

Nazwa projektu Rozporządzenie Rady Ministrów w sprawie progów uznania incydentu za poważny Ministerstwo wiodące i ministerstwa współpracujące Ministerstwo Cyfryzacji Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu Paweł Olszewski, Sekretarz Stanu w Ministerstwie Cyfryzacji Kontakt do opiekuna merytorycznego projektu Łukasz Wojewoda, dyrektor Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji, Marcin Wysocki, zastępca dyrektora Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji, e-mail: sekretariat.dc@cyfra.gov.pl tel. + 48 22 245 59 22	Data sporządzenia 02.09.2026 Źródło: art. 11 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20, 252, 815 i 1003) Nr w wykazie prac legislacyjnych i programowych Rady Ministrów: RD236
--	---

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, zwana dalej „ustawą”, nakłada na podmioty kluczowe oraz podmioty ważne obowiązek zgłaszania incydentów poważnych za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ustawy, do właściwego zespołu CSIRT sektorowego w terminie 72 godzin od momentu wykrycia incydentu. Incydent poważny został zdefiniowany w ustawie jako incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi przez podmiot kluczowy lub podmiot ważny, może powodować straty finansowe dla tego podmiotu lub incydent ten wpływa na inne osoby fizyczne, osoby prawne, jednostki organizacyjne nieposiadające osobowości prawnej przez wywołanie poważnej szkody materialnej lub niematerialnej. Jednocześnie ustawa przewiduje, że progi uznania incydentu za poważny zostaną ustalone w rozporządzeniu Rady Ministrów, wydanym na podstawie art. 11 ust. 4 ustawy. Określenie progów uznania incydentu za poważny umożliwi podmiotom z danego sektora ustalenie momentu, w którym powstaje obowiązek zgłoszenia incydentu poważnego do właściwego zespołu CSIRT sektorowego. Jest to również istotne, gdyż brak zgłoszenia incydentu poważnego przez podmiot kluczowy i podmiot ważny spowoduje konieczność nałożenia administracyjnej kary pieniężnej na dany podmiot. Ponadto incydenty poważne negatywnie oddziałują nie tylko na sam podmiot kluczowy lub podmiot ważny, w którym incydent wystąpił, ale też w istotny sposób oddziałują na użytkowników usług danego podmiotu oraz na społeczeństwo i gospodarkę. Stąd konieczne jest, aby incydenty poważne były zgłaszane do CSIRT sektorowych, aby mogły one zareagować na incydent i wesprzeć podmiot kluczowy lub podmiot ważny w jego obsłudze. Informacja o incydencie poważnym jest również istotna dla CSIRT-ów poziomu krajowego, które na bieżąco prowadzą szacowanie ryzyka na poziomie krajowym. Prawidłowe ustalenie progów uznania incydentu za incydent poważny z jednej strony powinno uwzględnić zdarzenia rzeczywiście niebezpieczne, z drugiej strony progi nie powinny dotyczyć zdarzeń, które mają nikły wpływ na funkcjonowanie podmiotu.

Dotychczas obowiązujące rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny (Dz. U. poz. 2180) zostało utrzymane w mocy do czasu wydania nowego rozporządzenia, nie dłużej niż przez 12 miesięcy od dnia wejścia w życie ustawy z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz. U. poz. 252). Jest to spójne z równocześnie trwającym okresem dostosowawczym dla podmiotów kluczowych i podmiotów ważnych, które do dnia 3 kwietnia 2027 r. mają podjąć niezbędne czynności techniczne i organizacyjne w celu stosowania ustawy. Dotychczas obowiązujące rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny nie obejmuje wszystkich nowych sektorów dodanych ustawą

z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, z tego powodu konieczne jest wydanie rozporządzenia, które określi nowe progi incydentu poważnego.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Podmioty kluczowe i podmioty ważne identyfikując incydent i rejestrując go, będą dokonywały klasyfikacji incydentu jako poważnego na podstawie progów uznawania incydentu za poważny. Progi te, w zależności od rodzaju zdarzenia, określają liczbę użytkowników, których dotyczy zakłócenie świadczenia usługi, czas oddziaływania incydentu na świadczoną usługę, zasięg geograficzny obszaru, którego dotyczy ten incydent lub inne czynniki charakterystyczne dla danego sektora lub podsektora.

Projektowane rozporządzenie zastępuje dotychczas obowiązujące rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny. W stosunku do obowiązujących przepisów wprowadza ono zmiany polegające w szczególności na dostosowaniu progów do aktualnych realiów funkcjonowania usług oraz wymagań wynikających z prawa Unii Europejskiej, w tym dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii Europejskiej, zmieniającą rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80).

Rozporządzenie określa progi uznania incydentu za poważny dla następujących sektorów i podsektorów:

Sektor	Podsektor (jeśli występuje)
Energia	Wydobywanie kopalin
	Energia elektryczna
	Ciepło
	Ropa i paliwa
	Gaz
	Energetyka jądrowa
	Wodór
Transport	Transport lotniczy
	Transport kolejowy
	Transport wodny
	Transport drogowy
Ochrona zdrowia	Udzielanie świadczeń zdrowotnych i zdrowie publiczne
	Produkcja i dystrybucja substancji czynnych, produktów leczniczych i wyrobów medycznych
Zaopatrzenie w wodę pitną i jej dystrybucja	
Zbiorowe odprowadzanie ścieków	
Infrastruktura cyfrowa	Infrastruktura cyfrowa z wyłączeniem komunikacji elektronicznej
	Komunikacja elektroniczna
Przestrzeń kosmiczna	
Podmioty publiczne	
Usługi pocztowe	
Inwestycje energetyki jądrowej	
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
Produkcja, wytwarzanie i dystrybucja chemikaliów	
Produkcja, przetwarzanie i dystrybucja żywności	
Produkcja¹	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
Badania naukowe	
Projektowane rozporządzenia oparto na dotychczasowym rozporządzeniu Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny w zakresie w jakim dotyczy dotychczasowych sektorów. W pozostałym zakresie uzupełniono progi uznania incydentu za poważny dla nowych sektorów. Przygotowując projektowane rozporządzenie uwzględniono fakt, że dla niektórych podmiotów kluczowych i podmiotów ważnych progi incydentu zostały ustalone w rozporządzeniu wykonawczym Komisji (UE) 2024/2690 z dnia 17 października 2024 r. ustanawiającym zasady stosowania dyrektywy (UE) 2022/2555 w odniesieniu do wymogów technicznych i metodycznych dotyczących środków zarządzania ryzykiem w cyberbezpieczeństwie oraz doprecyzowujące przypadki, w których incydent uznaje się za poważny w 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 i platform usług sieci społecznościowych oraz dostawców usług zaufania (Dz. Urz. UE L	

¹⁾ Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii Europejskiej, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80) odwołuje się w sektorze produkcji do klasyfikacji NACE. Podmiotem ważnym będą następujące rodzaje podmiotów:

- 1) Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 26 klasyfikacji NACE Rev. 2 – Produkcja komputerów, wyrobów elektronicznych i optycznych;
- 2) Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 27 klasyfikacji NACE Rev. 2 – Produkcja urządzeń elektrycznych;
- 3) Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 28 klasyfikacji NACE Rev. 2 – Produkcja maszyn i urządzeń, gdzie indziej niesklasyfikowana;
- 4) Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 29 klasyfikacji NACE Rev. 2 – Produkcja pojazdów silnikowych, produkcja przyczep i naczep;
- 5) Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 30 klasyfikacji NACE Rev. 2 – Produkcja pozostałego sprzętu transportowego.

Należy przy tym spełnić pozostałe przesłanki klasyfikacji jako podmiot ważny, takie jak kryteria wielkościowe i kryteria jurysdykcji polskiej.

Skonsolidowany tekst tej klasyfikacji wraz z dokładną informacją o podklasach jest dostępny pod adresem: <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:02006R1893-20250101>.

2024/2690 z 18.10.2024, z późn. zm.), zwanym dalej „rozporządzeniem wykonawczym”. Dlatego nie wskazano progów incydentów dla następujących rodzajów podmiotów:

Sektor	Rodzaj podmiotu
Infrastruktura cyfrowa	Dostawca usług DNS, z wyłączeniem operatorów głównych serwerów nazw.
	Rejestr nazw domen najwyższego poziomu (TLD).
	Dostawca chmury obliczeniowej.
	Dostawca usług centrum przetwarzania danych.
	Dostawca sieci dostarczania treści.
	Dostawca usług zaufania.
Zarządzanie usługami ICT	Dostawca usług zarządzanych.
	Dostawca usług zarządzanych w zakresie cyberbezpieczeństwa.
Dostawcy usług cyfrowych	Dostawca internetowej platformy handlowej.
	Dostawca wyszukiwarki internetowej.
	Dostawca platformy sieci usług społecznościowych.

W zakresie sektora „Infrastruktury cyfrowej” ustalono progi dla pozostałych podmiotów z tego sektora, którym Komisja Europejska nie ustaliła progów incydentów ww. rozporządzeniu wykonawczym, to jest dla dostawcy punktu wymiany ruchu internetowego, podmiotu świadczącego usługę rejestracji nazw domen oraz przedsiębiorcy komunikacji elektronicznej.

Pominięto również ustalenie progów uznania incydentu za poważny dla sektora bankowości i infrastruktury rynków finansowych, ponieważ progi te ustala rozporządzenie delegowane Komisji (UE) 2024/1772 z dnia 13 marca 2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do regulacyjnych standardów technicznych określających kryteria klasyfikacji incydentów związanych z ICT i cyberzagrożeń, progi istotności i szczegółowe informacje dotyczące zgłaszania poważnych incydentów (Dz. Urz. UE L 2024/1772 z 25.06.2024).

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Z uwagi na szczegółowość regulacji odstąpiono od analizy prawnoporównawczej projektu na tle innych państw.

4. Podmioty, na które oddziałuje projekt

Obecnie trwa proces samoidentyfikacji podmiotów kluczowych oraz podmiotów ważnych, który zakończy się do dnia 3 października 2026 r. Dopiero wtedy będzie znana liczba tych podmiotów. Lista podmiotów kluczowych oraz podmiotów ważnych będzie się zmieniać w czasie ze względu na dynamikę życia gospodarczego (podmioty są tworzone, przekształcane albo likwidowane) oraz przez działania organów właściwych do spraw cyberbezpieczeństwa, które weryfikują kompletności danych w wykazie podmiotów kluczowych i podmiotów ważnych.

Grupa	Wielkość	Źródło danych	Oddziaływanie
Podmioty kluczowe i podmioty ważne z sektora energii	239	REGON Dział 35 – wytwarzanie i zaopatrywanie w energię elektryczną, gaz, parę wodną, gorącą wodę i powietrze do układów klimatyzacyjnych Dział 49 – Transport lądowy oraz transport rurociągowy Podklasa 49.50.A Transport rurociągami paliw gazowych	Określenie kryteriów uznania incydentu za incydent poważny umożliwi podmiotom z danego sektora ustalenie momentu, w którym powstaje obowiązek zgłoszenia incydentu do właściwego zespołu CSIRT sektorowego. Dzięki temu podmioty będą mogły dostosować wewnętrzne procedury

			zgłaszania incydentów do projektowanych rozwiązań.
Podmioty kluczowe i podmioty ważne z podsektora komunikacji elektronicznej	Co najmniej 3784	Rejestr przedsiębiorców telekomunikacyjnych; w zakresie podmiotów świadczących usługę komunikacji interpersonalnej niewykorzystującej numerów (OTT-1) – rejestr przedsiębiorców telekomunikacyjnych nie obejmuje tego rodzaju podmiotów	Określenie kryteriów uznania incydentu za incydent poważny umożliwi podmiotom z danego sektora ustalenie momentu, w którym powstaje obowiązek zgłoszenia incydentu do właściwego zespołu CSIRT sektorowego. Dzięki temu podmioty będą mogły dostosować wewnętrzne procedury zgłaszania incydentów do projektowanych rozwiązań.
Podmioty kluczowe i podmioty ważne z sektora zaopatrzenia w wodę pitną i jej dystrybucja	269	REGON PKD Sekcja E dział 36 podklasa 3600Z Pobór, uzdatnianie i dostarczanie wody	Określenie kryteriów uznania incydentu za incydent poważny umożliwi podmiotom z danego sektora ustalenie momentu, w którym powstaje obowiązek zgłoszenia incydentu do właściwego zespołu CSIRT sektorowego. Dzięki temu podmioty będą mogły dostosować wewnętrzne procedury zgłaszania incydentów do projektowanych rozwiązań.
Podmioty kluczowe i podmioty ważne z sektora zbiorowego odprowadzania ścieków	99	REGON PKD sekcja E dział 37 podklasa 3700z Odprowadzanie i oczyszczanie ścieków	Określenie kryteriów uznania incydentu za incydent poważny umożliwi podmiotom z danego sektora ustalenie momentu, w którym powstaje obowiązek zgłoszenia incydentu do właściwego zespołu CSIRT sektorowego. Dzięki temu podmioty będą mogły dostosować wewnętrzne procedury zgłaszania incydentów do projektowanych rozwiązań.
Podmioty kluczowe i podmioty ważne – dostawcy punktu wymiany ruchu internetowego	kilkanaście podmiotów	Szacunki własne Ministerstwa Cyfryzacji	Określenie kryteriów uznania incydentu za incydent poważny umożliwi podmiotom z danego sektora ustalenie momentu, w którym powstaje

			obowiązek zgłoszenia incydentu do właściwego zespołu CSIRT sektorowego. Dzięki temu podmioty będą mogły dostosować wewnętrzne procedury zgłaszania incydentów do projektowanych rozwiązań.
Podmioty świadczące usługi rejestracji nazw domen	198	RAPORT ROCZNY NASK-BIP Rynek nazw domen. pl https://www.dns.pl/sites/default/files/2026-04/Raport-roczny-2025.pdf	Określenie kryteriów uznania incydentu za incydent poważny umożliwi podmiotom świadczącym usługi rejestracji nazw domen ustalenie momentu, w którym powstaje obowiązek zgłoszenia incydentu do właściwego zespołu CSIRT sektorowego. Dzięki temu podmioty będą mogły dostosować wewnętrzne procedury zgłaszania incydentów do projektowanych rozwiązań.
Podmioty kluczowe i podmioty ważne z sektora podmiotów publicznych	co najmniej 27 905	REGON	Określenie kryteriów uznania incydentu za incydent poważny umożliwi podmiotom z danego sektora ustalenie momentu, w którym powstaje obowiązek zgłoszenia incydentu do właściwego zespołu CSIRT sektorowego. Dzięki temu podmioty będą mogły dostosować wewnętrzne procedury zgłaszania incydentów do projektowanych rozwiązań.
Podmioty ważne z sektora poczty	280	Rejestr operatorów pocztowych	Określenie kryteriów uznania incydentu za incydent poważny umożliwi podmiotom z danego sektora ustalenie momentu, w którym powstaje obowiązek zgłoszenia incydentu do właściwego zespołu CSIRT sektorowego. Dzięki temu podmioty będą mogły dostosować wewnętrzne procedury

			zgłaszania incydentów do projektowanych rozwiązań.
Podmioty ważne z sektora inwestycji energetyki jądrowej	1	Szacunki własne Ministerstwa Cyfryzacji	Określenie kryteriów uznania incyduentu za incydent poważny umożliwi podmiotom z danego sektora ustalenie momentu, w którym powstaje obowiązek zgłoszenia incyduentu do właściwego zespołu CSIRT sektorowego. Dzięki temu podmioty będą mogły dostosować wewnętrzne procedury zgłaszania incydentów do projektowanych rozwiązań.
Podmioty ważne z sektora gospodarowania odpadami	276	REGON PKD: Sekcja E dział 38 podklasa 3811Z Zbieranie odpadów innych niż niebezpieczne Sekcja E dział 38 podklasa 3812Z Zbieranie odpadów niebezpiecznych Sekcja E dział 38 podklasa 3821Z Obróbka i usuwanie odpadów innych niż niebezpieczne Sekcja E dział 38 podklasa 3822Z Przetwarzanie i unieszkodliwianie odpadów niebezpiecznych Sekcja E dział 38 podklasa 3831Z Demontaż wyrobów zużytych Sekcja E dział 38 podklasa 3832Z Odzysk surowców z materiałów segregowanych Sekcja E dział 38 podklasa 3900Z Działalność związana z rekultywacją i pozostała działalność usługowa związana z gospodarką odpadami	Określenie kryteriów uznania incyduentu za incydent poważny umożliwi podmiotom z danego sektora ustalenie momentu, w którym powstaje obowiązek zgłoszenia incyduentu do właściwego zespołu CSIRT sektorowego. Dzięki temu podmioty będą mogły dostosować wewnętrzne procedury zgłaszania incydentów do projektowanych rozwiązań.
Podmioty kluczowe i podmioty ważne z sektora produkcja,	1139	REGON PKD:	Określenie kryteriów uznania incyduentu za incydent poważny umożliwi podmiotom z danego sektora

przetwarzanie i dystrybucja żywności		sekcja C dział 10 Produkcja artykułów spożywczych Seksja H dział 46 podklasa 4631Z Sprzedaż hurtowa owoców i warzyw Seksja H dział 46 podklasa 4632Z Sprzedaż hurtowa mięsa i wyrobów z mięsa Seksja H dział 46 podklasa 4633Z Sprzedaż hurtowa mleka, wyrobów mleczarskich, jaj, olejów i tłuszczów jadalnych Seksja H dział 46 podklasa 4634A Sprzedaż hurtowa napojów alkoholowych Seksja H dział 46 podklasa 4634B Sprzedaż hurtowa napojów bezalkoholowych	ustalenie momentu, w którym powstaje obowiązek zgłoszenia incyduentu do właściwego zespołu CSIRT sektorowego. Dzięki temu podmioty będą mogły dostosować wewnętrzne procedury zgłaszania incydentów do projektowanych rozwiązań.
Podmioty kluczowe i podmioty ważne z sektora produkcja, wytwarzanie i dystrybucja chemikaliów	205	REGON PKD sekcja C dział 20 Produkcja chemikaliów i wyrobów chemicznych	Określenie kryteriów uznania incyduentu za incydent poważny umożliwi podmiotom z danego sektora ustalenie momentu, w którym powstaje obowiązek zgłoszenia incyduentu do właściwego zespołu CSIRT sektorowego. Dzięki temu podmioty będą mogły dostosować wewnętrzne procedury zgłaszania incydentów do projektowanych rozwiązań.
Podmioty kluczowe i podmioty ważne z podsektora produkcji wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro	43	REGON PKD sekcja C dział 32 podklasa 3250z	Określenie kryteriów uznania incyduentu za incydent poważny umożliwi podmiotom z danego sektora ustalenie momentu, w którym powstaje obowiązek zgłoszenia incyduentu do właściwego zespołu CSIRT sektorowego.
Podmioty kluczowe i podmioty ważne z sektora produkcji, z wyłączeniem wyrobów medycznych	1074	REGON PKD sekcja C dział 26 Produkcja komputerów, wyrobów elektronicznych i optycznych	Określenie kryteriów uznania incyduentu za incydent poważny umożliwi podmiotom z danego sektora ustalenie momentu, w którym powstaje obowiązek zgłoszenia

		PKD sekcja C dział 27 Produkcja urządzeń elektrycznych PKD sekcja C dział 28 Produkcja maszyn i urządzeń, gdzie indziej niesklasyfikowana PKD sekcja C dział 29 Produkcja pojazdów samochodowych, przyczep i naczep, z wyłączeniem motocykli PKD sekcja C dział 30 Produkcja pozostałego sprzętu transportowego	incydentu do właściwego zespołu CSIRT sektorowego. Dzięki temu podmioty będą mogły dostosować wewnętrzne procedury zgłaszania incydentów do projektowanych rozwiązań.	
Podmioty z sektora naukowych	ważne badań	167	REGON PKD sekcja M dział 72 podklasa: 7219Z Badania naukowe i prace rozwojowe w dziedzinie pozostałych nauk przyrodniczych i technicznych 7220Z Badania naukowe i prace rozwojowe w dziedzinie nauk społecznych i humanistycznych	Określenie kryteriów uznania incydentu za incydent poważny umożliwi podmiotom z danego sektora ustalenie momentu, w którym powstaje obowiązek zgłoszenia incydentu do właściwego zespołu CSIRT sektorowego. Dzięki temu podmioty będą mogły dostosować wewnętrzne procedury zgłaszania incydentów do projektowanych rozwiązań.
CSIRT MON, CSIRT NASK, CSIRT GOV		3	Informacje ogólnodostępne	Prawidłowe określenie kryteriów uznania incydentu
CSIRT sektorowe	co najmniej 10 podmiotów obejmujących wszystkie sektory na podstawie ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa	Informacje ogólnodostępne	za incydent poważny umożliwi identyfikację i zgłaszanie incydentów w istotny sposób wpływających na społeczeństwo i gospodarkę do zespołów CSIRT, które następnie będą mogły podjąć działania w celu ich obsługi i ograniczenia skutków.	

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Stosownie do art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingsowej w procesie stanowienia prawa (Dz. U. z 2026 r. poz. 936) projekt rozporządzenia został udostępniony w Biuletynie Informacji Publicznej Ministerstwa Cyfryzacji. Ponadto, zgodnie z § 52 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2026 r. poz. 404), projekt rozporządzenia został udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.

W ramach 21-dniowych konsultacji publicznych projekt rozporządzenia otrzymały następujące podmioty:

- 1) 17 53C – Stowarzyszenie Na Rzecz Cyberbezpieczeństwa;
- 2) Amerykańska Izba Handlowa w Polsce;
- 3) Centrum Łukasiewicz – Sieć Badawcza Łukasiewicz;
- 4) European AI Forum;
- 5) FAIR MARKET INSTITUTE;
- 6) Federacja Konsumentów;
- 7) Fundacja Bezpieczna Cyberprzestrzeń;
- 8) Fundacja Centrum Bezpieczeństwa;
- 9) Fundacja Fabian Digital;
- 10) Fundacja Hackerspace Kraków
- 11) Fundacja im. Kazimierza Pułaskiego;
- 12) Fundacja Instytut Cyberbezpieczeństwa;
- 13) Fundacja Open Allies;
- 14) Fundacja OPOR;
- 15) Fundacja Rozwoju Obrotu Bezgotówkowego;
- 16) Green Rev Institute;
- 17) Instytut Kolejnictwa;
- 18) Internet Society Poland;
- 19) ISAC-GIG;
- 20) ISAC-JST;
- 21) ISAC-Kolej;
- 22) Izba Gospodarcza Lubuskich Winnic;
- 23) Izba Gospodarcza Medycyna Polska;
- 24) Izba Gospodarcza Urzędów OZE;
- 25) Izba Gospodarcza Właścicieli Punktów Aptecznych i Aptek;
- 26) Izba Gospodarcza Wodociągi Polskie;
- 27) Izba Gospodarczo Handlowa;
- 28) Izba Gospodarki Elektronicznej;
- 29) Izba Recyklingu i Odzysku Odpadów;
- 30) Konferencja Rektorów Akademickich Szkół Polskich;
- 31) Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji;
- 32) Krajowa Izba Gospodarcza;
- 33) Krajowa Izba Gospodarki Cyfrowej;
- 34) Krajowa Izba Kłastrów Energii i OZE;
- 35) Krajowa Izba Komunikacji Ethernetowej;
- 36) Krajowa Izba Producentów Ryb;
- 37) Krajowi Producenci Leków – PZPPF;
- 38) Krajowy Związek Banków Spółdzielczych;
- 39) Morskie Centrum Cyberbezpieczeństwa;
- 40) Naczelna Organizacja Techniczna;
- 41) Naczelna Rada Zrzeszeń Handlu i Usług;
- 42) Narodowy Instytut Cyberbezpieczeństwa;
- 43) Ogólnopolska Izba Gospodarcza Producentów Mebli;
- 44) Ogólnopolska Izba Gospodarcza Wyrobów Medycznych POLMED;
- 45) Ogólnopolski Związek Pracodawców – Niepublicznych Operatorów Poczтовых;
- 46) Polska Chmura – Związek Pracodawców;
- 47) Polska Federacja Producentów Żywności;

- 48) Polska Fundacja Przemysłu Kosmicznego;
- 49) Polska Izba Gazu Płynnego;
- 50) Polska Izba Gospodarcza Elektrotechniki;
- 51) Polska Izba Gospodarcza Energetyki Odnawialnej i Rozproszonej;
- 52) Polska Izba Gospodarcza Maszyn i Urządzeń Rolniczych;
- 53) Polska Izba Gospodarki Odpadami;
- 54) Polska Izba Handlu;
- 55) Polska Izba Informatyki i Telekomunikacji;
- 56) Polska Izba Informatyki Medycznej;
- 57) Polska Izba Kolei;
- 58) Polska Izba Komunikacji Elektronicznej;
- 59) Polska Izba Mleka;
- 60) Polska Izba Morskiej Energetyki Wiatrowej;
- 61) Polska Izba Motoryzacji;
- 62) Polska Izba Odzysku i Recyklingu Opakowań;
- 63) Polska Izba Producentów na Rzecz Obronności Kraju;
- 64) Polska Izba Przemysłu Chemicznego;
- 65) Polska Izba Przemysłu Farmaceutycznego i WYROBÓW MEDYCZNYCH „Polfarmed”;
- 66) Polska Izba Przemysłu Jachtowego i Sportów Wodnych: Polboat;
- 67) Polska Izba Wodoru;
- 68) Polska Izba Żywności Ekologicznej;
- 69) Polska Organizacja Handlu i Dystrybucji;
- 70) Polska Organizacja Przemysłu i Handlu Naftowego;
- 71) Polska Rada Biznesu;
- 72) Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland;
- 73) Polskie Centrum Badań i Certyfikacji S.A.;
- 74) Polskie Stowarzyszenie Energetyki Wiatrowej;
- 75) Polskie Stowarzyszenie Fotowoltaiki i Magazynowania Energii;
- 76) Polskie Towarzystwo Informatyczne;
- 77) Polskiej Izby Makaronu;
- 78) Polsko-Chińska Główna Izba Gospodarcza;
- 79) Porozumienie Zielonogórskie;
- 80) SoDA – Organizacja Pracodawców Usług IT;
- 81) Sektorowa Rada do spraw Kompetencji – Telekomunikacja i Cyberbezpieczeństwo;
- 82) Skandynawska–Polska Izba Gospodarcza;
- 83) Stowarzyszenie Absolwentów Studiów Cyberbezpieczeństwa MBA;
- 84) Stowarzyszenie Bezpieczeństwo Informacji w Telekomunikacji;
- 85) Stowarzyszenie Inżynierów Telekomunikacji;
- 86) Stowarzyszenie ISACA;
- 87) Stowarzyszenie ISSA Polska;
- 88) Stowarzyszenie Polish Data Center Association;
- 89) Sudecka Izba Przemysłowo-Handlowa;
- 90) Związek Armatorów Polskich;
- 91) Związek Banków Polskich;
- 92) Związek Cyfrowa Polska;
- 93) Związek Firm Biotechnologicznych;
- 94) Związek Polskich Armatorów Śródlądowych;
- 95) Związek Pracodawców Lotnictwa i Dronów;

- 96) Związek Pracodawców Sektora Kosmicznego: Space;
- 97) Związek Pracodawców Technologii Cyfrowych Lewiatan;
- 98) Związek Telewizji Kablowych w Polsce Izba Gospodarcza.

W ramach 21-dniowego opiniowania projekt rozporządzenia został skierowany do następujących podmiotów:

- 1) Agencji Bezpieczeństwa Wewnętrznego;
- 2) Agencji Wywiadu;
- 3) Biura Bezpieczeństwa Narodowego;
- 4) Biura do spraw Substancji Chemicznych;
- 5) Biura Rady Fiskalnej;
- 6) Centralnego Biura Antykorupcyjnego;
- 7) Centralnego Biura Zwalczania Cyberprzestępczości;
- 8) Centrum e-Zdrowie;
- 9) Centrum Projektów Polska Cyfrowa;
- 10) Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni;
- 11) Eksperckiego Centrum Szkolenia Cyberbezpieczeństwa;
- 12) Instytutu Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu;
- 13) Głównego Inspektoratu Farmaceutycznego;
- 14) Głównego Inspektoratu Sanitarnego;
- 15) Głównego Inspektoratu Pracy;
- 16) Instytutu Badawczego IDEAS – Państwowego Instytutu Badawczego;
- 17) Instytutu Łączności – Państwowego Instytutu Badawczego;
- 18) Kasy Rolniczego Ubezpieczenia Społecznego;
- 19) Kancelarii Sejmu;
- 20) Kancelarii Senatu;
- 21) Kancelarii Prezydenta;
- 22) Komisji Nadzoru Finansowego;
- 23) Komendy Głównej Policji;
- 24) Krajowego Biura Wyborczego;
- 25) Krajowej Rady Radiofonii i Telewizji;
- 26) Naczelnego Sądu Administracyjnego;
- 27) Najwyższej Izby Kontroli;
- 28) Narodowego Funduszu Zdrowia;
- 29) Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego;
- 30) Polskiego Centrum Akredytacyjnego;
- 31) Polskiej Akademii Nauk;
- 32) Polskiej Agencji Kosmicznej;
- 33) Polskiego Komitetu Normalizacyjnego;
- 34) Prezesa Głównego Urzędu Statystycznego;
- 35) Prezesa Urzędu Komunikacji Elektronicznej;
- 36) Prezesa Urzędu Ochrony Danych Osobowych;
- 37) Prezesa Urzędu Ochrony Konkurencji i Konsumentów;
- 38) Prezesa Urzędu Regulacji Energetyki;
- 39) Prezesa Urzędu Transportu Kolejowego;
- 40) Prokuraturii Generalnej Rzeczypospolitej Polskiej;
- 41) Rządowego Centrum Bezpieczeństwa;
- 42) Rzecznika Finansowego;
- 43) Rzecznika Małych i Średnich Przedsiębiorców;
- 44) Rzecznika Praw Dziecka;
- 45) Rzecznika Praw Obywatelskich;
- 46) Rzecznika Praw Pacjenta;
- 47) sądów apelacyjnych;
- 48) Sądu Najwyższego;
- 49) Służby Kontrwywiadu Wojskowego;

- 50) Służby Ochrony Państwa;
- 51) Służby Wywiadu Wojskowego;
- 52) Urzędu Dozoru Technicznego;
- 53) Urzędu Lotnictwa Cywilnego;
- 54) Urzędu Patentowego Rzeczypospolitej Polskiej;
- 55) Urzędu Zamówień Publicznych;
- 56) Wyższego Urzędu Górniczego;
- 57) wojewodów;
- 58) Zakładu Ubezpieczeń Społecznych;
- 59) Zakładu Unieszkodliwiania Odpadów Promieniotwórczych.

Projekt rozporządzenia został przekazany do zaopiniowania, z terminem przedstawienia opinii w terminie 30 dni, w trybie art. 16 ustawy z dnia 23 maja 1991 r. o organizacjach pracodawców (Dz. U. z 2025 r. poz. 423) do następujących podmiotów:

- 1) Związku Pracodawców Business Centre Club;
- 2) Pracodawców Rzeczypospolitej Polskiej;
- 3) Konfederacji „Lewiatan”;
- 4) Związku Przedsiębiorców i Pracodawców;
- 5) Związku Rzemiosła Polskiego;
- 6) Polskiego Towarzystwa Gospodarczego;
- 7) Federacji Przedsiębiorców Polskich.

Projekt rozporządzenia został przekazany do zaopiniowania, z 30 dniowym terminem na zajęcie stanowiska, przez Komisję Wspólną Rządu i Samorządu Terytorialnego, gdyż dotyczy problematyki samorządu terytorialnego, w tym także kwestii określających relacje pomiędzy samorządem terytorialnym a innymi organami administracji publicznej.

Projekt rozporządzenia nie wymaga zaopiniowania:

- 1) przez Radę do Spraw Cyfryzacji, o której mowa w ustawie 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), ponieważ nie dotyczy zakresu jej działalności;
- 2) przez Radę Działalności Pożytku Publicznego oraz Radę do Spraw Dialogu z Młodym Pokoleniem, o których mowa w ustawie z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie (Dz. U. z 2025 r. poz. 1338), gdyż nie dotyczy funkcjonowania organizacji pozarządowych oraz działalności pożytku publicznego oraz wolontariatu;
- 3) przez Radę Dialogu Społecznego, o której mowa w ustawie z dnia 24 lipca 2015 r. o Radzie Dialogu Społecznego i innych instytucjach dialogu społecznego (Dz. U. z 2026 r. poz. 836), gdyż nie dotyczy zapewnienia warunków rozwoju społeczno-gospodarczego oraz zwiększenia konkurencyjności polskiej gospodarki i spójności społecznej;
- 4) związki zawodowe, w trybie art. 19 ustawy z dnia 23 maja 1991 r. o związkach zawodowych (Dz. U. z 2026 r. poz. 549), ponieważ nie dotyczy działalności związków zawodowych.

Wyniki konsultacji publicznych i opiniowania zostaną przedstawione po ich zakończeniu w raporcie z konsultacji.

6. Wpływ na sektor finansów publicznych

[illegible]

[illegible]

Źródła finansowania	Projektowane regulacje nie mają wpływu na wydatki sektora finansów publicznych.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Wydatki związane z zarządzaniem incydentami i zgłaszaniem incydentów powinny być planowane przez podmioty publiczne na bieżąco na podstawie art. 8d pkt 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Projektowane regulacje nie wprowadzają w tym zakresie zmian.

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

		Skutki						
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	Łącznie (0-10)
W ujęciu pieniężnym (w mln zł, ceny stałe z 2026 r.)	duże przedsiębiorstwa	0	0	0	0	0	0	0
	sektor mikro-, małych i średnich przedsiębiorstw	0	0	0	0	0	0	0
	rodzina, obywatele oraz gospodarstwa domowe	0	0	0	0	0	0	0
W ujęciu niepieniężnym	duże przedsiębiorstwa	Duże przedsiębiorstwa, które są podmiotami kluczowymi lub podmiotami ważnymi uzyskują informacje, kiedy mają obowiązek zgłosić incydent do CSIRT sektorowego.						
	sektor mikro-, małych i średnich przedsiębiorstw	Średnie przedsiębiorstwa, które są podmiotami kluczowymi lub podmiotami ważnymi, a także w wyjątkowych przypadkach mikro i małe przedsiębiorstwa uzyskują informacje, kiedy mają obowiązek zgłosić incydent do CSIRT sektorowego.						
	rodzina, obywatele oraz gospodarstwa domowe	Incydenty poważne wpływają na świadczenie usług dla obywateli. Prawidłowe określenie kryteriów tego rodzaju zdarzeń pozwoli na ich identyfikację oraz szybką reakcję ze strony zespołów CSIRT.						
Niemierzalne								

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Projektowane regulacje wiążą się z koniecznością dostosowania wewnętrznych procedur zarządzania i zgłaszania incydentów w podmiotach kluczowych i podmiotach ważnych. Konieczne może okazać się przeprowadzenie szkoleń dla personelu realizującego te zadania.	
8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu		
☐ nie dotyczy		
Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☒ nie ☐ nie dotyczy	
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne: Kliknij lub naciśnij tutaj, aby wprowadzić tekst.	☐ zwiększenie liczby dokumentów ☒ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne: Kliknij lub naciśnij tutaj, aby wprowadzić tekst.	
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☒ tak ☐ nie ☐ nie dotyczy	
Komentarz: Dla dotychczasowych podmiotów krajowego systemu cyberbezpieczeństwa pozostawiono dobrze im znane progi incydentu poważnego. Progi będą nowością dla tych podmiotów kluczowych i podmiotów ważnych, które do tej pory nie kwalifikowały się jako operatorzy usług kluczowych. Obowiązek zgłoszenia incydentu poważnego wynika jednak z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.		
9. Wpływ na rynek pracy		
Projektowane rozporządzenie nie ma wpływu na rynek pracy.		
10. Wpływ na pozostałe obszary		
☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ sądy powszechne, administracyjne lub wojskowe	☐ demografia ☐ mienie państwowe ☐ inne: Kliknij lub naciśnij tutaj, aby wprowadzić tekst.	☒ informatyzacja ☐ zdrowie
Omówienie wpływu	Rozporządzenie określa progi incydentów poważnych, które wymagają obligatoryjnego zgłoszenia do jednego z CSIRT sektorowych. Prawidłowe określenie tych progów umożliwi adekwatną reakcję na incydenty, które rzeczywiście mają duży wpływ na społeczeństwo i gospodarkę.	
11. Planowane wykonanie przepisów aktu prawnego		
Rozporządzenie wejdzie w życie po upływie 14 dni od dnia ogłoszenia.		
12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?		
Po dwóch latach obowiązywania rozporządzenia zostanie przeprowadzona analiza adekwatności zastosowanych w rozporządzeniu kryteriów uznania incydentu za incydent poważny.		
13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)		
Brak		