Wersja 03.07.2024 r.

UZASADNIENIE

Wstęp, ogólna charakterystyka proponowanych regulacji

Projektowane rozwiązania mają na celu wdrożenie:

- ✓ rozwiązań zapewniających podstaw zarządzania ryzykiem, z uwzględnieniem postanowień Decyzji Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (Dz. Urz. UE L 347 z 20.12.2013, str. 924, L 250 z 04.10.2018, str. 1 oraz L 77A z 20.03.2019, str. 1), zwanej dalej „UMOL";
- ✓ dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz. Urz. UE L 333 z 27.12.2022 r. str. 164), zwaną dalej „dyrektywą CER".

UMOL Posiadanie planów zarządzania ryzykiem jest o tyle istotne, iż są one niezbędne do spełnienia tzw. warunkowości ex ante w perspektywie finansowej UE na lata 2021-2027, co ma przełożenie na możliwość pozyskiwania środków finansowych w ramach polityki spójności z Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego Plus, Funduszu Spójności oraz Europejskiego Funduszu Morskiego i Rybackiego.

Opracowanie dokumentów planistycznych w obszarze zarządzania ryzykiem jest bowiem bezpośrednio powiązane z jednym z warunków podstawowych perspektywy finansowej, który mówi o „osiągnięciu skutecznych ram zarządzania ryzykiem". Wskazuje się wprost na konieczność opracowania planu zarządzania ryzykiem na szczeblu krajowym lub regionalnym, powiązanego ze strategiami adaptacji do zmian klimatu. Ponadto państwa członkowskie opracowują oceny ryzyka na szczeblu krajowym lub niższym oraz udostępniają Komisji Europejskiej tzw. streszczenie istotnych elementów tych ocen.

Obowiązujące obecnie w tym obszarze regulacje ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym nie pozwalają w pełni odzwierciedlać w planach zarządzania kryzysowego kwestii dotyczących zarządzania ryzykiem. Istnieje zatem konieczność opracowywania planów zarządzania ryzykiem, na szczeblu krajowym lub odpowiednio niższym, wskazanie podmiotów odpowiedzialnych za ich opracowanie, zakresu merytorycznego takiego planu oraz określenie cyklu planowania.

Konieczne jest tym samym modyfikacja dotychczasowych rozwiązań w kierunku zapewnienia podstaw prawnych i organizacyjnych dotyczących kwestii zarządzania ryzykiem, co znajdzie odzwierciedlenie w projekcie w rozwiązaniach dotyczących dokumentów strategicznych w zakresie oceny ryzyka oraz treści planów zarządzania kryzysowego. Nowe regulacje pozwolą również na efektywne przekazywanie dokumentów o charakterze sprawozdawczym Komisji Europejskiej, m.in. „Streszczenia istotnych elementów krajowej oceny ryzyka" oraz „Streszczenia istotnych elementów krajowej oceny zdolności zarządzania ryzykiem".

W zakresie kwestii zarządzania ryzykiem, z uwzględnieniem postanowień UMOL przewiduje się wdrożenie zintegrowanego podejścia do zarządzania ryzykiem, obejmującego cały cykl

zarządzania, od oceny ryzyka poprzez przygotowanie planów zarządzania nim oraz wdrażanie środków zapobiegawczych i zapewniających gotowość do ich użycia.

Przewiduje się opracowanie na szczeblu centralnym dokumentu rządowego, tzw. Krajowej Oceny Ryzyka, który zastąpi obecnie funkcjonujący Raport o zagrożeniach bezpieczeństwa narodowego. Dotychczasowe doświadczenia wykazują, że Raport o zagrożeniach bezpieczeństwa narodowego jest dokumentem nadmiernie obszernym, mającym charakter quasi cyklicznej oceny zidentyfikowanych zagrożeń, a jednocześnie nie przekładającym się na procesy planistyczne dotyczące zarządzania ryzykiem.

Krajowa Ocena Ryzyka będzie funkcjonalnym dokumentem zawierającym zidentyfikowane zagrożenia o różnym charakterze (naturalne, techniczne, związane z konfliktem zbrojnym w tym hybrydowe, o charakterze terrorystycznym, z obszaru cyberbezpieczeństwa, itp.) oraz ocenę ryzyk wynikających z tych zagrożeń, pozwalającą określić cele strategiczne i priorytety na rzecz ich ograniczania. Istotne jest bowiem zrozumienie, że dopiero prawidłowo przeprowadzona ocena ryzyka, identyfikuje zagrożenia i obszary, w których konieczne jest podjęcie działań, w tym zwiększenie nakładów finansowych na realizację przedsięwzięć ograniczających.

Krajowa Ocena Ryzyka – w obszarze planowania cywilnego – wykorzystywana będzie wykorzystywana na potrzeby opracowania Krajowego Planu Zarządzania Kryzysowego oraz planów zarządzania kryzysowego ministrów, kierowników urzędów centralnych, wojewodów, jak również planów zarządzania kryzysowego na szczeblu powiatu oraz gminy. Każdy z planów będzie zawierał cześć obejmującą zarządzanie ryzykiem (działania w zakresie zapobiegania sytuacji kryzysowej oraz przygotowywania do jej wystąpienia) oraz cześć dotyczącą reagowania kryzysowego (działania w zakresie reagowania w przypadku wystąpienia sytuacji kryzysowej oraz usuwaniu jej skutków).

W przypadku planów na szczeblu gminnym – ujęcie w planie zarządzania kryzysowego kwestii dotyczących zarządzania ryzykiem będzie fakultatywne.

Konieczne będzie dostosowanie terminologii do regulacji unijnych, co stworzy efektywne narzędzia do prowadzenia oceny ryzyka i zarządzania nim. Jednocześnie zostaną ujednolicone terminy cyklów planistycznych krajowych z unijnymi, gdyż obowiązujące przepisy krajowe przewidują cykl 2-letni, podczas gdy unijne regulacje wskazują na 3-letnie cykle planistyczne. Nowy cykl planistyczny będzie obejmował 3 lata.

Wdrożenie rozwiązań zawartych w dyrektywie CER ma zapewnić ciągłości świadczenia usług kluczowych realizowanych w sektorach lub podsektorach wskazanych w dyrektywie CER.

Przewidywane rozwiązania skupiają się na:

- ✓ identyfikacji usług kluczowych świadczonych przez operatorów infrastruktury krytycznej z uwzględnieniem potencjalnych skutków zakłócenia zarówno w odniesieniu do funkcjonowania państwa jak i społeczeństwa;
- ✓ minimalizacja skutków zakłócenia poprzez wprowadzenie procesów oceny i zarządzania ryzykiem;

- ✓ uwzględnienie zadań związanych z ochroną usług kluczowych;
- ✓ modyfikacja obecnych rozwiązań dotyczących infrastruktury krytycznej jako niezbędnych elementów świadczenia usług kluczowych.

Wdrożenie rozwiązań zawartych w dyrektywie CER nie może odbyć się bez redefiniowania regulacji dotyczących infrastruktury krytycznej, która jest niezbędna do świadczenia usług kluczowych przez podmioty krytyczne, o których traktuje CER. W szczególności należy doprowadzić do spójności dotychczasowych systemów infrastruktury krytycznej z sektorami i podsektorami, o których mówi dyrektywa. Ponadto, biorąc pod uwagę że dyrektywa stanowi jedynie minimum harmonizacyjne, projekt zakłada nie tylko utrzymanie dotychczasowego poziomu ochrony infrastruktury krytycznej, ale również rozszerzenie ochrony o ochronę „infrastruktury krytycznej w budowie" oraz ochronę infrastruktury krytycznej mającej kluczowe znaczenie dla społeczności lokalnych.

Projektowane rozwiązania mają na celu wzmocnienie mechanizmów ochrony infrastruktury krytycznej, biorąc pod uwagę, iż stanowi ona rdzeń świadczenia usług dla państwa jak i obywateli. Wynikają one również z analizy przebiegu wojny w Ukrainie i pojawiających się działań o charakterze sabotażowym i hybrydowym.

Zmiany szczegółowe

Zakres stosowania ustawy (art. 1 pkt 2 ustawy nowelizującej)

Z uwagi na konieczność wdrożenia ww. rozwiązań w ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122) (dalej „ustawa z.k.") projektowana regulacja wprowadza rozdziały do tej ustawy w celu zachowania czytelności zawartych w niej regulacji. Zakres zmian dotyczy również konieczności zmiany zakresu przedmiotowego jak i podmiotowego ustawy z.k. Obok organów właściwych w sprawach zarządzania kryzysowego pojawią się organy właściwe do spraw podmiotów krytycznych, którym ustawa z.k. wskaże zadania i obowiązki oraz określi zasady ich finansowania. Ustawa z.k. zostanie również rozszerzona o kwestie związane z tzw. usługami kluczowymi świadczonymi przez podmioty krytyczne.

Słowniczek (art. 1 pkt 3 ustawy nowelizującej)

W projektowanych zmianach do słowniczka ustawy o zarządzaniu kryzysowym wskazać należy na:

- ✓ definicję sytuacji kryzysowej, która zostanie uzupełniona o kwestie dotyczące dziedzictwa kulturowego. Projekt nowelizacji w definicji sytuacji kryzysowej uwzględnia postanowienia decyzji Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności, która w art. 2 określa, że „Ochrona zapewniana w ramach unijnego mechanizmu obejmuje przede wszystkim ludzi, lecz także środowisko naturalne i mienie, w tym dziedzictwo kulturowe,

i chroni je przed wszystkimi rodzajami klęsk żywiołowych i katastrof spowodowanych przez człowieka, w tym następstwami ataków terrorystycznych".

Ponadto decyzja Parlamentu Europejskiego i Rady 2019/420 z dnia 13 marca 2019 r. zmieniająca decyzję nr 1313/2013/UE w sprawie Unijnego Mechanizmu Ochrony Ludności rozszerzyła katalog zagrożeń, jak też działań podejmowanych w sytuacji wystąpienia klęsk żywiołowych i katastrof spowodowanych przez człowieka. Brak regulacji dotyczących ochrony dziedzictwa kulturowego mógłby powodować, iż problematyka ta nie zostanie włączona do budowanego obecnie systemu przygotowań na zdarzenia nadzwyczajne, w szczególności w administracji publicznej różnych szczebli, między innymi poprzez podejmowane działania planistyczno-organizacyjne, szkoleniowe i kontrolne. Ponadto pozbawia instytucje kultury, w których zgromadzone są zbiory, a które stanowią dziedzictwo narodowe, z korzystania z zasobów ludzkich i sprzętowych, podmiotów wyspecjalizowanych w prowadzeniu akcji ratowniczych.

Uzupełnienie dotychczasowej treści definicji o wskazanie istoty zakłóceń funkcjonowania organów administracji publicznej związane jest z faktem, iż przepisy ustawy o zarządzaniu kryzysowym przede wszystkim statuują oraz wskazują obowiązki i kompetencje organów administracji publicznej w ramach systemu zarządzania kryzysowego. Ich niezakłócona działalność jest gwarantem działań podejmowanych na rzecz szeroko rozumianej ochrony ludności;

- ✓ szereg definicji bazujących na definicjach zawartych w dyrektywie CER, w tym definicji podmiotu krytycznego, podmiotu krytycznego, odporności podmiotu krytycznego, incydentów, które co do zasady wpływają lub mogą wpływać na niezakłócone świadczenie usługi kluczowej. Zdefiniowana również zostaje usługa kluczowa.

  Definicja tej usługi odnosi się do sektorów lub podsektorów wymienionych w projektowanym załączniku do ustawy z.k. Nawiązują one do załącznika dyrektywy CER oraz mają być w założeniu kompatybilne z regulacjami zawartymi w dyrektywie NIS2. Projekt wskazuje, że usługi kluczowe realizowane mogą być w sektorach energii, transportu, bankowości oraz sektora infrastruktury rynków, zdrowia, wody pitnej oraz ścieków, infrastruktury cyfrowej, administracji publicznej, przestrzeni kosmicznej, produkcji, przetwarzania i dystrybucji żywności, zarządzania usługami ICT, produkcji, wytwarzania i dystrybucji chemikaliów i innych produktów przemysłowych, usług pocztowych i kurierskich oraz gospodarowania odpadami;

- ✓ Redefiniowano pojęcie infrastruktury krytycznej jako infrastruktury służącej zapewnieniu funkcjonowania organów administracji publicznej, zapewnieniu funkcjonowania przedsiębiorców, zaspokajaniu potrzeb obywateli, w tym zapewniającej świadczenie wspomnianych usług kluczowych,

- ✓ Na potrzeby opracowania planów zarządzania kryzysowego jak również wdrażania rozwiązań dyrektywy CER oceny ryzyka oraz zarządzania nim zdefiniowano pojęcie ryzyka, zarządzania ryzykiem czy też oceny ryzyka. Uzupełnieniem w tym zakresie są definicje zagrożenia antagonistycznego jak i hybrydowego.

Dokumenty strategiczne (art. 1 pkt 6 ustawy nowelizującej)

Projekt wprowadza w ustawie z.k. rozdział „Dokumenty strategiczne". Do dokumentów strategicznych zalicza się tzw. Krajową Ocenę Ryzyka (zastępującą obecny Raport o zagrożeniach bezpieczeństwa narodowego), tak jak dotychczas Krajowy Plan Zarządzania Kryzysowego oraz Strategię Odporności Podmiotów Krytycznych, zastępującą Narodowy Program Ochrony Infrastruktury Krytycznej a obejmującą zarówno kwestie infrastruktury krytycznej jak i podmiotów krytycznych mających świadczyć usługi kluczowe.

Krajowa Ocena Ryzyka będzie opracowywana cyklicznie w celu dokonywania oceny ryzyka zidentyfikowanych zagrożeń. Będzie ona przyjmowana przez Radę Ministrów w drodze uchwały. Krajowa Ocena Ryzyka będzie punktem wyjścia dla programowania wielu procesów, gdyż Krajową Ocena Ryzyka uwzględnia się w:

- ✓ Krajowym Planie Zarządzania Kryzysowego oraz pozostałych planach zarządzania kryzysowego na wszystkich szczeblach zarządzania kryzysowego;
- ✓ procesach identyfikacji podmiotów krytycznych;
- ✓ opracowywaniu ocen ryzyka dla podmiotów krytycznych oraz wdrażaniu przez podmioty krytyczne środków w zakresie zwiększenia ich odporności;
- ✓ jak również innych dokumentach opracowywanych przez organy administracji publicznej w zakresie zarządzania kryzysowego.

Krajowa ocena ryzyka w założeniu ma zawierać zidentyfikowane istotne zagrożenia w podziale na wskazane w niej kategorie zagrożeń, ocenę ryzyka wynikającego ze zidentyfikowanych zagrożeń oraz streszczenie istotnych elementów oceny ryzyka w rozumieniu decyzji 1313/2013/EU.

Projekt Krajowej Oceny Ryzyka opracowuje Szef Rządowego Centrum Bezpieczeństwa (dalej „Centrum". Regulacje dotyczące opracowywania projektu Krajowej Oceny Ryzyka bazują na dotychczasowych doświadczeniach Centrum w opracowywaniu, koordynowaniu i przedkładaniu Radzie Ministrów obecnych dokumentów strategicznych w obszarze zarzadzania kryzysowego.

Projekt przewiduje analogiczne regulacje w zakresie opracowywania dokumentu w odniesieniu do Krajowego Planu Zarządzania Kryzysowego oraz Strategii Odporności Podmiotów Krytycznych.

Krajowy Plan Zarządzania Kryzysowego będzie przyjmowany uchwałą Rady Ministrów. KPZK będzie zawierał:

- ✓ część dotyczącą zarządzania ryzykiem;
- ✓ część dotyczącą reagowania kryzysowego;
- ✓ streszczenie istotnych elementów krajowej oceny zdolności zarządzania ryzykiem w rozumieniu decyzji 1313/2013/EU.

Strategia Odporności Podmiotów Krytycznych, będzie również przyjmowana przez Radę Ministrów, w drodze uchwały. Strategie w założeniu ma:

- ✓ określać cele strategiczne i priorytety w zakresie zapewnienia niezakłóconego świadczenia usług kluczowych przez podmioty krytyczne oraz niezakłóconego funkcjonowania infrastruktury krytycznej;
- ✓ określać zakresy działań oraz formy działań służące osiąganiu celów strategicznych i priorytetów przez m.in. organy do spraw podmiotów krytycznych, czy też ministrów oraz inne podmioty identyfikujące infrastrukturę krytyczną;
- ✓ opisywać procesy i środki niezbędnych do realizacji zadań w zakresie tworzenia rozwiązań organizacyjno-prawnych rynku usług kluczowych świadczonych przez podmioty krytyczne;
- ✓ określa zakres koordynacji działań właściwych organów w sprawach podmiotów krytycznych i podmiotów właściwych w sprawach cyberbezpieczeństwa, o których mowa w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 i 1703).

Dodatkowo przewiduje się nałożenie na Szefa Centrum obowiązku przekazywania Komisji Europejskiej streszczenia istotnych elementów oceny ryzyka oraz streszczenia istotnych elementów krajowej oceny zdolności zarządzania ryzykiem w rozumieniu decyzji 1313/2013/EU.

Plany zarządzania kryzysowego (art. 1 pkt 6 ustawy nowelizującej)

Projekt zakłada wprowadzenie regulacji dotyczących planów zarządzania kryzysowego na wszystkich szczeblach, z uwzględnieniem ich „podziału" na część zarzadzania ryzykiem oraz część reagowania kryzysowego. Regulacje zawarte w przepisach art. 5g – 5 j opisują szczegółowo elementy planów zarządzania kryzysowego na poszczególnych szczeblach.

Tak jak dotychczas przewiduje się, że plany zarządzania kryzysowego podlegają systematycznej aktualizacji w cyklu planowania nie dłuższym niż trzy lata (obecnie dwa lata) oraz uzgadnia się je z właściwymi podmiotami, w zakresie ich dotyczącym, planowanymi do wykorzystania przy realizacji przedsięwzięć określonych w planie.

W przypadku planów postępowania na wypadek wystąpienia sytuacji kryzysowej, opracowanych na podstawie odrębnych przepisów, z wyłączeniem planów sporządzanych na czas zewnętrznego zagrożenia bezpieczeństwa państwa i na czas wojny, stanowią one załączniki do planu zarządzania kryzysowego właściwego organu administracji publicznej.

Identyfikowanie infrastruktury krytycznej i potencjalnej infrastruktury krytycznej (art. 1 pkt 8 ustawy nowelizującej)

Obecne regulacje w zakresie m.in. identyfikowania infrastruktury krytycznej są „rozproszone" między przepisy ustawy, aktu wykonawczego do ustawy dotyczącego Narodowego Programu Ochrony Infrastruktury Krytycznej a sam Narodowy Program. Proponowane regulacje porządkują kwestie infrastruktury krytycznej wskazując czytelnie regulacje obejmujące:

- ✓ identyfikację oraz wyznaczanie infrastruktury krytycznej;
- ✓ gromadzenie i przetwarzanie informacji dotyczących zagrożeń infrastruktury krytycznej;
- ✓ opracowywanie i wdrażanie procedur na wypadek wystąpienia zagrożeń infrastruktury krytycznej;
- ✓ odtwarzanie infrastruktury krytycznej;
- ✓ współpracę między organami administracji publicznej a operatorami infrastruktury krytycznej w zakresie ich ochrony.

Projektowana regulacja wskazuje w art. 6f projektu kategorie kryteriów pozwalających zidentyfikować obiekty, urządzenia oraz instalacje lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje oraz sieci, systemy lub usługi jako infrastrukturę krytyczną, w tym kryteria sektorowe oraz kryteria przekrojowe. Jako wytyczną do wydania przez Radę Ministrów uchwały w sprawie kryteriów, wskazuje się znaczenie obiektów, urządzeń oraz instalacji lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji oraz sieci, systemów lub usług dla funkcjonowania państwa i zaspokajania potrzeb obywateli, w tym potrzeb lokalnych społeczności oraz świadczenia usług kluczowych.

Przyjmuje się, co do zasady, że obiekt, urządzenie oraz instalacja lub połączony ze sobą funkcjonalnie obiekty, urządzenia, instalacje oraz sieć, system lub usługa mogą zostać wpisane do wykazu infrastruktury krytycznej, jeżeli spełnia łącznie kryterium sektorowe oraz co najmniej jedno z kryteriów przekrojowych. Reguła ta nie będzie dotyczyć wojewodów, którzy stosują wyłącznie kryteria przekrojowe przy identyfikacji infrastruktury krytycznej (w założeniu będzie to obejmować lokalną infrastrukturę krytyczną zabezpieczającą potrzeby lokalnych społeczności). Pozostałe podmioty czyli ministrowie kierujący działami administracji rządowej, Komisja Nadzoru Finansowego oraz Szef Centrum korzystają z pełnego spektrum kryteriów przy identyfikacji infrastruktury krytycznej.

Zgodnie z art. 6i projektu ustawy – Szef Centrum prowadzi – jak obecnie – wykaz infrastruktury krytycznej, który zawiera:

- ✓ nazwę i lokalizację infrastruktury krytycznej;
- ✓ dane operatora infrastruktury krytycznej, w tym siedzibę i adres oraz numer identyfikacji podatkowej (NIP), jeżeli został nadany;
- ✓ wskazanie podmiotu identyfikującego infrastrukturę krytyczną.

Aktualne pozostają rozwiązania, które wskazują, że wykaz ma charter niejawny, a wyciągi z wykazu infrastruktury krytycznej znajdującej się na terenie poszczególnych województw – Szef Centrum przekazuje właściwym wojewodom, w celu realizacji zadań w zakresie ich ochrony.

W odniesieniu do zidentyfikowanej i ujętej w wykazie infrastruktury krytycznej ministrowie kierujący działami administracji rządowej, wojewodowie, Komisja Nadzoru Finansowego oraz Szef Centrum w zakresie swojej właściwości zapewniają bieżącą współpracę dotyczącą wyłanianej infrastruktury krytycznej, w tym m.in.

- ✓ prowadzą bieżącą wymianę informacji na temat bieżących zagrożeń;
- ✓ organizują fora ochrony infrastruktury krytycznej;
- ✓ udzielają wsparcia merytorycznego operatorom infrastruktury krytycznej w zakresie wdrażania dobrych praktyk dotyczących ochrony infrastruktury krytycznej.

W odniesieniu do wykazu potencjalnej infrastruktury krytycznej – obiekt, instalację, urządzenie lub usługę uznaje się za potencjalną infrastrukturę krytyczną, w przypadku gdy z założeń projektowych wynika, że może ona spełnić kryteria właściwe dla infrastruktury krytycznej. Na podstawie prowadzonych ustaleń można dokonać ujęcia w wykazie potencjalnej infrastruktury krytycznej, prowadzonym przez Szefa Centrum.

Po ujęciu w wykazie - minister kierujący działem administracji rządowej lub właściwym terytorialnie wojewodą we współpracy z Szefem Centrum przedstawiają operatorowi infrastruktury krytycznej informacje oraz dokumenty pozwalające na uwzględnienie wymogów dotyczących infrastruktury krytycznej w dokumentacji projektowej lub podczas realizacji inwestycji.

Obowiązki operatora infrastruktury krytycznej (art. 1 pkt 8 ustawy nowelizującej)

Projekt kładzie nacisk na zwiększenie ochrony zidentyfikowanej infrastruktury krytycznej. Doprecyzowano obowiązki operatorów infrastruktury krytycznej w zakresie jej ochrony, wskazując zadania polegające m.in. na:

- ✓ prowadzeniu systematycznej analizy zagrożeń dla infrastruktury krytycznej;
- ✓ wdrażaniu adekwatnych do przeprowadzonej analizy zagrożeń rozwiązań w zakresie bezpieczeństwa fizycznego, w tym ochrony fizycznej oraz zabezpieczeń technicznych, bezpieczeństwa osobowego dotyczącego pracowników i dostawców zewnętrznych, bezpieczeństwa teleinformatycznego, bezpieczeństwa prawnego oraz ciągłości działania i odtwarzania, w tym utrzymywania własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie infrastruktury krytycznej do czasu jej pełnego odtworzenia;
- ✓ bieżącą współpracę z organami administracji publicznej oraz Szefem Centrum przez przekazywanie i odbieranie informacji o zagrożeniach zakłócających lub mogących zakłócić funkcjonowanie infrastruktury krytycznej lub spodziewanych przerwach lub zakłóceniach w funkcjonowaniu infrastruktury krytycznej;
- ✓ sporządzanie i przekazywanie informacji w zakresie zapewnienia ochrony infrastruktury krytycznej odpowiednio na żądanie:
    - o ministra oraz Szefa Centrum,
    - o właściwego miejscowo wojewody;
- ✓ zapewnienie zdolności do ochrony informacji niejawnych w zakresie realizacji przedsięwzięć związanych z ochroną infrastruktury krytycznej.

Operator infrastruktury krytycznej będzie obowiązany do wdrażania rozwiązań dotyczących bezpieczeństwa infrastruktury krytycznej z uwzględnieniem tzw. minimalnych standardów. Rada Ministrów określi, w drodze rozporządzenia minimalne standardy ochrony infrastruktury krytycznej uwzględniając bezpieczeństwo fizyczne, techniczne, osobowe, teleinformatyczne, prawne oraz ciągłość działania jako przesłankę traktując lokalizację i charakterystykę infrastruktury krytycznej.

Dodatkowo przewiduje się, że operator będzie miał prawo do żądania od usługodawców w postępowaniach przetargowych lub zamówieniach:

- ✓ zdolności do ochrony informacji niejawnych oraz stosowania tych przepisów przy projektowaniu i wykonywaniu obiektów, urządzeń instalacji i innych systemów będących elementami infrastruktury krytycznej;
- ✓ certyfikatów potwierdzających posiadanie właściwych kompetencji i uprawnień

Operator infrastruktury krytycznej opracowuje, stosuje i aktualizuje dokumentację ochrony infrastruktury krytycznej, która zawiera:

- ✓ charakterystykę infrastruktury krytycznej oraz analizę zagrożeń dla tej infrastruktury;
- ✓ opis zastosowanych, adekwatnie do rodzaju zagrożeń środków bezpieczeństwa w zakresie zapewnienia bezpieczeństwa w obszarach, począwszy od bezpieczeństwa fizycznego, na ciągłości działania i odtwarzania skończywszy;
- ✓ opis zasobów umożliwiających podtrzymanie funkcjonowania infrastruktury krytycznej do czasu jej pełnego odtworzenia oraz opis współpracy z właściwymi podmiotami administracji publicznej dotyczący wymiany informacji o zdarzeniu zakłócającym lub mogącym zakłócić funkcjonowanie infrastruktury krytycznej oraz sposobu postępowania w przypadku takiego zdarzenia;
- ✓ procedury:
    - o działania w sytuacji zagrożenia lub zakłócenia funkcjonowania infrastruktury krytycznej,
    - o zapewnienia ciągłości funkcjonowania infrastruktury krytycznej,
    - o odtwarzania infrastruktury krytycznej;
- ✓ inne elementy niż wskazane powyżej, biorąc pod uwagę charakterystykę infrastruktury krytycznej.

Operator infrastruktury krytycznej co do zasady przedkłada oświadczenie o opracowaniu dokumentacji ochrony infrastruktury krytycznej oraz wdrożeniu minimalnych wymagań odpowiednio: ministrowi lub Szefowi Centrum, właściwemu miejscowo wojewodzie.

W przypadku braku możliwości wdrożenia rozwiązań dotyczących bezpieczeństwa, dokumentacja podlega uzgodnieniu odpowiednio z ministrem lub Szefem Centrum, właściwym miejscowo wojewodą.

Minister lub wojewoda w ramach ww. uzgadniania mogą wskazać podmioty administracji publicznej, od których operator będzie obowiązany uzyskać opinię na temat sporządzonej dokumentacji przed jej zatwierdzeniem.

W ramach obowiązków sprawozdawczych operator infrastruktury krytycznej sporządza, w terminie do dnia 31 marca każdego roku raport o stanie ochrony infrastruktury krytycznej za rok ubiegły.

Raport o stanie ochrony infrastruktury krytycznej zawiera w szczególności informacje dotyczące jej ochrony w zakresie zapewnienia bezpieczeństwa fizycznego, technicznego, osobowego, teleinformatycznego, prawnego oraz ciągłości działania i odtwarzania.

Raport o stanie ochrony infrastruktury krytycznej sporządza się z uwzględnieniem:

- ✓ analizy zagrożeń dla infrastruktury krytycznej oraz zagrożeń, które zakłóciły lub mogły zakłócić funkcjonowanie infrastruktury krytycznej, a nie były uwzględnione w tej analizie;
- ✓ wdrożonych rozwiązań dla bezpieczeństwa infrastruktury krytycznej oraz wyników przeprowadzonych kontroli i audytów odnoszących się do wdrożonych rozwiązań;
- ✓ opisu działań podjętych przez operatora infrastruktury krytycznej w przypadkach wystąpienia zagrożeń.

Raport o stanie ochrony infrastruktury krytycznej przekazywany jest odpowiednio: ministrowi lub Szefowi Centrum, właściwemu miejscowo wojewodzie.

Projekt przewiduje, że w celu realizacji zadań w zakresie zapewnienia bezpieczeństwa infrastruktury krytycznej - operator infrastruktury krytycznej wyznacza koordynatora do spraw ochrony infrastruktury krytycznej, który musi spełniać następujące kryteria:

- ✓ jest pracownikiem operatora infrastruktury krytycznej albo żołnierzem lub funkcjonariuszem pełniącym służbę w jednostce organizacyjnej będącej operatorem infrastruktury krytycznej;
- ✓ korzysta z pełni praw publicznych;
- ✓ posiada wiedzę, umiejętności i doświadczenie w zakresie zarządzania bezpieczeństwem, z uwzględnieniem przedmiotu działalności operatora infrastruktury krytycznej;
- ✓ nie był skazany prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe;
- ✓ spełnia wymagania bezpieczeństwa osobowego w zakresie dostępu do informacji niejawnych o klauzuli co najmniej „poufne”.

O wyznaczeniu koordynatora operator informuje odpowiednio: ministra lub Szefa Centrum, właściwego miejscowo wojewodę. Wyznaczony koordynator podlega bezpośrednio organowi zarządzającemu operatora infrastruktury krytycznej Operator infrastruktury krytycznej zapewnia koordynatorowi organizacyjne i techniczne warunki realizacji zadań, w tym dostęp do niezbędnych dokumentów i informacji.

W celu zapewnienia bezpieczeństwa osobowego – tak jak ma to miejsce obecnie – w przypadku pracownika zatrudnionego na stanowisku umożliwiającym dostęp do informacji o

bezpieczeństwie obiektu infrastruktury krytycznej i osoby ubiegającej się o zatrudnienie na tym stanowisku, operator infrastruktury krytycznej żąda od pracownika i tej osoby przedłożenia informacji dotyczących karalności, w tym informacji, czy ich dane osobowe są zgromadzone w Krajowym Rejestrze Karnym.

Dodatkowo operator infrastruktury krytycznej może żądać od pracownika danych biometrycznych w postaci odcisków linii papilarnych palców, głosu, obrazu rogówki, sieci żył palców lub biometrii twarzy, jeżeli podanie takich danych jest konieczne ze względu na kontrolę dostępu do informacji o bezpieczeństwie obiektu infrastruktury krytycznej i pomieszczeń.

Identyfikowanie podmiotów krytycznych (art. 1 pkt 8 ustawy nowelizującej)

W projekcie przyjęto założenie utrzymania i rozbudowania kwestii dotyczących infrastruktury krytycznej oraz tego, że podmiotem krytycznym może być operator tejże infrastruktury. Dyrektywa CER wskazuje na infrastrukturę krytyczną jako niezbędną do świadczenia usługi kluczowej a co za tym idzie możliwości uzyskania statusu podmiotu krytycznego.

Co do zasady więc – organ do spraw podmiotów krytycznych może ująć operatora infrastruktury krytycznej w wykazie podmiotów krytycznych jeżeli:

- ✓ świadczy co najmniej jedną usługę kluczową;
- ✓ incydent miałby istotny skutek zakłócający dla świadczenia usługi kluczowej.

Projekt zakłada, że istotność skutku zakłócającego incydentu dla świadczenia usługi kluczowej określana jest na podstawie progów istotności skutku zakłócającego. Rada Ministrów określi, w drodze rozporządzenia:

- ✓ wykaz usług kluczowych w podziale na sektory, podsektory i kategorie podmiotów wymienionych w załączniku do ustawy, uwzględniając znaczenie danej usługi dla utrzymania niezbędnych funkcji społecznych, niezbędnej działalności gospodarczej, zdrowia i bezpieczeństwa publicznego lub środowiska naturalnego;
- ✓ progi istotności skutku zakłócającego dla świadczenia usług kluczowych, wymienionych w wykazie usług kluczowych, z uwzględnieniem:
    - liczby użytkowników zależnych od usługi kluczowej świadczonej przez dany podmiot,
    - stopnia, w jakim inne sektory lub podsektory, o których mowa w załączniku do ustawy, są zależne od usługi świadczonej przez ten podmiot,
    - wpływu, jaki incydent - jeżeli chodzi o jego skalę i czas trwania - mógłby mieć na działalność gospodarczą i społeczną, środowisko, bezpieczeństwo publicznej lub na zdrowie ludności,
    - udziału podmiotu krytycznego w rynku w odniesieniu do świadczonej usługi kluczowej,
    - obszaru geograficzny, którego mógłby dotyczyć incydent,

- znaczenia podmiotu w utrzymywaniu wystarczającego poziomu świadczenia usługi kluczowej przy uwzględnieniu dostępności alternatywnych sposobów jej świadczenia,
- innych czynników charakterystycznych dla danego sektora lub podsektora jeżeli występują.

Wytyczną do wydania rozporządzenia jest potrzeba zapewnienia ochrony przed zagrożeniami życia lub zdrowia, znacznymi stratami majątkowymi oraz obniżeniem jakości świadczonej usługi kluczowej.

W celu identyfikacji podmiotu krytycznego i jego ujęcia w wykazie podmiotów krytycznych - organ do spraw podmiotów krytycznych może wystąpić do wybranego operatora infrastruktury krytycznej o udzielenie informacji, które umożliwią wstępną ocenę, czy spełnia warunki do uznania go za podmiot krytyczny, w szczególności w zakresie spełniania warunków uznania za podmiot krytyczny oraz dodatkowo wskazania infrastruktury krytycznej niezbędnej do świadczenia usługi kluczowej.

Organ do spraw podmiotów krytycznych przekazuje operatorowi dokumenty, w zakresie niezbędnym do udzielenia informacji oraz wskazuje termin udzielenia informacji. Wyznaczony termin nie może być krótszy niż 14 dni, licząc od dnia otrzymania wystąpienia przez operatora.

Operator infrastruktury krytycznej przekazuje organowi do spraw podmiotów krytycznych żądane informacje obejmujące możliwości spełniania warunków, wskazuje infrastrukturę krytyczną niezbędną do świadczenia usługi kluczowej.

Organ do spraw podmiotów krytycznych – w zakresie swojej właściwości – prowadzi wykaz podmiotów krytycznych, który zawiera podstawowe informacje takie jak:

- ✓ nazwę podmiotu krytycznego;
- ✓ siedzibę i adres;
- ✓ numer identyfikacji podatkowej (NIP), jeżeli został nadany;
- ✓ nazwę usługi kluczowej, zgodną z wykazem usług kluczowych;
- ✓ wskazanie sektora, podsektora i kategorii podmiotu;
- ✓ datę rozpoczęcia świadczenia usługi kluczowej;
- ✓ informację wskazującą, w których państwach członkowskich Unii Europejskiej podmiot został uznany za podmiot świadczący usługę kluczową;
- ✓ datę zakończenia świadczenia usługi kluczowej;
- ✓ datę wykreślenia z wykazu podmiotów krytycznych.

Wpis do wykazu podmiotów krytycznych dokonywany jest przez organ do spraw podmiotów krytycznych. Wpis do wykazu jest czynnością materialno-techniczną.

Organ do spraw podmiotów krytycznych informuje operatora infrastruktury krytycznej, w terminie 30 dni od dnia dokonania wpisu do wykazu podmiotów krytycznych, o ujęciu w wykazie oraz obowiązkach z tym związanych. Informację w tym zakresie organ do spraw podmiotów krytycznych przekazuje Szefowi Centrum.

W przypadku zakończenia świadczenia usługi kluczowej przez podmiot krytyczny organ do spraw podmiotów krytycznych dokonuje wykreślenia tego podmiotu z wykazu podmiotów krytycznych. Wykreślenie z wykazu, podobnie jak wpis, jest czynnością materialno-techniczną. Organ do spraw podmiotów krytycznych niezwłocznie informuje podmiot krytyczny o wykreśleniu z wykazu i dacie wykreślenia , jak również przekazuje informację w tym zakresie Szefowi Centrum.

Organy do spraw podmiotów krytycznych i Pojedynczy Punkt Kontaktowy (art. 1 pkt 8 ustawy nowelizującej)

Projekt przyjmuje, że organami do spraw podmiotów krytycznych są:

- ✓ dla sektora energii - minister właściwy do spraw energii;
- ✓ dla sektora transportu z wyłączeniem podsektora transportu wodnego - minister właściwy do spraw transportu;
- ✓ dla podsektora transportu wodnego - minister właściwy do spraw gospodarki morskiej oraz minister właściwy do spraw żeglugi śródlądowej;
- ✓ dla sektora bankowości oraz sektora infrastruktury rynków finansowych - Komisja Nadzoru Finansowego;
- ✓ dla sektora zdrowia - minister właściwy do spraw zdrowia;
- ✓ dla sektora wody pitnej oraz sektora ścieków - minister właściwy do spraw gospodarki wodnej;
- ✓ dla sektora infrastruktury cyfrowa - minister właściwy do spraw informatyzacji;
- ✓ dla sektora administracji publicznej – Prezes Rady Ministrów;
- ✓ dla sektora przestrzeni kosmicznej - minister właściwy do spraw gospodarki;
- ✓ dla sektora produkcji, przetwarzania i dystrybucji żywności - minister właściwy do spraw rolnictwa;
- ✓ dla sektora zarządzanie usługami ICT - minister właściwy do spraw informatyzacji;
- ✓ dla sektora produkcji, wytwarzania i dystrybucji chemikaliów i innych produktów przemysłowych – minister właściwy do spraw środowiska;
- ✓ dla sektora usług pocztowych i kurierskich - minister właściwy do spraw łączności;
- ✓ dla sektora gospodarowania odpadami – minister właściwy do spraw klimatu i zrównoważonego rozwoju.

Do standardowych zadań organu do spraw podmiotów krytycznych należy:

- ✓ prowadzenie bieżącej analizy operatorów infrastruktury krytycznej pod kątem uznania ich za podmiot krytyczny w danym sektorze lub podsektorze;
- ✓ prowadzenie bieżącej analizy podmiotów krytycznych w danym sektorze lub podsektorze pod kątem niespełniania warunków kwalifikujących dany podmiot jako podmiot krytyczny;
- ✓ prowadzenie wykazu podmiotów krytycznych w danym sektorze lub podsektorze, w tym dokonywanie wpisów do wykazu oraz wykreślania z wykazu;
- ✓ prowadzenie bieżącej wymiany informacji oraz współpracy w zakresie obsługi incydentów;
- ✓ monitorowanie stosowania przepisów ustawy przez podmioty krytyczne;
- ✓ prowadzenie kontroli podmiotów krytycznych;
- ✓ prowadzenie działań informacyjnych dotyczących dobrych praktyk, działań edukacyjnych i kampanii na rzecz poszerzania wiedzy i budowania odporności podmiotów krytycznych;
- ✓ uczestniczenie w planowaniu i organizowaniu ćwiczeń podmiotów krytycznych oraz w razie potrzeby udział w tych ćwiczeniach;
- ✓ współpraca z innymi organami do spraw podmiotów krytycznych oraz organami właściwymi do spraw cyberbezpieczeństwa, o których mowa w ustawie o ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa

Projekt zakłada, że organ do spraw podmiotów krytycznych może powierzyć realizację, w jego imieniu, wybranych zadań jednostkom podległym lub nadzorowanym przez ten organ. Powierzenie następuje na podstawie porozumienia, które określa się zasady sprawowania przez organ do spraw podmiotów krytycznych kontroli nad prawidłowym wykonywaniem powierzonych zadań.

W przypadku Prezesa Rady Ministrów – powierza on Szefowi Centrum realizację zadań organu do spraw podmiotów krytycznych w odniesieniu do sektora administracji publicznej, z wyłączeniem nakładania kar pieniężnych.

Poza realizacją zadań powierzonych przez Prezesa Rady Ministrów – Szef Centrum prowadzi Pojedynczy Punkt Kontaktowy, w celu zapewnienia wymiany informacji na potrzeby organów do spraw podmiotów krytycznych, do którego głównych zadań należy:

- ✓ odbieranie zgłoszeń incydentów istotnych z pojedynczych punktów kontaktowych w innych państwach członkowskich Unii Europejskiej;
- ✓ przekazywanie zgłoszeń incydentów istotnych dotyczących innych państw członkowskich Unii Europejskiej do pojedynczych punktów kontaktowych tych państw;
- ✓ opracowywanie i przekazywanie Komisji Europejskiej oraz Grupie do spraw Podmiotów Krytycznych sprawozdań dotyczących incydentów istotnych zgłaszanych przez podmioty krytyczne mających wpływ na ciągłość świadczonych przez nich usług kluczowych na terytorium Rzeczypospolitej Polskiej oraz ciągłość świadczonych usług kluczowych w państwach członkowskich Unii Europejskiej;

- ✓ zapewnienie reprezentacji Rzeczypospolitej Polskiej w Grupie do spraw Podmiotów Krytycznych;
- ✓ zapewnienie współpracy z Komisją Europejską w obszarze zapewnienia bezpieczeństwa świadczenia usług kluczowych;
- ✓ koordynacja współpracy między organami do spraw podmiotów krytycznych i organami administracji publicznej w Rzeczypospolitej Polskiej z odpowiednimi organami w państwach członkowskich Unii Europejskiej;
- ✓ zapewnienie wymiany informacji na potrzeby Grupy Współpracy oraz organami do spraw podmiotów krytycznych;
- ✓ współpracuje z pojedynczym punktem kontaktowym, o którym mowa w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
- ✓ zapewnia koordynację działań organów do spraw podmiotów krytycznych

Dodatkowo organy do spraw podmiotów krytycznych za pośrednictwem Pojedynczego Punktu Kontaktowego prowadzą konsultacje i bieżącą wymianę informacji z właściwymi organami państw członkowskich w przypadku gdy podmioty krytyczne korzystają z infrastruktury krytycznej, która jest fizycznie połączona na terytorium co najmniej dwóch państw członkowskich czy też zostały zidentyfikowane jako podmioty krytyczne w jednym państwie członkowskim i świadczą usługi kluczowe na rzecz innych państw członkowskich lub w innych państwach członkowskich.

Projektowane rozwiązania zawierają ponadto katalog informacji przekazywanych na linii Pojedynczy Punkt Kontaktowy - Grupa do spraw Podmiotów Krytycznych lub Pojedynczy Punkt Kontaktowy - Komisja Europejska. W ostatnim przypadku informacje obejmują:

- ✓ informacje o wyznaczonych organach do spraw podmiotów krytycznych, Pojedynczym Punkcie Kontaktowym, ich zadaniach oraz późniejszych zmianach w tym zakresie oraz przepisach dotyczących kar pieniężnych;
- ✓ informacje umożliwiające ocenę wdrażania dyrektywy Parlamentu Europejskiego i Rady w sprawie odporności podmiotów krytycznych;
- ✓ informacje o zadaniach organów właściwych w sprawach podmiotów krytycznych;
- ✓ informacje o środkach mających na celu zwiększenie odporności podmiotów krytycznych.

<u>Obowiązki podmiotów krytycznych (art. 1 pkt 8 ustawy nowelizującej)</u>

Operator infrastruktury krytycznej, ujęty w wykazie podmiotów krytycznych, jak również poinformowany o ujęciu przez właściwy organ jest obowiązany do realizacji zadań zapewniających niezakłócone świadczenia usługi kluczowej.

Podmiot krytyczny zobowiązany jest do wdrożenia tzw. zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej. Zintegrowany system zapewnia:

- ✓ prowadzenie systematycznej oceny ryzyka

- ✓ wdrożenie odpowiednich i proporcjonalnych do wyników oceny ryzyka rozwiązań organizacyjno-technicznych,
- ✓ bieżącą współpracę z właściwymi podmiotami administracji publicznej dotyczącą wymiany informacji o zagrożeniach i incydentach zakłócających lub mogących zakłócić funkcjonowanie usługi kluczowej oraz sposobu postępowania w przypadku takiego zdarzenia;
- ✓ gromadzenie informacji o zagrożeniach i incydentach zakłócających lub mogących zakłócić świadczenie usługi kluczowej;
- ✓ zarządzanie incydentami;
- ✓ stosowanie środków zapobiegających i ograniczających wpływ incydentów na świadczenie usługi kluczowej.

Podmiot krytyczny jest zobowiązany wdrażać rozwiązania organizacyjno-techniczne, z uwzględnieniem wymagań określonych w Polskich Normach, takich jak PN-EN ISO/IEC 27001, PN-EN ISO 22301, PN-EN 50131, PN-EN 60839, PN-EN 62676 czy też w minimalnych standardach ochrony infrastruktury krytycznej.

W celu zapewnienia wdrożenia rozwiązań na odpowiednim poziomie – podmiot krytyczny żąda od usługodawców w postępowaniach przetargowych lub zamówieniach zdolności do ochrony informacji niejawnych oraz stosowania tych przepisów przy projektowaniu i wykonywaniu obiektów, urządzeń instalacji i innych systemów będących elementami infrastruktury krytycznej oraz certyfikatów potwierdzających posiadanie właściwych kompetencji i uprawnień

Podmiot krytyczny ma obowiązek opracować, stosować i aktualizować dokumentację dotyczącą zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej. Dokumentacja może być prowadzona w postaci papierowej albo w postaci elektronicznej, a podmiot krytyczny jest obowiązany do ustanowienia nadzoru nad dokumentacją zapewniającego dostępność dokumentów wyłącznie dla osób upoważnionych, zgodnie z realizowanymi przez nie zadaniami, ochronę dokumentów przed uszkodzeniem, zniszczeniem, utratą, nieuprawnionym dostępem, niewłaściwym użyciem lub utratą integralności.

Kolejnym zadaniem przypisanym do podmiotu krytycznego jest zapewnienie obsługi incydentów, w tym klasyfikowanie incydent jako istotnego, na podstawie progów uznawania incydentu za istotny. Rada Ministrów określi, w drodze rozporządzenia, progi uznania incydentu za istotny według zdarzenia w poszczególnych sektorach i podsektorach określonych w załączniku do ustawy, uwzględniając:

- ✓ liczbę użytkowników dotkniętych zakłóceniem;
- ✓ czas trwania zakłócenia usługi kluczowej;
- ✓ obszar geograficzny, którego dotyczy zakłócenie;
- ✓ inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują.

Wytyczną do wydania rozporządzenia jest potrzeba zapewnienia ochrony przed zagrożeniami życia lub zdrowia ludzi, znacznymi stratami majątkowymi oraz zagrożeniem obniżenia jakości świadczonej usługi kluczowej.

Projekt przewiduje, że podmiot krytyczny ma obowiązek zgłosić incydent istotny, niezwłocznie, nie później jednak niż w terminie 24 godzin od momentu jego wystąpienia lub wykrycia do organu właściwego w sprawach podmiotów krytycznych oraz Szefa Centrum.

Projekt wskazuje na zakres informacji przekazywanych przy zgłaszaniu incydentu istotnego niezbędne do jego zgłoszenia. Podmiot krytyczny współdziała podczas obsługi incydentu istotnego z organem właściwym w sprawach podmiotów krytycznych lub Szefem Centrum, jak również informuje ich o usunięciu incydentu istotnego.

W trakcie obsługi zgłoszonego incydentu, zarówno organ do spraw podmiotów krytycznych jak i Szef Centrum mogą zwrócić się do podmiotu krytycznego o uzupełnienie zgłoszenia o informacje w zakresie niezbędnym do realizacji zadań w zakresie zapewnienia wsparcia w obsłudze incydentu.

Podmiot krytyczny może przekazywać organom właściwym do spraw podmiotów krytycznych oraz Szefowi Centrum informacje dotyczące incydentów innych niż istotne oraz zagrożeń dla niezakłóconego świadczenia usługi kluczowej.

Do innych obowiązków podmiotu krytycznego – w zakresie informowania określonych kategorii podmiotów należy obowiązek informowania:

- ✓ użytkowników świadczonej usługi kluczowej o zagrożeniach dla niezakłóconego świadczenia tej usługi i stosowaniu skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, w szczególności przez udostępnianie informacji na ten temat na swojej stronie internetowej;
- ✓ właściwych organów zarządzania kryzysowego o incydencie, w przypadku gdy może on doprowadzić do sytuacji kryzysowej.

W celu dokonania obiektywnej analizy bezpieczeństwa świadczenia usługi kluczowej – podmiot krytyczny ma obowiązek przeprowadzania, na własny koszt, co najmniej raz na 3 lata, audytu zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej, w zakresie obejmującym rozwiązania organizacyjno-techniczne wdrożone z uwzględnieniem Polskich Norm, o których mowa w projektowanych regulacjach.

Uprawienie do nakazania audytu podmiotowi krytycznemu ma również organ do spraw podmiotów krytycznych.

Co do zasady przewiduje się, że audyt może być prowadzony przez:

- ✓ jednostkę certyfikującą akredytowaną lub upoważnioną do certyfikacji na zgodność z Polskimi Normami wskazanymi w akcie wykonawczym wydanym na do ustawy;
- ✓ co najmniej dwóch audytorów, w tym jednego z ukończonym szkoleniem audytora wiodącego.

Mając na względzie bezpieczeństwo świadczenia usługi kluczowej – zakłada się, że audyt podmiotu krytycznego powinien być prowadzony przez usługodawców spełniających wymagania bezpieczeństwa osobowego i, jeśli ma to zastosowanie, przemysłowego w zakresie dostępu do informacji niejawnych o klauzuli „poufne".

Rada Ministrów określi, w drodze rozporządzenia wykaz:

- ✓ certyfikatów uprawniających do realizacji rozwiązań organizacyjno-technicznych;
- ✓ certyfikatów uprawniających do przeprowadzenia audytów, uwzględniając zakres wiedzy specjalistycznej wymaganej od osób lub podmiotów legitymujących się poszczególnymi certyfikatami oraz wymagane doświadczenie;
- ✓ Polskich Norm przeznaczonych do certyfikacji rozwiązań organizacyjno-technicznych.

Na podstawie zebranych dokumentów i dowodów jednostka certyfikująca lub audytorzy sporządzają pisemne sprawozdanie z przeprowadzonego audytu i przekazuje je podmiotowi krytycznemu wraz z dokumentacją z przeprowadzonego audytu.

Podmiot krytyczny ma obowiązek przedstawić kopię sprawozdania z przeprowadzonego audytu właściwemu organowi do spraw podmiotów krytycznych w terminie 7 dni roboczych.

Podmiot krytyczny – zgodnie z proponowanymi przepisami – zapewnia udział struktur organizacyjnych lub pracowników niezbędnych do zapewnienia niezakłóconego świadczenia usługi kluczowej w szkoleniach i ćwiczeniach, w tym w ćwiczeniach z zakresu obrony cywilnej, ochrony ludności, zarządzania kryzysowego oraz obronnych.

Podmiot krytyczny we współpracy z właściwym organem do spraw podmiotów krytycznych lub Szefem Centrum planuje i organizuje udział w szkoleniach i ćwiczeniach.

Podmiot krytyczny ma obowiązek wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z właściwymi podmiotami do spraw podmiotów krytycznych oraz Szefem Centrum, w szczególności zapewniającą koordynację obiegu informacji, zwaną dalej „osobą do kontaktów". Podmiot krytyczny wyznacza osobę do kontaktów w terminie 30 dni od dnia otrzymania informacji, o ujęciu w wykazie podmiotów świadczących usługi kluczowe.

Osoba do kontaktów jest pracownikiem podmiotu krytycznego, korzystającą z pełni praw publicznych, posiadającą wiedzę, umiejętności i doświadczenie w zakresie zarządzania bezpieczeństwem, z uwzględnieniem przedmiotu działalności podmiotu świadczące usługę kluczową. Dodatkowo nie może być skazana prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe jak również spełniać wymagania bezpieczeństwa osobowego w zakresie dostępu do informacji niejawnych o klauzuli „poufne".

Osoba do kontaktów podlega bezpośrednio organowi zarządzającemu podmiotu krytycznego, której to podmiot zapewnia osobie do kontaktów organizacyjne i techniczne warunki realizacji zadań. O wyznaczeniu osoby do kontaktów podmiot krytyczny informuje niezwłocznie właściwy organ do spraw podmiotów krytycznych oraz Szefa Centrum, przekazując dane tej osoby obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej.

W ramach zabezpieczenia osobowego podmiot krytyczny może prowadzić sprawdzenie przeszłości w przypadku swoich pracowników lub kandydatów na pracowników, którzy pełnią lub mogą pełnić newralgiczne role w strukturach organizacyjnych podmiotu krytycznego lub wykonywać zadania na jego rzecz oraz osób, które są lub mogą być upoważnieni do posiadania bezpośredniego lub zdalnego dostępu do budynków i terenów podmiotu krytycznego, obiegu informacji lub systemów kontroli, w tym w związku z bezpieczeństwem podmiotu krytycznego.

Newralgiczną rolę w strukturach organizacyjnych podmiotu krytycznego lub przy wykonywaniu zadań na jego rzecz są osoby

- ✓ reprezentujące podmiot krytyczny samodzielnie lub łącznie z innymi osobami na podstawie statutu, umowy lub innego aktu założycielskiego;
- ✓ pełniące funkcje kierownicze lub koordynacyjne;
- ✓ wykonujące zadania związane z procesami zapewniającymi niezakłócone świadczenie usługi kluczowej lub funkcjonowaniem infrastruktury krytycznej niezbędnej do świadczenia usługi kluczowej.

Sprawdzenie przeszłości obejmuje:

- ✓ potwierdzenie tożsamości osoby, która podlega sprawdzeniu przeszłości;
- ✓ sprawdzenie rejestrów karnych tej osoby pod kątem przestępstw, które miałyby znaczenie dla zajmowanego stanowiska lub w przypadku ubiegania się o to stanowisko we wszystkich państwach pobytu z ostatnich 5 lat;
- ✓ potwierdzenie informacji o zatrudnieniu, wykształceniu, zdobywaniu umiejętności, podnoszeniu kwalifikacji oraz wszystkich przerwach w zatrudnieniu z ostatnich 5 lat.

Podmiot krytyczny powtarza sprawdzenia w regularnych odstępach czasu nieprzekraczających pięciu lat.

<u>Podmiot krytyczny o szczególnym znaczeniu europejskim (art. 1 pkt 14 ustawy nowelizującej)</u>

Zgodnie z dyrektywa CER podmioty krytyczne działają zazwyczaj jako element w coraz większym stopniu wzajemnie powiązanej sieci świadczenia usług i infrastruktury oraz często świadczą usługi kluczowe w więcej niż jednym państwie członkowskim. Niektóre z tych podmiotów krytycznych mają szczególne znaczenie dla Unii i jej rynku wewnętrznego, ponieważ świadczą usługi kluczowe na rzecz co najmniej sześciu państw członkowskich lub w co najmniej sześciu państwach członkowskich, i zgodnie z unijną polityką w tym zakresie mogłyby korzystać ze szczególnego wsparcia na poziomie Unii. Aby tak się stało projekt przewiduje możliwość identyfikacji tzw. podmiot krytycznego o szczególnym znaczeniu europejskim. Aby zidentyfikować podmiot krytyczny o takiej kategorii podmiot krytyczny, zidentyfikowany na podstawie krajowych regulacji, informuje właściwy organ do spraw podmiotów krytycznych oraz Pojedynczy Punkt Kontaktowy o fakcie świadczenia usługi kluczowej na rzecz co najmniej sześciu państw członkowskich Unii Europejskiej lub w co najmniej sześciu państwach członkowskich Unii Europejskiej.

W takim przypadku organ właściwy organ do spraw podmiotów krytycznych, za pośrednictwem Pojedynczego Punktu Kontaktowego informuje Komisję Europejską o potencjalnym podmiocie krytycznym o szczególnym znaczeniu europejskim, przekazując niezbędne informacje na temat tego podmiotu.

Właściwy organ do spraw podmiotów krytycznych, za pośrednictwem Pojedynczego Punktu Kontaktowego, inicjuje i prowadzi konsultacje z Komisją Europejską oraz właściwymi organami państw członkowskich Unii Europejskiej w celu ustalenia, czy podmiot krytyczny świadczący usługę kluczową na terytorium Rzeczypospolitej Polskiej, świadczy ją na rzecz co najmniej sześciu państw członkowskich Unii Europejskiej lub w co najmniej sześciu państwach członkowskich Unii Europejskiej.

Na podstawie ustaleń będących wynikiem konsultacji właściwy organ do spraw podmiotów krytycznych informuje podmiot krytyczny o uznaniu za podmiot krytyczny o szczególnym znaczeniu europejskim oraz obowiązkach z tym związanych.

Organ do spraw podmiotów krytycznych, we współpracy z Pojedynczym Punktem Kontaktowym zapewnia współpracę z Komisją Europejską oraz właściwymi organami państw członkowskich, na rzecz którego lub w którym jest świadczona usługa kluczowa, w tym prowadzi wymianę informacji w zakresie oceny ryzyka podmiotu krytycznego o szczególnym znaczeniu europejskim, wdrażania odpowiednich i proporcjonalnych do wyników oceny ryzyka rozwiązań organizacyjno-technicznych służących zapewnieniu odporności tego podmiotu oraz działań z zakresu nadzoru oraz egzekwowania przepisów ustawy przez właściwy organ do spraw podmiotów krytycznych.

Właściwy organ do spraw podmiotów krytycznych, we współpracy z Pojedynczym Punktem Kontaktowym zapewnia współpracę z Komisją Europejską w zakresie zapewnienia obsługi tzw. misji doradczej, w tym:

- ✓ konsultuje program misji doradczej;
- ✓ koordynuje realizację czynności związanych z dostępem przedstawicieli misji doradczej do informacji oraz budynków, terenów i infrastruktury krytycznej podmiotu krytycznego o szczególnym znaczeniu europejskim;
- ✓ przeprowadza analizę sprawozdania z ustaleń misji doradczej

Właściwy organ do spraw podmiotów krytycznych we współpracy z Pojedynczym Punktem Kontaktowym:

- ✓ po dokonaniu analizy sprawozdania z ustaleń misji doradczej, przedkłada Komisji Europejskiej informację o stopniu wdrożenia rozwiązań organizacyjno-technicznych służących zapewnieniu odporności podmiotu krytycznego o szczególnym znaczeniu europejskim lub przedkłada rekomendacje w zakresie zwiększenia odporności tego podmiotu, w celu wydania przez Komisję Europejską opinii dotyczącej wywiązywania się z nałożonych obowiązków przez ten podmiot lub wskazującej środki, które można wprowadzić, aby zwiększyć odporność tego podmiotu;

- ✓ przekazuje opinię Komisji Europejskiej podmiotowi krytycznemu o szczególnym znaczeniu europejskim oraz zapewnia wsparcie w przypadku konieczności wdrożenia dodatkowych środków zwiększających odporność;
- ✓ informuje Komisję Europejską oraz właściwe organy państw członkowskich, na rzecz którego lub w którym jest świadczona usługa kluczowa, o środkach zwiększających odporność, wprowadzonych z uwzględnieniem opinii Komisji Europejskiej albo informację o braku konieczności wprowadzania tych środków.

Nadzór i kontrola podmiotów krytycznych (art. 1 pkt 8 ustawy nowelizującej)

Nadzór w zakresie stosowania przepisów ustawy sprawują organy do spraw podmiotów krytycznych w zakresie:

- ✓ spełniania przez podmioty krytyczne wymogów bezpieczeństwa dotyczących świadczenia usług kluczowych;
- ✓ wykonywania przez podmioty krytyczne obowiązków wynikających z ustawy dotyczących przeciwdziałania zagrożeniom dla świadczonych usług kluczowych i zgłaszania incydentów istotnych.

Przepisy przewidują, że w ramach nadzoru organ do spraw podmiotów krytycznych prowadzi kontrole podmiotów krytycznych oraz infrastruktury krytycznej należącej do tych podmiotów, przeprowadza lub zleca audyt zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej oraz nakłada kary pieniężne na podmioty krytyczne.

Do kontroli realizowanej wobec podmiotów:

- ✓ będących przedsiębiorcami stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. - Prawo przedsiębiorców;
- ✓ niebędących przedsiębiorcami stosuje się przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej określające zasady i tryb przeprowadzania kontroli.

Dodatkowo przepisy określają czynności kontrolne wobec podmiotów będących przedsiębiorcami.

Jeżeli na podstawie informacji zgromadzonych w protokole kontroli organ do spraw podmiotów krytycznych uzna, że mogło dojść do naruszenia przepisów ustawy przez podmiot kontrolowany, przekazuje zalecenia pokontrolne dotyczące usunięcia nieprawidłowości. Od zaleceń pokontrolnych nie przysługują środki odwoławcze.

Dodatkowo podmiot kontrolowany ma obowiązek, w wyznaczonym terminie, poinformować organ do spraw podmiotów krytycznych o sposobie wykonania zaleceń.

Kary pieniężne dla podmiotów krytycznych (art. 1 pkt 8ustawy nowelizującej)

Projekt przewiduje katalog kar za brak realizacji obowiązków wynikających z projektowanej ustawy. Kary pieniężne nakładają, w drodze decyzji, właściwe organy do spraw podmiotów krytycznych.

Wpływy z tytułu kar pieniężnych:

- ✓ w 50% przychód Funduszu Cyberbezpieczeństwa, o którym mowa w art. 2 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa, w zakresie maksymalnej kwoty prognozowanych kosztów związanych z przyznaniem świadczenia teleinformatycznego, o którym mowa w art. 5 tej ustawy;
- ✓ w 50 % przychód Państwowego Fundusz Ochrony Ludności, o którym mowa w art. 119 ustawy o ochronie ludności i obronie cywilnej.

Pozostałe zmiany w ustawie o zarządzaniu kryzysowym

- ✓ (art. 1 pkt 10-11 ustawy nowelizującej) propozycja dokonania zmian w zakresie poleceń Prezesa Rady Ministrów, o których mowa w art. 7a i 7ba i dalszych ustawy o zarządzaniu kryzysowym jest propozycją dostosowującą do nowych uregulowań w zakresie usług kluczowych. W zmienianych przepisach przedmiotem poleceń będzie nie tylko infrastruktura krytyczna lecz również usługa kluczowa;
- ✓ (art. 1 pkt 12 ustawy nowelizującej) zmiana w obrębie art. 10 ustawy o zarządzaniu kryzysowym jest dostosowaniem do zmiany nazwy „dyrektora Centrum" na „Szefa Centrum";
- ✓ (art. 1 pkt 13 ustawy nowelizującej) dodanie nowych art. 11b - 11 e w brzmieniu ma na celu przede wszystkim dostosowanie przepisów do stanu faktycznego. Centrum w praktyce realizuje zadania w zakresie planowania cywilnego wynikającego z członkostwa w Organizacji Traktatu Północnoatlantyckiego, Centrum, w tym koordynuje udział przedstawicieli Rzeczypospolitej Polskiej w pracach prowadzonych na forum NATO (np. Komitetu Odporności NATO) oraz zapewnia wsparcie merytoryczne prowadzonych prac czy też uruchamiania przedsięwzięcia i procedur systemu zarzadzania kryzysowego NATO.

  W przypadku tworzenie i funkcjonowanie systemu teleinformatycznego wykorzystywanego jako narzędzie wspierające realizację zadań zarządzania kryzysowego – w projektowanych przepisach wskazano podstawowe rozwiązania organizacyjno-prawne funkcjonowania rozwiązań, które mają zapewnić zgłaszanie informacji o potencjalnych zagrożeniach oraz zaistniałych zagrożeniach, gromadzenie informacji o zagrożeniach oraz analizę tych informacji, gromadzenie informacji o siłach i środkach niezbędnych do realizacji zadań zarządzania kryzysowego oraz agregowanie i korelowanie pozyskiwanych informacji.

  Ze względu na dynamikę zmian w środowisku bezpieczeństwa system należy uznać za niezbędny dla tworzenia wspólnej świadomości sytuacyjnej, w tym w zakresie dostępnych

zasobów. Obecnie gromadzenie danych dotyczących sił i środków nie jest ustandaryzowane, co utrudnia zarówno gromadzenie danych, jak i ich analizę.

Rosnąca rola zdolności do analizowania i zbierana danych z dużej liczby sensorów należących do różnych podmiotów powinna w jak najszybszym czasie przełożyć się na poprawienie obecnej zdolności do wymiany zweryfikowanych już informacji, zarówno na potrzeby zarządzania kryzysami, jak i uruchamiania zasobów na potrzeby ograniczania skutków kryzysów. W nawiązaniu do cyklu Boyda obserwacja sensoryczna wpływa na powstanie możliwie pełnego obrazy wydarzeń, co warunkuje podjęcie w jak najkrótszym czasie opartej o wiarygodne dane decyzji o uruchomieniu odpowiednich zasobów. Ostatnim elementem jest skierowanie aktywowanych zasobów w rejon sytuacji kryzysowej na każdym poziomie administracji publicznej;

- ✓ (art. 1 pkt 14 ustawy nowelizującej) zmiany w art. 12 ustawy o zarządzaniu kryzysowym są dostosowaniem do zmian w zakresie planów zarzadzania kryzysowego, wynikających z dostosowania do UMOL;
- ✓ (art. 1 pkt 15 ustawy nowelizującej) uchylenie w art. 13 ustawy o zarządzaniu kryzysowym ust. 2a jest zmianą, która w założeniu ma zaktywizować resorty do posiadania w pełni funkcjonalnych resortowych centrów zarządzania kryzysowego, stosownie do zapisu art. 13 ust. 1 ustawy o zarządzaniu kryzysowym (ze względu na sprawy związane z zapewnieniem bezpieczeństwa narodowego, w tym ochrony ludności lub gospodarczych podstaw bezpieczeństwa państwa). Nie ulega zmianie konstrukcja przewidująca delegację dla Rady Ministrów do wydania rozporządzenia określającego m.in. organy administracji rządowej które mają obowiązek utworzyć centra zarządzania kryzysowego;
- ✓ (art. 1 pkt 16, 17, 18 ustawy nowelizującej) zmiany w art. 14 w ust. 4, art. 20b oraz art. 21a ustawy o zarządzaniu kryzysowym są dostosowaniem do zmiany nazwy „dyrektora Centrum" na „Szefa Centrum";
- ✓ (art. 1 pkt 20 ustawy nowelizującej) wprowadzenie do art. 26 ustawy o zarządzaniu kryzysowym ust. 4a jest wynikową zmian w zakresie nowej planistyki na potrzeby zarządzania kryzysowego. Zgodnie z propozycją, wskazuje się precyzyjnie, że środki finansowe z rezerwy celowej, tworzonej na potrzeby zarządzania kryzysowego, mogą być przeznaczone na realizację przedsięwzięć związanych z zarządzaniem ryzykiem oraz reagowaniem w przypadku wystąpienia sytuacji kryzysowej oraz usuwaniem jej skutków i odtwarzaniem zasobów.

<u>Zmiany w innych ustawach (art. 2 -12 ustawy nowelizującej)</u>

- ✓ ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2018 r. poz. 2142 i 2245 oraz z 2019 r. poz. 1495) – zmiana wynikowa – zmiana definicji infrastruktury krytycznej oraz systematyki ustawy o zarządzaniu kryzysowym;
- ✓ ustawie z dnia 29 listopada 2000 r. - Prawo atomowe (Dz. U. z 2023 r. poz. 1890 oraz z 2024 r. poz. 834) – zmiana wynikowa – dostosowanie do zmiany nazwy „dyrektora Centrum" na „Szefa Centrum;

- ✓ ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2024 r. poz. 812) – zmiany wynikowe – zmiana definicji infrastruktury krytycznej oraz systematyki ustawy o zarządzaniu kryzysowym;
- ✓ ustawa z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw aktywów państwowych oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych (Dz. U. z 2020 r. poz. 2173 oraz z 2024 r. poz. 834) – zmiana wynikowa – dostosowanie do systematyki ustawy o zarządzaniu kryzysowym oraz do zmiany nazwy „dyrektora Centrum" na „Szefa Centrum. Ponadto zmiany obejmują kwestię możliwości łączenia funkcji koordynatora infrastruktury krytycznej z pełnomocnikiem do spraw ochrony infrastruktury krytycznej, o którym mowa w tej ustawie;
- ✓ ustawa z dnia 14 grudnia 2012 r. o odpadach (Dz. U. z 2019 r. poz. 701, 730, 1403 i 1579) – zmiana wynikowa – zmiana definicji infrastruktury krytycznej oraz systematyki ustawy o zarządzaniu kryzysowym;
- ✓ ustawa z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2024 r. poz. 383) – zmiana wynikowa – zmiana definicji infrastruktury krytycznej oraz systematyki ustawy o zarządzaniu kryzysowym;
- ✓ ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560 oraz z 2019 r. poz. 2020 i 2248) – zmiany wynikowe – zmiana definicji infrastruktury krytycznej oraz systematyki ustawy o zarządzaniu kryzysowym;
- ✓ ustawa z dnia 17 grudnia 2020 r. o rezerwach strategicznych (Dz. U. z 2023 r. poz. 294) – zmiany wynikowe do ustawy o zarządzaniu kryzysowym;
- ✓ ustawa z dnia 27 stycznia 2023 r. o kontroli niektórych inwestycji (Dz. U. z 2023 r. poz. 415 oraz z 2024 r. poz. 834) – zmiana wynikowa – dostosowanie do zmiany nazwy „dyrektora Centrum" na „Szefa Centrum";
- ✓ ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. poz. 1703) – zmiana wynikowa – dostosowanie do zmiany nazwy „dyrektora Centrum" na „Szefa Centrum".

Przepisy przejściowe i końcowe (art. 13-35 ustawy nowelizującej)

Krajowa Ocena Ryzyka zostanie sporządzona po raz pierwszy w terminie do dnia 17 stycznia 2026 r.

Strategia Odporności Podmiotów Krytycznych zostanie sporządzona po raz pierwszy w terminie do dnia 17 stycznia 2026 r.

Krajowy Plan Zarządzania Kryzysowego w brzmieniu nadanym projektowaną ustawą zostaną sporządzone po raz pierwszy w terminie do dnia 1 września 2026 r. Pozostałe plany zarządzania kryzysowego sporządza się po raz pierwszy w terminie w terminie 6 miesięcy od dnia przyjęcia Krajowego Planu Zarządzania Kryzysowego.

Plany sporządzone po raz pierwszy nie zawierają oceny osiągniętych efektów oraz wniosków z wdrożonych działań.

Plany zarządzania kryzysowego sporządzone i zatwierdzone na podstawie dotychczasowych przepisów pozostają w mocy do czasu sporządzenia nowych planów.

Szczegółowe kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi, w brzmieniu dotychczasowym, pozostają w mocy do czasu sporządzenia nowych kryteriów.

Jednolity wykaz obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej w brzmieniu dotychczasowym, pozostaje w mocy do czasu sporządzenia nowego wykazu i może być w tym czasie aktualizowany.

Właściciele, posiadacze samoistni i zależni obiektów instalacji, urządzeń i usług ujętych w jednolitym wykazie infrastruktury krytycznej w brzmieniu dotychczasowym, realizują zadania w zakresie ochrony infrastruktury krytycznej na podstawie dotychczasowych przepisów do czasu ujęcia w „nowym" wykazie infrastruktury krytycznej.

Kryteria identyfikacji infrastruktury krytycznej w brzmieniu nadanym projektowaną ustawą zostaną sporządzone po raz pierwszy w terminie do dnia 17 stycznia 2026 r.

Wykaz infrastruktury krytycznej w brzmieniu nadanym projektowaną ustawą, zostanie sporządzony w terminie do dnia 17 stycznia 2026 r.

Projektowany przepis art. 26 ust. 4a ustawy o zarządzaniu kryzysowym będzie miał zastosowanie po raz pierwszy do opracowania budżetów jednostek samorządu terytorialnego na 2025 r.

Przepisy wykonawcze wydane na podstawie art. 21a ustawy zmienianej w art. 1 w brzmieniu dotychczasowym zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 21a ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą, jednak nie dłużej niż przez 12 miesięcy od dnia wejścia w życie niniejszej ustawy.

System teleinformatyczny wykorzystywany jako narzędzie wspierające realizację zadań zarządzania kryzysowego zostanie wdrożony w terminie 24 miesięcy od dnia wejścia w życie ustawy.

Załącznik do ustawy określa sektory, a w ich obrębie, podsektory. Wskazane w załączniku obszary, bazują na wskazanych w dyrektywie CER, jak również zostały w części skorelowane z sektorami, które muszą zostać zaimplementowane z dyrektywy NIS2.

Projektowana ustawa wejdzie w życie po upływie 14 dni od dnia jej ogłoszenia. Taki termin jest wystraczający aby właściwe podmioty miały czas na zapoznanie się z nimi. Termin ten jest też konieczny z uwagi na konieczność jak najszybszego wdrożenia rozwiązań zawartych w dyrektywie CER.

Pozostałe informacje

Projekt ustawy nie zawiera przepisów technicznych w rozumieniu przepisów 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 w związku z tym nie podlega procedurze notyfikacji.

Projekt ustawy jest zgodny z przepisami prawa Unii Europejskiej i służy ich stosowaniu.

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

Projekt ustawy stosownie do wymogów art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248) oraz zgodnie z § 52 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2022 r. poz. 348) został zamieszczony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Bezpieczeństwa.