zakresie wpływu na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa.**

Rekomendacje te wydaje się po uzyskaniu opinii Kolegium do Spraw Cyberbezpieczeństwa lub z urzędu po uzyskaniu przez Pełnomocnika informacji o cyberzagrożeniu, która uprawdopodobni możliwość wystąpienia incydentu krytycznego.

Lista dotychczas wydanych rekomendacji jest dostępna pod adresem: https://dane.gov.pl/pl/dataset/20102/resource/897674,wykaz-rekomendacji-penomocnika-rzadu-do-spraw-cyberbezpieczenstwa/table?page=1&per_page=20&q=&sort=

2. **Nowe przepisy umożliwią wydawanie przez Pełnomocnika rekomendacji określających środki techniczne i organizacyjne stosowane w celu zwiększenia bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa.**

Ten dokument będzie publikowany na stronie podmiotowej Pełnomocnika w BIP. W takiej formie będą mogły być wydawane Narodowe Standardy Cyberbezpieczeństwa, a także inne zbiory dobrych praktyk. Podkreślić należy, że rekomendacje będą formalnie niewiążące. Decyzja o uwzględnieniu tych środków będzie należała wyłącznie do podmiotów krajowego systemu cyberbezpieczeństwa. Dzięki rekomendacjom uzyskają one fachową wiedzę, dzięki czemu będą mogły wprowadzić adekwatne do oszacowanego ryzyka zabezpieczenia.

10.8. Czy Minister Cyfryzacji zaraz po wejściu w życie ustawy o KSC opublikuje listę Dostawców Wysokiego Ryzyka?

Nie. Samo wejście w życie przepisów nie oznacza, że muszą one zostać wykorzystane.

Procedura uznania dostawcy za dostawcę wysokiego ryzyka, która została zawarta w ustawie o KSC, daje możliwość eliminacji niebezpiecznego sprzętu lub usług z kluczowych dla funkcjonowania państwa systemów informacyjnych. Ponadto, nawet w przypadku zastosowania tej procedury, decyzja nie będzie dotyczyła całego asortymentu danego podmiotu, a jedynie typów sprzętu lub oprogramowania wskazanych w samej decyzji.



11. Nadzór nad podmiotami kluczowymi i ważnymi

11.1. Kim są organy właściwe do spraw cyberbezpieczeństwa?

Organy właściwe do spraw cyberbezpieczeństwa sprawują nadzór nad podmiotami kluczowymi i podmiotami ważnymi.

Sektor wraz z organem właściwym:

Energia – Minister Energii

Transport – Minister Infrastruktury

Bankowość i infrastruktura rynków finansowych – Komisja Nadzoru Finansowego

Ochrona zdrowia – Minister Zdrowia; Minister Obrony Narodowej

Zaopatrzenie w wodę pitną i jej dystrybucja – Minister Infrastruktury

Zbiorowe odprowadzanie ścieków – Minister Infrastruktury

Infrastruktura cyfrowa

- ✓ Infrastruktura cyfrowa z wyłączeniem komunikacji elektronicznej – Minister Cyfryzacji, Minister Obrony Narodowej
- ✓ Komunikacja elektroniczna – Prezes Urzędu Komunikacji Elektronicznej

Zarządzanie usługami ICT – Minister Cyfryzacji

Przestrzeń kosmiczna – Minister Finansów i Gospodarki

Podmioty publiczne – Minister Cyfryzacji, Minister Finansów i Gospodarki, Minister Obrony Narodowej

Usługi pocztowe – Prezes Urzędu Komunikacji Elektronicznej

Inwestycje energetyki jądrowej – Minister Energii

Gospodarowanie odpadami – Minister Klimatu i Środowiska

Produkcja, wytwarzanie i dystrybucja chemikaliów – Minister Finansów i Gospodarki

Produkcja, przetwarzanie i dystrybucja żywności – Minister Rolnictwa i Rozwoju Wsi

Produkcja

- ✓ Produkcja wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro – Minister Zdrowia



- ✓ Produkcja komputerów, wyrobów elektronicznych i optycznych – Minister Finansów i Gospodarki
- ✓ Produkcja urządzeń elektrycznych – Minister Finansów i Gospodarki
- ✓ Produkcja maszyn i urządzeń, gdzie indziej niesklasyfikowana – Minister Finansów i Gospodarki
- ✓ Produkcja pojazdów samochodowych, przyczep i naczep – Minister Finansów i Gospodarki
- ✓ Produkcja pozostałego sprzętu transportowego – Minister Finansów i Gospodarki

Dostawcy usług cyfrowych – Minister Cyfryzacji

Badania naukowe – Minister Nauki, Minister Obrony Narodowej

Podmioty publiczne – Minister Cyfryzacji

11.2. Co w przypadku gdy ten sam podmiot będzie podlegał pod kilka organów właściwych do spraw cyberbezpieczeństwa?

Organy właściwe do spraw cyberbezpieczeństwa będą mogły wspólnie sprawować nadzór, w tym wspólnie prowadzić kontrole, nad podmiotami kluczowymi lub podmiotami ważnymi. Ponadto będą mogły przyjąć wspólną metodykę nadzoru nad podmiotami, które podlegają pod kilka organów. Jednym z elementów tej metodyki powinno być przyjęcie mechanizmu, który przeciwdziałałby wydawaniu wzajemnie sprzecznych zaleceń pokontrolnych wobec tego samego podmiotu.

11.3. Kto jest organem właściwym do spraw cyberbezpieczeństwa dla podmiotów publicznych?

Co do zasady organem właściwym do spraw cyberbezpieczeństwa dla podmiotów publicznych jest Minister Cyfryzacji.

Wyjątki:

Dla podmiotów podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych oraz dla urzędu obsługującego tego Ministra – Minister Obrony Narodowej.

Organem właściwym do spraw cyberbezpieczeństwa w sektorze podmiotów publicznych dla jednostek organizacyjnych podległych ministrowi właściwemu do spraw finansów publicznych lub przez niego nadzorowanych, urzędu obsługującego tego ministra oraz spółki Aplikacje Krytyczne, jest minister właściwy do spraw finansów publicznych.



Dla podmiotów publicznych, który jest wymieniony w innym sektorze niż sektor podmiotów publicznych organem właściwym do spraw cyberbezpieczeństwa jest organ właściwy dla danego sektora

przykładem jest Rządowa Agencja Rezerw Strategicznych dla której organem właściwym będzie Minister Energii. Wyjątek ten nie dotyczy samorządowych podmiotów publicznych.

11.4. Jakie są środki nadzoru nad podmiotami kluczowymi?

Spośród czynności nadzorczych warto wskazać:

- podejmowanie kontroli przez organ właściwy do spraw cyberbezpieczeństwa
- nakazanie audytu ad hoc
- przeprowadzenie oceny bezpieczeństwa systemu informacyjnego
- żądanie udzielenia informacji, danych i dokumentów od podmiotu
- wniosek o udzielenie dowodów realizacji wymogów SZBI

Organ właściwy do spraw cyberbezpieczeństwa może wystąpić do podmiotu z ostrzeżeniem, w którym wskaże czynności które należy podjąć w celu dostosowania się do wymogów ustawy.

Organ właściwy do spraw cyberbezpieczeństwa może nakazać środki egzekwujące obowiązki ustawowe wobec podmiotu kluczowego:

- Nakaz:
 - podjęcia określonych czynności dotyczących obsługi incydentu
 - zaniechania naruszania przepisów ustawy
 - zapewnienia zgodności SZBI z wymogami ustawy
 - zgłoszenia incydentu poważnego
 - poinformowania użytkowników usług o cyberzagrożeniu oraz o możliwych środkach które należy podjąć w reakcji na to zagrożenie
 - wdrożenia zaleceń wydanych w wyniku audytu bezpieczeństwa systemu informacyjnego
 - Podanie do wiadomości publicznej informacji o naruszeniu przepisów ustawy lub o incydencie poważnym w podmiocie
- Wyznaczyć urzędnika monitorującego działalność danego podmiotu, nie dłużej niż przez miesiąc.

Środkiem ostatecznym jest wniosek o zawieszenie, ograniczenie lub cofnięcie zezwolenia czy koncesji na daną działalność.

11.5. Jakie są środki nadzoru nad podmiotami ważnymi?

Spośród czynności nadzorczych warto wskazać:



- podejmowanie kontroli przez organ właściwy do spraw cyberbezpieczeństwa
- nakazanie audytu ad hoc
- przeprowadzenie oceny bezpieczeństwa systemu informacyjnego
- żądanie udzielenia informacji, danych i dokumentów od podmiotu
- wniosek o udzielenie dowodów realizacji wymogów SZBI.

Organ właściwy do spraw cyberbezpieczeństwa może wystąpić do podmiotu z ostrzeżeniem, w którym wskaże czynności które należy podjąć w celu dostosowania się do wymogów ustawy.

Organ właściwy do spraw cyberbezpieczeństwa może nakazać środki egzekwujące obowiązki ustawowe wobec podmiotu ważnego:

- Nakaz:
 - podjęcia określonych czynności dotyczących obsługi incydentu
 - zaniechania naruszania przepisów ustawy
 - zapewnienia zgodności SZBI z wymogami ustawy
 - zgłoszenia incydentu poważnego
 - poinformowania użytkowników usług o cyberzagrożeniu oraz o możliwych środkach które należy podjąć w reakcji na to zagrożenie
 - wdrożenia zaleceń wydanych w wyniku audytu bezpieczeństwa systemu informacyjnego
 - Podanie do wiadomości publicznej informacji o naruszeniu przepisów ustawy lub o incydencie poważnym w podmiocie.

11.6. Czym są dowody realizacji wymogów SZBI?

Organ właściwy do spraw cyberbezpieczeństwa może prosić podmiot kluczowy lub podmiot ważny o przedstawienie dowodów realizacji systemu zarządzania bezpieczeństwem informacji. Mogą być dokumenty np. procedury, polityki, upoważnienia, zakresy obowiązków ale również relacje personelu. Wymagane jest udowodnienie stosowania przepisów ustawy a nie przedstawienie formalnie poprawnych dokumentów.



12. Kary pieniężne

12.1. Czy kary pieniężne będą nakładane od razu po wejściu w życie ustawy?

Nie, kary pieniężne będą nakładane dopiero po 2 latach od wejścia w życie ustawy, tj. po 3.04.2028. Wyjątkiem jest kara ekstraordynaryjna.

12.2. Kto nakłada kary pieniężne?

Kary pieniężne są nakładane na podmioty ważne i kluczowe przez organ właściwy do sprawy cyberbezpieczeństwa w danym sektorze. Dla przykładu kary pieniężne dla sektora usług pocztowych będzie nakładał Prezes Urzędu Komunikacji Elektronicznej.

W szczególnych przypadkach kary pieniężne będzie mógł również nakładać Minister właściwy do spraw informatyzacji. Karze takiej podlega:

- podmiot świadczący usługi rejestracji nazw domen, który nie wykonuje obowiązków, o których mowa w art. 16b i art. 16c;
- rejestr nazw domen najwyższego poziomu (TLD), który nie wykonuje obowiązków, o których mowa w art. 16b i art. 16c;
- producent lub dostawca, który nie przekazał dokumentacji badanego produktu ICT lub usługi ICT na wezwanie CSIRT MON, CSIRT NASK lub CSIRT GOV;

Natomiast w przypadku podmiotu finansowego w rozumieniu rozporządzenia 2022/2554 kary nakłada organ w rozumieniu tego rozporządzenia.

12.3. Jakie kary może nałożyć organ właściwy do spraw cyberbezpieczeństwa?

Kary są jednym ze środków nadzorczych, niezależnym od pozostałych. Środki nadzorcze mają charakter prewencyjny oraz następczy. Decyzja o wydaniu kary pieniężnej poprzedzona jest ostrzeżeniem i informowaniem o wstępnych ustaleniach.

Kary pieniężne dzielą się na fakultatywne, obligatoryjne, okresowe oraz karę ekstraordynaryjną – karę do 100 mln zł.

12.4. Jak wysokie mogą być kary pieniężne?

Dla podmiotu kluczowego	Dla podmiotu ważnego
10 mln euro lub	7 mln euro lub



2% przychodów osiągniętych przez podmiot kluczowy z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary, przy czym zastosowanie ma kwota wyższa	1,4% przychodów osiągniętych przez podmiot ważny z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary
Nie mniejsza niż 20 000 zł	Nie mniejsza niż 15 000 zł

Wysokość kar dla kierownika podmiotu	
Dla podmiotu publicznego	Dla podmiotu prywatnego
W kwocie nie większej niż 100 % otrzymywanego przez ukaranego wynagrodzenia	W kwocie nie większej niż 300 % otrzymywanego przez ukaranego wynagrodzenia

12.5. Czym jest kara okresowa?

W celu przymuszenia podmiotu do wykonania nałożonych na niego obowiązków, organ właściwy do spraw cyberbezpieczeństwa może nałożyć na ten podmiot, w drodze decyzji, okresową karę pieniężną.

Nakładana jest za każdy dzień opóźnienia wykonania decyzji, w wysokości od 500 zł do 100 000 zł.

12.6. Czym jest kara ekstraordynaryjna?

Jest to specjalna kara stosowana tylko przy poważnych naruszeniach. Kara ta może wynosić maksymalnie 100 mln zł, a przestankami do jej nałożenia są:

- ✓ bezpośrednio i poważne cyberzagrożenie dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi,
- ✓ oraz zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług .

12.7. Czy organ właściwy do spraw cyberbezpieczeństwa ostrzega podmiot przed nałożeniem kary?

Tak, w przypadku uzasadnionego podejrzenia, że działania lub zaniechania podmiotu kluczowego lub podmiotu ważnego mogą naruszać przepisy ustawy, organ właściwy do spraw cyberbezpieczeństwa kieruje do tego podmiotu pismo w formie elektronicznej z ostrzeżeniem, w którym wskazuje czynności, jakie należy podjąć w celu zapobieżenia lub zaprzestania naruszania przepisów ustawy wraz z terminem na ich wykonanie.



12.8. Czy organ właściwy do spraw cyberbezpieczeństwa informuje o wstępnych ustaleniach?

Tak, organ właściwy do spraw cyberbezpieczeństwa przed zastosowaniem środków oraz przed nałożeniem kary pieniężnej, informuje podmiot o wstępnych ustaleniach, które mogą prowadzić do wydania decyzji. Informacja zawiera szczegółowe uzasadnienie potwierdzające zasadność zamiaru zastosowania środków lub nałożenia kary pieniężnej.

Organ właściwy do spraw cyberbezpieczeństwa może odstąpić od poinformowania o wstępnych ustaleniach w przypadku, gdy utrudniłoby to natychmiastowe działanie w celu zapobieżenia incydom, reakcji na nie lub mogłoby mieć niekorzystny wpływ na bezpieczeństwo państwa lub porządek publiczny.

Jednocześnie podmiot może w terminie 7 dni, przedstawić swoje stanowisko, do którego organ właściwy do spraw cyberbezpieczeństwa musi się ustosunkować, uwzględniając stanowisko lub odrzucając wraz ze stosownym uzasadnieniem.

12.9. Jakie są przesłanki nałożenia kary pieniężnej?

Karze pieniężnej podlega podmiot kluczowy lub podmiot ważny, który:

- Nie wpisał się do wykazu w terminie,
- nie uzupełnił brakujących danych w wykazie,
- nie dokonał korekty danych pomimo wezwania,
- wprowadził niezgodne ze stanem faktycznym dane do wykazu,
- nie przeprowadza systematycznego szacowania ryzyka wystąpienia incydentu i nie zarządza tym ryzykiem,
- nie wdrożył SZBI,
- nie wyznaczył osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami KSC,
- nie przeprowadził audytu w terminie,
- uniemożliwia wykonywanie kontroli,
- uniemożliwia lub utrudnia pracę urzędnikowi monitorującemu,
- nie przekazuje na żądanie organu właściwego ds. cyberbezpieczeństwa informacji i dokumentów niezbędnych do wykonywania obowiązków z zakresu nadzoru i kontroli,
- nie wykonał w wyznaczonym terminie zaleceń pokontrolnych,
- w przypadku decyzji (wydanej dostawcy wysokiego ryzyka) nie wycofał na sprzętu lub oprogramowania,
- nie przekazał informacji pomimo wniosku o wycofanych typach produktów ICT, rodzajach usług ICT i konkretnych procesach ICT,
- nie wdrożył w terminie określonym w poleceniu zabezpieczającym określonego zachowania,
- uniemożliwia wykonywanie kontroli,



- uniemożliwia lub utrudnia pracę urzędnikowi monitorującemu,
- nie przekazuje na żądanie organu właściwego ds. cyberbezpieczeństwa informacji i dokumentów niezbędnych do wykonywania obowiązków z zakresu nadzoru i kontroli,
- nie wykonał w wyznaczonym terminie zaleceń pokontrolnych,
- w przypadku decyzji (wydanej dostawcy wysokiego ryzyka) nie wycofał na sprzętu lub oprogramowania,
- nie przekazał informacji pomimo wniosku o wycofanych typach produktów ICT, rodzajach usług ICT i konkretnych procesach ICT,
- nie wdrożył w terminie określonym w poleceniu zabezpieczającym określonego zachowania,
- nie współpracuje podczas obsługi incydentu poważnego lub krytycznego z właściwym CSIRT,
- nie usunął podatności po wezwaniu przez właściwy CSIRT,
- nie powołał wewnętrznej struktury odpowiedzialnej za cyberbezpieczeństwo lub nie zawarł umowy z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa,
- nie korzysta z systemu teleinformatycznego na podstawie porozumienia zawartego z ministrem.

12.10. Jakie są przestanki nałożenia kary pieniężnej na kierownika podmiotu?

Karze pieniężnej może podlegać kierownik podmiotu kluczowego lub podmiotu ważnego, który:

- nie wykonuje co najmniej jednego z obowiązków dotyczących wykazu,
- nie wykonuje co najmniej jednego z obowiązków dotyczących SZBI,
- nie przeszedł raz do roku obowiązkowego szkolenia z zakresu cyberbezpieczeństwa,
- nie dopilnował, aby osoba realizująca zadania z zakresu cyberbezpieczeństwa przed rozpoczęciem ich wykonywania przedstawiła zaświadczenie o niekaralności za przestępstwa przeciwko ochronie informacji,
- nie wyznaczył co najmniej dwóch osób do kontaktu z podmiotami KSC,
- nie zapewnił użytkownikowi możliwości zgłoszenia cyberzagrożenia,
- Nie wykonuje co najmniej jednego z obowiązków dotyczących postępowania z dokumentacją,
- nie wykonuje co najmniej jednego z obowiązków dotyczących obsługi incydentów,
- przekazał sprawozdanie końcowe, niezawierające określonych elementów,
- nie wykonuje obowiązku dotyczącego sprawozdań,
- nie wykonuje obowiązku dotyczącego wewnętrznych struktur,
- nie wykonuje co najmniej jednego z obowiązków dotyczących audytu.



12.11. Jakie są kryteria analizy przed nałożeniem kary pieniężnej?

Głównymi kryteriami analizy przed nałożeniem kary pieniężnej jest waga naruszenia i znaczenie naruszonych przepisów ustawy, czas trwania naruszenia, wcześniejsze poważne naruszenia ze strony danego podmiotu

oraz

wysokość przychodu uzyskanego z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary pieniężnej, gdzie dla podmiotu prywatnego głównym kryterium jest wysokość przychodu, dla podmiotów publicznych możliwości finansowe oparte o m.in. środki budżetowe, a dla kierownika podmiotu jego możliwości finansowe.

12.12. Czy organ właściwy do spraw cyberbezpieczeństwa może odstąpić od nałożenia kary pieniężnej?

Tak, jeżeli waga naruszenia i znaczenie naruszonych przepisów są znikome, a podmiot albo kierownik podmiotu zaprzestał naruszania prawa lub naprawił wyrządzoną szkodę organ może odstąpić od nałożenia kary.

12.13. Czy postępowanie nakładania kary może zostać umorzone?

Co do zasady tak, ale tylko na zasadach określonych w Kodeksie Postępowania Administracyjnego, w szczególności gdy postępowanie stało się bezprzedmiotowe.

12.14. Jakie są elementy poważnego naruszenia?

Elementami poważnego naruszenia jest m.in.:

- powtarzające się naruszenie,
- niezgłoszenie lub nieobsłużenie incydentów poważnych,
- nieusunięcie uchybień zgodnie z wiążącymi nakazami organów właściwych do spraw cyberbezpieczeństwa,
- utrudnianie prowadzenia audytów lub działań monitorujących nakazanych przez organ właściwy do spraw cyberbezpieczeństwa po stwierdzeniu naruszenia,
- dostarczanie nieprawdziwych lub rażąco niedokładnych informacji w odniesieniu do środków zarządzania ryzykiem w cyberbezpieczeństwie lub obowiązków zgłaszania incydentów poważnych.



13. Obowiązki rejestratorów nazw domen [NOWE – aktualizacja czerwiec 2026 r.]

13.1. Czy należy podać swoje dane, aby być abonentem nazwy domeny internetowej? [NOWE – aktualizacja czerwiec 2026 r.]

Zgodnie z art. 16b ustawy o KSC, baza danych dotyczących rejestracji nazw domen zawiera m.in. dane dotyczące abonenta nazwy domeny, takie jak imię i nazwisko lub nazwa, adres poczty elektronicznej, numer telefonu. Oznacza to, że gromadzenie takich danych stanowi obowiązek prawny, a każdy abonent nazwy domeny musi być możliwy do zidentyfikowania. Brak podania takich danych oznacza brak możliwości uzyskania lub utrzymania statusu abonenta nazwy domeny internetowej.

13.2. Jakie dane musi podać abonent nazwy domeny? [NOWE – aktualizacja czerwiec 2026 r.]

Zgodnie z art. 16b ustawy o KSC, baza danych dotyczących rejestracji nazw domen zawiera m.in. dane, które musi podać abonent nazwy domeny, czyli imię i nazwisko lub nazwę, adres poczty elektronicznej, numer telefonu. Rejestry nazw domen najwyższego poziomu (TLD) i podmioty świadczące usługi rejestracji nazw domen mogą gromadzić także inne istotne informacje związane z identyfikacją abonentów nazw domeny, takie jak, np. adresy, numery lub inne oznaczenia identyfikacyjne abonenta nazwy domeny zawarte w rejestrach publicznych (np. KRS, CEiDG).

13.3. Kto gromadzi i przechowuje dane podawane przez abonentów nazw domeny? [NOWE – aktualizacja czerwiec 2026 r.]

Zgodnie z art. 16b ustawy o KSC, dane dotyczące rejestracji nazw domen zbierają i przechowują podmioty świadczące usługi rejestracji nazw domen i rejestry nazw domen najwyższego poziomu (TLD). Podział zadań w tym zakresie kształtuje się według relacji formalnych obowiązujących dla danej domeny najwyższego poziomu (TLD). Może on polegać na tym, że podmioty świadczące usługi rejestracji nazw domen gromadzą dane podane przez abonenta nazw domen i następnie wprowadzają je do bazy rejestru nazw domen najwyższego poziomu (TLD). Podmioty świadczące usługi rejestracji nazw domen to rejestratorzy. Mogą to być także agenci działający w ich imieniu.



13.4. Czy relacje prawne abonentów nazw domeny z rejestrami nazw domen najwyższego poziomu (TLD) i podmiotami świadczącymi usługi rejestracji nazw domen są ustanawiane na podstawie ustawy o KSC? [NOWE – aktualizacja czerwiec 2026 r.]

Ustawa o KSC reguluje funkcjonowanie krajowego systemu cyberbezpieczeństwa oraz związane z tym obowiązki m.in. rejestrów nazw domen najwyższego poziomu (TLD) i podmiotów świadczących usługi rejestracji nazw domen. W pozostałym zakresie relacje prawne abonentów nazw domeny z rejestrami nazw domen najwyższego poziomu (TLD) i podmiotami świadczącymi usługi rejestracji nazw domen nie są regulowane przepisami ustawy o KSC, lecz zawieranyymi pomiędzy tymi podmiotami umowami, regulaminami, itp.

13.5. Gdzie będą publikowane dane dotyczące rejestracji nazwy domeny? [NOWE – aktualizacja czerwiec 2026 r.]

Dane dotyczące rejestracji nazwy domeny muszą być publikowane na stronie internetowej przez rejestry nazw domen najwyższego poziomu (TLD) i podmioty świadczące usługi rejestracji nazw domen. Może to nastąpić np. przez zamieszczenie danych w ogólnodostępnej bazie abonentów upublicznianej przez rejestr nazw domen najwyższego poziomu (TLD), czyli bazach takich jak Whois.

13.6. Czy dane osobowe dotyczące abonentów nazw domen podlegają publikacji? [NOWE – aktualizacja czerwiec 2026 r.]

Ustawa o KSC nie wprowadza takiego obowiązku, wobec czego zastosowanie w tym zakresie mają przepisy dotyczące ochrony danych osobowych, tym samym co do zasady dane osobowe nie powinny być publikowane. Nie jest natomiast wykluczone publikowanie takich danych jeżeli zapewniona została odpowiednia podstawa prawna wynikająca z RODO (np. jeżeli abonent nazwy domeny udzielił w tym zakresie stosownej zgody), a dany rejestr nazw domen najwyższego poziomu (TLD) technicznie dopuszcza możliwość publikowania takich danych.

13.7. Czy numer telefonu i adres e-mail abonenta nazwy domeny podlegają publikacji? [NOWE – aktualizacja czerwiec 2026 r.]

Dane osób fizycznych, korzystających z ochrony wynikającej z RODO, nie są objęte obowiązkiem publikowania. Dane innych abonentów nazw domen podlegają obowiązkowej publikacji, co dotyczy także adresu e-mail i numeru



telefonu. Adresy e-mail są tworzone zawsze w domenach internetowych, więc każdy abonent nazwy domeny ma możliwość ich tworzenia. Zgodnie z zaleceniami zawartymi w motywach dyrektywy NIS2, taki abonent powinien mieć na uwadze to, aby jego adres e-mail nie zawierał danych osobowych, podając adres generyczny (np. kontakt@, biuro@, domeny@, itp.). W odmiennym przypadku taki abonent musiałby wskazać podmiotowi świadczącemu usługi rejestracji nazw domen i rejestrowi nazw domen najwyższego poziomu (TLD), że zapewnił w wymaganym zakresie istnienie odpowiedniej podstawy prawnej wynikającej z RODO, ponieważ przekazywałby tym podmiotom dane dotyczące osoby fizycznej (np. swojego pracownika, zleceniobiorcy, itp.).

13.8. Czy abonent nazwy domeny może wskazać adres e-mail rejestratora zamiast swojego adresu e-mail? [NOWE – aktualizacja czerwiec 2026 r.]

Nie. W każdym przypadku abonent nazwy domeny zobowiązany jest wskazać przypisany do siebie adres e-mail. Abonent nazwy domeny może korzystać z usług innych podmiotów, w tym swojego rejestratora, w celu utworzenia i technicznej lub administracyjnej obsługi adresu e-mail, jednakże adres taki podlega przypisaniu do samego abonenta. Spełnia on bowiem funkcję identyfikacyjną oraz powinien umożliwiać komunikację z abonentem nazwy domeny.

13.9. Czy rejestrator to punkt kontaktowy zarządzający nazwą domeny? [NOWE – aktualizacja czerwiec 2026 r.]

Są to różne kategorie podmiotów. Rejestratorzy to główna kategoria podmiotów świadczących usługi rejestracji nazw domen (dalsze kategorie to agenci rejestratorów). Natomiast punkty kontaktowe zarządzające nazwą domeny to specyficzna kategoria usługodawców, którzy działają tylko w odniesieniu do tych domen najwyższego poziomu (TLD), w których zostało to dopuszczone. Informacji na ten temat należy poszukiwać w politykach i procedurach publikowanych przez rejestry nazw domen najwyższego poziomu (TLD), zgodnie z art. 16b ustawy o KSC. W przypadku braku informacji o takim dopuszczeniu, dane dotyczące takich podmiotów nie są umieszczane w bazie danych dotyczącej rejestracji nazw domen.

13.10. Czy abonent nazwy domeny musi brać udział w weryfikacji danych dotyczących rejestracji nazwy domeny i czemu ona służy? [NOWE – aktualizacja czerwiec 2026 r.]

Zgodnie z art. 16b ustawy o KSC, realizacja weryfikacji danych dotyczących rejestracji nazw domen stanowi obowiązek prawny, wobec czego abonent musi brać w niej udział. Procedury weryfikacyjne powinny być wyważone i



proporcjonalne. Mogą one dotyczyć po prostu aktualności danych, ale czasami wiążą się z nadużyciami pojawiającymi się w Internecie, w tym tzw. „kradzieżą tożsamości” lub tzw. „uprowadzeniem domeny”. Z tego względu weryfikacja jest obowiązkowo prowadzona przy rejestracji nazwy domeny, ale może też być powtarzana, zależnie od okoliczności danego przypadku.

13.11. Jakie dane podlegają weryfikacji? [NOWE – aktualizacja czerwiec 2026 r.]

Zgodnie z art. 16b ustawy o KSC, konieczne jest zweryfikowanie co najmniej jednego ze sposobów kontaktu z abonentem nazwy domeny. Zasady z tym związane powinny wynikać z polityk i procedur publikowanych przez rejestry nazw domen najwyższego poziomu (TLD) i podmioty świadczące usługi rejestracji nazw domen, zgodnie z art. 16b ustawy o KSC. Zależnie od okoliczności danego przypadku konieczna może okazać się weryfikacja więcej niż jednego ze sposobów kontaktu z abonentem nazwy domeny (zarówno w zakresie komunikacji z wykorzystaniem poczty elektronicznej jak i numeru telefonu) lub bardziej szczegółowa weryfikacja, w tym wymagająca przedstawienia dokumentów potwierdzających tożsamość osoby fizycznej.

13.12. Jakie są terminy związane z przekazywaniem i weryfikacją danych dotyczących abonenta nazwy domeny? [NOWE – aktualizacja czerwiec 2026 r.]

Ustawa o KSC nie określa wprost terminów w tym zakresie, natomiast wymaga, aby określone działania były podejmowane niezwłocznie. Odpowiednie terminy powinny być komunikowane przez rejestry nazw domen najwyższego poziomu (TLD) i podmioty świadczące usługi rejestracji nazw domen, w szczególności w treści polityk i procedur publikowanych zgodnie z art. 16b ustawy o KSC.

13.13. Jakie mogą być skutki niepodania danych przez abonenta nazwy domeny lub zaniedbania udziału w procedurach weryfikacyjnych? [NOWE – aktualizacja czerwiec 2026 r.]

Zgodnie z art. 16b ustawy o KSC, gromadzenie danych dotyczących rejestracji nazw domen stanowi obowiązek prawny. To samo dotyczy weryfikacji danych dotyczących rejestracji nazw domen. Odpowiednie standardy z tym związane oraz skutki ich niedotrzymania powinny być komunikowane przez rejestry nazw domen najwyższego poziomu (TLD) i podmioty świadczące usługi rejestracji nazw domen, w treści polityk i procedur publikowanych zgodnie z art. 16b ustawy o KSC. W przypadku, gdy abonent nazwy domeny nie zapewnia wymaganego udziału w tych działaniach, w szczególności nie dopełnia standardów wynikających z takich



polityk i procedur (np. przekracza wynikające z nich terminy) może być to traktowane jako naruszenie uniemożliwiające rejestrom nazw domen najwyższego poziomu (TLD) i podmiotom świadczącym usługi rejestracji nazw domen realizację obowiązków wynikających z ustawy o KSC. Skutkiem takiej sytuacji może być brak możliwości uzyskania lub utrzymania statusu abonenta nazwy domeny internetowej, przy czym tak daleko idące środki nie powinny być stosowane bez uprzedniego wezwania abonenta nazwy domeny do dopełnienia wymagań.

13.14. Czy abonent nazwy domeny powinien brać udział w dostosowaniu bazy danych dotyczących rejestracji nazw domen do nowych regulacji? [NOWE – aktualizacja czerwiec 2026 r.]

Tak. Rejestry nazw domen najwyższego poziomu (TLD) i podmioty świadczące usługi rejestracji nazw domen powinny dostosować swoje bazy danych dotyczące rejestracji nazw domen oraz opublikować polityki i procedury, o których mowa w art. 16b ustawy o KSC, w terminie 12 miesięcy liczonych od dnia 3 kwietnia 2026 r. Do tego czasu prowadzone będą działania dostosowawcze, co powinni uwzględniać także abonenci nazw domen w zakresie, który ich dotyczy, czyli przede wszystkim brać udział w procedurach weryfikacyjnych, uzupełniać brakujące dane (np. numer telefonu). Rejestry nazw domen najwyższego poziomu (TLD) i podmioty świadczące usługi rejestracji nazw domen są uprawnione do wymagania od abonentów zaangażowania w takie działania także w okresie dostosowawczym.

13.15. Kto jest podmiotem świadczącym usługi rejestracji nazw domen? [NOWE – aktualizacja czerwiec 2026 r.]

Zgodnie z art. 2 pkt 11 d ustawy o KSC, podmiot świadczący usługi rejestracji nazw domen oznacza rejestratora lub agenta działającego w imieniu rejestratorów, w tym dostawcę lub odsprzedawcę usług w zakresie prywatnej rejestracji lub pośrednictwa w rejestracji. Ustawa o KSC ani Dyrektywa NIS 2 nie zawiera definicji legalnej pojęcia rejestratora ani agenta rejestratora. Oba pojęcia opisuje natomiast ENISA (The European Union Agency for Cybersecurity – Agencja Unii Europejskiej ds. Cyberbezpieczeństwa) w dokumencie pt. *DNS Identity – Verification and Authentication of Domain Name Owners* (<https://www.enisa.europa.eu/publications/dns-identity>).

W powołanym dokumencie rejestratora (*registrar*) definiuje się jako jednostkę organizacyjną, która umożliwia osobom fizycznym i podmiotom (abonentom) rejestrowanie nazw domen. W trakcie procesu rejestracji rejestrator weryfikuje, czy żądana nazwa domeny spełnia polityki operatora rejestru, a następnie przekazuje tę nazwę oraz inne wymagane informacje do operatora rejestru. Rejestratorzy są również zobowiązani do gromadzenia informacji od abonentów



i udostępniania tych informacji publicznie. Po dokonaniu rejestracji, abonenci mogą wprowadzać zmiany w konfiguracji swojej domeny za pośrednictwem narzędzi udostępnianych przez rejestratora. Rejestratorzy mogą sprzedawać nazwy domen w wielu domenach najwyższego poziomu (TLD) i posiadają umowne relacje z każdym z tych rejestrów.

Z kolei pojęcie „reseller nazw domen” jest opisywane jako „podmiot zewnętrzny oferujący usługi rejestracji nazw domen za pośrednictwem rejestratora (...)”.

13.16. Do kiedy należy wdrożyć obowiązki wynikające z art. 16 b ustawy o KSC? [NOWE – aktualizacja czerwiec 2026 r.]

3 kwietnia 2027 r. – jest to koniec terminu na wdrożenie obowiązków wynikających z ustawy o KSC (koniec okresu dostosowawczego) dla rejestrów domen najwyższego poziomu oraz rejestratorów.

13.17. Kto może żądać udostępnienia danych o domenie? [NOWE – aktualizacja czerwiec 2026 r.]

Prawo do żądania danych dotyczących rejestracji nazw domen, które mają znaczenie dla prowadzonego postępowania lub czynności wyjaśniających w sprawie o wykroczenie, z zachowaniem przepisów dotyczących ochrony danych osobowych, mają określone w art. 16c ustawy o KSC organy i instytucje. Są to m.in. sądy, prokuratura, Policja, Prezes Urzędu Komunikacji Elektronicznej oraz zespoły CSIRT odpowiedzialne za cyberbezpieczeństwo.

13.18. Czy przy udostępnianiu danych trzeba przestrzegać ochrony danych osobowych? [NOWE – aktualizacja czerwiec 2026 r.]

Tak. Nawet gdy dane są przekazywane organom państwowym, trzeba stosować przepisy o ochronie danych osobowych. Oznacza to m.in. obowiązek odpowiedniego zabezpieczenia danych.

13.19. W jakiej formie składa się żądanie udostępnienia danych? [NOWE – aktualizacja czerwiec 2026 r.]

Żądanie musi być złożone w formie elektronicznej. Dzięki temu możliwe jest szybkie przekazanie informacji i zachowanie odpowiedniej dokumentacji. Żądanie musi być podpisane w sposób potwierdzający jego autentyczność, np. podpisem kwalifikowanym lub podpisem zaufanym. Ma to zapewnić bezpieczeństwo i pewność, że pochodzi od uprawnionego podmiotu. Organ składający wniosek



musi wyjaśnić, dlaczego potrzebuje danych domenowych. Pozwala to ocenić, czy żądanie jest zgodne z prawem.

13.20. W jakim terminie należy odpowiedzieć na żądanie? [NOWE – aktualizacja czerwiec 2026 r.]

Rejestr lub podmiot świadczący usługi rejestracji nazw domen ma obowiązek odpowiedzieć najpóźniej w ciągu 72 godzin od otrzymania żądania. Termin ten ma zapewnić sprawne działanie organów i szybkie reagowanie na zagrożenia.



14. Inne

14.1. Czy istnieją dodatkowe przepisy unijne określające wymagania cyberbezpieczeństwa dla niektórych podmiotów kluczowych i podmiotów ważnych?

Tak. Działając na podstawie upoważnienia zawartego w art. 21 ust. 5 dyrektywy NIS 2 Komisja Europejska wydała rozporządzenie wykonawcze Komisji (UE) 2024/2690 <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32024R2690>.

Rozporządzenie to zostało oparte na następujących dokumentach normalizacyjnych:

- ISO/IEC 27001
- ISO/IEC 27002
- ETSI EN 319401 - General Policy Requirements for Trust Service Providers
- CEN/TS 18026:2024 - Three-level approach for a set of cybersecurity requirements for cloud services

Środki techniczne i organizacyjne określono w załączniku do rozporządzenia.

W niektórych przypadkach, gdy załącznik posługuje się wyrażeniami np.: "w stosownych przypadkach" można odstąpić od stosowania wskazanych w załączniku środków, jeżeli nie jest to właściwe - wymaga to jednak udokumentowania.

Przykład: zakres zdarzeń, które podmioty kluczowe i podmioty ważne monitorują w swoich systemach

Ponadto podmioty kluczowe z podsektora energii elektrycznej stosują, w ramach systemu zarządzania bezpieczeństwem informacji i ciągłości działania środki określone w rozporządzeniu delegowanym Komisji (UE) 2024/1366 z dnia 11 marca 2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/943 poprzez ustanowienie kodeksu sieci dotyczącego zasad sektorowych w zakresie aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej.

14.2. Jaka jest relacja pomiędzy ustawą o KSC a rozporządzeniem DORA?

W zakresie sektora bankowości i infrastruktury rynków finansowych ustawa wskazuje, że pierwszeństwo przed nią mają przepisy rozporządzenia DORA. Ma to wyeliminować wątpliwości wynikające z funkcjonowania w tym obszarze, tych dwóch aktów prawnych. Dyrektywa NIS 2 w artykule 4 wskazuje na



pierwszeństwo sektorowych aktów unijnych z zakresu cyberbezpieczeństwa w zakresie środków zarządzania ryzykiem oraz zgłaszania incydentów. Komunikat Komisji – Wytyczne Komisji dotyczące stosowania art. 4 ust. 1 i 2 dyrektywy (UE) 2022/2555 (NIS 2) 2023/C 328/02 wskazuje, że rozporządzenie DORA jest takim aktem w zakresie podmiotów kluczowych i podmiotów ważnych z sektora bankowości i infrastruktury rynków finansowych.

Zgodnie z art. 8i ustawy o KSC, pierwszeństwo nad ustawą o KSC mają regulacje DORA, z tym że do podmiotów kluczowych i podmiotów ważnych z sektora bankowości i infrastruktury rynków finansowych stosuje się przepisy art. 3a (czynności dopuszczalne w ramach obsługi incydentów), art. 5 ust. 1–3 (kryteria podmiotu kluczowego i podmiotu ważnego), art. 7–7m (przepisy o wykazie podmiotów kluczowych i podmiotów ważnych), art. 8 ust. 1 pkt 1 (obowiązek prowadzenia systematycznego szacowania ryzyka wystąpienia incydentu) i pkt 2 lit. j (obowiązek stosowania podstawowych zasad cyberhigieny), art. 8h (dopuszczalność wymiany informacji), art. 9 (obowiązki w zakresie wyznaczenia osób kontaktowych), art. 11 ust. 1 pkt 5 i 6 (współdziałanie z CSIRT podczas zgłoszenia incydentów), art. 13 (dobrowolne przekazywanie informacji do CSIRT), art. 16 (stosowanie obowiązków po raz pierwszy), art. 26a ust. 2–4 (zgłoszenia podatności w ramach skoordynowanego ujawniania podatności), art. 32 (uprawnienie CSIRT do wykonywania niezbędnych działań technicznych), art. 33 ust. 5, 7 oraz 8 (rekomendacje Pełnomocnika), art. 36a, art. 36b (ocena bezpieczeństwa), art. 37 (wyłączenie ustawy z dnia 6 września 2021 r. o dostępie do informacji publicznej przy informacjach o podatnościach, incydentach i cyberzagrożeniach), art. 43 (uprawnienie organu do żądania informacji), art. 45 ust. 3, art. 46 ust. 1 pkt 1, 2, 4–7 i oraz ust. 4–6 (obowiązek korzystania z systemu teleinformatycznego S46), art. 67a (rekomendacje Pełnomocnika), art. 67c, art. 67d oraz, art. 67g, art. 67h oraz art. 67i (postępowanie w sprawie uznania za dostawcę wysokiego ryzyka oraz polecenie zabezpieczające) ustawy o KSC.

14.3. Czy podleganie pod Rozporządzenie (WE) nr 1907/2006 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2006 r. w sprawie rejestracji, oceny, udzielania zezwoleń i stosowanych ograniczeń w zakresie chemikaliów i utworzenia Europejskiej Agencji Chemikaliów (REACH) oznacza automatyczne objęcie ustawą o KSC?

Nie. REACH i ustawa o KSC regulują różne obszary. O objęciu ustawą o KSC decyduje identyfikacja podmiotu jako podmiotu ważnego lub kluczowego w rozumieniu wyłącznie NIS2 oraz ustawy o Krajowym Systemie Cyberbezpieczeństwa, w tym wypadku kluczowy będzie załącznik nr 2 do ustawy wskazujący na sektory ważne.



14.4. Czy podmiot należący do sektora „Produkcja, wytwarzanie i dystrybucja chemikaliów” jest objęty także obowiązkami wynikającymi z rozporządzenia REACH?

Nie zawsze. Dyrektywa NIS 2 w tym sektorze jedynie w zakresie definicyjnym odwołuje się do REACH i nie wskazuje, że podmiot należący do tego sektora zawsze objęty jest wskazanymi w REACH obowiązkami. To REACH definiuje jakiego rodzaju podmioty objęte są obowiązkami wynikającymi z tego aktu.

14.5. Czy sformułowanie „Przedsiębiorstwa zajmujące się wytwarzaniem (...) mieszanin chemicznych”, użyte w załączniku nr 2 do ustawy o KSC, należy interpretować szerzej niż definicję „producenta” REACH?

Nie. Dyrektywa NIS2 w sektorze „Produkcja, wytwarzanie i dystrybucja chemikaliów” w zakresie definicyjnym odwołuje się do rozporządzenia REACH, z uwagi na to Rozporządzenie REACH należy brać pod uwagę przy identyfikacji w zakresie definiującym wyrób, producenta i dystrybutora.

14.6. Czy przedsiębiorstwa zajmujące się produkcją lub dystrybucją substancji lub mieszanin obejmują też dalszych użytkowników?

Co do zasady nie. W załączniku nr 2 (podmioty ważne) ustawy o KSC, ta kategoria odsyła wprost do definicji z rozporządzenia REACH, tj. producenta substancji przez dystrybutora. „Dalszy użytkownik” jest odrębną kategorią w rozporządzeniu REACH i nie jest wskazany w tym odesłaniu.

14.7. Czy pojęcie systemu informacyjnego należy odnosić do całego środowiska teleinformatycznego organizacji czy do każdego systemu oddzielnie? [NOWE – aktualizacja czerwiec 2026 r.]

System informacyjny zgodnie z przewidzianą definicją to każdy z systemów, przy pomocy którego jest świadczona usługa, w tym realizowane zadanie publiczne. W tym zakresie każdy z tych systemów powinien być zinwentaryzowany oraz powinien zostać uwzględniony w SZBI na podstawie art. 8 ustawy o KSC. Zgodnie z art. 8 ustawy o KSC, podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot. W przypadku występowania kilku lub większej liczby systemów, SZBI może zostać wdrożone na poziomie całego podmiotu kluczowego



lub podmiotu ważnego, a poszczególne odwołania do systemów informacyjnych z uwagi na ich specyfikę mogą stanowić poszczególne elementy SZBI.

14.8. Czy urządzenia autonomiczne i rozwiązania smart city mieszczą się w definicji systemu informacyjnego nawet jak nie łączą się z siecią telekomunikacyjną? [NOWE – aktualizacja czerwiec 2026 r.]

Tak. Zgodnie z definicją wskazaną w ustawie o KSC:

System informacyjny:

- a) system teleinformatyczny, o którym mowa w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2025 r. poz. 1703 oraz z 2026 r. poz. 160), lub
- b) urządzenie lub grupę połączonych urządzeń i oprogramowania zaprogramowanych w celu przetwarzania danych

-wraz z danymi przetwarzanymi w postaci elektronicznej;

Definicja wyraźnie odróżnia systemy teleinformatyczne i przetwarzane w nich dane oraz urządzenia i przetwarzane w nich dane. Zwrot „urządzenie lub grupę połączonych urządzeń” wskazuje, że może to być pojedyncze urządzenia służące do przetwarzania danych jak i grupa połączonych urządzeń (co wskazuje na konieczność wykorzystywania sieci telekomunikacyjnych). Nawet więc jeżeli dane urządzenie nie jest połączone z siecią telekomunikacyjną, a przetwarza dane dla potrzeb świadczenia usługi, w tym realizacji zadania publicznego, to objęte jest definicją systemu informacyjnego w rozumieniu ww. ustawy.

14.9. Czy informacje o podatnościach i incydentach JST mogą zostać wyłączone z udostępnienia jako informacje związane z bezpieczeństwem publicznym lub bezpieczeństwem państwa, o którym mowa w art. 37 i 38 ustawy o KSC? [NOWE – aktualizacja czerwiec 2026 r.]

Informacje dotyczące podatności, incydentów, cyberzagrożeń oraz o ryzyku wystąpienia incydentów nie są udostępniane na gruncie ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej. Nie są również udostępniane na podstawie ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego, z wyjątkiem informacji, których udostępnienie nie zagrażałoby bezpieczeństwu państwa lub bezpieczeństwu publicznemu.



14.10. Jak należy rozumieć pojęcie usługi na gruncie ustawy o KSC?

Usługę należy rozumieć szeroko, jako *działalność gospodarczą służącą do zaspokajania potrzeb ludzi*. W tym znaczeniu usługą będzie również produkcja.

Usługą jest także zadanie publiczne realizowane przez podmiot publiczny.

14.11. Czy Ministerstwo zapewnia materiały wspierające wdrożenie ustawy o KSC?

Zachęcamy przy tym do regularnego korzystania ze strony <https://cyber.gov.pl/> oraz serwisu CERT Polska <https://moje.cert.pl/> aby na bieżąco podnosić wiedzę z zakresu cyberbezpieczeństwa.

Ministerstwo Cyfryzacji zachęca do stosowania z mechanizmów uwierzytelniania wieloskładnikowego, tam gdzie jest to możliwe. Poza tym polecamy materiał przygotowany przez zespół CERT Polska

<https://cert.pl/posts/2022/01/rekomendacje-techniczne-systemow-uwierzytelniania/> oraz <https://cert.pl/posts/2022/01/kompleksowo-o-haslach/>.

Ministerstwo Cyfryzacji prowadzi bezpłatne szkolenia dla podmiotów krajowego systemu cyberbezpieczeństwa – harmonogram jest dostępny pod adresem: <https://www.gov.pl/web/baza-wiedzy/harmonogramszkolen>.

14.12. Czy podmioty publiczne mają obowiązek stosować wymogi cyberbezpieczeństwa zawarte w rozporządzeniu w sprawie Krajowych Ram Interoperacyjności? [NOWE – aktualizacja czerwiec 2026 r.]

Obowiązki dotyczące cyberbezpieczeństwa podmiotów publicznych znajdują się w ustawie o KSC. Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, będzie zmienione - zostaną z niego usunięte przepisy dotyczące wdrożenia systemu zarządzania bezpieczeństwem informacji. Będzie ono zmienione do 22 lutego 2027 r., co wynika z art. 15 ustawy z dnia 25 lipca 2025 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw. Do czasu zmiany rozporządzenia ono nadal obowiązuje.