MAM INCYDENT · WSTĘPNA KWALIFIKACJA

Plan działania po incydencie

Zaszyfrowane pliki, żądanie okupu · wykryto cz 12.11.2026, godz. 15:02 · podmiot kluczowy w KSC · administrator danych

Wstępna kwalifikacja na podstawie odpowiedzi użytkownika · stan prawny na 11.11.2026

NAJBLIŻSZY TERMIN

Do pt 13.11.2026, godz. 15:02

Dotyczy: KSC · Złóż wczesne ostrzeżenie. W chwili pobrania planu zostało 18 h 59 min. Obowiązki (wstępnie): 7, w tym z terminem liczonym w godzinach: 3. Do ustalenia i zalecenia: 2. Informacje: 0.

Terminy i pozycje wyniku

Do kiedy	Co	Podstawa
pt 13.11, 15:02 zostało 18 h 59 min	KSC **Złóż wczesne ostrzeżenie**	art. 11 ust. 1 pkt 4 KSC, art. 11 ust. 2 KSC, art. 12 ust. 1 KSC, art. 12 ust. 2 KSC, art. 44 ust. 1 ustawy z 23.01.2026 (Dz.U. 2026 poz. 252), art. 2 pkt 7 KSC
nd 15.11, 15:02 zostało 2 d 18 h	KSC **Zgłoś incydent poważny (zgłoszenie w 72 h)**	art. 11 ust. 1 pkt 4a KSC, art. 12 ust. 3 KSC, art. 12 ust. 5 KSC
nd 15.11, 17:02 zostało 2 d 20 h	RODO **Zgłoś naruszenie Prezesowi UODO**	art. 33 ust. 1 RODO, art. 33 ust. 3 RODO, art. 33 ust. 4 RODO, art. 46 ust. 1 pkt 7 KSC, komunikat UODO z 3.11.2026 (rekomendacja)
bez zbędnej zwłoki — nie czekaj na upływ 72 h	RODO **Zawiadom osoby, których dane dotyczą — wstępnie ryzyko jest wysokie**	art. 34 ust. 1 RODO, art. 34 ust. 2 RODO, art. 34 ust. 3 lit. a–c RODO
na bieżąco	RODO **Wpisz naruszenie do rejestru naruszeń**	art. 33 ust. 5 RODO, wytyczne EROD 9/2022, pkt 125 (wytyczne, nie przepis)
miesiąc od dnia zgłoszenia	KSC **Złóż sprawozdanie końcowe**	art. 11 ust. 1 pkt 4b i 4c KSC, art. 12b ust. 1 i 2 KSC, art. 12a KSC
niezwłocznie — ustawa nie podaje terminu	KSC **Poinformuj użytkowników swoich usług**	art. 11 ust. 2b KSC
sprawdź przed zgłoszeniem	KSC **Właściwy CSIRT: CSIRT NASK**	art. 26 ust. 6 pkt 1 lit. j KSC, art. 26 ust. 7 pkt 6 KSC, art. 7 ust. 2 pkt 21 i 22 KSC, art. 44 ust. 1 ustawy z 23.01.2026 (Dz.U. 2026 poz. 252)
bez terminu — do ustalenia	Organy ścigania **Rozważ zawiadomienie Policji lub prokuratury**	zalecenie LabLogic — dobra praktyka, nie przepis, art. 12 ust. 2 zdanie drugie KSC

Liczone od godziny, którą podałeś. To, kiedy nastąpiło wykrycie i stwierdzenie, ocenia administrator albo podmiot objęty KSC. Termin to ostatnia chwila. Zgłoś wcześniej, gdy tylko możesz.

Pierwsza pomoc

- [x] Zapisz godzinę wykrycia i to, kto zauważył zdarzenie. Od teraz prowadź krótki dziennik: kto, co i o której zrobił.
- [x] Odłącz zainfekowane komputery od sieci (kabel i Wi-Fi). Nie wyłączaj ich.
- [x] Odłącz od sieci dyski z kopiami zapasowymi, zanim też zostaną zaszyfrowane.
- [x] Nie płać okupu i nie kontaktuj się z przestępcami.
- [ ] Zmień hasła administratorów z czystego urządzenia.
- [ ] Sprawdź, czy przed zaszyfrowaniem dane nie zostały wykradzione (komunikat przestępców, nietypowy ruch wychodzący). To zmienia ocenę naruszenia.
- [ ] Niczego nie kasuj. Zachowaj dowody, czyli zrzuty ekranu, maile z nagłówkami i logi.
- [ ] Powiadom kierownictwo. Decyzję o zgłoszeniu podejmuje organizacja, a terminy biegną także w weekend.
- [ ] Jeśli masz ubezpieczenie od ryzyk cybernetycznych, zgłoś zdarzenie ubezpieczycielowi. Polisy często wymagają szybkiego zgłoszenia.

POTRZEBUJESZ POMOCY?

Zadzwoń do LabLogic: +48 504 920 875 (dni robocze 8–16)

Jeśli termin mija w ciągu kilku godzin, nie czekaj na telefon. Zgłoś sam i uzupełnij zgłoszenie później.

Wynik krok po kroku

OBOWIĄZKI

KSC Złóż wczesne ostrzeżenie

Zgłaszasz w S46, czyli w systemie teleinformatycznym z art. 46 ustawy, który prowadzi minister właściwy do spraw informatyzacji. Wczesne ostrzeżenie nie wymaga znajomości przyczyny. Podajesz dane podmiotu i osób do kontaktu, moment wystąpienia i wykrycia incydentu oraz to, czy mógł być wywołany bezprawnie i czy dotyczy innych państw UE. Możesz poprosić o wytyczne i wsparcie techniczne. Adresat: CSIRT NASK — szczegóły w pozycji „Właściwy CSIRT: CSIRT NASK".

do pt 13.11.2026, godz. 15:02

Podstawa: art. 11 ust. 1 pkt 4 KSC, art. 11 ust. 2 KSC, art. 12 ust. 1 KSC, art. 12 ust. 2 KSC, art. 44 ust. 1 ustawy z 23.01.2026 (Dz.U. 2026 poz. 252), art. 2 pkt 7 KSC

KSC Zgłoś incydent poważny (zgłoszenie w 72 h)

Zgłoszenie opisuje wpływ incydentu na usługę, jego przyczyny i przebieg oraz podjęte działania zapobiegawcze i naprawcze. Adresat i kanał są te same co przy wczesnym ostrzeżeniu. Termin 72 h biegnie od wykrycia, nie od wczesnego ostrzeżenia. Przekazujesz to, co wiesz w chwili zgłoszenia, i uzupełniasz w trakcie obsługi.

do nd 15.11.2026, godz. 15:02

Podstawa: art. 11 ust. 1 pkt 4a KSC, art. 12 ust. 3 KSC, art. 12 ust. 5 KSC

RODO **Zawiadom osoby, których dane dotyczą — wstępnie ryzyko jest wysokie**

Z Twoich odpowiedzi wynika, że naruszenie może powodować wysokie ryzyko dla osób. Napisz prostym językiem, co się stało i jakie mogą być skutki. Dodaj, co robisz i co osoby mogą zrobić same, np. zastrzec PESEL lub zmienić hasła. Podaj kontakt do IOD albo innego punktu kontaktowego. Zawiadomienie nie jest wymagane w trzech przypadkach z art. 34 ust. 3, m.in. gdy przed zdarzeniem zaszyfrowałeś dane, a klucz pozostał bezpieczny, albo gdy później usunąłeś wysokie ryzyko. Zaszyfrowanie plików przez napastnika nie jest takim zabezpieczeniem. Gdy zawiadomienie każdej osoby wymagałoby niewspółmiernie dużego wysiłku, zastępuje je publiczny komunikat albo równie skuteczny środek.

bez zbędnej zwłoki — nie czekaj na upływ 72 h

Podstawa: art. 34 ust. 1 RODO, art. 34 ust. 2 RODO, art. 34 ust. 3 lit. a–c RODO

RODO **Zgłoś naruszenie Prezesowi UODO**

Zgłoś bez zbędnej zwłoki, w miarę możliwości w 72 h od stwierdzenia naruszenia. Zgłoszenie opisuje charakter naruszenia, możliwe konsekwencje i zastosowane środki. Podaje też kontakt do IOD albo innego punktu kontaktowego. Informacje możesz uzupełniać później — lepiej zgłosić niepełne niż po terminie. Po terminie dołącz wyjaśnienie przyczyn opóźnienia. Podmiot kluczowy lub ważny może zgłosić naruszenie także przez S46.

do nd 15.11.2026, godz. 17:02

Podstawa: art. 33 ust. 1 RODO, art. 33 ust. 3 RODO, art. 33 ust. 4 RODO, art. 46 ust. 1 pkt 7 KSC, komunikat UODO z 3.11.2026 (rekomendacja)

RODO **Wpisz naruszenie do rejestru naruszeń**

Opisz każde naruszenie, także niezgłoszone. Zapisz okoliczności, skutki i działania zaradcze. EROD zaleca zapisać też uzasadnienie decyzji, zwłaszcza gdy nie zgłaszasz naruszenia. Dokumentacja ma pozwolić Prezesowi UODO sprawdzić, czy przestrzegasz art. 33.

na bieżąco

Podstawa: art. 33 ust. 5 RODO, wytyczne EROD 9/2022, pkt 125 (wytyczne, nie przepis)

KSC **Złóż sprawozdanie końcowe**

Sprawozdanie składasz w ciągu miesiąca od dnia, w którym zgłosisz incydent poważny. Jeśli obsługa jeszcze trwa, w tym terminie składasz sprawozdanie z postępu, a końcowe w miesiąc od zakończenia obsługi. Sprawozdanie okresowe składasz tylko na wniosek CSIRT.

miesiąc od dnia zgłoszenia

Podstawa: art. 11 ust. 1 pkt 4b i 4c KSC, art. 12b ust. 1 i 2 KSC, art. 12a KSC

KSC **Poinformuj użytkowników swoich usług**

Gdy incydent poważny niekorzystnie wpływa na Twoje usługi, informujesz o nim ich użytkowników. Ustawa nie podaje terminu ani formy. Zalecam zrobić to niezwłocznie i zachować treść komunikatu.

niezwłocznie — ustawa nie podaje terminu

Podstawa: art. 11 ust. 2b KSC

DO USTALENIA I ZALECENIA

KSC **Właściwy CSIRT: CSIRT NASK**

Według Twojej odpowiedzi właściwy jest CSIRT NASK. Ustawa przypisuje mu podmioty kluczowe i ważne, których nie obejmuje CSIRT MON ani CSIRT GOV. Wyjątkiem jest incydent w systemach ujętych w wykazie infrastruktury krytycznej — wtedy właściwy jest CSIRT GOV. Potwierdź to w swoim wpisie w wykazie podmiotów kluczowych i ważnych. Do dnia komunikatu o zdolności operacyjnej CSIRT sektorowego zgłoszenia przyjmuje CSIRT MON, NASK albo GOV. CSIRT INFRASTRUKTURA (transport, woda pitna, ścieki) i CSIRT Cyfra (infrastruktura cyfrowa) ustanowiono 30.06.2026. Na 11.11.2026 nie odnalazłem komunikatu o ich zdolności operacyjnej. Dla zgłoszeń z art. 11 ustawa wskazuje S46. Gdy nie możesz zgłosić przez S46, zgłaszasz w sposób, który właściwy CSIRT określił w komunikacie w Biuletynie Informacji Publicznej. Zachowaj dowód zgłoszenia.

sprawdź przed zgłoszeniem

Podstawa: art. 26 ust. 6 pkt 1 lit. j KSC, art. 26 ust. 7 pkt 6 KSC, art. 7 ust. 2 pkt 21 i 22 KSC, art. 44 ust. 1 ustawy z 23.01.2026 (Dz.U. 2026 poz. 252)

Organy ścigania **Rozważ zawiadomienie Policji lub prokuratury**

Zachowaj dowody. Jeśli doszło do przestępstwa, rozważ zawiadomienie Policji lub prokuratury i zachowaj potwierdzenie. Gdy incydent poważny wyczerpuje znamiona przestępstwa, CSIRT w odpowiedzi na wczesne ostrzeżenie przekazuje informację, jak zgłosić go organom ścigania.

bez terminu — do ustalenia

Podstawa: zalecenie LabLogic — dobra praktyka, nie przepis, art. 12 ust. 2 zdanie drugie KSC

Jak powstał ten wynik

- Rola wobec danych (według odpowiedzi): administrator.
- RODO, ryzyko dla osób (ocena wstępna): wysokie — dane: kontaktowe, PESEL lub dowód, finansowe; liczba osób: 101–1000. Kryteria narzędzia są ostrożnościowe. Oceny dokonuje administrator (art. 33 ust. 1 i art. 34 ust. 1 RODO).
- KSC, status: podmiot kluczowy (według odpowiedzi).
- KSC, incydent poważny (ocena wstępna): tak — usługa nie działała kilka godzin lub dłużej albo nadal nie działa (definicja z art. 2 pkt 7 KSC; progów sektorowych narzędzie nie liczy).
- KSC, czy obowiązek zgłaszania już wiąże: tak — operator usługi kluczowej sprzed 3.04.2026 zgłasza od 3.10.2026 (art. 33 ust. 4 ustawy z 23.01.2026).
- KSC, adresat zgłoszenia: CSIRT NASK (według odpowiedzi). Właściwość wynika z art. 26 ust. 5–7 KSC, a wpis w wykazie podmiotów kluczowych i ważnych ją wskazuje (art. 7 ust. 2 pkt 21 i 22 KSC).
- Pytania bez odpowiedzi albo z odpowiedzią „nie wiem”: straty i szkoda. Dla nich wynik przyjmuje wariant ostrożniejszy.

Co zawiera zgłoszenie

Skrót wymagań z przepisów; pełne brzmienie jest w części „Podstawy prawne”. Formularz organu może wymagać więcej. Odhaczaj to, co już masz. Termin biegnie także wtedy, gdy nie masz kompletu informacji.

Zgłoszenie do Prezesa UODO — art. 33 ust. 3 RODO

- ☐ charakter naruszenia, w miarę możliwości z kategoriami i przybliżoną liczbą osób oraz wpisów danych
- ☐ imię, nazwisko i dane kontaktowe IOD albo inny punkt kontaktowy
- ☐ możliwe konsekwencje naruszenia
- ☐ środki zastosowane lub proponowane, w tym ograniczające negatywne skutki

Zawiadomienie osób, których dane dotyczą — art. 34 ust. 2 RODO

- [ ] charakter naruszenia opisany jasnym i prostym językiem
- [ ] imię, nazwisko i dane kontaktowe IOD albo inny punkt kontaktowy
- [ ] możliwe konsekwencje naruszenia
- [ ] środki zastosowane lub proponowane, w tym ograniczające negatywne skutki

Wczesne ostrzeżenie (KSC) — art. 12 ust. 1 KSC

- [ ] dane podmiotu: firma, numer z rejestru, siedziba i adres
- [ ] osoba zgłaszająca: imię, nazwisko, telefon i e-mail służbowy
- [ ] osoba uprawniona do wyjaśnień: imię, nazwisko, telefon i e-mail służbowy
- [ ] moment wystąpienia i wykrycia incydentu oraz czas jego trwania
- [ ] czy incydent wywołano działaniem bezprawnym lub w złej wierze — jeżeli da się to ocenić
- [ ] czy incydent dotyczy innych państw członkowskich UE
- [ ] oznaczenie informacji stanowiących tajemnice prawnie chronione, w tym tajemnicę przedsiębiorstwa (art. 12 ust. 8)

Zgłoszenie incydentu poważnego (KSC) — art. 12 ust. 3 KSC

- [ ] wpływ na usługę: która usługa, liczba użytkowników, zasięg geograficzny i wpływ na inne podmioty
- [ ] przyczyny, przebieg i prawdopodobne skutki dla systemów lub usług
- [ ] podjęte działania zapobiegawcze
- [ ] podjęte działania naprawcze
- [ ] aktualizacja danych z wczesnego ostrzeżenia, jeżeli się zmieniły
- [ ] oznaczenie informacji stanowiących tajemnice prawnie chronione, w tym tajemnicę przedsiębiorstwa (art. 12 ust. 8)

Sprawozdanie końcowe (KSC) — art. 12a KSC

- [ ] szczegółowy opis incydentu, w tym zakłócenia i szkody
- [ ] rodzaj zagrożenia lub prawdopodobna przyczyna
- [ ] zastosowane i wdrażane środki ograniczające ryzyko
- [ ] skutki transgraniczne, jeżeli wystąpiły

Karta zdarzenia

Rodzaj	Zaszyfrowane pliki, żądanie okupu
Wykryto	cz 12.11.2026, godz. 15:02
Stwierdzono naruszenie danych	cz 12.11.2026, godz. 17:02
Rola wobec danych	administrator
Status KSC według odpowiedzi	podmiot kluczowy
Telekomunikacja / podmiot krytyczny	nie
Operator usługi kluczowej przed 3.04.2026	tak
Podmiot kluczowy lub ważny od	nie dotyczy (operator usługi kluczowej)
Właściwy CSIRT według odpowiedzi	CSIRT NASK
Sektor finansowy	nie
Dane osobowe	tak (kontaktowe, PESEL lub dowód, finansowe)
Liczba osób	101–1000
Dane zaszyfrowane przed zdarzeniem, klucz bezpieczny	nie dotyczy tego rodzaju zdarzenia
Wpływ na usługę	usługa nadal nie działa albo działa gorzej
Straty finansowe albo szkoda dla innych	nie wiadomo
Działanie celowe	tak

Do uzupełnienia w Twojej dokumentacji

Narzędzie nie pyta o nazwę Twojej organizacji. Te pola uzupełnij sam, zanim dołączysz plan do akt sprawy.

Organizacja	
Kto zauważył zdarzenie	
Kiedy incydent wystąpił (jeśli wcześniej, niż go wykryto)	
Kto i kiedy stwierdził naruszenie danych	
Kto podjął decyzję o zgłoszeniu albo o jego braku, kiedy i dlaczego	
Numer zgłoszenia w S46 / u Prezesa UODO	
Wersja planu (kolejny numer; zastępuje plan z dnia)	
Sporządził (imię, nazwisko, data)	
Zweryfikował — IOD lub doradca (data, zmiany wobec wyniku narzędzia)	
Zatwierdził (imię, nazwisko, data, podpis)	

JAK KORZYSTAĆ Z PLANU

Plan powstał na Twoim urządzeniu

Powstał w Twojej przeglądarce z odpowiedzi, które podałeś, i nie został nigdzie wysłany. Przechowuj go jak dokumentację incydentu, bo opisuje zdarzenie w Twojej organizacji. Gdy dowiesz się czegoś nowego, wróć do narzędzia na incydent.lablogic.pl, zmień odpowiedzi i pobierz nową wersję.

Podstawy prawne — brzmienie przepisów

Fragmenty przepisów, na których opiera się wynik. Wielokropek w nawiasie oznacza skrót. Pełny tekst znajdziesz w aktach wymienionych niżej. Godziny w planie podano według czasu ustawionego na urządzeniu.

art. 11 ust. 1 pkt 4 KSC

„zgłasza wczesne ostrzeżenie o incydencie poważnym niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do właściwego CSIRT sektorowego”

art. 11 ust. 2 KSC

„Wczesne ostrzeżenie […] są przekazywane za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1.”

art. 12 ust. 1 KSC

„Wczesne ostrzeżenie, o którym mowa w art. 11 ust. 1 pkt 4, zawiera: 1) dane podmiotu zgłaszającego […]; 4) wskazanie momentu wystąpienia i wykrycia incydentu poważnego oraz czas jego trwania; 5) wskazanie, czy incydent poważny został wywołany działaniem bezprawnym lub działaniem w złej wierze, jeżeli możliwe jest dokonanie takiej oceny; 6) określenie, czy incydent dotyczy innych państw członkowskich Unii Europejskiej”

art. 12 ust. 2 KSC
„CSIRT sektorowy nie później niż w ciągu 24 godzin przekazuje podmiotowi zgłaszającemu wytyczne dotyczące wdrożenia środków lub udziela dodatkowego wsparcia technicznego”

art. 44 ust. 1 ustawy z 23.01.2026 (Dz.U. 2026 poz. 252)
„Do dnia wydania komunikatu, o którym mowa w art. 42 ust. 2 […], podmioty kluczowe lub podmioty ważne zgłaszają incydenty poważne zgodnie z art. 11–12b […] do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV.”

art. 2 pkt 7 KSC
„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”

art. 11 ust. 1 pkt 4a KSC
„zgłasza incydent poważny niezwłocznie, nie później niż w ciągu 72 godzin od momentu jego wykrycia, do właściwego CSIRT sektorowego”

art. 12 ust. 3 KSC
„Zgłoszenie, o którym mowa w art. 11 ust. 1 pkt 4a, zawiera: 1) opis wpływu incydentu poważnego na świadczenie usługi […]; 2) opis przyczyn tego incydentu, sposób jego przebiegu oraz prawdopodobne skutki oddziaływania na systemy informacyjne lub świadczone usługi; 3) informacje o podjętych działaniach zapobiegawczych; 4) informacje o podjętych działaniach naprawczych; 5) aktualizację informacji, o których mowa w ust. 1, jeżeli nastąpiła ich zmiana”

art. 12 ust. 5 KSC
„Podmiot kluczowy lub podmiot ważny przekazuje informacje znane mu w chwili dokonywania zgłoszenia, o którym mowa w art. 11 ust. 1 pkt 4a, które uzupełnia w trakcie obsługi incydentu poważnego.”

art. 34 ust. 1 RODO
„Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.”

art. 34 ust. 2 RODO
„jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d)”

art. 34 ust. 3 lit. a–c RODO
„Zawiadomienie […] nie jest wymagane […]: a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony […], w szczególności środki takie jak szyfrowanie […]; b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka […]; c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat […]”

art. 33 ust. 1 RODO
„administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu […], chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.”

art. 33 ust. 3 RODO
„Zgłoszenie, o którym mowa w ust. 1, musi co najmniej: a) opisywać charakter naruszenia ochrony danych osobowych […]; b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego […]; c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych; d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu”

art. 33 ust. 4 RODO
„Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.”

art. 46 ust. 1 pkt 7 KSC
„dokonywanie zgłoszenia naruszenia ochrony danych osobowych, o którym mowa w art. 33 rozporządzenia 2016/679 […], przez podmioty kluczowe lub podmioty ważne”

art. 33 ust. 5 RODO
„Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.”

art. 11 ust. 1 pkt 4b i 4c KSC
„przekazuje, na wniosek właściwego CSIRT sektorowego, sprawozdanie okresowe [...]; przekazuje [...] sprawozdanie końcowe z obsługi incydentu poważnego, nie później niż w ciągu miesiąca od dnia zgłoszenia, o którym mowa w pkt 4a”

art. 12b ust. 1 i 2 KSC
„W przypadku gdy obsługa incydentu poważnego nie zakończyła się w terminie składania sprawozdania końcowego [...] przekazuje [...] sprawozdanie z postępu obsługi tego incydentu [...] sprawozdanie końcowe nie później niż w ciągu miesiąca od zakończenia obsługi incydentu poważnego.”

art. 12a KSC
„Sprawozdanie końcowe, o którym mowa w art. 11 ust. 1 pkt 4c, zawiera: 1) szczegółowy opis incydentu poważnego, w tym spowodowane zakłócenia i szkody; 2) rodzaj zagrożenia lub przyczynę, która prawdopodobnie była źródłem incydentu; 3) zastosowane i wdrażane środki ograniczające ryzyko; 4) transgraniczne skutki incydentu, jeżeli wystąpiły”

art. 11 ust. 2b KSC
„Podmiot kluczowy lub podmiot ważny informuje użytkowników swoich usług o incydencie poważnym, jeżeli ma on niekorzystny wpływ na świadczenie tych usług.”

art. 26 ust. 6 pkt 1 lit. j KSC
„podmioty kluczowe lub podmioty ważne, z wyjątkiem wymienionych w ust. 5 i 7”

art. 26 ust. 7 pkt 6 KSC
„podmioty, o których mowa w ust. 6, jeżeli incydent dotyczy systemów teleinformatycznych lub sieci teleinformatycznych objętych wykazem”

art. 7 ust. 2 pkt 21 i 22 KSC
„Wykaz zawiera: [...] 21) wskazanie CSIRT sektorowego właściwego dla podmiotu kluczowego lub podmiotu ważnego; 22) wskazanie CSIRT MON, CSIRT NASK lub CSIRT GOV właściwego dla podmiotu kluczowego lub podmiotu ważnego”

art. 12 ust. 2 zdanie drugie KSC
„a w przypadku incydentu poważnego wyczerpującego znamiona przestępstwa również informacje o sposobie zgłoszenia organom ścigania”

Akty i materiały

- Rozporządzenie (UE) 2016/679 (RODO)
  eur-lex.europa.eu/eli/reg/2016/679/oj/pol
- Ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa
  isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560
- Ustawa z 23 stycznia 2026 r. o zmianie ustawy o KSC oraz niektórych innych ustaw
  isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20260000252
- Komunikat Prezesa UODO z 3.11.2026 „Naruszenie ochrony danych osobowych rekomendujemy zgłosić przez S46”
  uodo.gov.pl/pl/138/4650
- Wytyczne EROD 9/2022 w sprawie zgłaszania naruszeń ochrony danych osobowych, wersja 2.0
  www.edpb.europa.eu/documents/guideline/guidelines-92022-on-personal-data-breach-notification-under-gdpr_pl

LABLOGIC · RODO I NIS2/KSC

Jeśli potrzebujesz wsparcia

Michał Rutkowski, inspektor ochrony danych i doradca NIS2/KSC. Pomagam firmom i instytucjom przejść przez incydent, a potem uporządkować ochronę danych i cyberbezpieczeństwo.

Obsługa incydentu i naruszenia

Kwalifikacja zdarzenia, zgłoszenia do CSIRT i Prezesa UODO, zawiadomienia osób, rejestr naruszeń i sprawozdanie końcowe. Zaczynam od rozmowy telefonicznej.
lablogic.pl/incydenty-i-naruszenia

Zewnętrzny inspektor ochrony danych

Stałe pełnienie funkcji IOD: bieżące doradztwo, rejestry, żądania osób i kontakt z Prezesem UODO.
lablogic.pl/zewnetrzny-iod-dpo

Wdrożenie NIS2 i KSC

Ustalenie statusu organizacji, wniosek o wpis do wykazu, system zarządzania bezpieczeństwem informacji i procedura obsługi incydentów.
lablogic.pl/nis2-ksc

Szkolenia i ćwiczenia

Szkolenia dla kierownictwa i pracowników oraz ćwiczenia z obsługi incydentu na scenariuszu podobnym do Twojego.
lablogic.pl/szkolenia-rodo-nis2

Przed rozmową przygotuj

- Ten plan i godziny wykrycia oraz stwierdzenia naruszenia.
- Listę systemów i usług, które nie działają.
- Informację, czy kopie zapasowe są całe i odłączone od sieci.
- Kontakt do osoby, która może podejmować decyzje w organizacji.

Zadzwoń albo napisz

+48 504 920 875

m.rutkowski@lablogic.pl · lablogic.pl

Telefon odbieram w dni robocze w godz. 8–16. Poza tymi godzinami zostaw numer w formularzu na incydent.lablogic.pl — oddzwonię w najbliższym dniu roboczym. Pierwsza rozmowa jest bezpłatna i do niczego nie zobowiązuje.

Wstępna kwalifikacja z narzędzia LabLogic (wersja 1.14 z 12.11.2026, stan prawny na 11.11.2026). Nie jest opinią prawną. Wynik zależy od odpowiedzi, które podałeś. Terminy liczone są od godzin, które podałeś.
LabLogic Consulting Michał Rutkowski · ul. Wolności 15/6, 81-327 Gdynia · NIP 958-097-21-14 · REGON 193029560