Informacja o ustawie z dnia 29 maja 2026 r. o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw

Głównymi celami ustawy jest:

- wzmocnienie systemu zarządzania kryzysowego poprzez wprowadzenie rozwiązań zapewniających efektywne zarządzanie 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,
- wdrożenie 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,
- wzmocnienie ochrony infrastruktury krytycznej, w szczególności niezbędnej do świadczenia tzw. usług kluczowych przez podmioty krytyczne,
- wdrożenie rozwiązań umożliwiających wzmocnienie ochrony najważniejszych dla państwa obszarów, obiektów i urządzeń, w szczególności infrastruktury morskiej.

Zgodnie z nowym brzmieniem przepisu o zakresie przedmiotowym ustawy o zarządzaniu kryzysowym ustawa ta określa:

1) organy właściwe w sprawach zarządzania kryzysowego oraz zadania i zasady działania tych organów;
2) organy właściwe w sprawach identyfikacji infrastruktury krytycznej oraz ich zadania;
3) zadania i obowiązki operatorów infrastruktury krytycznej;
4) usługi kluczowe oraz zadania i obowiązki podmiotów krytycznych;
5) organy do spraw podmiotów krytycznych oraz ich zadania;
6) zasady sprawowania nadzoru nad podmiotami krytycznymi oraz ich kontroli;
7) zasady finansowania zadań, o których mowa w pkt 1–6.

W zakresie przepisów dotyczących 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, zwanej dalej „decyzją UMOL" ustawa przewiduje wdrożenie zintegrowanego podejścia do zarządzania ryzykiem, obejmującego cały cykl zarządzania, od oceny ryzyka przez przygotowanie planów zarządzania nim oraz wdrażanie środków zapobiegawczych i zapewniających gotowość do ich użycia.

Ustawa przewiduje opracowanie na szczeblu centralnym dokumentu rządowego - Krajowej Oceny Ryzyka przyjmowanego przez Radę Ministrów w formie uchwały, 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 ryzyka.

Krajowa Ocena Ryzyka – w obszarze planowania cywilnego – będzie wykorzystywana na potrzeby opracowywania planów zarządzania ryzykiem (działania w zakresie zapobiegania sytuacji kryzysowej oraz przygotowywania do jej wystąpienia) oraz planów reagowania kryzysowego (działania w zakresie reagowania w przypadku wystąpienia sytuacji kryzysowej oraz usuwaniu jej skutków) ministrów, kierowników urzędów centralnych, wojewodów, jak również planów zarządzania kryzysowego na szczeblu powiatowym oraz gminnym.

Planistyka na szczeblu krajowym w zakresie zarządzania ryzykiem, zgodnie ze zmienioną ustawą o zarzadzaniu kryzysowym, będzie obejmować opracowanie Krajowego Planu Zarządzania Ryzykiem oraz Krajowego Planu Reagowania Kryzysowego i będzie należała do obowiązków Dyrektora Rządowego Centrum Bezpieczeństwa (RCB).

Opracowywane obecnie plany zarządzania kryzysowego podzielone zostaną na plany zarządzania ryzykiem oraz plany reagowania kryzysowego. Plany zarządzania ryzykiem poza dyrektorem RCB będą opracowywać również ministrowie kierujący działem administracji rządowej (plan zarządzania ryzykiem ministra kierującego działem administracji rządowej), Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Agencji Wywiadu oraz Szef Centralnego Biura Antykorupcyjnego (plan zarządzania ryzykiem odpowiednio Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Agencji Wywiadu oraz Szefa Centralnego Biura Antykorupcyjnego), kierownik urzędu centralnego wskazany przez ministra kierującego działem administracji rządowej, któremu podlega lub przez którego jest nadzorowany (plan

zarządzania ryzykiem kierownika urzędu centralnego), wojewoda (wojewódzki plan zarządzania ryzykiem), starosta (powiatowy plan zarządzania ryzykiem), wójt (burmistrz, prezydent miasta) – (gminny plan zarządzania ryzykiem). Analogicznie te same organy będą opracowywać analogiczne plany reagowania kryzysowego.

Ustawa ujednolica terminy cyklów planistycznych do regulacji unijnych. Nowy cykl planistyczny będzie obejmował 3 lata. Dodatkowo przewiduje się, że Krajowa Ocena Ryzyka oraz Krajowy Plan Zarządzania Ryzykiem będą punktami odniesienia do opracowania dokumentów udostępnianych Komisji Europejskiej w ramach realizacji postanowień decyzji UMOL, tj. streszczenia istotnych elementów krajowej oceny ryzyka oraz streszczenia istotnych elementów krajowej oceny zdolności zarządzania ryzykiem.

W zakresie wdrożenia 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, str. 164), zwaną dalej „dyrektywą 2022/2557", wprowadzane regulacje dotyczą w szczególności:

- identyfikacji usług kluczowych świadczonych przez operatorów infrastruktury krytycznej z uwzględnieniem potencjalnych skutków zakłócenia usług,
- minimalizacji skutków zakłócenia usług poprzez wprowadzenie procesów oceny i zarządzania ryzykiem,
- modyfikacji obecnych rozwiązań w zakresie ochrony infrastruktury krytycznej, która jest niezbędnym elementem świadczenia usług kluczowych przez podmioty krytyczne,
- identyfikacji i wyznaczanie podmiotów krytycznych (w tym podmiotów krytycznych o szczególnym znaczeniu europejskim) w podziale na tzw. sektory i podsektory, o których mowa w dyrektywie 2022/2557, jak również regulacje w zakresie nadzoru nad podmiotami krytycznymi oraz egzekwowania przepisów,
- obowiązków opracowania krajowej strategii w zakresie zwiększenia odporności podmiotów krytycznych,
- obowiązków podmiotów krytycznych mających na celu zwiększenie ich odporności i zdolności do świadczenia usług kluczowych niezbędnych dla utrzymania funkcji społecznych lub niezbędnej działalności gospodarczej,
- wskazanie organów odpowiedzialnych za prawidłowe stosowanie, jak również egzekwowanie przepisów na szczeblu krajowym oraz na poziomie sektorowym,
- wyznaczenie tzw. pojedynczego punktu kontaktowego zapewniającego współpracę transgraniczną z pojedynczymi punktami kontaktowymi innych państw członkowskich

oraz z powoływaną na mocy dyrektywy 2022/2557 tzw. Grupą ds. Odporności Podmiotów Krytycznych,

- określenia mechanizmów wsparcia podmiotów krytycznych obejmujących opracowanie wytycznych oraz metodyk, pomoc w organizacji ćwiczeń mających na celu sprawdzenie odporności podmiotów krytycznych, jak również zapewnienie doradztwa i szkoleń personelu tychże podmiotów,
- zapewnienia mechanizmów sporządzania ocen ryzyka podmiotów krytycznych, stanowiących m.in. podstawę do projektowania i wdrażania środków dla zwiększenia odporności,
- określenia środków, które muszą być wprowadzone przez podmioty krytyczne dla zwiększenia ich odporności obejmujących środki techniczne, środki bezpieczeństwa oraz środki organizacyjne,
- wskazania mechanizmów sporządzania planów zwiększania odporności podmiotów krytycznych lub wskazania innych, tożsamych co do treści dokumentów,
- wskazania mechanizmów wymiany informacji między podmiotami krytycznymi a właściwymi organami m.in. w zakresie zgłaszania zdarzeń zakłócających funkcjonowanie świadczenia usług przez podmioty krytyczne, jak również na rzecz bieżącego monitorowania zdarzeń lub zagrożeń mogących mieć wpływ na świadczenie usług przez podmioty krytyczne,
- mechanizmów koordynacji tzw. misji doradczych realizowanych przez Komisję Europejską w odniesieniu do podmiotów krytycznych o szczególnym znaczeniu europejskim,
- mechanizmów przeprowadzania audytów lub kontroli podmiotów krytycznych,
- wskazanie sankcji mających zastosowanie w przypadku naruszeń przepisów krajowych przyjętych na podstawie dyrektywy 2022/2557.

Zmieniana ustawa o zarządzaniu kryzysowym wprowadza definicję usługi kluczowej rozumianej jako usługę, która ma decydujące znaczenie dla utrzymania niezbędnych funkcji społecznych, niezbędnej działalności gospodarczej, zdrowia i bezpieczeństwa publicznego lub środowiska, natomiast wykaz tych usług w poszczególnych sektorach lub podsektorach z jednoczesnym wskazaniem kategorii podmiotów mogących świadczyć usługi określi Rada Ministrów w drodze rozporządzenia (art. 6zp ust. 3 ustawy o zarządzaniu kryzysowym). Usługi kluczowe, co do zasady, będą realizowane przez operatorów infrastruktury krytycznej, za pomocą posiadanej przez nich infrastruktury.

Ustawa definiuje podmioty krytyczne, jako operatora infrastruktury krytycznej wpisanego do wykazu podmiotów krytycznych, natomiast przez podmiot krytyczny o szczególnym znaczeniu europejskim ustawa rozumie podmiot krytyczny świadczący co najmniej jedną usługę kluczową lub świadczący te same lub podobne usługi kluczowe na rzecz co najmniej sześciu państw członkowskich Unii Europejskiej lub w co najmniej sześciu państwach członkowskich Unii Europejskiej, uznany za taki podmiot przez Komisję Europejską. Podmioty krytyczne będą identyfikowane przez wskazane ustawą organy do spraw podmiotów krytycznych i ujmowane w wykazach podmiotów krytycznych, prowadzonych przez te organy, zgodnie z ich właściwością. Podmiot krytyczny będzie obowiązany w szczególności do (rozdział 11 ustawy o zarządzaniu kryzysowym) wdrożenia zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej obejmującego:

1) przeprowadzenie nierzadziej niż raz na 2 lata oceny ryzyka;
2) wdrożenie odpowiednich i proporcjonalnych do wyników oceny ryzyka rozwiązań organizacyjno-technicznych, dotyczących bezpieczeństwa świadczonej usługi (w tym infrastruktury krytycznej, za pomocą której świadczona jest usługa kluczowa), z uwzględnieniem polskich norm;
3) bieżącą współpracę z właściwymi organami zarządzania kryzysowego oraz służbami, strażami i inspekcjami dotyczącą wymiany informacji o zagrożeniach i incydentach zakłócających lub mogących zakłócić funkcjonowanie usługi kluczowej oraz sposobu postępowania w przypadku takiego zdarzenia;
4) gromadzenie informacji o zagrożeniach i incydentach zakłócających lub mogących zakłócić świadczenie usługi kluczowej;
5) zarządzanie incydentami;
6) stosowanie środków zapobiegających i ograniczających wpływ incydentów na świadczenie usługi kluczowej.

Ustawa określa również sposób identyfikacji i wyznaczania tzw. podmiotu krytycznego o szczególnym znaczeniu europejskim (rozdział 12 ustawy o zarządzaniu kryzysowym).

Ustawa w rozdziale 8 zmienianej ustawy o zarządzaniu kryzysowym wskazuje organy do spraw podmiotów krytycznych w poszczególnych sektorach i podsektorach oraz określa ich zadania. Zgodnie z ustawą organ do spraw podmiotów krytycznych:

1) prowadzi bieżącą analizę operatorów infrastruktury krytycznej pod względem uznania ich za podmiot krytyczny w danym sektorze lub podsektorze;

2) prowadzi bieżącą analizę podmiotów krytycznych w danym sektorze lub podsektorze pod względem niespełniania warunków kwalifikujących dany podmiot jako podmiot krytyczny;
3) składa wnioski o dokonanie wpisu do wykazu podmiotów krytycznych oraz wykreślenia z tego wykazu;
4) prowadzi bieżącą wymianę informacji z podmiotami krytycznymi oraz ułatwia dobrowolną wymianę informacji między podmiotami krytycznymi w danym sektorze lub podsektorze;
5) współpracuje z podmiotami krytycznymi w danym sektorze lub podsektorze w zakresie obsługi incydentów;
6) monitoruje stosowanie przepisów ustawy przez podmioty krytyczne;
7) prowadzi kontrole podmiotów krytycznych;
8) prowadzi działania informacyjne dotyczące dobrych praktyk, działań edukacyjnych i kampanii na rzecz poszerzania wiedzy i budowania odporności podmiotów krytycznych;
9) uczestniczy w planowaniu i organizowaniu ćwiczeń podmiotów krytycznych oraz w razie potrzeby bierze w nich udział;
10) współpracuje z innymi organami do spraw podmiotów krytycznych oraz organami właściwymi do spraw cyberbezpieczeństwa, o których mowa w art. 41 ustawy o krajowym systemie cyberbezpieczeństwa;
11) współpracuje, za pośrednictwem Pojedynczego Punktu Kontaktowego, z odpowiednimi organami państw członkowskich Unii Europejskiej;
12) nakłada kary pieniężne na podmioty krytyczne.

Mając na względzie dotychczasowa praktykę w zakresie koordynacji zadań na szczeblu krajowym w zakresie ochrony infrastruktury krytycznej ustawa przewiduje szereg zadań dla Dyrektora RCB, do których w szczególności należeć będzie:

1) monitorowanie wdrażania Krajowej Strategii Odporności Podmiotów Krytycznych;
2) prowadzenie wykazu infrastruktury krytycznej;
3) prowadzenie wykazu potencjalnej infrastruktury krytycznej;
4) opracowywanie rocznych sprawozdań dotyczących tzw. incydentów istotnych zgłaszanych przez podmioty krytyczne, mających wpływ na ciągłość świadczonych przez nich usług kluczowych;

5) prowadzenie działań informacyjnych dotyczących dobrych praktyk, działań edukacyjnych i kampanii na rzecz poszerzania wiedzy i budowania świadomości w zakresie bezpieczeństwa świadczenia usług kluczowych przez podmioty krytyczne;
6) gromadzenie informacji o incydentach istotnych, które zostały przekazane przez inne państwa członkowskie Unii Europejskiej;
7) udostępnianie informacji i dobrych praktyk związanych ze zgłaszaniem incydentów istotnych przez podmioty krytyczne, uzyskane z tzw. Grupy do spraw Odporności Podmiotów Krytycznych;
8) prowadzenie Pojedynczego Punktu Kontaktowego, który wykonuje funkcję łącznikową w celu zapewnienia współpracy transgranicznej z pojedynczymi punktami kontaktowymi innych państw członkowskich i z Grupą ds. Odporności Podmiotów Krytycznych. Ponadto Pojedynczy Punkt Kontaktowy będzie wykonywał również funkcję łącznikową z Komisją i zapewniał współpracę z państwami trzecimi. Do jego zadań należeć m.in. będzie:
   - 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 raz na 2 lata Komisji Europejskiej oraz Grupie do spraw Odporności Podmiotów Krytycznych sprawozdań dotyczących incydentów istotnych zgłaszanych przez podmioty krytyczne mających wpływ na ciągłość świadczonych przez nie usług kluczowych na terytorium Rzeczypospolitej Polskiej oraz ciągłość świadczonych usług kluczowych w państwach członkowskich Unii Europejskiej;
   - zapewnienie reprezentacji Rzeczypospolitej Polskiej w Grupie do spraw Odporności Podmiotów Krytycznych;
   - zapewnienie współpracy z Komisją Europejską w obszarze bezpieczeństwa świadczenia usług kluczowych;
   - koordynacja współpracy między organami do spraw podmiotów krytycznych a organami administracji publicznej w Rzeczypospolitej Polskiej z odpowiednimi organami w państwach członkowskich Unii Europejskiej;

- zapewnienie wymiany informacji na potrzeby Grupy Współpracy, o której mowa w dyrektywie 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającej dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80, z późn. zm.6), oraz organów właściwych do spraw cyberbezpieczeństwa, o których mowa w art. 41 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
- współpraca z Pojedynczym Punktem Kontaktowym, o którym mowa w art. 4 pkt 18 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

W zakresie nadzoru i kontroli podmiotów krytycznych (rozdział 13 ustawy o zarządzaniu kryzysowym) – ustawa przewiduje, iż nadzór w zakresie stosowania przepisów ustawy sprawują organy do spraw podmiotów krytycznych w zakresie:

1) spełniania przez podmioty krytyczne wymogów bezpieczeństwa dotyczących świadczenia usług kluczowych;
2) wykonywania przez podmioty krytyczne obowiązków dotyczących przeciwdziałania zagrożeniom dla świadczonych usług kluczowych i zgłaszania incydentów istotnych.

W ramach nadzoru organ do spraw podmiotów krytycznych prowadzi kontrole podmiotów krytycznych, przeprowadza lub zleca audyt rozwiązań dotyczących bezpieczeństwa świadczenia usługi kluczowej oraz nakłada kary pieniężne na podmioty krytyczne określone w ustawie (rozdział 15 ustawy o zarządzaniu kryzysowym) .

Ustawa przewiduje, iż do kontroli realizowanej wobec podmiotów będących przedsiębiorcami stosuje się przepisy ustawy – Prawo przedsiębiorców, a do podmiotów niebędących przedsiębiorcami stosuje się przepisy ustawy o kontroli w administracji rządowej.

Zgodnie ze zmienioną ustawą o zarzadzaniu kryzysowym, w celu zwiększenia odporności podmiotów krytycznych, Rada Ministrów, w drodze uchwały, będzie przyjmować Krajową Strategię Odporności Podmiotów Krytycznych, jako dokument o charakterze strategicznym w celu jak najlepszego doboru działań zmierzających do identyfikacji podmiotów krytycznych, zbudowania ich odporności i zapewnienia niezakłóconego świadczenia usług kluczowych. Strategia ta określi cele i priorytety w zakresie zapewnienia niezakłóconego świadczenia usług kluczowych przez podmioty krytyczne i operatorów infrastruktury krytycznej jak również określi wszelkie niezbędne zakresy działań oraz formy działań służące osiąganiu tych celów. Strategia wskaże również podmioty właściwe do

realizacji postanowień strategii oraz określi ich role. Ustawa zawiera zasady i tryb opracowywania tejże Strategii.

Ustawa zawiera także regulacje wykraczające poza implementację dyrektywy 2022/2557, które są jednak niezbędne do jej prawidłowego wdrożenia, a przede wszystkim funkcjonowania tych rozwiązań w praktyce. Regulacje te dotyczą identyfikacji i ochrony infrastruktury krytycznej. Ponadto, biorąc pod uwagę że dyrektywa stanowi jedynie minimum harmonizacyjne, ustawa zakłada nie tylko utrzymanie dotychczasowego poziomu ochrony infrastruktury krytycznej, ale również wprowadzenie dodatkowych mechanizmów zapewniających jej ochronę, nawet już na etapie jej projektowania lub budowy. Rozwiązania te mają na celu wzmocnienie mechanizmów ochrony infrastruktury krytycznej, biorąc pod uwagę, iż stanowi ona rdzeń świadczenia usług niezbędnych dla funkcjonowania państwa oraz jego obywateli. Wynikają one również z analizy przebiegu wojny w Ukrainie i pojawiających się działań o charakterze sabotażowym i hybrydowym.

Ustawa przewiduje, że Rada Ministrów określi, w drodze uchwały, która ma stanowić dokument niejawny, kryteria pozwalające identyfikować obiekt, urządzenie, instalację, sieć, system lub usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy lub usługi jako infrastrukturę krytyczną obejmujące:

1) kryteria sektorowe – progi, w tym progi liczbowe, charakteryzujące zdolność obiektu, urządzenia, instalacji, sieci, systemu lub usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów lub usług do zapewnienia funkcjonowania organów administracji publicznej, zapewnienia funkcjonowania przedsiębiorstw, zaspokajania potrzeb obywateli oraz zapewnienia świadczenia usług kluczowych;
2) kryteria przekrojowe – progi odnoszące się do znaczenia obiektu, urządzenia, instalacji, sieci, systemu lub usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów lub usług obejmujące:
    a) kryteria ofiar w ludziach – oceniane w odniesieniu do ewentualnej liczby ofiar śmiertelnych lub liczby rannych,
    b) kryteria ewakuacji – oceniane w odniesieniu do liczby osób ewakuowanych lub czasu ewakuacji,
    c) kryteria skutków ekonomicznych – oceniane w odniesieniu do znaczenia strat ekonomicznych lub pogorszenia jakości świadczenia usług kluczowych,

d) kryteria skutków społecznych – oceniane w odniesieniu do wpływu na zaufanie opinii publicznej lub zakłócenia codziennego życia obywateli, w tym utraty dostępu do usług kluczowych,
e) kryteria wpływu międzynarodowego – oceniane w odniesieniu do pogorszenia wizerunku kraju na arenie międzynarodowej lub możliwości realizacji zobowiązań międzynarodowych,
f) kryteria unikatowości – oceniane w odniesieniu do braku możliwości zastąpienia lub odtworzenia w akceptowalnym czasie.

Jednocześnie ustawa określa mechanizm identyfikacji infrastruktury krytycznej przez ministrów kierującymi działami administracji rządowej, wojewodów oraz przez inne podmioty, w zakresie ich właściwości. Ustawa wskazuje też ramy współpracy na linii administracja publiczna – przedsiębiorcy, będący operatorami infrastruktury krytycznej. W celu zapewnienia właściwego poziomu ochrony infrastruktury krytycznej przewiduje się, że Rada Ministrów określi, w drodze rozporządzenia, minimalne wymagania w zakresie bezpieczeństwa fizycznego, technicznego, osobowego, cyberbezpieczeństwa, prawnego oraz ciągłości działania, niezbędne do wdrażania rozwiązań zapewniających ochronę tej infrastruktury.

Do obowiązków operatorów infrastruktury krytycznej będzie należało prowadzenie bieżącej analizy zagrożeń dla infrastruktury krytycznej, opracowanie i wdrożenie rozwiązań w zakresie infrastruktury krytycznej uwzględniającej minimalne standardy. Dodatkowo operator będzie obowiązany do opracowania i prowadzenia niejawnej dokumentacji ochrony infrastruktury krytycznej odzwierciedlającej wdrożone rozwiązania, która to dokumentacja zastąpi obecne plany ochrony infrastruktury krytycznej.

Operator infrastruktury krytycznej będzie również sporządzał, w terminie do dnia 31 marca każdego roku, raport o stanie ochrony infrastruktury krytycznej za rok ubiegły. Będzie to element weryfikujący poziom ochrony infrastruktury krytycznej oraz stopień wdrożenia rozwiązań w tym zakresie zawierający w szczególności informacje dotyczące funkcjonowania ochrony infrastruktury krytycznej w zakresie zapewnienia bezpieczeństwa fizycznego, technicznego, osobowego, teleinformatycznego, prawnego oraz zapewnienia planów ciągłości działania i odtwarzania. Raportowanie o stanie infrastruktury krytycznej w obowiązującym stanie prawnym dotyczy tylko systemu zaopatrzenia w energię, surowce energetyczne i paliwa. Dotychczas raporty te w powyżej wskazanym systemie sporządzane były z częstotliwością raz na kwartał. W odniesieniu do pozostałych systemów obowiązywało raportowanie doraźne. Ustawa przewiduje obowiązek okresowego raportowania przez

wszystkich operatorów infrastruktury krytycznej, a cykl raportowania zostanie ujednolicony i będzie wynosił 12 miesięcy.

Ustawa przewiduje także wprowadzenie instytucji koordynatora do spraw ochrony infrastruktury krytycznej u operatorów infrastruktury krytycznej. Operatorzy infrastruktury krytycznej będą obowiązani wyznaczać osoby koordynujące działania na linii operator – organy administracji publicznej, co jest analogią do obecnie wyznaczonych tzw. osób kontaktowych, funkcjonujących u operatorów infrastruktury krytycznej.

Zmieniana ustawa o zarządzaniu kryzysowym w rozdziale 16 przewiduje wyłączenia stosowania przepisów, a mianowicie do podmiotów krytycznych z sektora bankowości i infrastruktury rynków finansowych nie stosuje się przepisów rozdziałów 11–15, z wyjątkiem art. 6zt ust. 1 pkt 1, pkt 2 lit. b–d, f, h oraz i, pkt 3 oraz ust. 2–11, art. 6zu ust. 1, ust. 2 pkt 3, 4 i 6 oraz ust. 3–6, art. 6zx, art. 6zy, art. 6zzb oraz art. 6zzd, a do podmiotów krytycznych z sektora infrastruktury cyfrowej nie stosuje się przepisów rozdziałów 11–15.

Ponadto, do pozostałych najważniejszych zmian w ustawie o zarządzaniu kryzysowym należą, w szczególności:

- zmiana w zakresie poleceń Prezesa Rady Ministrów, o których mowa w art. 7a ustawy o zarządzaniu kryzysowym polegająca na tym, że przedmiotem poleceń będzie nie tylko zapewnienie właściwego funkcjonowania, ochrony, wzmocnienia oraz odbudowy infrastruktury krytycznej lecz również zapewnienie niezakłóconego świadczenia usługi kluczowej,
- wskazanie jako zadań Rządowego Centrum Bezpieczeństwa przewidzianych do realizacji zadań, o których mowa w art. 22 ustawy o ochronie ludności i obronie cywilnej; w art. 22 tejże ustawy wskazano, iż do zadań Rządowego Centrum Bezpieczeństwa należy m.in. monitorowanie zagrożeń oraz powiadamianie, ostrzeganie i alarmowanie ludności o zagrożeniach, realizacja zobowiązań wynikających z uczestnictwa Rzeczypospolitej Polskiej w Organizacji Traktatu Północnoatlantyckiego i Unii Europejskiej w zakresie budowania odporności państwa na zagrożenia, opracowanie krajowego planu ewakuacji i koordynowanie sporządzania przez wojewodów wojewódzkich planów ewakuacji ludności, zapewnianie wymiany informacji związanych z ochroną ludności i obroną cywilną na potrzeby Prezesa Rady Ministrów, Rady Ministrów i ministra właściwego do spraw wewnętrznych, zapewnienie wymiany informacji na potrzeby realizacji zadań ochrony ludności i obrony cywilnej oraz zapewnienie wymiany informacji w ramach międzynarodowej współpracy w obszarze ludności i zobowiązań sojuszniczych,

– dodanie art. 11b, które ma na celu przede wszystkim dostosowanie przepisów do stanu faktycznego; RCB w praktyce realizuje zadania w zakresie planowania cywilnego wynikającego z członkostwa w Organizacji Traktatu Północnoatlantyckiego, wobec czego RCB 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 procedury systemu zarządzania kryzysowego NATO,
– zmiany w art. 12 oraz art. 14 ustawy o zarządzaniu kryzysowym dostosowujące do zmian w zakresie planów zarządzania kryzysowego,
– zmiana w art. 25 ust. 3 tej ustawy polegająca na doprecyzowaniu jednego z zadań Sił Zbrojnych Rzeczypospolitej Polskiej realizowanego na rzecz zarzadzania kryzysowego,
– przesądzenie w art. 26 tej ustawy możliwości przeznaczenia środków finansowych z rezerwy celowej na pomoc finansową udzielaną innym jednostkom samorządu terytorialnego na realizację przez te jednostki przedsięwzięć z zakresu zarządzania kryzysowego,
– dodanie załącznika do ustawy określającego sektory, a w ich obrębie podsektory i kategorie podmiotów krytycznych (wskazane w załączniku obszary, bazują na obszarach wskazanych w dyrektywie 2022/2557).

Ustawa przewiduje wprowadzenie do porządku prawnego regulacji, które pozwolą na wzmocnienie ochrony najważniejszych dla państwa obszarów, obiektów i urządzeń, w tym morskiej infrastruktury krytycznej. W tym zakresie najistotniejsze zmiany wprowadzono w ustawie o ochronie osób i mienia oraz w ustawie o ochronie żeglugi i portów morskich. W odniesieniu do pierwszej z wymienionych ustaw przewiduje się przepisy, które m.in. umożliwią stosowanie określonych w tej ustawie środków ochrony fizycznej i zabezpieczenia technicznego w odniesieniu do obiektów portowych w rozumieniu ustawy o ochronie żeglugi i portów morskich, sztucznych wysp, konstrukcji i urządzeń w polskich obszarach morskich, o których mowa w ustawie o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej, kabli i rurociągów układanych i utrzymywanych w obszarach morskich Rzeczypospolitej Polskiej, o których mowa w ustawie o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej, a także morskich farm wiatrowych, o których mowa w ustawie o promowaniu wytwarzania energii elektrycznej w morskich farmach wiatrowych. Równolegle dokonuje się rozszerzenia uprawnień pracowników ochrony o możliwość podejmowania dodatkowych działań względem infrastruktury portowej w celu zapewnienia

jej większego poziomu zabezpieczenia. Jednocześnie ustawa przewiduje zmiany przepisów, mające na celu usprawnienie przepływu informacji pomiędzy poszczególnymi podmiotami odpowiedzialnymi za zapewnienie ochrony tej infrastruktury. Z kolei w ustawie o ochronie żeglugi i portów morskich powołuje się Centrum Bezpieczeństwa Morskiego (CBM), które będzie stanowiło wyraz międzysektorowego i wieloinstytucjonalnego podejścia w odniesieniu do ochrony szeroko rozumianej infrastruktury morskiej. Oczekiwanym efektem będzie zwiększenie odporności tej infrastruktury na wszelkiego rodzaju ataki, w tym o charakterze hybrydowym. Do zadań CBM będzie należało m.in. bieżące monitorowanie zagrożeń oraz wspieranie współpracy, w tym wymiany informacji, pomiędzy służbami i podmiotami realizującymi zadania w zakresie ochrony infrastruktury morskiej, statków, granicy państwa na morzu, a także ochrony życia lub zdrowia ludzi, mienia i środowiska znajdujących się na polskich obszarach morskich w tym w wyłącznej strefie ekonomicznej. Funkcję CBM będzie pełniła komórka organizacyjna Straży Granicznej, do której oddelegowani będą również przedstawiciele innych służb oraz podmiotów właściwych do zapewnienia realizacji poszczególnych zadań CBM. W ramach CBM będą współdziałali przedstawiciele Ministra Obrony Narodowej, Szefa Służby Kontrwywiadu Wojskowego, Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Agencji Wywiadu, Szefa Służby Wywiadu Wojskowego, Komendanta Głównego Policji, Komendanta Głównego Państwowej Straży Pożarnej, Szefa Krajowej Administracji Skarbowej, Dyrektora Morskiej Służby Poszukiwania i Ratownictwa, dyrektorów urzędów morskich oraz właściwych terytorialnie wojewodów, a także operatorów infrastruktury krytycznej. CBM będzie realizowało swoje zadania w sposób ciągły, tj. w systemie całodobowym. Ponadto w ustawie o ochronie żeglugi i portów morskich wprowadza się przepisy umożliwiające zniszczenie, unieruchomienie lub przejmowanie kontroli nad bezzałogowym obiektem pływającym, w przypadkach gdy przebieg operacji lub działania takiego obiektu stanowiłoby lub mogłoby stanowić szeroko rozumiane zagrożenie dla bezpieczeństwa, w tym zagrożenie dla chronionych obiektów, urządzeń lub obszarów. Analogiczne rozwiązania wprowadza się w ustawie o środkach przymusu bezpośredniego oraz broni palnej względem bezzałogowych obiektów lądowych.

Do pozostałych najważniejszych zmian wprowadzonych uchwaloną ustawą w innych ustawach poza zmianami wynikowymi należą, w szczególności zmiany:

- w zakresie ustawy o drogach publicznych oraz ustawy o transporcie kolejowym polegające na wprowadzeniu przepisów umożliwiających niezwłoczne zapewnienie pełnej, niezakłóconej przepustowości niektórych odcinków dróg publicznych lub infrastruktury kolejowej przez wprowadzenie w sytuacji kryzysowej, jeżeli wymagają tego potrzeby

obronności lub istotny interes bezpieczeństwa państwa, przez właściwego miejscowo wojewodę, w drodze rozporządzenia porządkowego, czasowego ograniczenia w korzystaniu z dróg publicznych lub infrastruktury kolejowej,

- w zakresie ustawy o Policji oraz ustawy o Straży Granicznej polegające na wprowadzeniu przepisu umożliwiającego Komendantowi Głównemu Policji, Komendantowi CBŚP, CBZC lub komendantowi wojewódzkiemu Policji, a także Komendantowi Głównemu Straży Granicznej, Komendantowi BSWSG lub komendantowi oddziału Straży Granicznej w określonych przypadkach m.in. po wprowadzeniu trzeciego lub czwartego stopnia alarmowego, o których mowa w ustawie o działaniach antyterrorystycznych, podjęcie decyzji o dopuszczalności zastosowania przez Policję lub SG urządzeń uniemożliwiających telekomunikację na określonym obszarze, przez czas niezbędny do wyeliminowania zagrożenia lub jego skutków, z uwzględnieniem konieczności minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych,
- w zakresie ustawy o ochronie przeciwpożarowej dotyczące korelacji planów ratowniczych z planami reagowania kryzysowego,
- w zakresie ustawy 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 dotyczące usankcjonowania obowiązku powoływania zastępcy Pełnomocnika do spraw ochrony infrastruktury krytycznej, zapewnienia ministrowi właściwemu do spraw aktywów państwowych narzędzi dyscyplinujących zarządy spółek oraz Pełnomocników i ich zastępców, wydłużenie terminów przysługujących ministrowi właściwemu do spraw aktywów państwowych na zgłoszenia sprzeciwu wobec określonych czynności spółki stanowiących zagrożenie dla funkcjonowania, ciągłości działania oraz integralności infrastruktury krytycznej z 14 do 45 dni od dnia otrzymania przez ministra właściwego do spraw aktywów państwowych informacji o podjęciu przez organy spółki uchwały oraz z 30 do 60 dni w przypadku dokonania tych czynności przez zarząd spółki, wydłużenie terminu z 7 do 10 dni, który przysługuje ministrowi właściwemu do spraw energii lub ministrowi właściwemu do spraw gospodarki surowcami energetycznymi, w zakresie wyrażenia opinii dotyczącej określonych ustawowo czynności spółki, które mogą stwarzać zagrożenie dla infrastruktury krytycznej,
- w zakresie ustawy o środkach przymusu bezpośredniego i broni palnej dotyczące uzupełnienia definicji wykorzystania środka przymusu bezpośredniego o zastosowanie

tego środka również wobec bezzałogowego obiektu pływającego oraz bezzałogowego obiektu lądowego oraz dodania przepisów, które umożliwią niszczenie, unieruchamianie i przejmowania kontroli nad tymi obiektami; konsekwencją zmian w ustawie o środkach przymusu bezpośredniego i broni palnej są zmiany w ustawach pragmatycznych poszczególnych służb (ustawa o Policji, Straży Granicznej, Służbie Ochrony Państwa, Żandarmerii Wojskowej),

- w zakresie ustawy o działaniach antyterrorystycznych dotyczące usprawnienia funkcjonowania sztabu koordynacyjnego Szefa ABW oraz wykonywanych przez Policję działań sprawdzających zabezpieczenia infrastruktury krytycznej w przypadku wprowadzenia stopni alarmowych i ograniczenie obowiązku dokonywania przedmiotowych sprawdzeń tylko do obiektów wskazanych przez Komendanta Głównego Policji w uzgodnieniu z Szefem ABW bowiem obecnie obowiązek ten dotyczy wszystkich obiektów infrastruktury krytycznej i obowiązuje począwszy od wprowadzenia drugiego stopnia alarmowego, kiedy nie jest znany dokładny cel zamachu, w rezultacie sprawdzenia te w przypadku części obiektów nie znajdują uzasadnienia, a jedynie powodują istotne zaangażowanie sił i środków Policji, które w takich przypadkach powinny być przesunięte na wybrane (faktycznie zagrożone) obiekty infrastruktury krytycznej,
- w zakresie ustawy o Służbie Ochrony Państwa dotyczące umożliwienia Komendantowi SOP w określonych przypadkach podjęcie decyzji o dopuszczalności zastosowania urządzeń uniemożliwiających telekomunikację na określonym obszarze przez czas niezbędny do wykonywania czynności przez SOP, z uwzględnieniem konieczności minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych,
- w zakresie ustawy o rezerwach strategicznych dotyczące doprecyzowania kręgu podmiotów uczestniczących w opracowywaniu projektu Rządowego Programu Rezerw Strategicznych przez włączenie w ten proces ministra właściwego do spraw gospodarki surowcami energetycznymi oraz wprowadzenie szeregu przepisów zwiększających efektywność i szybkości działania Agencji Rezerw Strategicznych w sytuacjach kryzysowych, w szczególności w związku z włączeniem Agencji do systemu obrony cywilnej i ochrony ludności; zmiany stworzą podstawy do rozwinięcia nowych kompetencji Agencji w obszarach tworzenia i utrzymywania nowych rodzajów rezerw strategicznych oraz w zakresie uczestnictwa Agencji w procedurach związanych z międzynarodowymi mechanizmami przewidzianymi na wypadek sytuacji kryzysowych oraz zwiększenia elastyczności i sprawności w działaniach Agencji przez zmodyfikowanie

instytucji zadań powierzonych w celu szybkiego i sprawnego reagowania w sytuacjach kryzysowych,

- w zakresie ustawy o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa przez uzupełnienie wpływów do Funduszu Cyberbezpieczeństwa o wpływy z kar pieniężnych, o których mowa w ustawie o zarządzaniu kryzysowym,
- w zakresie ustawy – Prawo komunikacji elektronicznej polegające na uchyleniu art. 42 tej ustawy będącej wynikiem zmian wprowadzonych w ustawach o Policji, Straży Granicznej, Służbie Ochrony Państwa oraz ustawy o zarządzaniu kryzysowym dotyczącymi możliwości zastosowania urządzeń uniemożliwiających telekomunikację na określonym obszarze, przez czas niezbędny do wyeliminowania zagrożenia lub jego skutków, z uwzględnieniem konieczności minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych,
- w zakresie ustawy o ochronie ludności i obronie cywilnej dotyczącym skorelowania rozwiązań w zakresie planistyki zarządzania kryzysowego oraz planistyki dotyczącej ochrony ludności i obrony cywilnej m.in. przez zapewnienie udziału Szefa Sztabu Generalnego Wojska Polskiego w opracowaniu krajowego planu ewakuacji ludności.

Zgodnie z najważniejszymi przepisami przejściowymi ustawy Krajowa Ocena Ryzyka zostanie sporządzona po raz pierwszy w terminie 6 miesięcy od dnia wejścia w życie ustawy, tak samo jak Krajowa Strategia Odporności Podmiotów Krytycznych. Krajowy Plan Zarządzania Ryzykiem Rada Ministrów przyjmie po raz pierwszy w terminie 12 miesięcy od dnia wejścia w życie ustawy. Plany zarządzania ryzykiem właściwych organów zostaną zatwierdzone po raz pierwszy w terminie 3 miesięcy od dnia przyjęcia Krajowego Planu Zarządzania Ryzykiem. Powiatowe plany zarządzania ryzykiem zostaną zaś zatwierdzone po raz pierwszy w terminie 3 miesięcy od dnia zatwierdzenia po raz pierwszy właściwego wojewódzkiego planu zarządzania ryzykiem. Gminne plany zarządzania ryzykiem zostaną zatwierdzane po raz pierwszy w terminie 3 miesięcy od dnia zatwierdzenia po raz pierwszy właściwego powiatowego planu zarządzania ryzykiem. W przypadku Krajowego Planu Reagowania Kryzysowego – Rada Ministrów przyjmuje po raz pierwszy ten plan w terminie 9 miesięcy od dnia przyjęcia Krajowego Planu Zarządzania Ryzykiem. Plany reagowania kryzysowego właściwych organów zostaną zatwierdzone po raz pierwszy w terminie 3 miesięcy od dnia przyjęcia Krajowego Planu Reagowania Kryzysowego. Powiatowe plany reagowania kryzysowego zostaną zatwierdzane po raz pierwszy w terminie 3 miesięcy od dnia zatwierdzenia po raz pierwszy właściwego wojewódzkiego planu reagowania

kryzysowego, natomiast gminne plany reagowania kryzysowego zostaną zatwierdzane po raz pierwszy w terminie 3 miesięcy od dnia zatwierdzenia po raz pierwszy właściwego powiatowego planu reagowania kryzysowego.

Dotychczasowe plany zarządzania kryzysowego zatwierdzone na podstawie dotychczasowych przepisów pozostają w mocy do dnia przyjęcia lub zatwierdzenia nowych planów i mogą być w tym czasie aktualizowane. Szczegółowe kryteria pozwalające wyodrębnić infrastrukturę krytyczną pozostają w mocy do czasu przyjęcia nowych kryteriów. Nowe kryteria Rada Ministrów przyjmuje po raz pierwszy w terminie 3 miesięcy od dnia wejścia w życie ustawy. Jednolity wykaz obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej pozostaje w mocy do czasu sporządzenia nowego wykazu i może być w tym czasie aktualizowany. Plany ochrony infrastruktury krytycznej pozostają w mocy do czasu dokonania wpisu infrastruktury krytycznej do nowego wykazu oraz opracowania dokumentacji ochrony infrastruktury krytycznej i mogą być w tym czasie aktualizowane. Właściciele oraz posiadacze samoistni i zależni obiektów, instalacji, urządzeń i usług ujętych w jednolitym wykazie realizują zadania w zakresie ochrony infrastruktury krytycznej na podstawie dotychczasowych przepisów do czasu ujęcia w „nowym" wykazie infrastruktury krytycznej. Organy do spraw podmiotów krytycznych po raz pierwszy identyfikują podmioty krytyczne i wpisują je do wykazu podmiotów krytycznych w terminie 9 miesięcy od dnia wejścia w życie ustawy. Pojedynczy Punkt Kontaktowy po raz pierwszy opracowuje i przekazuje Komisji Europejskiej oraz Grupie do spraw Odporności Podmiotów Krytycznych sprawozdanie dotyczące 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 w terminie do dnia 17 lipca 2028 r. Komendant Główny Straży Granicznej w terminie 7 dni od dnia wejścia w życie przepisów dotyczących Centrum Bezpieczeństwa Morskiego (wchodzą w życie po 6 miesiącach od dnia ogłoszenia projektu ustawy) wyznacza spośród oficerów Straży Granicznej Pełnomocnika Komendanta Głównego Straży Granicznej do spraw utworzenia Centrum Bezpieczeństwa Morskiego w celu podjęcia czynności przygotowawczych i organizacyjnych niezbędnych do rozpoczęcia funkcjonowania Centrum Bezpieczeństwa Morskiego, w szczególności wskazania lokalizacji i pomieszczeń, wyposażenia w niezbędny sprzęt, zapewnienia funkcjonalności i komplementarności odpowiednich systemów teleinformatycznych i stanowisk pracy oraz wspierania procesu oddelegowania przedstawicieli innych podmiotów

do Straży Granicznej do wykonywania zadań CBM. Pełnomocnik zakończy swoją działalność z dniem utworzenia Centrum Bezpieczeństwa Morskiego.

Ustawa określa również maksymalne limity wydatków z budżetu państwa dla poszczególnych części budżetowych będących skutkiem finansowym wejścia w życie ustawy.

Ustawa przewiduje wejście w życie po upływie 14 dni od dnia ogłoszenia.