

Poziom	Typ	Definicja / opis	Kryteria kwalifikacji	Obowiązki zgłoszeniowe
INCYDENT POWAŻNY (art. 2 pkt 7 KSC)	Naruszenie ochrony danych osobowych (w rozumieniu RODO)	Poważne naruszenie ochrony danych osobowych związane z wysokim ryzykiem naruszenia praw i wolności osób fizycznych (pracowników, współpracowników, odbiorców usług, kontrahentów).	Ocena wg Załącznika Nr 1 „Metodyka oceny naruszeń ochrony danych osobowych”	Zgłoszenie do UODO w ciągu 72 godzin od stwierdzenia naruszenia (art. 33 RODO). Zawiadomienie osób, których dane dotyczą — jeśli wymagane (art. 34 RODO).
INCYDENT POWAŻNY (art. 2 pkt 7 KSC)	Incydent SZBI	<p>Incydent, który powoduje lub może spowodować: (1) poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi przez podmiot kluczowy lub podmiot ważny — nie jak dotychczas: usługi kluczowej przez operatora usługi kluczowej; (2) straty finansowe dla podmiotu kluczowego/ważnego; lub (3) poważną szkodę materialną albo niematerialną dla innych osób fizycznych, prawnych lub jednostek organizacyjnych</p> <p>• Czas trwania Incydentu jest</p>	<p>Warunek bezwzględny I — nastąpił skuteczny i nieuprawniony dostęp do sieci i systemów informatycznych podmiotu (w tym gdy może spowodować utratę danych) LUB powstała sytuacja kryzysowa / uruchomiony plan ciągłości działania dla usług krytycznych LUB</p> <p>Warunek bezwzględny II — spełnione zostały co najmniej dwa z poniższych kryteriów A–E: A. UŻYTKOWNICY USŁUGI Spełnione, gdy wystąpi co najmniej jeden z warunków: liczba użytkowników dotkniętych incydem powoduje niedostępność usługi lub uniemożliwia prawidłowe korzystanie z niej przez znaczącą ich</p>	<p>Podmiot kluczowy i podmiot ważny (art. 11 ust. 1 KSC):</p> <p>① Wczesne ostrzeżenie — niezwłocznie, nie później niż 24 godziny od wykrycia → właściwy CSIRT sektorowy (system S46)</p> <p>② Zgłoszenie incydentu poważnego — niezwłocznie, nie później niż 72 godziny od wykrycia → właściwy CSIRT sektorowy (system S46)</p>

Poziom	Typ	Definicja / opis	Kryteria kwalifikacji	Obowiązki zgłoszeniowe
		<p>dłuższy niż 8 godziny.</p> <ul style="list-style-type: none"> Przerwa w świadczeniu krytycznych usług SP przekracza 2 godziny. przerwę w realizacji zadań publicznych trwającą dłużej niż 8 godzin (jeden dzień roboczy urzędu); paraliż zadań krytycznych z zakresu obronności, bezpieczeństwa państwa, ochrony ludności czy obrony cywilnej trwający powyżej 4 godzin; trwającą dłużej niż 4 godziny niedostępność systemu obsługującego rejestr publiczny, dziennika urzędowego, Węzła Krajowego Identyfikacji Elektronicznej lub aplikacji mObywatel; atak ransomware, czyli sytuację, w której dane w systemie informacyjnym zostały zaszyfrowane 	<p>liczbę; wpływ incydentu w dużym stopniu przełoży się na świadczenie usług przez podmiot lub wpłynie na odbiorców usługi. <i>Jeżeli liczby użytkowników nie można określić — Zespół Reagowania szacuje je na podstawie danych z porównywalnych okresów.</i> B. SKUTKI REPUTACYJNE Spełnione, gdy wystąpi co najmniej jeden z warunków: incydent opisany w mediach ogólnopolskich; powtarzające się skargi użytkowników usługi; podmiot nie będzie lub prawdopodobnie nie będzie w stanie spełnić wymogów ustawowych/regulacyjnych h. C. CZAS TRWANIA I PRZERWA W ŚWIADCZENIU USŁUG Spełnione, gdy wystąpi co najmniej jeden z warunków: czas trwania incydentu > 24 godziny; przerwa w usługach IT wspierających krytyczne lub istotne funkcje > 2 godziny. D. UTRATA DANYCH Spełnione, gdy wystąpi co najmniej jeden z warunków: <i>dostępność</i> — dane stały się tymczasowo lub trwale niedostępne/nienadające się do użytku; <i>autentyczność</i> — spadek</p>	<p>③ Sprawozdanie okresowe — na wniosek CSIRT sektorowego ④ Sprawozdanie końcowe — nie później niż 1 miesiąc od dnia zgłoszenia; jeśli obsługa się nie zakończyła — sprawozdanie z postępu, a końcowe w ciągu miesiąca od zakończenia obsługi ⑤ Informowanie użytkowników — o incydencie, który ma niekorzystny wpływ na świadczenie usług Podmiot publiczny będący podmiotem ważnym (art. 12c KSC i Q&A pkt 6.12); ma uproszczone obowiązki zgłoszeniowe. Nie składa:</p>

Poziom	Typ	Definicja / opis	Kryteria kwalifikacji	Obowiązki zgłoszeniowe
		<p>i skierowano do jednostki żądanie okupu;</p> <ul style="list-style-type: none"> naruszenie danych takie jak np. wyciek, zniszczenie lub sfalszowanie danych (utrata poufności, integralności lub autentyczności) dotyczące co najmniej 10 proc. użytkowników danego systemu; zdarzenie skutkujące śmiercią, ciężkim uszkodzeniem ciała, uszczerbkiem na zdrowiu więcej niż jednej osoby, ujawnieniem tajemnicy prawnie chronionej lub stratami finansowymi przekraczającymi 2 mln zł 	<p>wiarygodności źródła danych; <i>integralność</i> — nieuprawniona modyfikacja skutkująca niedokładnością lub niekompletnością danych; <i>poufność</i> — nieuprawniona osoba/system uzyskały dostęp do danych lub dane zostały im ujawnione; podmiot nie będzie w stanie spełnić wymogów ustawowych/regulacyjnych; udany, złośliwy i nieuprawniony dostęp mogący spowodować utratę danych. E. SKUTKI FINANSOWE Koszty i straty poniesione przez podmiot przekroczyły lub prawdopodobnie przekroczą [...] PLN (<i>próg zostanie określony w rozporządzeniu RM</i> <i>wydanym na podstawie art. 11 ust. 4 KSC — dla sektorów nieobjętych rozporządzeniem wykonawczym KE 2024/2690 Do czasu jego wejścia w życie stosuje się ocenę ekspercką na podstawie wewnętrznej procedury.</i>) Kilka incydentów, które indywidualnie nie osiągnęły progu incydentu poważnego, traktuje się łącznie jako jeden incydent poważny, jeżeli: (1) wystąpiły ≥ 2 razy w ciągu 6 miesięcy, (2) mają</p>	<p>wczesnego ostrzeżenia, sprawozdania okresowego, sprawozdania z postępu, sprawozdania końcowego. Składa wyłącznie zgłoszenie incydentu poważnego w terminie 72 godzin od wykrycia Dostawca usług zaufania (art. 11 ust. 1a KSC): zgłasza incydent poważny w ciągu 24 godzin od wykrycia.</p>

Poziom	Typ	Definicja / opis	Kryteria kwalifikacji	Obowiązki zgłoszeniowe
			tę samą widoczną pierwotną przyczynę oraz (3) łącznie spełniają kryteria A–E.	
INCYDENT ZNACZĄCY (kategoria wewnętrzna SZBI — brak odrębnej definicji ustawowej w KSC)	Naruszenie ochrony danych osobowych (w rozumieniu RODO)	Naruszenie, przy którym występuje ryzyko dla praw i wolności osób fizycznych (pracowników, współpracowników, odbiorców usług, kontrahentów), lecz nie osiąga poziomu wysokiego ryzyka.	Ocena wg Załącznika Nr 1 „Metodyka oceny naruszeń ochrony danych osobowych”	W zależności od wyniku oceny ryzyka — możliwe zgłoszenie do UODO. Obowiązkowa dokumentacja wewnętrzna (art. 33 ust. 5 RODO).
INCYDENT ZNACZĄCY (kategoria wewnętrzna SZBI — brak odrębnej definicji ustawowej w KSC)	Incident SZBI	Incident, który nie spełnia kryteriów incydentu poważnego z art. 2 pkt 7 KSC — w szczególności nie doszło do skutecznego i nieuprawnionego dostępu do sieci i systemów informatycznych podmiotu, lecz incydent wywołał mierzalny, negatywny wpływ na funkcjonowanie podmiotu lub realizację jego usług/zadań publicznych.	Warunek wykluczający: Brak skutecznego i nieuprawnionego dostępu do sieci/systemów IT podmiotu. ORAZ spełnienie co najmniej dwóch z kryteriów A–E: A. UŻYTKOWNICY USŁUGI Spełnione, gdy wystąpi co najmniej jeden z warunków: incydent powoduje niedostępność usługi dla wszystkich użytkowników; wpływ incydentu nie przełoży się istotnie na dalsze świadczenie usług przez podmiot. B. SKUTKI REPUTACYJNE Spełnione, gdy: incydent niesie potencjalne szkody dla reputacji podmiotu, ale bez wpływu na spełnienie wymogów ustawowych/regulacyjnych	Obsługa wewnętrzna zgodnie z procedurami SZBI podmiotu. Brak ustawowego obowiązku zgłoszenia do CSIRT jako incydent poważny. Możliwe dobrowolne zgłoszenie do właściwego CSIRT przez system S46 (art. 13 ust. 1 pkt 1 KSC) Rejestracja w wewnętrznym

Poziom	Typ	Definicja / opis	Kryteria kwalifikacji	Obowiązki zgłoszeniowe
			<p>h. C. CZAS TRWANIA I PRZERWA W ŚWIADCZENIU USŁUG Spełnione, gdy wystąpi co najmniej jeden z warunków: czas trwania incydentu wynosi od 6 do 24 godzin; przerwa w usługach IT wspierających krytyczne lub istotne funkcje < 2 godziny. D. UTRATA DANYCH Spełnione, gdy wystąpi co najmniej jeden z warunków: <i>dostępność</i> — dane stały się tymczasowo w ograniczonym zakresie niedostępne; <i>integralność</i> — modyfikacja skutkująca tymczasową i ograniczoną niedokładnością lub niekompletnością danych; <i>poufność</i> — nieuprawniony dostęp do danych przez pracownika podmiotu. E. SKUTKI FINANSOWE Koszty i straty nie przekroczyły lub prawdopodobnie nie przekroczą [...] PLN (<i>próg do uzupełnienia</i>).</p>	rejestrze incydentów.
<p>INCYDENT ZNIKOMY (kategoria wewnętrzna SZBI — brak odrębnej definicji ustawowej w KSC)</p>	<p>Naruszenie ochrony danych osobowych (w rozumieniu RODO)</p>	<p>Naruszenie z małym prawdopodobieństwem ryzyka dla praw i wolności osób fizycznych.</p>	<p>→ Ocena wg Załącznika Nr 1 „Metodyka oceny naruszeń ochrony danych osobowych”</p>	<p>Brak obowiązku zgłoszenia do UODO. Obowiązkowa dokumentacja wewnętrzna (art. 33 ust. 5 RODO —</p>

Poziom	Typ	Definicja / opis	Kryteria kwalifikacji	Obowiązki zgłoszeniowe
				ewidencja naruszeń).
<p>INCYDENT ZNIKOMY (kategoria wewnętrzna SZBI — brak odrębnej definicji ustawowej w KSC)</p>	<p>Incydent SZBI</p>	<p>Incydent o minimalnym wpływie na organizację i interesariuszy — nie spełnia kryteriów incydentu poważnego ani znaczącego.</p>	<p>Łącznie spełnione muszą być wszystkie warunki: brak skutecznego i nieuprawnionego dostępu do sieci/systemów IT podmiotu; minimalny wpływ na organizację i interesariuszy — niewielkie ryzyko reputacyjne; czas przerwy w świadczeniu usług < 2 godziny i dotyczy wyłącznie systemów wspierających niekrytyczne usługi / zadania publiczne podmiotu; utrata danych ograniczona do niewielkich, izolowanych obszarów bez wpływu na podstawową działalność; skutki finansowe nie przekraczają [...] PLN (próg do uzupełnienia).</p>	<p>Wyłącznie wewnętrzna dokumentacja i rejestracja. Brak ustawowego obowiązku zewnętrznego zgłoszenia.</p>