U Z A S A D N I E N I E

Projektowane rozporządzenie stanowi wykonanie upoważnienia ustawowego zawartego w 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), zwanej dalej „ustawą”, i określa progi uznania incydentu za poważny według rodzaju zdarzenia w poszczególnych sektorach i podsektorach określonych w załączniku nr 1 i 2 do ustawy. Wydając projektowane rozporządzenie Rada Ministrów uwzględnia:

1) liczbę użytkowników, których dotyczy zakłócenie świadczenia usługi;
2) czas oddziaływania incydentu na świadczoną usługę;
3) zasięg geograficzny obszaru, którego dotyczy incydent;
4) inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują.

– kierując się potrzebą zapewnienia ochrony przed zagrożeniem życia lub zdrowia ludzi, znacznymi stratami majątkowymi oraz obniżeniem jakości świadczonej usługi.

Projektowane rozporządzenie zastępuje dotychczas obowiązujące rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny (Dz. U. poz. 2180). 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, 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	
	Produkcja wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro

Produkcja[1)]	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 rozporządzenie będzie wykorzystywane przez podmioty kluczowe i podmioty ważne w procesie zgłaszania i obsługi incydentu. Podmioty kluczowe i podmioty ważne identyfikując incydent i rejestrując go, będą dokonywały klasyfikacji incydentu na podstawie progów uznawania incydentu za poważny. Przyjęte wartości progowe odzwierciedlają, w zależności od rodzaju zdarzenia, liczbę użytkowników, których dotyczy zakłócenie świadczenia usługi, czas oddziaływania incydentu na świadczoną usługę, zasięg geograficzny obszaru, którego dotyczy incydent lub inne czynniki charakterystyczne dla danego sektora lub podsektora. Przyjęto, że wystarczy spełnienie jednego z progów, aby incydent stał się incydentem poważnym, niezależnie od pozostałych wartości progów w obrębie danego sektora.

[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, 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 27 klasyfikacji NACE Rev. 2;
2) Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 28 klasyfikacji NACE Rev. 2;
3) Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 29 klasyfikacji NACE Rev. 2;
4) Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 30 klasyfikacji NACE Rev. 2.

Przedsiębiorca ma spełniać pozostałe przesłanki klasyfikacji jako podmiot ważny tj. 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.

Rozporządzenie 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. Prace nad niniejszym projektem rozporządzenia wykorzystano do ponownej oceny dotychczasowych progów uznania incydentu za poważny dla dotychczasowych sektorów.

W przypadku wielu sektorów wskazano, że incydentem poważnym jest zdarzenie, które spowodowało straty finansowe przekraczające 2 000 000 zł. Jest to nawiązanie do rozporządzenia wykonawczego Komisji (UE) 2024/2690 z dnia 17 października 2024 r. ustanawiającego 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 2024/2690 z 18.10.2024, z późn. zm.), zwanym dalej „rozporządzeniem wykonawczym”. W tym rozporządzeniu wykonawczym wskazano, że incydentem poważnym jest incydent, który spowodował lub może spowodować stratę finansową dla odpowiedniego podmiotu, która przekracza 500 000 EUR.

W sektorach związanych z produkcją czy przemysłem wskazano, że incydentem poważnym jest incydent, który spowodował co najmniej jedną z poniżej wymienionych okoliczności:

a) śmierć człowieka,
b) ciężki uszczerbek na zdrowiu,
c) inny niż ciężki uszczerbek na zdrowiu więcej niż jednej osoby,
d) straty finansowe przekraczające 2 000 000 zł,
e) ujawnienie tajemnicy prawnie chronionej w tym tajemnicy przedsiębiorstwa.

Są to sektory związane z różnymi urządzeniami, które wymagają obsługi człowieka, chociażby w celu konserwacji tych urządzeń. Dlatego należało uwzględnić wpływ incydentu na zdrowie lub życie człowieka w tych sektorach. Istotna w tych sektorach jest także ochrona tajemnicy prawnie chronionej.

W przypadku sektora energii powtórzono dotychczasowe progi uznania incydentu za poważny pochodzące z rozporządzenia Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny. W przypadku nowych podsektorów np. wodoru progi zostały uzupełnione.

Progi w sektorze transportu zostały także powtórzone z rozporządzenia Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny.

W sektorze ochrony zdrowia co do zasady pozostawiono dotychczasowe progi uzupełniając je dla tych podmiotów, które wcześniej nie znalazły się w krajowym systemie cyberbezpieczeństwa, w tym dla podsektora *Produkcja i dystrybucja substancji czynnych, produktów leczniczych i wyrobów medycznych*.

W przypadku sektora zaopatrzenia w wodę pitną i jej dystrybucji pozostawiono dotychczasowe progi uznania incydentu za poważny. Włączenie do regulacji sektora zbiorowego odprowadzania ścieków nie uzasadniało modyfikacji obowiązujących progów, które pozostają odpowiednie również dla podmiotów prowadzących działalność w tym sektorze.

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 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 w 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).

W sektorze przestrzeni kosmicznej – wskazano dwa rodzaje zdarzeń, które będą incydentami poważnymi. Pierwszy to incydent dotyczący funkcjonowania operatora

infrastruktury naziemnej, który wspiera świadczenie usług kosmicznych. Incydentem poważnym będzie przede wszystkim incydent, który spowodował niedostępność usługi powyżej 8 godzin – czyli jednego dnia roboczego. Ponadto incydentem poważnym będzie także incydent, który spowodował nieprzewidziane zdarzenie związane z wykonywaniem działalności kosmicznej, o której mowa w art. 52 ustawy z dnia 13 lutego 2026 r. o działalności kosmicznej (Dz. U. poz. 465).

Incydentem poważnym będzie również incydent dotyczący działalności Polskiej Agencji Kosmicznej, który skutkuje brakiem możliwości realizacji przez Polską Agencję Kosmiczną zadania lub obowiązku przez okres dłuższy niż 8 godzin. Ponadto incydentem poważnym, związanym z działalnością Polskiej Agencji Kosmicznej będzie incydent, który spowodował niemożliwość realizacji zadań z zakresu obronności, bezpieczeństwa państwa, ochrony ludności, obrony cywilnej oraz bezpieczeństwa i porządku publicznego powyżej 4 godzin.

Incydentem poważnym będzie także incydent polegający na niedostępności systemu informacyjnego, prowadzonego przez Prezesa Polskiej Agencji Kosmicznej zgodnie z art. 44 ust. 2 ustawy z dnia 13 lutego 2026 r. o działalności kosmicznej, obsługującego Krajowy Rejestr Obiektów Kosmicznych powyżej 4 godzin.

W sektorze podmiotów publicznych, który jest nowym sektorem, jako rodzaj zdarzenia będącego incydentem poważnym wskazano incydent dotyczący realizacji zadania publicznego. Jako jeden z progów w sektorze podmiotów publicznych wskazano, że incydentem poważnym będzie incydent, który narusza poufność, integralność lub autentyczność przetwarzanych danych oraz dotyczy danych co najmniej 10% użytkowników systemu informacyjnego służącego realizacji zadania publicznego. Chciano zapewnić, aby nie podlegały zgłoszeniom incydenty o niewielkim charakterze. Jednocześnie próg nie może być zbyt wysoki, dlatego wstępnie założono, że tym progiem powinien być 10% użytkowników systemu informacyjnego. Jeżeli incydent będzie dotyczył danych poniżej 10% użytkowników systemu informacyjnego to może być zrealizowany jeden z pozostałych progów incydentu. Celowo w tym zakresie nie odwołano się do atrybutu dostępności, ponieważ tego atrybutu dotyczą inne progi uznania incydentu za poważny w tym sektorze.

Przyjęto, że niedopuszczalna jest sytuacja, w której wskutek wystąpienia incydentu podmiot publiczny nie jest w stanie realizować zadań publicznych przez jeden dzień roboczy, tj. 8 godzin. Takie zdarzenie powinno być zgłoszone w systemie informatycznym, o którym

mowa w art. 46 ustawy do zespołu CSIRT odpowiedzialnego za podmioty publiczne. W niektórych wypadkach wprowadzono wyjątki. Przede wszystkim, jeżeli incydent spowodował brak niemożliwość realizacji zadań z zakresu obronności, bezpieczeństwa państwa, ochrony ludności, obrony cywilnej oraz bezpieczeństwa i porządku publicznego powyżej 4 godzin to taki incydent również będzie incydentem poważnym. Skrócenie tego czasu (z 8 do 4 godzin) jest spowodowane istotnością tych zadań dla zapewnienia sprawnego funkcjonowania państwa w czasie kryzysowym. Incydentem poważnym będzie także incydent, który spowodował brak dostępności systemu informacyjnego obsługującego rejestr publiczny powyżej 4 godzin. Rejestry publiczne są bardzo ważne dla zapewnienia sprawnego obrotu gospodarczego oraz dla dokonywania różnych czynności prawnych. Sytuacja, w której wskutek incydentu przez połowę dnia roboczego nie jest dostępny rejestr publiczny może istotnie utrudniać prowadzenie działalności gospodarczej. Dotyczy to w szczególności przedsiębiorców oraz podmiotów świadczących na ich rzecz obsługę prawną, którzy przed zawarciem umowy są zobowiązani do zweryfikowania danych w rejestrze publicznym. Ograniczenie dostępu do takich danych może prowadzić do opóźnień w obrocie gospodarczym oraz utrudniać realizację obowiązków ustawowych.

Incydentem poważnym będzie także incydent polegający na ujawnieniu tajemnicy prawnie chronionej. Podmioty publiczne są zobowiązane do ochrony wszelkiego rodzaju tajemnic prawnie chronionych od informacji niejawnych po tajemnicę przedsiębiorstwa. Stąd też każdy incydent, który prowadzi do ujawnienia tajemnicy prawnie chronionej winien być uznany za incydent poważny.

Niedostępność dziennika urzędowego przez okres dłuższy niż 4 godziny stanowi istotne zagrożenie dla bezpieczeństwa prawnego. Dostęp do aktualnych informacji o obowiązującym stanie prawnym jest niezbędny dla prawidłowego funkcjonowania obywateli, przedsiębiorców i organów publicznych. Szczególne znaczenie ma to w przypadku aktów normatywnych o krótkim okresie vacatio legis oraz innych aktów urzędowych wpływających na bieżące funkcjonowanie społeczeństwa i gospodarki.

Incydentem poważnym jest również incydent skutkujący niedostępnością węzła krajowego identyfikacji elektronicznej przez okres dłuższy niż 4 godziny. Węzeł krajowy identyfikacji elektronicznej stanowi kluczowy element infrastruktury umożliwiającej uwierzytelnianie użytkowników w krajowych usługach online przy wykorzystaniu środków identyfikacji elektronicznej wydanych przez różne podmioty w ramach systemów identyfikacji

elektronicznej. Jego prawidłowe i nieprzerwane funkcjonowanie ma zasadnicze znaczenie dla zapewnienia obywatelom i przedsiębiorcom dostępu do usług świadczonych drogą elektroniczną. Z tego względu niedostępność przekraczająca 4 godziny powinna być kwalifikowana jako incydent poważny, gdyż może istotnie ograniczać lub uniemożliwiać korzystanie z usług publicznych online, prowadząc do zakłóceń w realizacji spraw urzędowych oraz wykonywaniu obowiązków przez użytkowników.

Incydentem poważnym jest również incydent skutkujący niedostępnością Węzła Krajowego Identyfikacji Elektronicznej powyżej 4 godzin. Węzeł Krajowy Identyfikacji Elektronicznej pośredniczy w uwierzytelnianiu w krajowych usługach online za pomocą środków identyfikacji elektronicznej wydanych przez różne podmioty w ramach systemów identyfikacji elektronicznej. Z uwagi na jego kluczowe znaczenie dla zapewnienia dostępu do usług świadczonych drogą elektroniczną powinien być on jak najczęściej dostępny do użytku przez społeczeństwo.

Incydentem poważnym jest także incydent skutkujący niedostępnością aplikacji mObywatel powyżej 4 godzin (pół dnia roboczego). System mObywatel to system teleinformatyczny zapewniający funkcjonalności niezbędne do działania aplikacji mObywatel oraz usług udostępnianych w tej aplikacji. W aplikacji mObywatel udostępniane są różne usługi umożliwiające komunikację obywatela z administracją publiczną, dlatego ważne jest zapewnienie jej dostępności.

Incydentem poważnym w podmiocie publicznym jest również incydent, który doprowadził do śmierci człowieka, ciężkiego uszczerbku na zdrowiu lub innego uszczerbku na zdrowiu – więcej niż jednej osoby. Podmioty publiczne stanowią bardzo liczną i zróżnicowaną grupę, która realizuje szeroki zakres zadań publicznych, korzystając z wielu systemów informacyjnych. Systemy te mogą wpierać procesy mające bezpośredni wpływ na życie, zdrowie lub bezpieczeństwo ludzi. Z tego względu incydentem poważnym należy uznać, każdy incydent, którego skutkiem jest śmierć, ciężki uszczerbek na zdrowiu lub innego uszczerbku na zdrowiu – więcej niż jednej osoby.

Incydentem poważnym jest również incydent polegający na zaszyfrowaniu danych przetwarzanych w systemie informacyjnym podmiotu publicznego, jeżeli w związku z tym do

podmiotu publicznego zostało skierowane żądanie okupu w zamian za odszyfrowanie danych. Dotyczy to incydentów spowodowanych oprogramowaniem typu ransomware[2)].

Incydentem poważnym w Zakładzie Unieszkodliwiania Odpadów Promieniotwórczych jest również incydent spełniający odrębne kryteria właściwe dla działalności tego podmiotu. Ze względu na jego odmienną charakterystykę wyodrębniono dla niego progi uznania incydentu za poważny.

Incydent poważny wyodrębniono także dla usług pocztowych. Pomimo cyfryzacji usług i komunikacji – usługi pocztowe nadal odgrywają istotną rolę we współczesnym społeczeństwie informacyjnym – umożliwiają bowiem funkcjonowanie branży e-commerce poprzez dostarczanie paczek z zamówionymi produktami. Zaproponowane progi incydentów w tym sektorze pozwalają, przy szczególnie dużych utrudnieniach związanych z usługami pocztowymi, reakcję właściwego CSIRT sektorowego funkcjonującego w Urzędzie Komunikacji Elektronicznej.

W przypadku sektora inwestycji energetyki jądrowej incydentem poważnym będzie incydent dotyczący budowy obiektu energetyki jądrowej. Incydentem poważnym w tym sektorze będzie incydent, który spowodował:

- nieplanowany wyciek substancji radioaktywnych do środowiska,
- śmierć człowieka,
- ciężki uszczerbek na zdrowiu,
- inny niż ciężki uszczerbek na zdrowiu więcej niż jednej osoby,
- szkodę w wielkich rozmiarach,
- promieniotwórcze skażenie środowiska lub
- ujawnienie tajemnicy prawnie chronionej.

Wprowadzono także progi uznania incydentu za poważny dla nowego sektora gospodarowania odpadami. Obejmie on incydenty dotyczące zbierania, transportu, przetwarzania, sprzedaży lub obrotu odpadami. Założono, że jeden dzień roboczy – 8 godzin – niedostępności systemu informacyjnego służących zbieraniu, transportu, przetwarzania, sprzedaży lub obrotu odpadami znacząco utrudnia gospodarowanie odpadami i powinien być uznany jako incydent poważny. Dodatkowym progiem uznania incydentu za poważny w tym sektorze jest sytuacja, gdy incydent spowodował szkodę w środowisku. Jest to zasadne z uwagi

---

2) https://cert.pl/uploads/docs/CERT_Polska_Poradnik_ransomware.pdf

na to, że nieprawidłowe gospodarowanie odpadami negatywnie oddziałuje na środowisko. W zakresie sektora gospodarowania odpadami należy zwrócić uwagę, że progi incydentu dotyczą zdarzeń związanymi z odpadami, a nie tylko zakaźnymi odpadami medycznymi i zakaźnymi odpadami weterynaryjnymi. Ustawa z dnia 14 grudnia 2012 r. o odpadach (Dz. U. z 2023 r. poz. 1587, z późn. zm.) pod pojęciem odpadu rozumie każdą substancję lub przedmiot, których posiadacz pozbywa się, zamierza się pozbyć lub do których pozbycia się jest obowiązany. Wobec tego nie można w tym zakresie zawęzić progów tylko do zdarzeń związanych z zakaźnymi odpadami medycznymi i zakaźnymi odpadami weterynaryjnymi.

Wprowadzono także progi uznania incydentu za poważny dla nowego sektora produkcji, wytwarzania i dystrybucji chemikaliów. Obejmie to incydenty dotyczące produkcji substancji, ich dystrybucji, dystrybucji substancji lub mieszanin, a także wytwarzania z substancji lub mieszanin wyrobów. Założono, że jeden dzień roboczy – 8 godzin – zakłócenia łańcuchów dostaw w tym obszarze powinien być uznany jako incydent poważny. Dodatkowym progiem uznania incydentu za poważny w tym sektorze jest sytuacja, gdy incydent spowodował skażenie chemiczne.

W przypadku sektora produkcji, przetwarzania i dystrybucji żywności rodzajem zdarzenia będzie incydent dotyczący przemysłowego przetwarzania lub produkcji żywności i hurtowej dystrybucji żywności. Założono, że przerwa trwająca jeden dzień roboczy powoduje straty przedsiębiorstwa spożywczego i zakłóca ciągłość łańcucha dostaw żywności. Dlatego wskazano, że incydentem poważnym będzie incydent, który skutkuje przerwą w przemysłowym przetwarzaniu lub produkcją żywności, w okresie dłuższym niż 8 godziny lub incydent, który skutkuje przerwą w hurtowej dystrybucji żywności przez okres powyżej 8 godzin. Ponadto mając na uwadze bezpieczeństwo żywności wskazano, że incydentem poważnym będzie incydent, który doprowadził do przekroczenia maksymalnych poziomów substancji zanieczyszczających w produkowanej lub dystrybuowanej żywności.

Poziomy te zostały określone w dwóch aktach normatywnych:

- rozporządzeniu Komisji (UE) 2023/915 z dnia 25 kwietnia 2023 r. w sprawie najwyższych dopuszczalnych poziomów niektórych zanieczyszczeń w żywności oraz uchylające rozporządzenie (WE) nr 1881/2006 ((Dz. Urz. UE. L 119, str. 103) oraz w

– rozporządzeniu Ministra Zdrowia z dnia 25 września 2012 r. w sprawie określenia maksymalnych poziomów substancji zanieczyszczających, które mogą znajdować się w tłuszczach stosowanych do smażenia, oraz kryteriów dla metod analitycznych stosowanych do ich oznaczania (Dz. U. poz. 1096).

Sektor produkcji składa się z kilku podsektorów. Wskazano rodzaj zdarzenia, który odpowiada nazwie podsektora. Założono, że przerwa trwająca jeden dzień roboczy powoduje straty przedsiębiorstwa i zakłóca ciągłość łańcucha dostaw danego produktu. Dlatego przerwa w produkcji trwająca powyżej 8 godzin jest incydentem poważnym. Przedsiębiorstwa w tym sektorze zmagają się z ryzykiem szpiegostwa przemysłowego. Dlatego wskazano, że incydentem poważnym będzie incydent, który spowodował ujawnienie tajemnicy prawnie chronionej, w tym tajemnicy przedsiębiorstwa. Obejmować to będzie także inne rodzaje tajemnic prawnie chronionych – warto bowiem zauważyć, że w sektorze tym znajdują się także przedsiębiorstwa zajmujące się produkcją na potrzeby wojskowe.

W sektorze badań naukowych wyróżniono dwa rodzaje incydentów co jest związane z różnym obciążeniem regulacyjnym podmiotów w tym sektorze. Incydent dotyczący prowadzenia badań naukowych będzie zgłaszany przez organizacje badawcze. Organizacje badawcze są obowiązane wdrożyć pełen system zarządzania bezpieczeństwem informacji zgodny z art. 8 ustawy. Jako próg uznania incydentu za incydent poważny wskazano sytuację, w której incydent skutkuje niedostępnością systemów informacyjnym służących badaniom naukowym dłuższą niż 8 godzin. Przyjęto bowiem, że jeden dzień roboczy niedostępności systemów informacyjnych organizacji badawczej może w znaczący sposób utrudnić jej funkcjonowanie.

Poza organizacjami badawczymi w sektorze badań naukowych znajdują się także pozostałe podmioty sektora szkolnictwa wyższego i nauki. Te podmioty stosują uproszczone wymogi z zakresu cyberbezpieczeństwa, które są określone w załączniku nr 4 do ustawy. Tutaj jako próg uznania incydentu za incydent poważny wskazano sytuację, w której incydent skutkuje niedostępnością systemów informacyjnym służących realizacji zadań i obowiązków podmiotu powyżej 8 godzin. Przyjęto bowiem, że jeden dzień roboczy niedostępności systemów informacyjnych podmiotu szkolnictwa wyższego może w znaczący sposób utrudnić jego funkcjonowanie. Warto mieć tutaj na uwadze, że podmioty szkolnictwa wyższego w tym także uczelnie mają swoje systemy informacyjne np. systemy obsługi studiów, w których zawarte są informacje o postępach w nauce studentów i słuchaczy. Systemy te umożliwiają

również rejestrację na egzaminy na studiach, dlatego niedostępność takiego systemu w bardzo negatywny sposób wpływa na studentów w trakcie rejestracji na egzaminy.

Obowiązek zgłoszenia incydentu poważnego może być postrzegany jako obciążenie, jednak trzeba podkreślić, że wiąże się z tym możliwość uzyskania pomocy właściwego CSIRT sektorowego na etapie reagowania na incydent. Ponadto są to zdarzenia, które mogą uniemożliwiać świadczenie usług przez dany podmiot kluczowy lub podmiot ważny – a zgłoszenie incydentu poważnego oraz pomoc zespołu CSIRT przyspieszy skuteczne zarządzanie incydentem.

Na koniec warto podkreślić, że zgodnie z art. 8 ust. 1 pkt 1 ustawy podmiot kluczowy lub podmiot ważny mają obowiązek prowadzenia systematycznego szacowania ryzyka wystąpienia incydentu oraz obowiązek zarządzanie tym ryzykiem. Obowiązki te nie dotyczą wyłącznie incydentów poważnych, ale generalnie incydentów, które mogą wystąpić w danym podmiocie. Jeżeli szacowanie ryzyka w podmiocie ograniczy się tylko do szacowania ryzyka wystąpienia incydentu poważnego w podmiocie to podmiot nie będzie wykonywał w prawidłowy sposób wspomnianego przepisu co powinno być wykryte w trakcie audytu, kontroli lub przeglądu systemu zarządzania bezpieczeństwem informacji.

Projektowane rozporządzenie wejdzie w życie po upływie 14 dni od dnia ogłoszenia.

Nie jest konieczne wprowadzenie przepisów przejściowych, ponieważ projektowane rozporządzenie nie nakłada nowych obowiązków o charakterze technicznym lub organizacyjnym, których wdrożenie wymagałoby dodatkowego czasu dostosowawczego, a jedynie aktualizuje i doprecyzowuje dotychczas obowiązujące progi uznania incydentu za poważny. Jak wspomniano wyżej obecnie trwa okres dostosowawczy dla podmiotów kluczowych i podmiotów ważnych – bezwzględny obowiązek zgłaszania incydentów poważny zaistnieje po 3 kwietnia 2027 r.

Stosownie do postanowień art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2026 r. poz. 936), projekt rozporządzenia zostanie udostępniony w Biuletynie Informacji Publicznej. 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 zostanie udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.

Jednocześnie należy wskazać, że nie ma możliwości podjęcia alternatywnych w stosunku do projektowanej regulacji środków umożliwiających osiągnięcie zamierzonego celu.

Projekt rozporządzenia jest zgodny z prawem Unii Europejskiej.

Projekt rozporządzenia nie podlega przedstawieniu właściwym organom i instytucjom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Projektowane rozporządzenie nie zawiera przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597) i nie podlega notyfikacji Komisji Europejskiej.

Projektowane rozporządzenie nie będzie wymagało notyfikacji Komisji Europejskiej w trybie ustawy z dnia 30 kwietnia 2004 r. o postępowaniu w sprawach dotyczących pomocy publicznej (Dz. U. z 2026 r. poz. 500).

Wejście w życie projektowanego rozporządzenia będzie miało wpływ na działalność średnich przedsiębiorców, którzy są podmiotami kluczowymi lub podmiotami ważnymi. Niezależnie od wielkości podmiotu rozporządzenie będzie miało wpływ na podmioty świadczące usługi rejestracji nazw domen oraz na przedsiębiorców komunikacji elektronicznej. Wynika to z przepisów ustawy, które nakładają na te podmioty obowiązek zgłoszenia incydentu poważnego niezależnie od wielkości podmiotu. Okazjonalnie może się zdarzyć, że projektowane rozporządzenie będzie miało wpływ na mikroprzedsiębiorców i małych przedsiębiorców z innych sektorów. Przypadek taki może mieć miejsce, jeżeli będzie dotyczyć podmiotów krytycznych (w rozumieniu dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylającej dyrektywę Rady 2008/114/WE (Dz. Urz. UE L 333 z 27.12.2022, str. 164) oraz podmiotów, które zostały uznane jako podmiot kluczowy albo podmiot ważny w drodze decyzji administracyjnej. Są to jednak sytuacje wyjątkowe.