Projekt, 30.06.2025 r. etap - Stały Komitet Rady Ministrów

U S T A W A

z dnia …… 2025 r.

o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw[1)2)]

Art. 1. W ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122 oraz z 2024 r. poz. 834, 1222, 1473, 1572 i 1907) wprowadza się następujące zmiany:

1) do tytułu ustawy dodaje się załącznik nr 1 w brzmieniu:

"1) Niniejsza ustawa w zakresie swojej regulacji wdraża dyrektywę 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).";

2) po tytule ustawy wprowadza się oznaczenie „Rozdział 1 Przepisy ogólne”;

3) art. 1 otrzymuje brzmienie:

„Art. 1. 1. Ustawa określa:

1) organy właściwe w sprawach zarządzania kryzysowego oraz ich zadania i zasady działania;

2) organy właściwe w sprawach identyfikacji i ochrony infrastruktury krytycznej;

3) zadania i obowiązki operatorów infrastruktury krytycznej;

---

1) Niniejsza ustawa w zakresie swojej regulacji wdraża dyrektywę 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).

2) Niniejszą ustawą zmienia się ustawy: ustawę z dnia 21 marca 1985 r. o drogach publicznych, ustawę z dnia 6 kwietnia 1990 r. o Policji, ustawę z dnia 12 października 1990 r. o Straży Granicznej, ustawę z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej, ustawę z dnia 22 sierpnia 1997 r. o ochronie osób i mienia, ustawę z dnia 29 listopada 2000 r. - Prawo atomowe, ustawę z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych, ustawę z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, ustawę z dnia 28 marca 2003 r. o transporcie kolejowym, ustawę z dnia 11 marca 2004 r. o ochronie zdrowia zwierząt oraz zwalczaniu chorób zakaźnych zwierząt, ustawę z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich, ustawę 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, ustawę z dnia 14 grudnia 2012 r. o odpadach, ustawę z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, ustawę z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych, ustawę z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa, ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, ustawę z dnia 17 grudnia 2020 r. o rezerwach strategicznych, ustawę z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa, oraz ustawę z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej.

4) usługi kluczowe oraz zadania i obowiązki podmiotów krytycznych;
5) organy właściwe do spraw podmiotów krytycznych oraz zadania i obowiązki tych organów;
6) zasady sprawowania nadzoru nad podmiotami krytycznymi oraz ich kontroli;
7) zasady finansowania zadań, o których mowa w pkt 1-6.

2. Ustawy w zakresie, o którym mowa w:

1) ust. 1 pkt 3 i 4, nie stosuje się do organów oraz jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych;
2) ust. 1 pkt 4 nie stosuje się do podmiotów, które w zakresie swojej działalności prowadzą postępowania przygotowawcze, o których mowa w art. 297 ustawy z dnia 6 czerwca 1997 r. - Kodeks postępowania karnego (Dz. U. z 2024 r. poz. 37, 1222 i 1248).";

4) w art. 3:
   a) pkt 1 otrzymuje brzmienie:
      „1) sytuacji kryzysowej – należy przez to rozumieć sytuację wpływającą negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach, środowiska lub dziedzictwa kulturowego, wywołującą znaczne ograniczenia w działaniu właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków lub zakłócenia obsługi tych organów;”,
   b) po pkt 1 dodaje się pkt 1a - 1g w brzmieniu:
      „1a) podmiocie krytycznym - należy przez to rozumieć operatora infrastruktury krytycznej wpisanego do wykazu podmiotów krytycznych, realizującego co najmniej jedną usługę kluczową, prowadzącego działalność w sektorze lub podsektorze wymienionym w załączniku do ustawy oraz posiadającego infrastrukturę krytyczną na terytorium Rzeczypospolitej Polskiej lub na obszarach morskich Rzeczypospolitej Polskiej, o których mowa w ustawie z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej (Dz. U. z 2023 r. poz. 960, 1688, 2029 oraz z 2024 r. poz. 731 i 834);
      1b) podmiocie krytycznym o szczególnym znaczeniu europejskim - należy przez to rozumieć podmiot krytyczny świadczący co najmniej jedną usługę kluczową lub podobną usługę kluczową, 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;

1c) podmiot publiczny - podmiot wskazany w załączniku do ustawy w sektorze administracji publicznej;

1d) odporności podmiotu krytycznego - należy przez to rozumieć zdolność do zapobiegania incydentowi, ochrony przed incydentem realizowanej w drodze zaplanowanych działań, z wykorzystaniem posiadanych zasobów, reagowania w przypadku wystąpienia incydentu i jego absorbowania oraz adaptacji i usuwania skutków incydentu, w tym odtwarzania infrastruktury krytycznej niezbędnej do świadczenia usługi kluczowej;

1e) usłudze kluczowej - należy przez to rozumieć usługę, która ma decydujące znaczenie dla utrzymania niezbędnych funkcji społecznych, niezbędnej działalności gospodarczej, zdrowia i bezpieczeństwa publicznego lub środowiska, wskazaną w przepisach aktu wykonawczego wydanego na podstawie art. 6zp ust. 3 pkt 1;

1f) incydencie – należy przez to rozumieć każde zdarzenie mające lub mogące mieć niekorzystny wpływ na świadczenie usługi kluczowej;

1g) incydent istotny – incydent, który powoduje lub może spowodować istotne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej, spełniający progi uznania incydentu za istotny wskazane w przepisach aktu wykonawczego wydanego na podstawie art. 6zv ust. 4;",

c) pkt 2 otrzymuje brzmienie:

„2) infrastrukturze krytycznej - należy przez to rozumieć obiekt, urządzenie, instalację, sieć, system oraz usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi niezbędne do:

a) realizacji ważnych interesów państwa, w tym zapewnienia funkcjonowania organów administracji publicznej,

b) zapewnienia funkcjonowania przedsiębiorstw,

c) zaspokajania oraz utrzymania potrzeb obywateli, w tym potrzeb o charakterze lokalnym,

d) zapewnienia świadczenia usług kluczowych;",

d) uchyla się pkt 2a,

e) po pkt 2a dodaje się pkt 2b w brzmieniu:

"2b) potencjalnej infrastrukturze krytycznej – należy przez to rozumieć obiekt, urządzenie, instalację, sieć, system oraz usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi będące w fazie projektowania lub budowy, które po ich zakończeniu mogą być niezbędne do:

a) realizacji ważnych interesów państwa, w tym zapewnienia funkcjonowania organów administracji publicznej,

b) zapewnienia funkcjonowania przedsiębiorstw,

c) zaspokajania oraz utrzymywania potrzeb obywateli, w tym potrzeb o charakterze lokalnym,

d) zapewniające świadczenie usług kluczowych;

f) pkt 3 otrzymuje brzmienie:

„3) ochronie infrastruktury krytycznej - należy przez to rozumieć wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działania oraz integralności infrastruktury krytycznej;”,

g) po pkt 3 dodaje się pkt 3a w brzmieniu:

"3a) operatorze infrastruktury krytycznej – należy przez to rozumieć właściciela lub posiadacza obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług wpisanych do wykazu infrastruktury krytycznej;",

h) pkt 8 otrzymuje brzmienie:

"8) siatce bezpieczeństwa – należy przez to rozumieć zestawienie potencjalnych zagrożeń ze wskazaniem podmiotu wiodącego oraz podmiotów współpracujących w realizacji działań, o których mowa w art. 2;”,

i) uchyla się pkt 9 i 10,

j) w pkt 11 kropkę zastępuje się średnikiem i dodaje się pkt 12-30 w brzmieniu:

„12) ryzyku – należy przez to rozumieć prawdopodobieństwo wystąpienia zagrożenia wraz z jego skutkami;

13) ocenie ryzyka - należy przez to rozumieć proces identyfikacji zagrożenia, podatności na zagrożenie, prawdopodobieństwa wystąpienia zagrożenia oraz skutków wystąpienia zagrożenia, który określa wartość ryzyka;

14) zarządzaniu ryzykiem – należy przez to rozumieć działania polegające na:
    a) ocenie ryzyka,
    b) planowaniu działań postępowania z ryzykiem,
    c) wdrażaniu działań postępowania z ryzykiem,
    d) osiąganiu gotowości do reagowania w przypadku wystąpienia sytuacji kryzysowej,
    f) okresowej ocenie osiągniętych efektów;
15) module zadaniowym – należy przez to rozumieć zestawienie przedsięwzięć i zadań przewidzianych do realizacji w sytuacji kryzysowej przez podmioty wskazane w siatce bezpieczeństwa, z wykorzystaniem własnych sił i środków, a także możliwego, zaplanowanego i uzgodnionego wsparcia ze strony innych podmiotów wskazanych w siatce bezpieczeństwa;
16) planach zarządzania kryzysowego – należy przez to rozumieć plany zarządzania ryzykiem oraz plany reagowania kryzysowego;
17) planach zarządzania ryzykiem – należy przez to rozumieć Krajowy Plan Zarządzania Ryzykiem, plany zarządzania ryzykiem ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych oraz wojewódzkie, powiatowe i gminne plany zarządzania ryzykiem;
18) planach reagowania kryzysowego – należy przez to rozumieć Krajowy Plan Reagowania Kryzysowego, plany reagowania kryzysowego ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych oraz wojewódzkie, powiatowe i gminne plany reagowania kryzysowego;
19) decyzji 1313/2013/UE – należy przez to rozumieć decyzję 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, z późn. zm.[3)]);
20) Grupie do spraw Odporności Podmiotów Krytycznych - należy przez to rozumieć grupę, o której mowa w art. 19 dyrektywy 2022/2557;
21) misji doradczej – należy przez to rozumieć misję doradczą, o której mowa w art. 18 ust. 1 dyrektywy 2022/2557;

[3)] Zmiany wymienionej decyzji zostały ogłoszone w Dz. Urz. UE L 250 z 04.10.2018, str. 1 oraz Dz. Urz. UE L 77A z 20.03.2019, str. 1.

22) zagrożeniu hybrydowym - należy przez to rozumieć kombinację wrogich działań realizowanych przy zastosowaniu środków politycznych, gospodarczych, dyplomatycznych, informacyjnych, militarnych lub innych, które nie stanowią agresji militarnej w ujęciu prawa międzynarodowego;
23) zagrożeniu antagonistycznym - należy przez to rozumieć rodzaj zagrożenia hybrydowego ukierunkowanego przeciwko usługom kluczowym i infrastrukturze krytycznej niezbędnej do świadczenia tych usług, realizowanego w sposób celowy i świadomy, bez względu na motywację postępowania;
24) normie – należy przez to rozumieć normę, o której mowa w art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej, zmieniające dyrektywy Rady 89/686/EWG i 93/15/EWG oraz dyrektywy Parlamentu Europejskiego i Rady 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE oraz uchylające decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE (Dz.U. L 316 z 14.11.2012, s. 12);
25) specyfikacji technicznej – należy przez to rozumieć specyfikację techniczną, o której mowa w art. 2 pkt 4 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej, zmieniające dyrektywy Rady 89/686/EWG i 93/15/EWG oraz dyrektywy Parlamentu Europejskiego i Rady 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE oraz uchylające decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE (Dz.U. L 316 z 14.11.2012, s. 12);
26) jednostce certyfikującej – należy przez to rozumieć jednostkę oceniającą zgodność akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 1854 oraz z 2024 r. poz. 1089) lub upoważnioną do certyfikacji zgodnie z przepisami ustawy z dnia 12 września 2002 r. o normalizacji (Dz. U. z 2015 r. poz. 1483);

27) certyfikacie - należy przez to rozumieć dokument wydany przez jednostkę certyfikującą potwierdzający, że wyrób, instalacja, system, proces, usługa lub osoba spełniają odpowiednie wymagania;

28) certyfikacji - należy przez to rozumieć działania jednostki certyfikującej, wykazujące, że wyrób, instalacja, system, proces, usługa lub osoba spełniają odpowiednie wymagania;

29) zdolności do ochrony informacji niejawnych – należy przez to rozumieć spełnienie wymagań określonych w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2024 r. poz. 632 i 1222);

30) realizacji zadań z zakresu obrony cywilnej oraz ochrony ludności – należy przez to rozumieć zadania, o których mowa w ustawie z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz. U. poz. 1907).”;

5) w art. 4 w ust. 1 po pkt 1 dodaje się pkt 1a w brzmieniu:

„1a) prowadzenie oceny ryzyka;”,

6) uchyla się art. 5-6d,

7) po art. 6d dodaje się rozdziały 2-14 w brzmieniu:

„Rozdział 2

Dokumenty strategiczne

Art. 6e. 1. W celu dokonania oceny ryzyka zidentyfikowanych zagrożeń opracowuje się Krajową Ocenę Ryzyka, zwaną dalej „KOR”. Rada Ministrów przyjmuje KOR w drodze uchwały.

2. KOR zawiera:

1) zidentyfikowane istotne zagrożenia, w szczególności:

a) stanowiące katastrofę naturalną lub awarię techniczną w rozumieniu przepisów ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz. U. z 2017 r. poz. 1897),

b) hybrydowe,

c) cyberbezpieczeństwa,

d) o charakterze terrorystycznym,

e) mogące spowodować niedostępność usług kluczowych,

f) inne mogące spowodować znaczące negatywne skutki dla ludności, gospodarki lub dóbr kultury;

2) zagrożenia niezidentyfikowane jednoznacznie, które mogą wystąpić w przyszłości;
3) ocenę ryzyka wystąpienia zidentyfikowanych istotnych zagrożeń.

3. Przy opracowaniu oceny ryzyka uwzględnia się w szczególności:

1) zagrożenia, o których mowa w ust. 2 pkt 1;
2) powiązania między zagrożeniami wynikające z oddziaływań transgranicznych, zależności międzysektorowych i zmian klimatu;
3) ogólną ocenę ryzyka przeprowadzoną na podstawie art. 6 ust. 1 decyzji nr 1313/2013/UE;
4) dane o stratach i szkodach spowodowanych przez zagrożenia wskazane w ust. 2 pkt 1, gromadzone przez podmioty, o których mowa w art. 6g ust. 2;
5) inne istotne oceny ryzyka przeprowadzone zgodnie z wymogami właściwych sektorowych aktów Unii Europejskiej.

4. Ocena ryzyka w odniesieniu do podmiotów krytycznych uwzględnia dodatkowo:

1) wykaz usług kluczowych, o którym mowa w akcie wykonawczym wydanym na podstawie art. 6zp ust. 3;
2) zidentyfikowane zagrożenia antagonistyczne;
3) ryzyka określane jako potencjalne straty lub potencjalne zakłócenia spowodowane incydentami, wyrażane jako wypadkowe skali tych strat lub zakłóceń oraz prawdopodobieństwa wystąpienia takich incydentów;
4) istotne ryzyka wynikające ze stopnia wzajemnej zależności między sektorami określonymi w załączniku do ustawy;
5) zależność ciągłości działania usług kluczowych od funkcjonowania podmiotów znajdujących się w innych państwach członkowskich i państwach trzecich;
6) wpływ znaczącego zakłócenia w jednym sektorze na inne sektory, w tym wszelkie istotne czynniki ryzyka dla obywateli i rynku wewnętrznego;
7) wpływ, jaki znaczące zakłócenie w jednym sektorze może mieć wpływ na inne sektory, w tym wszelkie istotne czynniki ryzyka dla obywateli i rynku wewnętrznego;
8) informacje dotyczące incydentów zgłaszanych przez podmioty krytyczne świadczące usługi kluczowe.

5. Projekt KOR opracowuje dyrektor Rządowego Centrum Bezpieczeństwa, zwanego dalej „Centrum”.

6. Na potrzeby opracowania projektu KOR dyrektor Centrum wydaje wytyczne do jego opracowania obejmujące elementy, o których mowa w ust. 2, oraz uwzględniając elementy, o których mowa w ust. 3 i 4.

7. Dyrektor Centrum przekazuje wytyczne:

1) ministrom kierującym działami administracji rządowej;
2) Szefowi Agencji Bezpieczeństwa Wewnętrznego, Szefowi Agencji Wywiadu oraz Szefowi Centralnego Biura Antykorupcyjnego;
3) wojewodom;
4) Pełnomocnikowi Rządu do spraw Cyberbezpieczeństwa;
5) innym niż wymienione w pkt 1-4 podmiotom, jeżeli jest to konieczne.

8. Organy i podmioty, o których mowa w ust. 7, opracowują, w zakresie swojej właściwości, z uwzględnieniem wytycznych propozycje do ujęcia w projekcie KOR i przekazują je dyrektorowi Centrum we wskazanym przez niego terminie.

9. Organy i podmioty, o których mowa w ust. 7, przekazują dyrektorowi Centrum propozycje wraz z danymi stanowiącymi podstawę do ich przygotowania, z wyłączeniem informacji niejawnych.

10. Dyrektor Centrum może wystąpić do organów i podmiotów, o których mowa w ust. 7, o przekazanie dodatkowych propozycji, jeżeli uzna, że ich umieszczenie w KOR jest niezbędne. Dyrektor Centrum uzasadnia wystąpienie przekazania dodatkowych propozycji.

11. Propozycje przekazane przez ministra kierującego działem administracji rządowej uwzględniają propozycje kierownika urzędu centralnego podległego temu ministrowi lub przez niego nadzorowanego.

12. Kierownik urzędu centralnego podległy ministrowi kierującemu działem administracji rządowej lub przez niego nadzorowany opracowuje i przekazuje wkład do propozycji ministra kierującego działem administracji rządowej.

13. Dyrektor Centrum przedkłada Radzie Ministrów projekt KOR nie rzadziej niż raz na trzy lata.

14. KOR uwzględnia się w:

1) planach zarządzania kryzysowego;
2) procesach identyfikacji podmiotów krytycznych;
3) opracowywaniu ocen ryzyka podmiotów krytycznych oraz wdrażaniu przez podmioty krytyczne środków w zakresie zwiększenia ich odporności;

4) innych dokumentach opracowywanych przez organy administracji publicznej w zakresie zarządzania kryzysowego.

15. Dyrektor Centrum, na podstawie KOR, opracowuje i udostępnia Komisji Europejskiej streszczenie istotnych elementów oceny ryzyka, o której mowa w art. 6 ust. 1 lit. a decyzji 1313/2013/UE.

16. Dyrektor Centrum, na podstawie KOR, opracowuje i udostępnia Komisji Europejskiej informacje dotyczące rodzajów ryzyka oraz wyników oceny ryzyka w odniesieniu do sektorów i podsektorów, o których mowa w załączniku do ustawy, w terminie trzech miesięcy od przyjęcia KOR.

17. Dyrektor Centrum udostępnia KOR na stronie podmiotowej Biuletynu Informacji Publicznej Centrum.

Art. 6f. 1. W celu zwiększenia odporności podmiotów krytycznych opracowuje się Strategię Odporności Podmiotów Krytycznych, zwaną dalej „Strategią”. Rada Ministrów przyjmuje Strategię w drodze uchwały.

2. Strategia:

1) określa cele strategiczne i priorytety w zakresie zapewnienia niezakłóconego świadczenia usług kluczowych przez podmioty krytyczne oraz niezakłóconego funkcjonowania infrastruktury krytycznej, z uwzględnieniem powiązań między zagrożeniami wynikającymi z oddziaływań transgranicznych oraz zależności międzysektorowych;
2) określa zakresy działań oraz formy działań służące osiąganiu celów strategicznych i priorytetów przez:
   a) organy właściwe w sprawach podmiotów krytycznych,
   b) ministrów kierujących działami administracji rządowej, którzy identyfikują infrastrukturę krytyczną,
   c) Komisję Nadzoru Finansowego identyfikującego, w zakresie swojej właściwości infrastrukturę krytyczną,
   d) wojewodów, którzy identyfikują infrastrukturę krytyczną,
   e) podmioty niewymienione w lit. a-d, zaangażowane we wdrażanie i realizację Strategii;
3) zawiera opisy:
   a) procesów identyfikujących podmioty krytyczne,

b) środków niezbędnych do zwiększenia ogólnej odporności podmiotów krytycznych, w tym opis oceny ryzyka, o której mowa w KOR,

c) procesów wspierania podmiotów krytycznych przez podmioty, o których mowa w pkt 2 lit. a-d,

d) środków mających na celu ułatwienie wypełniania obowiązków wynikających z rozdziału III dyrektywy 2022/2557 przez małe i średnie przedsiębiorstwa, w rozumieniu załącznika do zalecenia Komisji 2003/361/W, które zostały zidentyfikowane jako podmioty krytyczne;

4) określa zakres koordynacji działań organów do spraw podmiotów krytycznych i organów właściwych do spraw 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 oraz z 2024 r. poz. 834).

3. Na potrzeby opracowania projektu Strategii dyrektor Centrum wydaje wytyczne do jej opracowania obejmujące elementy, o których mowa w ust. 2.

4. Dyrektor Centrum przekazuje wytyczne:

1) ministrom kierującym działami administracji rządowej;

2) Szefowi Agencji Bezpieczeństwa Wewnętrznego, Szefowi Agencji Wywiadu oraz Szefowi Centralnego Biura Antykorupcyjnego;

3) Komisji Nadzoru Finansowego;

4) wojewodom;

5) innym niż wymienione w pkt 1-4 podmiotom, jeżeli jest to konieczne.

5. Organy i podmioty, o których mowa w ust. 4, opracowują, w zakresie swojej właściwości, z uwzględnieniem wytycznych propozycje do ujęcia w projekcie Strategii i przekazują je dyrektorowi Centrum we wskazanym przez niego terminie.

6. Organy i podmioty, o których mowa w ust. 4, przekazują dyrektorowi Centrum propozycje wraz z danymi stanowiącymi podstawę do ich przygotowania, z wyłączeniem informacji niejawnych.

7. Dyrektor Centrum może wystąpić do organów i podmiotów, o których mowa w ust. 4, o przekazanie dodatkowych propozycji, jeżeli uzna, że ich umieszczenie w Strategii jest niezbędne. Dyrektor Centrum uzasadnia wystąpienie o przekazanie dodatkowych propozycji.

8. Propozycje przekazane przez ministra kierującego działem administracji rządowej uwzględniają propozycje kierownika urzędu centralnego podległego temu ministrowi lub przez niego nadzorowanego.

9. Kierownik urzędu centralnego podległy ministrowi kierującego działem administracji rządowej lub przez niego nadzorowany opracowuje i przekazuje wkład do propozycji ministra kierującego działem administracji rządowej.

10. Dyrektor Centrum może udostępnić opracowany projekt Strategii na stronie podmiotowej Biuletynu Informacji Publicznej Centrum.

11. Dyrektor Centrum kieruje projekt Strategii do 30-dniowych konsultacji publicznych, z przeprowadzenia których sporządza raport, wskazując główne tezy zawarte w stanowiskach zgłoszonych do projektu Strategii oraz odniesienie się do nich.

12. Dyrektor Centrum udostępnia raport, o którym mowa w ust. 11, na stronie podmiotowej Biuletynu Informacji Publicznej Centrum.

13. Dyrektor Centrum przedkłada Radzie Ministrów projekt Strategii raz na trzy lata.

14. Dyrektor Centrum udostępnia Strategię na stronie podmiotowej Biuletynu Informacji Publicznej Centrum.

15. Dyrektor Centrum udostępnia Komisji Europejskiej Strategię najpóźniej w terminie trzech miesięcy od jej przyjęcia.

16. Przepisy ust. 3-15 stosuje się do aktualizacji Strategii.

17. Dyrektor Centrum monitoruje wdrażanie postanowień Strategii oraz w terminie do dnia 31 marca każdego roku przedkłada Radzie Ministrów sprawozdanie z jej wdrażania za poprzedni rok.

Rozdział 3

Plany zarządzania kryzysowego

Art. 6g. 1. Plany zarządzania ryzykiem zawierają:

1) cele strategiczne;
2) opis zasad współdziałania między podmiotami wskazanymi w siatce bezpieczeństwa;
3) uporządkowaną listę działań na rzecz ograniczenia ryzyka katastrof naturalnych lub awarii technicznych w zakresie organizacyjnym, technicznym i finansowym, z uwzględnieniem:
   a) hierarchii działań,

b) ram czasowych ich realizacji,

c) podmiotów wiodących oraz współpracujących przy ich wykonywaniu,

d) sposobów finansowania oraz wysokości nakładów finansowych,

e) oceny osiągniętych efektów oraz wniosków z wdrożonych działań.

2. Plany zarządzania ryzykiem opracowują:

1) dyrektor Centrum - Krajowy Plan Zarządzania Ryzykiem, zwany dalej "KPZR";

2) minister kierujący działem administracji rządowej - plan zarządzania ryzykiem ministra kierującego działem administracji rządowej;

3) 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;

4) kierownik urzędu centralnego wskazany przez ministra kierującego działem administracji rządowej, któremu podlega lub jest przez tego ministra nadzorowany - plan zarządzania ryzykiem kierownika urzędu centralnego;

5) wojewoda – wojewódzki plan zarządzania ryzykiem;

6) starosta - powiatowy plan zarządzania ryzykiem;

7) wójt (burmistrz, prezydent miasta) - gminny plan zarządzania ryzykiem.

3. Plany zarządzania ryzykiem, o których mowa w ust. 2, opracowuje się z uwzględnieniem zagrożeń wskazanych w Krajowej Ocenie Ryzyka.

4. Plany zarządzania ryzykiem, o których mowa w ust. 2pkt 2-5, opracowuje się z zachowaniem spójności z KPZR.

5. W planach, o których mowa w ust. 2 pkt 6 i 7 uwzględnia się postanowienia KPZR.

Art. 6h. 1. Na potrzeby opracowania projektu KPZR dyrektor Centrum wydaje wytyczne do jego opracowania, obejmujące elementy, o których mowa w art. 6g ust. 1.

2. Dyrektor Centrum przekazuje wytyczne:

1) ministrom kierującym działami administracji rządowej;

2) Szefowi Agencji Bezpieczeństwa Wewnętrznego, Szefowi Agencji Wywiadu oraz Szefowi Centralnego Biura Antykorupcyjnego;

3) wojewodom;

4) innym niż wymienione w pkt 1-3 podmiotom, jeżeli jest to konieczne.

3. Organy i podmioty, o których mowa w ust. 2, opracowują, w zakresie swojej właściwości, z uwzględnieniem wytycznych propozycje do ujęcia w projekcie KPZR i przekazują je dyrektorowi Centrum we wskazanym przez niego terminie.

4. Organy i podmioty, o których mowa w ust. 2, przekazują dyrektorowi Centrum propozycje wraz z danymi stanowiącymi podstawę do ich przygotowania, z wyłączeniem informacji niejawnych.

5. Dyrektor Centrum może wystąpić do organów i podmiotów, o których mowa w ust. 2, o przekazanie dodatkowych propozycji, jeżeli uzna, że ich umieszczenie w KPZR jest niezbędne.

6. Propozycje przekazane przez ministra kierującego działem administracji rządowej uwzględniają propozycje kierownika urzędu centralnego podległego temu ministrowi lub przez niego nadzorowanego.

7. Kierownik urzędu centralnego podległy ministrowi kierującego działem administracji rządowej lub przez niego nadzorowany opracowuje i przekazuje wkład do propozycji ministra kierującego działem administracji rządowej.

8. Dyrektor Centrum przedkłada Radzie Ministrów projekt KPZR nie rzadziej niż raz na trzy lata. Rada Ministrów przyjmuje KPZR w drodze uchwały.

9. Na podstawie KPZR dyrektor Centrum opracowuje i udostępnia Komisji Europejskiej streszczenie istotnych elementów krajowej oceny zdolności zarządzania ryzykiem, o której mowa w art. 6 ust. 1 lit. b decyzji 1313/2013/UE.

Art. 6i. 1. Plan zarządzania ryzykiem ministra kierującego działem administracji rządowej obejmuje własny plan zarządzania ryzykiem oraz plany zarządzania ryzykiem kierowników urzędów centralnych podległych temu ministrowi lub przez niego nadzorowanych.

2. Minister kierujący działem administracji, w zakresie swojej właściwości, wskazuje kierownika urzędu centralnego podległego lub nadzorowanego, który jest zobowiązany do opracowania własnego planu zarządzania ryzykiem.

3. Plan zarządzania ryzykiem Ministra Obrony Narodowej uwzględnia plany zarządzania ryzykiem Szefa Służby Kontrwywiadu Wojskowego oraz Szefa Służby Wywiadu Wojskowego.

4. Minister kierujący działem administracji rządowej, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Agencji Wywiadu, Szef Centralnego Biura Antykorupcyjnego:

1) uzgadnia projekt planu zarządzania ryzykiem z dyrektorem Centrum pod względem spójności z KPZR;
2) zatwierdza uzgodniony plan zarządzania ryzykiem;
3) przekazuje kopię zatwierdzonego planu zarządzania ryzykiem dyrektorowi Centrum.

5. Kierownik urzędu centralnego, o którym mowa w ust. 2:

1) uzgadnia projekt planu zarządzania ryzykiem z ministrem kierującym działem administracji rządowej, któremu podlega lub przez którego jest nadzorowany;
2) uzgadnia projekt planu zarządzania ryzykiem z dyrektorem Centrum pod względem spójności z KPZR;
3) zatwierdza uzgodniony plan zarządzania ryzykiem;
4) przekazuje kopię zatwierdzonego planu zarządzania ryzykiem właściwemu ministrowi oraz dyrektorowi Centrum.

6. Wojewoda:

1) przekazuje projekt wojewódzkiego planu zarządzania ryzykiem do zatwierdzenia ministrowi właściwemu do spraw administracji publicznej;
2) przekazuje zatwierdzony wojewódzki plan zarządzania ryzykiem do wiadomości dyrektorowi Centrum.

7. Starosta przekazuje projekt powiatowego planu zarządzania ryzykiem do zatwierdzenia właściwemu wojewodzie.

8. Wójt (burmistrz, prezydent miasta) przekazuje projekt gminnego planu zarządzania ryzykiem do zatwierdzenia właściwemu staroście.

Art. 6j. 1. Plany reagowania kryzysowego opracowują:

1) dyrektor Centrum - Krajowy Plan Reagowania Kryzysowego , zwany dalej "KPRK";
2) minister kierujący działem administracji rządowej - plan reagowania kryzysowego ministra kierującego działem administracji rządowej;
3) Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Agencji Wywiadu oraz Szef Centralnego Biura Antykorupcyjnego - plan reagowania kryzysowego odpowiednio Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Agencji Wywiadu oraz Szefa Centralnego Biura Antykorupcyjnego;

4) kierownik urzędu centralnego wskazany przez ministra kierującego działem administracji rządowej, któremu podlega lub jest przez tego ministra nadzorowany - plan reagowania kryzysowego kierownika urzędu centralnego;
5) wojewoda – wojewódzki plan reagowania kryzysowego;
6) starosta - powiatowy plan reagowania kryzysowego;
7) wójt (burmistrz, prezydent miasta) - gminny plan reagowania kryzysowego.

2. Plany reagowania kryzysowego, o których mowa w ust. 1, opracowuje się w odniesieniu do zagrożeń wskazanych w Krajowej Ocenie Ryzyka oraz z uwzględnieniem odpowiedniego planu zarządzania ryzykiem.

3. Plany reagowania kryzysowego, o których mowa w ust. 1 pkt 2-5, opracowuje się z zachowaniem spójności z KPRK.

Art. 6k. 1. KPRK zawiera:

1) określenie zadań i obowiązków uczestników zarządzania kryzysowego w formie siatki bezpieczeństwa w zakresie reagowania w przypadku wystąpienia sytuacji kryzysowej oraz usuwania jej skutków;
2) zasady współdziałania między uczestnikami, o których mowa w pkt 1, w tym wymiany informacji w relacjach krajowych i międzynarodowych;
3) zestawienie sił i środków planowanych do wykorzystania w sytuacjach kryzysowych lub w zakresie realizacji zadań związanych z ochroną ludności oraz obroną cywilną;
4) zestawienie modułów zadaniowych pogrupowanych w katalogi;
5) załączniki określające:
   a) opis organizacji systemu monitorowania zagrożeń, ostrzegania i alarmowania,
   b) opis organizację łączności,
   c) opis informowania ludności o zagrożeniach i sposobach postępowania na wypadek zagrożeń,
   d) procedury oceniania i dokumentowania strat i szkód,
   e) procedury uruchamiania rezerw strategicznych,
   f) procedury realizacji zadań związanych z ochroną ludności oraz obroną cywilną;
   g) procedury reagowania kryzysowego – standardowe procedury operacyjne,
   h) priorytety w zakresie ochrony oraz odtwarzania infrastruktury krytycznej.

2. Dyrektor Centrum we współpracy z podmiotami, o których mowa w art. 6j ust. 1 pkt 2-5, opracowuje projekt KPRK.

3. Dyrektor Centrum przedkłada projekt KPRK Radzie Ministrów nie rzadziej niż raz na trzy lata. Rada Ministrów przyjmuje KPRK w drodze uchwały.

Art. 6l. 1. Plan reagowania kryzysowego ministra kierującego działem administracji rządowej, Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Agencji Wywiadu, Szefa Centralnego Biura Antykorupcyjnego oraz kierownika urzędu centralnego podległego ministrowi kierującemu działem administracji rządowej lub przez niego nadzorowanego zawiera:

1) określenie zadań i obowiązków uczestników zarządzania kryzysowego w formie siatki bezpieczeństwa w zakresie reagowania w przypadku wystąpienia sytuacji kryzysowej oraz usuwania jej skutków;
2) określenie zadań w zakresie monitorowania zagrożeń;
3) zestawienie przedsięwzięć realizowanych w ramach przypisanych katalogów i modułów zadaniowych wraz z ich opisem;
4) określenie organizacji realizacji zadań z zakresu ochrony infrastruktury krytycznej lub zapewnienia ciągłości świadczenia usług kluczowych.

2. Plan reagowania kryzysowego ministra kierującego działem administracji rządowej obejmuje własny plan reagowania kryzysowego oraz plany reagowania kryzysowego kierowników urzędów centralnych podległych temu ministrowi lub przez niego nadzorowanych.

3. Minister kierujący działem administracji, w zakresie swojej właściwości, wskazuje kierownika urzędu centralnego podległego lub nadzorowanego, który jest zobowiązany do opracowania własnego planu reagowania kryzysowego.

4. Plan reagowania kryzysowego Ministra Obrony Narodowej uwzględnia plany reagowania kryzysowego Szefa Służby Kontrwywiadu Wojskowego oraz Szefa Służby Wywiadu Wojskowego.

5. Minister kierujący działem administracji rządowej, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Agencji Wywiadu, Szef Centralnego Biura Antykorupcyjnego:

1) uzgadnia projekt planu reagowania kryzysowego z dyrektorem Centrum pod względem spójności z KPRK;
2) zatwierdza uzgodniony plan reagowania kryzysowego;
3) przekazuje kopię zatwierdzonego planu reagowania kryzysowego dyrektorowi Centrum.

6. Kierownik urzędu centralnego, o którym mowa w ust. 3:

1) uzgadnia projekt planu reagowania kryzysowego z ministrem kierującym działem administracji rządowej, któremu podlega lub przez którego jest nadzorowany;
2) uzgadnia projekt planu reagowania kryzysowego z dyrektorem Centrum pod względem spójności z KPRK;
3) zatwierdza uzgodniony plan reagowania kryzysowego;
4) przekazuje kopię zatwierdzonego planu reagowania kryzysowego właściwemu ministrowi oraz dyrektorowi Centrum.

Art. 6m. 1. Wojewódzki plan reagowania kryzysowego zawiera:

1) elementy, o których mowa w art. 6k ust. 1 pkt 1–3 i 5 oraz art. 6l ust. 1 pkt 2 i 3;
2) zestawienie przedsięwzięć minimalizujących skutki zakłócenia funkcjonowania infrastruktury krytycznej dla ludności na terenie województwa wraz z ich opisem.

2. Wojewoda:

1) przekazuje projekt wojewódzkiego planu reagowania kryzysowego do zatwierdzenia ministrowi właściwemu do spraw administracji publicznej;
2) przekazuje zatwierdzony wojewódzki plan reagowania kryzysowego do wiadomości dyrektorowi Centrum.

Art. 6n. 1. Powiatowy plan reagowania kryzysowego oraz gminny plan reagowania kryzysowego zawiera:

1) elementy, o których mowa w art. 6k ust. 1 pkt 1–3 i 5 oraz art. 6l ust. 1 pkt 2 i 3;
2) zestawienie przedsięwzięć minimalizujących skutki zakłócenia funkcjonowania infrastruktury krytycznej dla ludności na terenie właściwej jednostki samorządu terytorialnego, wraz z ich opisem.

2. Starosta przekazuje projekt powiatowego planu reagowania kryzysowego do zatwierdzenia właściwemu wojewodzie.

3. Wójt (burmistrz, prezydent miasta) przekazuje projekt gminnego planu reagowania kryzysowego do zatwierdzenia właściwemu staroście.

Art. 6o. 1. Plany zarządzania kryzysowego podlegają systematycznej aktualizacji w cyklu planowania nie dłuższym niż trzy lata.

2. Plany zarządzania kryzysowego uzgadnia się z właściwymi podmiotami, w zakresie ich dotyczącym, planowanymi do wykorzystania przy realizacji przedsięwzięć określonych w planie.

3. Przy opracowywaniu planów zarządzania kryzysowego uwzględnia się:

1) zawarte umowy i porozumienia,
2) plany opracowane na podstawie odrębnych przepisów, w tym wynikające z aktów Unii Europejskiej

- niezbędne do realizacji przedsięwzięć określonych w planach zarządzania kryzysowego.

4. Minister kierujący działem administracji rządowej może wydać, w drodze zarządzenia, wytyczne do opracowania planów zarządzania kryzysowego kierowników urzędów centralnych podległych temu ministrowi lub przez niego nadzorowanych, kierując się zachowaniem spójności z planami zarządzania kryzysowego opracowywanego przez ministra.

Rozdział 4

Infrastruktura krytyczna

Art. 6p. Zadania dotyczące infrastruktury krytycznej obejmują:

1) identyfikację oraz wyznaczanie infrastruktury krytycznej;
2) gromadzenie i przetwarzanie informacji dotyczących zagrożeń infrastruktury krytycznej;
3) opracowywanie i wdrażanie procedur na wypadek wystąpienia zagrożeń infrastruktury krytycznej;
4) odtwarzanie infrastruktury krytycznej;
5) współpracę między organami administracji publicznej a operatorami infrastruktury krytycznej w zakresie ochrony infrastruktury krytycznej.

Art. 6q. 1. Organami właściwymi w sprawie identyfikacji infrastruktury krytycznej oraz współpracy z operatorami infrastruktury krytycznej, w zakresie swoich właściwości, są:

1) ministrowie kierujący działami administracji rządowej;
2) wojewodowie;
3) Komisja Nadzoru Finansowego.

2. Organy w zakresie realizacji zadań, o których mowa w ust. 1, współpracują z dyrektorem Centrum.

3. Minister kierujący działem administracji rządowej, wojewoda, Komisja Nadzoru Finansowego, w zakresie swojej właściwości, oraz dyrektor Centrum, zapewniają bieżącą współpracę z operatorem infrastruktury krytycznej, w szczególności przez:

1) prowadzenie bieżącej wymiany informacji na temat zagrożeń;
2) prowadzenie działań informacyjnych dotyczących dobrych praktyk, działań edukacyjnych na rzecz poszerzania wiedzy w zakresie bezpieczeństwa oraz zapewnienia funkcjonowania infrastruktury krytycznej, w tym organizowanie, konferencji, seminariów lub forów wymiany wiedzy;
3) udzielanie wsparcia merytorycznego operatorom infrastruktury krytycznej:
   a) w zakresie wdrażania dobrych praktyk oraz niezbędnych rozwiązań dotyczących ochrony infrastruktury krytycznej,
   b) w celu zapewnienia właściwego funkcjonowania infrastruktury krytycznej, jej ochrony lub odbudowy,
   c) w sytuacji kryzysowej lub w przypadku możliwości wystąpienia sytuacji kryzysowej.

Rozdział 5

Identyfikowanie infrastruktury krytycznej

Art. 6r. 1. Dyrektor Centrum prowadzi wykaz infrastruktury krytycznej w celu zapewnienia:

1) identyfikacji obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług jako infrastruktury krytycznej;
2) realizacji zadań w zakresie ochrony infrastruktury krytycznej.

2. Wykaz zawiera:

1) nazwę i lokalizację infrastruktury krytycznej, w tym wskazanie infrastruktury krytycznej niezbędnej do świadczenia usług kluczowych;
2) dane operatora infrastruktury krytycznej, w tym siedzibę i adres oraz numer identyfikacji podatkowej (NIP), jeżeli został nadany;
3) wskazanie organu identyfikującego infrastrukturę krytyczną.

3. Wykaz prowadzony jest w postaci elektronicznej. Do wykazu stosuje się przepisy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.

4. Obiekt, urządzenie, instalacja, sieć, system oraz usługa lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi zostają wpisane do wykazu w przypadku gdy spełniają kryteria, o których mowa w przepisach wydanych na podstawie aktu wykonawczego, o którym mowa w ust. 5.

5. Rada Ministrów określi, w drodze uchwały, kryteria pozwalające identyfikować obiekt, urządzenie, instalację, sieć, system oraz usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi jako infrastrukturę krytyczną, w tym:

1) kryteria sektorowe – progi, w tym progi liczbowe, charakteryzujące zdolność obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz 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 oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz 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 świadczenia jakości usług kluczowych,
   d) kryteria skutków społecznych – oceniane w odniesieniu do wpływu na zaufanie opinii publicznej lub zakłócenia codziennego życia obywateli, w tym utraty 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

- uwzględniając sektory lub podsektory, o których mowa w załączniku do ustawy, znaczenie obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączone ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług dla realizacji interesów państwa, funkcjonowania przedsiębiorców, zaspokajania potrzeb obywateli, w tym potrzeb o charakterze lokalnym oraz zapewnienia świadczenia usług kluczowych.

6. Do uchwały stosuje się przepisy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.

Art. 6s. 1. Dyrektor Centrum dokonuje wpisu do wykazu infrastruktury krytycznej na podstawie wniosku złożonego przez:

1) ministra kierującego działem administracji rządowej;
2) właściwego miejscowo wojewodę;
3) Komisję Nadzoru Finansowego.

2. Dyrektor Centrum opracowuje wyciągi z wykazu infrastruktury krytycznej znajdującej się na terenie poszczególnych województw i przekazuje je właściwym wojewodom.

Art. 6t. 1. Minister kierujący działem administracji rządowej we współpracy z dyrektorem Centrum identyfikuje obiekt, urządzenie, instalację, sieć, system oraz usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi mogące stanowić infrastrukturę krytyczną.

2. W przypadku identyfikacji prowadzonej przez ministra kierującego działem administracji rządowej, obiekt, urządzenie, instalację, sieć, system oraz usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi zostają wpisane do wykazu infrastruktury krytycznej, jeżeli spełniają łącznie kryterium sektorowe, o którym mowa w art. 6r ust. 5 pkt 1, oraz co najmniej jedno z kryteriów przekrojowych, o których mowa w art. 6r ust. 5 pkt 2.

3. Minister kierujący działem administracji rządowej może wystąpić do właściciela lub posiadacza obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług o udzielenie informacji, które umożliwią ocenę, czy spełniają one warunki do uznania ich za infrastrukturę krytyczną, przekazując dokumenty niezbędne do udzielenia informacji.

4. Minister kierujący działem administracji rządowej w wystąpieniu, o którym mowa w ust. 3, wskazuje termin udzielenia informacji. Wyznaczony termin nie może być krótszy niż 14 dni, licząc od dnia otrzymania wystąpienia przez podmiot.

5. Minister kierujący działem administracji rządowej składa do dyrektora Centrum wniosek o wpis obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usługi do wykazu infrastruktury krytycznej. Wniosek zawiera informacje obejmujące:

1) nazwę i lokalizację obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług;
2) dane właściciela lub posiadacza obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług w tym siedzibę i adres oraz numer identyfikacji podatkowej (NIP), jeżeli został nadany.

6. Wniosek sporządza się i składa na piśmie utrwalonym w postaci elektronicznej, opatrzonym kwalifikowanym podpisem elektronicznym, podpisem osobistym, podpisem zaufanym albo kwalifikowaną pieczęcią elektroniczną.

Art. 6u. 1. Wojewoda we współpracy z dyrektorem Centrum identyfikuje obiekt, urządzenie, instalację lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje oraz sieć, system lub usługę mogące stanowić infrastrukturę krytyczną na terenie województwa.

2. W przypadku identyfikacji prowadzonej przez wojewodę, obiekt, urządzenie, instalację, sieć, system oraz usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi mogą zostać wpisane do wykazu infrastruktury krytycznej, jeżeli spełniają co najmniej jedno z kryteriów przekrojowych, o których mowa w art. 6r ust. 5 pkt 2. Przepis art. 6t ust. 3-6 stosuje się odpowiednio.

Art. 6v. 1. Komisja Nadzoru Finansowego, w zakresie swojej właściwości, we współpracy z dyrektorem Centrum, identyfikuje obiekt, urządzenie, instalację, sieć, system oraz usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi mogące stanowić infrastrukturę krytyczną.

2. W przypadku identyfikacji prowadzonej przez Komisję Nadzoru Finansowego, obiekt, urządzenie, instalacja, sieć, system oraz usługa lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi mogą zostać wpisane do wykazu infrastruktury krytycznej, jeżeli spełniają łącznie kryterium sektorowe, o którym mowa w art. 6r ust. 5 pkt 1, oraz co najmniej jedno z kryteriów, o których mowa w art. 6r ust. 5 pkt 2. Przepis art. 6t ust. 3-6 stosuje się odpowiednio.

Art. 6w. 1. Dyrektor Centrum informuje właściciela lub posiadacza obiektu, obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług o dokonaniu

wpisu do wykazu infrastruktury krytycznej oraz obowiązkach z tym związanych w terminie 30 dni od wpisu do wykazu.

2. Informacje o realizacji czynności, o których mowa w ust. 1, dyrektor Centrum przekazuje organowi wnioskującemu o wpis do wykazu.

Art. 6x. Organy, o których mowa w art. 6s ust. 1, oraz dyrektor Centrum, prowadzą bieżącą wymianę informacji dotyczących realizacji czynności w zakresie identyfikacji obiektów, urządzeń, instalacji, sieci, systemów oraz usług lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług, które mogą zostać wpisane do wykazu infrastruktury krytycznej.

Rozdział 6

Identyfikowanie potencjalnej infrastruktury krytycznej

Art. 6y. 1. Dyrektor Centrum prowadzi wykaz potencjalnej infrastruktury krytycznej w celu zapewnienia:

1) identyfikacji obiektu, urządzenia, instalacji, sieci, systemu oraz usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług, będących na etapie projektowania lub budowy jako potencjalnej infrastruktury krytycznej;
2) realizacji zadań w zakresie ochrony potencjalnej infrastruktury krytycznej.

2. Wykaz zawiera:

1) nazwę i lokalizację potencjalnej infrastruktury krytycznej;
2) dane podmiotu będącego inwestorem, w rozumieniu ustawy z dnia 7 lipca 1994 r. – Prawo budowlane (Dz. U. z 2024 r. poz. 555 i 834), prowadzącego prace projektowe lub budowlane dotyczące potencjalnej infrastruktury krytycznej, w tym siedzibę i adres oraz numer identyfikacji podatkowej (NIP), jeżeli został nadany;
3) wskazanie organu identyfikującego potencjalną infrastrukturę krytyczną.

3. Wykaz prowadzony jest w postaci elektronicznej. Do wykazu stosuje się przepisy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.

4. Obiekt, urządzenie, instalacja, sieć, system oraz usługa lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi, które są na etapie projektowania lub budowy mogą zostać wpisane do wykazu w przypadku gdy z założeń wynika, że spełnią kryteria, o których mowa w przepisach wydanych na podstawie aktu wykonawczego wydanego na podstawie art. 6r ust. 5.

Art. 6z. Dyrektor Centrum dokonuje wpisu do wykazu potencjalnej infrastruktury krytycznej na podstawie wniosku złożonego przez:

1) ministra kierującego działem administracji rządowej;
2) właściwego miejscowo wojewodę;
3) Komisję Nadzoru Finansowego.

Art. 6za. 1. Minister kierujący działem administracji rządowej, we współpracy z dyrektorem Centrum oraz inwestorem identyfikuje potencjalną infrastrukturę krytyczną. Przepisy art. 6t ust. 2-6 stosuje się odpowiednio.

2. Wojewoda, we współpracy z dyrektorem Centrum oraz inwestorem identyfikuje potencjalną infrastrukturę krytyczną. Przepisy art. 6u ust. 2 oraz art. 6t ust. 3-6 stosuje się odpowiednio.

3. Komisja Nadzoru Finansowego, we współpracy z dyrektorem Centrum oraz inwestorem identyfikuje potencjalną infrastrukturę krytyczną. Przepisy art. 6v ust. 2 oraz art. 6t ust. 3-6 stosuje się odpowiednio.

Art. 6zb. 1. Dyrektor Centrum informuje inwestora o dokonaniu wpisu do wykazu potencjalnej infrastruktury krytycznej oraz obowiązkach z tym związanych w terminie 30 dni od wpisu do wykazu.

2. Informacje o realizacji czynności, o których mowa w ust. 1, dyrektor Centrum przekazuje organowi wnioskującemu o wpis do wykazu.

Art. 6zc. Organy, o których mowa w art. 6z, w zakresie swojej właściwości, we współpracy z dyrektorem Centrum, przedstawiają inwestorowi informacje oraz dokumenty pozwalające na uwzględnienie wymogów dotyczących infrastruktury krytycznej w dokumentacji projektowej lub podczas realizacji inwestycji oraz zapewniają bieżącą współpracę w zakresie, o którym mowa w art. 6p.

Art. 6zd. Podmioty, o których mowa w art. 6z oraz dyrektor Centrum, prowadzą bieżącą wymianę informacji dotyczących realizacji czynności w zakresie identyfikacji obiektów, urządzeń, instalacji, sieci, systemów oraz usług lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów oraz usług będących w fazie projektowania lub budowy, które mogą zostać wpisane do wykazu potencjalnej infrastruktury krytycznej.

Rozdział 7

Obowiązki operatora infrastruktury krytycznej

Art. 6ze. 1. Operator infrastruktury krytycznej zapewnia jej ochronę, w szczególności przez:

1) prowadzenie systematycznej analizy zagrożeń dla infrastruktury krytycznej;
2) wdrażanie adekwatnych do wyników przeprowadzonej analizy zagrożeń rozwiązań w zakresie:
   a) bezpieczeństwa fizycznego, w tym ochrony fizycznej oraz zabezpieczeń technicznych uwzględniających kontrolę dostępu,
   b) bezpieczeństwa technicznego,
   c) bezpieczeństwa osobowego dotyczącego pracowników i dostawców zewnętrznych,
   d) cyberbezpieczeństwa,
   e) bezpieczeństwa prawnego,
   f) ciągłości działania i odtwarzania, w tym utrzymywania własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie infrastruktury krytycznej do czasu jej pełnego odtworzenia;
3) bieżącą współpracę z organami zarządzania kryzysowego, służbami, stażami i inspekcjami oraz dyrektorem Centrum przez przekazywanie i odbieranie informacji o:
   a) zagrożeniach zakłócających lub mogących zakłócić funkcjonowanie infrastruktury krytycznej,
   b) spodziewanych przerwach lub zakłóceniach w funkcjonowaniu infrastruktury krytycznej;
4) sporządzanie i przekazywanie informacji w zakresie zapewnienia ochrony infrastruktury krytycznej na żądanie:
   a) odpowiednio:
      - ministra, o którym mowa w art. 6t ust. 1,
      - właściwego miejscowo wojewody,
      - Komisji Nadzoru Finansowego,
   b) dyrektora Centrum,
   c) Szefa Agencji Bezpieczeństwa Wewnętrznego oraz Szefa Agencji Wywiadu;

5) zapewnienie zdolności do ochrony informacji niejawnych w zakresie realizacji przedsięwzięć związanych z ochroną infrastruktury krytycznej.

2. Operator infrastruktury krytycznej przeprowadza po raz pierwszy analizę zagrożeń, o której mowa w ust. 1 pkt 1, w terminie 6 miesięcy od dnia otrzymania informacji o dokonaniu wpisu do wykazu infrastruktury krytycznej.

3. Operator infrastruktury krytycznej wdraża rozwiązania, o których mowa w ust. 1 pkt 2 w terminie 6 miesięcy od dnia przeprowadzenia po raz pierwszy analizy zagrożeń, a następnie stosowanie do potrzeb, w zależności od wyników przeprowadzonej analizy zagrożeń.

4. Rada Ministrów określa, w drodze rozporządzenia, minimalne wymagania w zakresie bezpieczeństwa fizycznego, technicznego, osobowego, cyberbezpieczeństwa, prawnego oraz ciągłości działania, niezbędne do wdrażania rozwiązań, o których mowa w ust. 1 pkt 2, mając na uwadze:

1) rekomendacje o charakterze specjalistycznym w zakresie ochrony infrastruktury krytycznej, niezbędne do wdrażania rozwiązań w zakresie bezpieczeństwa infrastruktury krytycznej;
2) lokalizację i charakterystykę infrastruktury krytycznej;
3) potrzebę podejmowania działań zapewniających bezpieczeństwo infrastruktury krytycznej.

5. Operator infrastruktury krytycznej, przy opracowywaniu i zawieraniu umów zapewnianiających wdrażanie rozwiązań, o których mowa w ust. 1 pkt 2, żąda od usługodawców:

1) certyfikatów, uwzględniając równoważne, zgodnie z zasadami wzajemnego uznawania w Unii Europejskiej lub w przypadku ich braku innych dokumentów właściwych dla poszczególnych rozwiązań, potwierdzających posiadanie odpowiednich kompetencji i uprawnień niezbędnych do ich realizacji;
2) potwierdzenia zdolności do ochrony informacji niejawnych oraz stosowania przepisów o ochronie informacji niejawnych, jeżeli opracowanie, przygotowanie i wykonanie umowy wiążą się dostępem do informacji niejawnych.

6. Minister kierujący działem administracji rządowej, właściwy terytorialnie wojewoda lub Komisja Nadzoru Finansowego, po zasięgnięciu opinii właściwych sektorowych rad do spraw kompetencji, o których mowa w art. 4c ust. 1 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (Dz.

U. z 2024 r. poz. 419), może opracować i udostępnić na stronie podmiotowej Biuletynu Informacji Publicznej zestawienie certyfikatów lub innych dokumentów właściwych dla realizacji rozwiązań wskazanych w ust. 1 pkt 2.

7. Minister kierujący działem administracji rządowej, właściwy terytorialnie wojewoda lub Komisja Nadzoru Finansowego, w zakresie swojej właściwości, we współpracy z dyrektorem Centrum ustalają klauzule tajności oraz szczegółowe wymagania dotyczące ochrony informacji niejawnych związanych z realizacją przez operatora infrastruktury krytycznej przedsięwzięć związanych z ochroną tej infrastruktury.

Art. 6zf. 1. Operator infrastruktury krytycznej opracowuje, stosuje i na bieżąco aktualizuje dokumentację ochrony infrastruktury krytycznej.

2. Dokumentacja ochrony infrastruktury krytycznej, zawiera:

1) charakterystykę infrastruktury krytycznej oraz analizę zagrożeń, o której mowa w art. 6ze ust. 1 pkt 1;
2) opis zastosowanych, adekwatnie do przeprowadzonej analizy zagrożeń, rozwiązań w zakresie:
   a) bezpieczeństwa fizycznego, w tym opis organizacji i wykonywania ochrony fizycznej infrastruktury krytycznej, w tym dane specjalistycznej uzbrojonej formacji ochronnej chroniącej infrastrukturę krytyczną, o której mowa w art. 2 pkt 7 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2021 r. poz. 1995) – jeżeli występuje,
   b) bezpieczeństwa technicznego,
   c) bezpieczeństwa osobowego,
   d) cyberbezpieczeństwa,
   e) bezpieczeństwa prawnego,
   f) ciągłości działania i odtwarzania;
3) opis:
   a) zasobów umożliwiających podtrzymanie funkcjonowania infrastruktury krytycznej do czasu jej pełnego odtworzenia,
   b) współpracy z organami zarządzania kryzysowego, służbami, stażami i inspekcjami oraz dyrektorem Centrum dotyczący wymiany informacji o zdarzeniu zakłócającym lub mogącym zakłócić funkcjonowanie

infrastruktury krytycznej oraz sposobu postępowania w przypadku takiego zdarzenia;

4) procedury:
   a) działania w sytuacji zagrożenia lub zakłócenia funkcjonowania infrastruktury krytycznej,
   b) zapewnienia ciągłości funkcjonowania infrastruktury krytycznej,
   c) odtwarzania infrastruktury krytycznej;
5) inne elementy niż wskazane w pkt 1-4, biorąc pod uwagę charakterystykę infrastruktury krytycznej.

3. Procedury, o których mowa w ust. 2 pkt 4 lit. a, uzgadnia się z właściwymi organami zarządzania kryzysowego, służbami, stażami i inspekcjami, w zakresie ich dotyczącym, planowanymi do wykorzystania w realizacji przedsięwzięć określonych w dokumentacji

4. Do dokumentacji ochrony infrastruktury krytycznej stosuje się przepisy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.

5. Operator infrastruktury krytycznej w terminie 15 miesięcy od uzyskania informacji o dokonaniu wpisu do wykazu infrastruktury krytycznej przedkłada oświadczenie o opracowaniu dokumentacji ochrony infrastruktury krytycznej, odpowiednio:

1) ministrowi, o którym mowa w art. 6t ust. 1;
2) właściwemu miejscowo wojewodzie;
3) Komisji Nadzoru Finansowego;
4) dyrektorowi Centrum.

6. Operator infrastruktury krytycznej może dołączyć do oświadczenia, o którym mowa w ust. 5, informację o braku możliwości wdrożenia określonych rozwiązań, wskazując przyczynę braku wdrożenia wraz z uzasadnieniem. Operator infrastruktury krytycznej uzgadnia odpowiednio z ministrem, wojewodą lub Komisją Nadzoru Finansowego działania mające na celu wdrożenie brakujących rozwiązań.

7. Operator infrastruktury krytycznej przekazuje dokumentację ochrony infrastruktury krytycznej na żądanie organów, o których mowa w ust. 4 pkt 1-3 oraz dyrektora Centrum.

8. Operator infrastruktury krytycznej będący jednocześnie podmiotem kluczowym w rozumieniu przepisów ustawy z dnia 5 lipca 2018 r. o krajowym systemie

cyberbezpieczeństwa uwzględnia w dokumentacji, o której mowa w ust. 1, dokumentację dotyczącą bezpieczeństwa systemu informacyjnego, o której mowa w art. 10 tej ustawy.

Art. 6zg. 1. Operator infrastruktury krytycznej sporządza, w terminie do dnia 31 marca każdego roku raport o stanie ochrony infrastruktury krytycznej za rok ubiegły.

2. Raport o stanie ochrony infrastruktury krytycznej zawiera w szczególności informacje dotyczące jej ochrony w zakresie zapewnienia:

1) bezpieczeństwa fizycznego;
2) bezpieczeństwa technicznego;
3) bezpieczeństwa osobowego;
4) cyberbezpieczeństwa;
5) bezpieczeństwa prawnego;
6) ciągłości działania i odtwarzania.

3. Raport o stanie ochrony infrastruktury krytycznej sporządza się z uwzględnieniem:

1) analizy zagrożeń dla infrastruktury krytycznej, o której mowa w art. 6ze ust. 1 pkt 1;
2) wdrożonych rozwiązań, o których mowa w art. 6ze ust. 1 pkt 2;
3) zagrożeń, które zakłóciły lub mogły zakłócić funkcjonowanie infrastruktury krytycznej, a nie były uwzględnione w analizie, o której mowa w art. 6ze ust. 1 pkt 1;
4) wyników przeprowadzonych kontroli i audytów odnoszących się do wdrożonych rozwiązań, o których mowa w art. 6ze ust. 1 pkt 2;
5) opisu działań podjętych przez operatora infrastruktury krytycznej w przypadkach wystąpienia zagrożeń.

4. Operator infrastruktury krytycznej przekazuje, w terminie do dnia 31 marca każdego roku, raport o stanie ochrony infrastruktury krytycznej odpowiednio:

1) ministrowi, o którym mowa w art. 6t ust. 1;
2) właściwemu miejscowo wojewodzie;
3) Komisji Nadzoru Finansowego.

5. Operator infrastruktury krytycznej przekazuje raport o stanie ochrony infrastruktury krytycznej na żądanie dyrektora Centrum, Szefa Agencji Bezpieczeństwa Wewnętrznego lub Szefa Agencji Wywiadu.

6. Do raportu o stanie ochrony infrastruktury krytycznej stosuje się przepisy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.

Art. 6zh.1. 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.

2. Operator infrastruktury krytycznej żąda od pracownika danych biometrycznych w postaci odcisków linii papilarnych palców, głosu, obrazu rogówki, sieci żył palców lub biometrii twarzy, które są odpowiednie do wdrożonych środków kontroli dostępu niezbędnych dla ochrony szczególnie ważnych informacji o bezpieczeństwie infrastruktury krytycznej lub dostępu do stref, obiektów lub pomieszczeń wymagających szczególnej kontroli.

3. Operator infrastruktury krytycznej przetwarza informacje i dane, o których mowa w ust. 1 i 2 przez okres uzasadniony celem przetwarzania.

Art. 6zi. 1. W celu realizacji zadań, o których mowa w art. 6ze ust. 1, art. 6zf ust. 1 oraz art. 6zg ust. 1, operator infrastruktury krytycznej wyznacza koordynatora ochrony infrastruktury krytycznej oraz zastępcę koordynatora ochrony infrastruktury krytycznej.

2. Operator infrastruktury krytycznej wyznacza koordynatora ochrony infrastruktury krytycznej oraz zastępcę koordynatora ochrony infrastruktury krytycznej w terminie 30 dni od dnia otrzymania informacji o ujęciu w wykazie infrastruktury krytycznej.

3. Zastępca koordynatora infrastruktury krytycznej zastępuje koordynatora w czasie jego nieobecności lub czasowej niemożności wykonywania przez niego obowiązków.

4. Koordynatorem ochrony infrastruktury krytycznej może być osoba, która:

1) jest pracownikiem operatora infrastruktury krytycznej albo żołnierzem lub funkcjonariuszem pełniącym służbę w jednostce organizacyjnej będącej operatorem infrastruktury krytycznej;
2) korzysta z pełni praw publicznych;
3) posiada wiedzę, umiejętności i doświadczenie w zakresie zarządzania bezpieczeństwem, z uwzględnieniem przedmiotu działalności operatora infrastruktury krytycznej;
4) nie była skazana prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe;

5) spełnia wymagania bezpieczeństwa osobowego w zakresie dostępu do informacji niejawnych o klauzuli ustalonej w trybie określonym w art. 6ze ust. 7.

5. Koordynator ochrony infrastruktury krytycznej podlega bezpośrednio organowi zarządzającemu operatora infrastruktury krytycznej.

6. O wyznaczeniu koordynatora operator infrastruktury krytycznej informuje odpowiednio:

1) ministra, o którym mowa w art. 6t ust. 1;
2) właściwego miejscowo wojewodę;
3) Komisję Nadzoru Finansowego;
4) dyrektora Centrum.

7. Operator infrastruktury krytycznej zapewnia koordynatorowi ochrony infrastruktury krytycznej organizacyjne i techniczne warunki realizacji zadań, w tym dostęp do niezbędnych dokumentów i informacji.

8. Przepisy ust. 4-7 stosuje się do zastępcy koordynatora ochrony infrastruktury krytycznej.

Art. 6zj. Do obowiązków inwestora w zakresie ochrony potencjalnej infrastruktury krytycznej nie stosuje się rozdziału 7 ustawy, z wyjątkiem przepisu art. 6ze ust. 1 pkt 1 i pkt 2 lit. a, pkt 3 lit. a oraz pkt 4, art. 6zf ust. 2 pkt 1 i 2 lit. a oraz pkt 4 lit. a.

Rozdział 8

Organy do spraw podmiotów krytycznych

Art. 6zk.1. Organami do spraw podmiotów krytycznych są:

1) dla sektora energii:
   a) minister właściwy do spraw energii w podsektorach:
      - energii elektrycznej,
      - ciepła,
   b) minister właściwy do spraw gospodarki surowcami energetycznymi w podsektorach:
      - wydobywania kopalin,
      - ropy i paliw,
      - gazu,
      - energetyki jądrowej,
      - wodoru;

2) dla sektora transportu:
   a) minister właściwy do spraw transportu w podsektorach:
      - transport lotniczy,
      - transport kolejowy,
      - transport publiczny,
      - transport drogowy,
   b) minister właściwy do spraw gospodarki morskiej oraz minister właściwy do spraw żeglugi śródlądowej w podsektorze transportu wodnego;
3) dla sektora bankowości oraz infrastruktury rynków finansowych - Komisja Nadzoru Finansowego;
4) dla sektora ochrony zdrowia - minister właściwy do spraw zdrowia;
5) dla sektora zaopatrzenia w wodę pitną i jej dystrybucji oraz sektora zbiorowego odprowadzania ścieków - minister właściwy do spraw gospodarki wodnej;
6) dla sektora infrastruktury cyfrowej - minister właściwy do spraw informatyzacji;
7) dla sektora administracji publicznej – minister właściwy do spraw administracji publicznej;
8) dla sektora przestrzeni kosmicznej - minister właściwy do spraw gospodarki;
9) dla sektora produkcji, przetwarzania i dystrybucji żywności - minister właściwy do spraw rolnictwa;
10) dla sektora zarządzania usługami ICT - minister właściwy do spraw informatyzacji;
11) dla sektora produkcji, wytwarzania i dystrybucji chemikaliów – minister właściwy do spraw gospodarki;
12) dla sektora usług pocztowych - Prezes Urzędu Komunikacji Elektronicznej;
13) dla sektora gospodarowania odpadami – minister właściwy do spraw klimatu;
14) dla sektora finansów publicznych - minister właściwy do spraw finansów publicznych.

2. Dla podmiotu publicznego, który jest wymieniony w innym sektorze niż sektor administracji publicznej, organem do spraw podmiotów krytycznych jest organ właściwy dla danego sektora.

Art. 6zl. Organ do spraw podmiotów krytycznych:

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

2) prowadzi bieżącą analizę podmiotów krytycznych w danym sektorze lub podsektorze pod kątem 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 ustawie o ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
11) współpracuje, za pośrednictwem Pojedynczego Punktu Kontaktowego z odpowiednimi organami państw członkowskich;
12) nakłada kary pieniężne na podmiot krytyczny.

Rozdział 9

Pojedynczy Punkt Kontaktowy

Art. 6zm. 1. Dyrektor Centrum prowadzi Pojedynczy Punkt Kontaktowy do którego zadań należy:

1) odbieranie zgłoszeń incydentów istotnych z pojedynczych punktów kontaktowych w innych państwach członkowskich Unii Europejskiej;
2) przekazywanie zgłoszeń incydentów istotnych dotyczących innych państw członkowskich Unii Europejskiej do pojedynczych punktów kontaktowych tych państw;

3) opracowywanie i przekazywanie raz na dwa lata Komisji Europejskiej oraz Grupie do spraw Odporności 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;
4) zapewnienie reprezentacji Rzeczypospolitej Polskiej w Grupie do spraw Odporności Podmiotów Krytycznych;
5) zapewnienie współpracy z Komisją Europejską w obszarze zapewnienia bezpieczeństwa świadczenia usług kluczowych;
6) koordynacja współpracy między organami do spraw podmiotów krytycznych i organami administracji publicznej w Rzeczypospolitej Polskiej z odpowiednimi organami w państwach członkowskich Unii Europejskiej;
7) zapewnienie wymiany informacji na potrzeby Grupy Współpracy, o której mowa w dyrektywie (UE) 2022/2555 oraz organów właściwych do spraw cyberbezpieczeństwa;
8) współpraca z pojedynczym punktem kontaktowym, o którym mowa w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

2. Pojedynczy Punkt Kontaktowy przekazuje Grupie do spraw Odporności Podmiotów Krytycznych:

1) informacje na temat infrastruktury krytycznej zlokalizowanej na terytorium Rzeczypospolitej Polskiej służącej realizacji usług kluczowych w innych państwach członkowskich;
2) dobre praktyki związane ze zgłaszaniem i obsługą incydentów istotnych;
3) propozycje do programu prac Grupy do spraw Odporności Podmiotów Krytycznych;
4) dobre praktyki krajowe dotyczące podnoszenia świadomości, szkoleń, badań i rozwoju w obszarze zapewnienia ciągłości świadczenia usług kluczowych;
5) dobre praktyki w odniesieniu do identyfikowania podmiotów krytycznych, w tym w odniesieniu do występujących w dwóch lub większej liczbie państw członkowskich Unii Europejskiej zależności dotyczących ryzyka i incydentów.

3. Dane przekazywane Grupie do spraw Odporności Podmiotów Krytycznych nie obejmują informacji, które dotyczą bezpieczeństwa narodowego oraz porządku publicznego.

4. Pojedynczy Punkt Kontaktowy przekazuje organom do spraw podmiotów krytycznych oraz innym organom administracji publicznej zgodnie z ich właściwością informacje pochodzące z Grupy do spraw Odporności Podmiotów Krytycznych dotyczące:

1) analiz i ocen krajowych strategii państw członkowskich Unii Europejskiej w zakresie odporności podmiotów krytycznych, a także dobrych praktyk w obszarze zapewnienia świadczenia usług kluczowych;
2) wytycznych o charakterze strategicznym w obszarze zapewnienia świadczenia usług kluczowych;
3) dobrych praktyk w zakresie wymiany informacji związanych ze zgłaszaniem w Unii Europejskiej incydentów istotnych przez podmioty krytyczne;
4) dobrych praktyk w krajach członkowskich Unii Europejskiej dotyczących innowacji badań i rozwoju w zakresie budowania odporności podmiotów krytycznych;
5) dobrych praktyk w zakresie identyfikowania podmiotów krytycznych przez państwa członkowskie Unii Europejskiej, w tym w odniesieniu do transgranicznych i międzysektorowych zależności, dotyczących ryzyka i incydentów.

5. Pojedynczy Punkt Kontaktowy przekazuje Komisji Europejskiej:

1) niezwłocznie informacje o:
   a) wyznaczonych organach do spraw podmiotów krytycznych, Pojedynczym Punkcie Kontaktowym, ich zadaniach oraz późniejszych zmianach w tym zakresie,
   b) przepisach dotyczących kar pieniężnych;
2) raz na dwa lata informacje umożliwiające ocenę wdrażania dyrektywy 2022/2557, obejmujące w szczególności:
   a) środki umożliwiające identyfikację podmiotów krytycznych,
   b) wykaz usług kluczowych,
   c) liczbę zidentyfikowanych podmiotów krytycznych w każdym sektorze lub podsektorze, o którym mowa w załączniku do ustawy, oraz wskazanie ich znaczenia w odniesieniu do tego sektora lub podsektora,
   d) progi istotności skutku zakłócającego dla świadczonej usługi kluczowej brane pod uwagę przy kwalifikowaniu podmiotów jako podmiotów krytycznych, przedstawiane wprost lub w formie zagregowanej;

3) informacje o środkach mających na celu zwiększenie odporności podmiotów krytycznych.

Art. 6zn. 1. Na potrzeby realizacji zadań, o których mowa w art. 6zl, organy do spraw podmiotów krytycznych, za pośrednictwem Pojedynczego Punktu Kontaktowego, prowadzą konsultacje z właściwymi organami państw członkowskich w przypadku gdy podmioty krytyczne:

1) korzystają z infrastruktury krytycznej, która jest fizycznie połączona na terytorium co najmniej dwóch państw członkowskich;
2) są częścią struktur przedsiębiorstw połączonych lub powiązanych z podmiotami krytycznymi w innych państwach członkowskich;
3) zostały zidentyfikowane jako podmioty krytyczne w jednym państwie członkowskim i świadczą usługi kluczowe na rzecz innych państw członkowskich lub w innych państwach członkowskich.

2. W konsultacjach, o których mowa w ust. 1, organy do spraw podmiotów krytycznych wypracowują, w zależności od potrzeb, rozwiązania w zakresie zwiększania odporności lub redukcji obciążeń administracyjnych podmiotów krytycznych.

Rozdział 10

Identyfikowanie podmiotów krytycznych

Art. 6zo. 1. Dyrektor Centrum prowadzi wykaz podmiotów krytycznych w celu zapewnienia:

1) identyfikacji pomiotów krytycznych;
2) prowadzenia czynności nadzorczych nad podmiotami krytycznymi.

2. Wykaz podmiotów krytycznych zawiera:

1) nazwę (firmę) podmiotu krytycznego;
2) siedzibę i adres oraz adres do doręczeń elektronicznych;
3) numer identyfikacji podatkowej (NIP), jeżeli został nadany;
4) nazwę usługi kluczowej, zgodną z wykazem usług kluczowych;
5) wskazanie sektora, podsektora i kategorii podmiotu;
6) datę rozpoczęcia świadczenia usługi kluczowej;
7) informację wskazującą, w których państwach członkowskich Unii Europejskiej podmiot został uznany za podmiot świadczący usługę kluczową;
8) datę zakończenia świadczenia usługi kluczowej;

9) datę wykreślenia z wykazu podmiotów krytycznych.

3. Wykaz podmiotów krytycznych prowadzony jest w systemie teleinformatycznym, o którym mowa w art. 46 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

4. Do danych, o których mowa w ust. 2, nie stosuje się przepisów ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902) oraz ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystaniu informacji sektora publicznego (Dz. U. z 2023 r. poz. 1524).

5. Dane, o których mowa w ust. 2, w zakresie niezbędnym do realizacji ich ustawowych zadań, organ właściwy do spraw podmiotów krytycznych udostępnia, na wniosek, następującym podmiotom:

1) Agencji Bezpieczeństwa Wewnętrznego;
2) Agencji Wywiadu;
3) Centralnemu Biuru Antykorupcyjnemu;
4) organom Krajowej Administracji Skarbowej;
5) Policji;
6) Pełnomocnikowi Rządu do spraw Cyberbezpieczeństwa;
7) Prezesowi Urzędu Ochrony Danych Osobowych;
8) Prokuratorii Generalnej Rzeczypospolitej Polskiej;
9) prokuraturze;
10) sądom;
11) Służbie Kontrwywiadu Wojskowego;
12) Służbie Ochrony Państwa;
13) Służbie Wywiadu Wojskowego;
14) Straży Granicznej;
15) Żandarmerii Wojskowej;
16) wojewodom;
17) podmiotowi, w ramach którego funkcjonuje Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT) poziomu krajowego;
18) organom właściwym do spraw cyberbezpieczeństwa, o których mowa w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Art. 6zp. 1. Operator infrastruktury krytycznej zostaje wpisany do wykazu podmiotów krytycznych w przypadku gdy:

1) świadczy co najmniej jedną usługę kluczową;
2) incydent miałby istotny skutek zakłócający dla świadczenia usługi kluczowej.

2. Istotność skutku zakłócającego incydentu dla świadczenia usługi kluczowej, o którym mowa w ust. 1 pkt 2, jest określana na podstawie progów istotności skutku zakłócającego określonych w przepisach aktu wykonawczego, o którym mowa w ust. 3.

3. Rada Ministrów określi, w drodze rozporządzenia:

1) wykaz usług kluczowych w podziale na sektory, podsektory i kategorie podmiotów wymienionych w załączniku do ustawy,
2) progi istotności skutku zakłócającego dla świadczenia usług kluczowych, wymienionych w wykazie usług kluczowych, z uwzględnieniem:
   a) liczby użytkowników zależnych od usługi kluczowej świadczonej przez dany podmiot,
   b) stopnia, w jakim inne sektory lub podsektory, o których mowa w załączniku do ustawy, są zależne od usługi świadczonej przez ten podmiot,
   c) 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,
   d) udziału podmiotu krytycznego w rynku w odniesieniu do świadczonej usługi kluczowej,
   e) obszaru geograficznego , którego mógłby dotyczyć incydent, biorąc pod uwagę wpływ transgraniczny oraz stopień odizolowania geograficznego,
   f) znaczenia podmiotu w utrzymywaniu wystarczającego poziomu świadczenia usługi kluczowej przy uwzględnieniu dostępności alternatywnych sposobów jej świadczenia,
   g) innych czynników charakterystycznych dla danego sektora lub podsektora jeżeli występują

- uwzględniając znaczenie danej usługi dla utrzymania niezbędnych funkcji społecznych, niezbędnej działalności gospodarczej, zdrowia i bezpieczeństwa publicznego lub środowiska naturalnego oraz obniżenia jakości świadczonej usługi kluczowej.

Art. 6zq. 1. W celu podjęcia decyzji o dokonaniu wpisu do wykazu podmiotów krytycznych organ do spraw podmiotów krytycznych występuje do operatora infrastruktury krytycznej o udzielenie informacji, które umożliwią wstępną ocenę, czy spełnia warunki do uznania za podmiot krytyczny, w szczególności w zakresie spełniania

warunków, o których mowa w art. 6zp ust. 1 oraz wskazania infrastruktury krytycznej niezbędnej do świadczenia usługi kluczowej.

2. Organ do spraw podmiotów krytycznych w wystąpieniu, o którym mowa w ust. 1:

1) przekazuje operatorowi infrastruktury krytycznej dokumenty w zakresie niezbędnym do udzielenia informacji;
2) wskazuje termin udzielenia informacji, nie krótszy niż 14 dni, licząc od dnia otrzymania wystąpienia przez operatora infrastruktury krytycznej.

3. Operator infrastruktury krytycznej przekazuje organowi do spraw podmiotów krytycznych informacje żądane w wystąpieniu, wskazując jednocześnie infrastrukturę krytyczną niezbędną do świadczenia usługi kluczowej, w tym:

1) infrastrukturę krytyczną innego operatora;
2) obiekt, urządzenie, instalację, sieć, system oraz usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi, którego właściciel lub posiadacz nie jest operatorem infrastruktury krytycznej.

Art. 6zr. 1. Organ do spraw podmiotów krytycznych składa wniosek o wpis do wykazu podmiotów krytycznych zawierający dane, o których mowa w art. 6zo ust. 2 pkt 1-7.

2. Wpis operatora infrastruktury krytycznej do wykazu podmiotów krytycznych dokonuje się z chwilą złożenia wniosku w systemie teleinformatycznym, o którym mowa w art. 46 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

3. Organ do spraw podmiotów krytycznych niezwłocznie, nie później jednak niż w ciągu miesiąca, informuje operatora infrastruktury krytycznej o dokonania wpisu do wykazu podmiotów krytycznych oraz obowiązkach z tym związanych.

4. Informację, o której mowa w ust. 3, organ do spraw podmiotów krytycznych niezwłocznie przekazuje:

1) dyrektorowi Centrum;
2) odpowiedniemu organowi właściwemu do spraw cyberbezpieczeństwa.

5. Dyrektor Centrum może weryfikować dane zawarte we wpisie do wykazu ze stanem faktycznym.

6. Dyrektor Centrum poprawia, z urzędu, oczywiste omyki i błędy pisarskie zawarte we wpisie do wykazu.

Art. 6zs. 1. Podmiot krytyczny w przypadku zakończenia świadczenia usługi kluczowej niezwłocznie informuje właściwy organ do spraw podmiotów krytycznych o tym fakcie.

2. W przypadku zakończenia świadczenia usługi kluczowej przez podmiot krytyczny, organ do spraw podmiotów krytycznych składa wniosek o wykreślenie podmiotu krytycznego z wykazu, zawierający dane, o których mowa w art. 6zo ust. 2 pkt 1-8.

3. Wykreślenie podmiotu krytycznego z wykazu dokonuje się z chwilą złożenia wniosku w systemie teleinformatycznym, o którym mowa w art. 46 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

4. Organ do spraw podmiotów krytycznych niezwłocznie, nie później jednak niż w ciągu miesiąca, informuje podmiot krytyczny o wykreśleniu z wykazu i dacie wykreślenia.

5. Informację, o której mowa w ust. 4, organ do spraw podmiotów krytycznych przekazuje niezwłocznie:

1) dyrektorowi Centrum;

2) odpowiedniemu organowi właściwemu do spraw cyberbezpieczeństwa.

6. Dyrektor Centrum może weryfikować dane zawarte we wniosku o wykreślenie podmiotu krytycznego z wykazu ze stanem faktycznym.

7. Dyrektor Centrum poprawia, z urzędu, oczywiste omyki i błędy pisarskie zawarte we wniosku o wykreślenie podmiotu krytycznego z wykazu.

Rozdział 11

Obowiązki podmiotów krytycznych

Art. 6zt. 1. Podmiot krytyczny wdraża zintegrowany system zarządzania bezpieczeństwem świadczenia usługi kluczowej obejmujący:

1) przeprowadzenie nie rzadziej niż raz na 2 lata oceny ryzyka z uwzględnieniem:
   a) zagrożeń i związanych z tym ryzyk wymienionych w Krajowej Ocenie Ryzyka oraz innych zagrożeń charakterystycznych dla świadczonej usługi kluczowej, w tym zagrożeń antagonistycznych,
   b) stopnia zależności innych sektorów lub podsektorów określonych w załączniku do ustawy od usługi kluczowej świadczonej przez podmiot krytyczny oraz

stopnia zależności tego podmiotu krytycznego od usług kluczowych świadczonych przez inne podmioty w innych sektorach, w tym w stosownych przypadkach w sąsiadujących państwach członkowskich Unii Europejskiej i w państwach trzecich,

c) identyfikacji alternatywnych łańcuchów dostaw w celu przywrócenia świadczenia usługi kluczowej,

d) ocen ryzyka prowadzonych na podstawie odrębnych przepisów;

2) wdrożenie odpowiednich i proporcjonalnych do wyników oceny ryzyka rozwiązań organizacyjno-technicznych, w szczególności:

a) polityk zarządzania ryzykiem,

b) bezpieczeństwa fizycznego, w tym ochrony fizycznej budynków i terenów należących do podmiotu krytycznego oraz zabezpieczeń technicznych, uwzględniających kontrolę dostępu,

c) ochrony infrastruktury krytycznej niezbędnej do świadczenia usługi kluczowej, zgodnie z wymogami ochrony infrastruktury krytycznej, o których mowa w przepisach rozdziału 7 ustawy,

d) bezpieczeństwa osobowego dotyczącego pracowników i dostawców zewnętrznych,

e) cyberbezpieczeństwa, zgodnie z wymogami dotyczącymi podmiotów kluczowych, o których mowa w przepisach ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa,

f) bezpieczeństwa prawnego świadczenia usługi kluczowej,

g) ciągłości działania i odtwarzania, w tym utrzymywania własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie świadczenia usługi kluczowej do czasu jej pełnego odtworzenia,

h) zdolności do ochrony informacji niejawnych w niezbędnym zakresie do zapewnienia świadczenia usługi kluczowej,

i) szkoleń i ćwiczeń personelu w celu jego przygotowania na różnego rodzaju zagrożenia i incydenty,

j) realizacji okresowych audytów i certyfikacji;

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.

2. Rozwiązania organizacyjno-techniczne, o których mowa w ust. 1 pkt 2, powinny spełniać wymagania określone w normach, wskazanych w akcie wykonawczym wydanym na podstawie ust. 5.

3. Podmiot krytyczny przeprowadza po raz pierwszy ocenę ryzyka, o której mowa w ust. 1 pkt 1, w terminie 9 miesięcy od otrzymania informacji o ujęciu w wykazie podmiotów krytycznych.

4. Podmiot krytyczny wdraża rozwiązania organizacyjno-techniczne, o których mowa w ust. 1 pkt 2, w terminie 3 miesięcy od dnia przeprowadzenia po raz pierwszy oceny ryzyka, a następnie stosownie do potrzeb, w zależności od wyników przeprowadzonej oceny ryzyka.

5. Rada Ministrów określi w drodze rozporządzenia wykaz norm, które podmiot krytyczny uwzględnia przy wdrażaniu rozwiązań organizacyjno-technicznych, o których mowa w ust. 1 pkt 2, mając na względzie:

1) zarządzanie bezpieczeństwem informacji;

2) zarządzanie ciągłością działania usługi kluczowej;

3) zapewnienie bezpieczeństwa fizycznego, w tym ochrony fizycznej budynków i terenów należących do podmiotu krytycznego oraz zabezpieczeń technicznych, uwzględniających kontrolę dostępu.

6. Organ do spraw podmiotów krytycznych może opracować, odrębnie dla nadzorowanego sektora lub podsektora i udostępnić na swojej stronie podmiotowej Biuletynu Informacji Publicznej zestawienie wymogów dokumentów normalizacyjnych, o których mowa w art. 2 pkt 3 ustawy z dnia 12 września 2002 r. o normalizacji (Dz. U. z 2015 r. poz. 1483), które podmiot krytyczny uwzględnia przy wdrażaniu rozwiązań organizacyjno-technicznych wskazanych w ust. 1 pkt 2.

7. W celu wdrożenia rozwiązań organizacyjno-technicznych, o których mowa w ust. 1 pkt 2, podmiot krytyczny uwzględnia specyfikacje techniczne określone w aktach

wykonawczych Komisji Europejskiej, wydanych na podstawie art. 13 ust. 6 dyrektywy 2022/2557.

8. Podmiot krytyczny, przy opracowywaniu i zawieraniu umów zapewniających wdrożenie rozwiązań, o których mowa w ust. 1 pkt 2, żąda od usługodawców:

1) certyfikatów, uwzględniając równoważne, zgodnie z zasadami wzajemnego uznawania w Unii Europejskiej lub w przypadku ich braku innych dokumentów właściwych dla poszczególnych rozwiązań, potwierdzających posiadanie odpowiednich kompetencji i uprawnień niezbędnych do ich realizacji;
2) potwierdzenia zdolności do ochrony informacji niejawnych oraz stosowania przepisów o ochronie informacji niejawnych, jeżeli opracowanie, przygotowanie i wykonanie umowy wiążą się dostępem do informacji niejawnych.

9. Organ do spraw podmiotów krytycznych, po zasięgnięciu opinii właściwych sektorowych rad do spraw kompetencji, o których mowa w art. 4c ust. 1 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (Dz. U. z 2024 r. poz. 419), może opracować i udostępnić na stronie podmiotowej Biuletynu Informacji Publicznej zestawienie certyfikatów lub innych dokumentów właściwych dla realizacji rozwiązań wskazanych w ust. 1 pkt 2.

10. Organ do spraw podmiotów krytycznych we współpracy z dyrektorem Centrum ustala klauzulę tajności oraz szczegółowe wymagania dotyczące ochrony informacji niejawnych związanych z realizacją przez podmiot krytyczny przedsięwzięć związanych z zapewnieniem bezpieczeństwa świadczenia usługi kluczowej.

11. W przypadku gdy podmiot krytyczny prowadzi ocenę ryzyka oraz opracowuje dokumentację dotyczącą oceny ryzyka na podstawie odrębnych przepisów, odpowiadającą przepisom rozdziału 11 ustawy, uznaje się wymóg prowadzenia oceny ryzyka za spełniony w całości lub w części.

Art. 6zu.1. Podmiot krytyczny opracowuje, stosuje i aktualizuje dokumentację dotyczącą zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej.

2. Dokumentację, o której mowa w ust. 1, stanowią:

1) dokumentacja dotycząca systemu zarządzania bezpieczeństwem informacji;
2) dokumentacja systemu zarządzania ciągłością działania usługi kluczowej;

3) dokumentacja ochrony fizycznej oraz zabezpieczeń technicznych, o których mowa w art. 6zt ust. 1 pkt 2 lit. b oraz bezpieczeństwa osobowego, o którym mowa w art. 6zt ust. 1 pkt 2 lit. d;
4) dokumentacja ochrony infrastruktury krytycznej, o której mowa w art. 6zf ust. 1;
5) dokumentacja cyberbezpieczeństwa, opracowywana zgodnie z wymogami dla podmiotów kluczowych, o których mowa w przepisach ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
6) inne elementy niż wskazane w pkt 1-5, biorąc pod uwagę rodzaj świadczonej usługi kluczowej.

3. Dokumentacja może być prowadzona w postaci papierowej lub w postaci elektronicznej.

4. Podmiot krytyczny po raz pierwszy sporządza dokumentację w terminie 15 miesięcy od otrzymania informacji o ujęciu w wykazie podmiotów krytycznych, a następnie stosownie do potrzeb dokonuje jej aktualizacji.

5. Podmiot krytyczny jest obowiązany do ustanowienia nadzoru nad dokumentacją zapewniającego:
1) dostępność dokumentów wyłącznie dla osób upoważnionych, zgodnie z realizowanymi przez nie zadaniami;
2) ochronę dokumentów przed uszkodzeniem, zniszczeniem, utratą, nieuprawnionym dostępem, niewłaściwym użyciem lub utratą integralności.

6. Podmiot krytyczny przechowuje dokumentację przez co najmniej 2 lata od dnia jej wycofania z użytkowania lub zakończenia świadczenia usługi, liczony od 1 stycznia roku następującego po roku, w którym wygasa okres jej przechowywania. Przepisu nie stosuje się do podmiotów podlegających ustawie z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2020 r. poz. 164).

Art. 6zv. 1. Podmiot krytyczny jest obowiązany do zarządzania incydentem, w tym:
1) zapewnienia obsługi incydentu;
2) zapewnienia dostępu do informacji o zarejestrowanym incydencie organowi do spraw podmiotów krytycznych oraz dyrektorowi Centrum;
3) klasyfikowania incydentu jako istotnego, na podstawie progów uznawania incydentu za istotny, określonych w przepisach wykonawczych wydanych na podstawie ust. 4;
4) zgłaszania incydentu istotnego niezwłocznie, nie później niż w terminie 24 godzin od momentu jego wystąpienia lub wykrycia:

a) właściwemu organowi do spraw podmiotów krytycznych oraz dyrektorowi Centrum,

b) Szefowi Agencji Bezpieczeństwa Wewnętrznego,

c) podmiotowi, w ramach którego funkcjonuje Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT) poziomu krajowego;

5) współdziałania podczas obsługi incydentu istotnego z właściwym organem do spraw podmiotów krytycznych lub dyrektorem Centrum;

6) informowania właściwego organu do spraw podmiotów krytycznych oraz dyrektora Centrum o usunięciu incydentu istotnego;

7) w szczególnie uzasadnionych przypadkach przekazywania sprawozdania z czynności, o których mowa w pkt 1-6 organowi do spraw podmiotów krytycznych oraz dyrektorowi Centrum w terminie nie dłuższym niż 30 dni od dnia wystąpienia incydentu istotnego.

2. Zgłoszenie, o którym mowa w ust. 1 pkt 4, dokonuje się za pomocą systemu, o którym mowa w art. 46 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

3. W przypadku braku możliwości dokonania zgłoszenia w systemie, o którym mowa w art. 46 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, zgłoszenie przekazywane jest na piśmie utrwalonym w postaci elektronicznej, opatrzonym kwalifikowanym podpisem elektronicznym, podpisem osobistym, podpisem zaufanym albo kwalifikowaną pieczęcią elektroniczną.

4. Rada Ministrów określi, w drodze rozporządzenia, progi uznania incydentu za istotny według zdarzenia w poszczególnych sektorach i podsektorach określonych w załączniku do ustawy, uwzględniając:

1) liczbę użytkowników dotkniętych zakłóceniem,

2) czas trwania zakłócenia usługi kluczowej,

3) obszar geograficzny, którego dotyczy zakłócenie biorąc pod uwagę stopień odizolowania geograficznego,

4) inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują

- kierując się potrzebą zapewnienia ochrony przed zagrożeniami życia lub zdrowia ludzi, znacznymi stratami majątkowymi oraz zagrożeniem obniżenia jakości świadczonej usługi kluczowej.

Art. 6zw. 1. Zgłoszenie, o którym mowa w art. 6zv ust. 1 pkt 4, zawiera:

1) dane podmiotu zgłaszającego, w tym firmę przedsiębiorcy, numer we właściwym rejestrze, siedzibę i adres;
2) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby dokonującej zgłoszenia;
3) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji;
4) opis wpływu incydentu istotnego na świadczenie usługi kluczowej, w tym:
   a) usługi kluczowej zgłaszającego, na którą incydent miał wpływ,
   b) liczbę użytkowników usługi kluczowej, na których incydent miał wpływ,
   c) moment wystąpienia i wykrycia incydentu istotnego oraz czas jego trwania,
   d) obszar geograficzny, którego dotyczy incydent istotny,
   e) wpływ incydentu istotnego na świadczenie usług kluczowych przez inne podmioty krytyczne,
   f) przyczynę zaistnienia incydentu istotnego i sposób jego przebiegu oraz skutki jego oddziaływania na świadczoną usługę kluczową;
5) informacje umożliwiające właściwemu organowi do spraw podmiotów krytycznych oraz dyrektorowi Centrum określenie, czy incydent istotny dotyczy innych państw członkowskich Unii Europejskiej;
6) informacje o podjętych działaniach zapobiegawczych;
7) informacje o podjętych działaniach naprawczych;
8) inne istotne informacje.

2. Podmiot krytyczny przekazuje informacje znane mu w chwili dokonywania zgłoszenia, które uzupełnia w trakcie obsługi incydentu istotnego.

3. Organ do spraw podmiotów krytycznych oraz dyrektor Centrum mogą zwrócić się do podmiotu krytycznego o uzupełnienie zgłoszenia o informacje w zakresie niezbędnym do realizacji zadań, o których mowa w ustawie.

4. Organ do spraw podmiotów krytycznych, za pośrednictwem Pojedynczego Punktu Kontaktowego, informuje Komisję Europejską o incydencie istotnym, który ma lub może mieć wpływ na ciągłość świadczenia usługi kluczowej na rzecz co najmniej sześciu państw członkowskich Unii Europejskiej lub w co najmniej sześciu państwach członkowskich Unii Europejskiej.

5. Organ do spraw podmiotów krytycznych informuje opinię publiczną o incydencie istotnym, jeżeli uzna, że leży to w interesie publicznym.

Art. 6zx.1. Podmiot krytyczny może przekazywać właściwym organom do spraw podmiotów krytycznych oraz dyrektorowi Centrum informacje dotyczące:

1) incydentów innych niż istotne;

2) zagrożeń dla niezakłóconego świadczenia usługi kluczowej.

2. Informacje, o których mowa w ust. 1, są przekazywane na piśmie utrwalonym w postaci elektronicznej, opatrzonym kwalifikowanym podpisem elektronicznym, podpisem osobistym, podpisem zaufanym albo kwalifikowaną pieczęcią elektroniczną, a w przypadku braku możliwości przekazania w postaci elektronicznej, przy użyciu innych dostępnych środków komunikacji.

Art. 6zy. Podmiot krytyczny informuje 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.

Art. 6zz. 1. Podmiot krytyczny przeprowadza na własny koszt, co najmniej raz na 3 lata, audyt zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej, zwanego dalej "audytem" w zakresie:

1) zarządzania bezpieczeństwem informacji;

2) zarządzania ciągłością działania usługi kluczowej;

3) zapewnienia bezpieczeństwa fizycznego, w tym ochrony fizycznej budynków i terenów należących do podmiotu krytycznego oraz zabezpieczeń technicznych, uwzględniających kontrolę dostępu.

2. Podmiot krytyczny przedstawia w postaci elektronicznej kopię raportu z przeprowadzonego audytu, o którym mowa w ust. 1, organowi do spraw podmiotów krytycznych, w terminie trzech dni roboczych od dnia jego otrzymania przez podmiot krytyczny.

3. W przypadku wystąpienia incydentu istotnego, organ do spraw podmiotów krytycznych może nakazać podmiotowi krytycznemu, w drodze decyzji, przeprowadzenie zewnętrznego audytu, wraz z określeniem terminu przekazania kopii raportu z przeprowadzonego audytu i wskazaniem kategorii podmiotów do przeprowadzenia audytu. Organ do spraw podmiotów krytycznych może również określić zakres audytu oraz nadać decyzji rygor natychmiastowej wykonalności.

Art. 6zza. 1. Audyt może być prowadzony przez:

1) jednostkę certyfikującą właściwą w zakresie, o którym mowa w art. 6zz ust. 1;

2) co najmniej dwóch audytorów, w tym jednego z ukończonym szkoleniem audytora wiodącego, posiadających certyfikaty określone w akcie wykonawczym, o którym mowa w ust. 10

- spełniających wymagania bezpieczeństwa osobowego i przemysłowego w zakresie dostępu do informacji niejawnych o klauzuli „poufne”.

2. Wymogu posiadania dostępu do informacji niejawnych o klauzuli "poufne" nie stosuje się do audytorów, o których mowa w art. 6zza ust. 1 pkt 2, w przypadku gdy są oni pracownikami podmiotu krytycznego.

3. Jednostka certyfikująca lub audytorzy są obowiązani do zachowania w tajemnicy informacji uzyskanych w związku z przeprowadzanym audytem, z zachowaniem przepisów o ochronie informacji niejawnych i innych informacji prawnie chronionych.

4. Audyt nie może być przeprowadzony przez osobę realizującą w podmiocie audytowanym zadania, o których mowa w art. 6zt ust. 1, art. 6zu ust. 1 oraz art. 6zv ust. 1, lub która realizowała te zadania w podmiocie audytowanym nie później niż w terminie 1 roku przed rozpoczęciem audytu.

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

6. Obowiązek przeprowadzenia audytu uznaje się za spełniony w przypadku posiadania przez podmiot krytyczny certyfikatów w zakresie, o którym mowa w art. 6zz ust. 1.

7. Podmiot krytyczny przedstawia kopię raportu z przeprowadzonego audytu lub certyfikatu, o którym mowa w ust. 6, właściwemu organowi do spraw podmiotów krytycznych w terminie 7 dni roboczych od dnia jego otrzymania lub dyrektorowi Centrum na jego uzasadniony wniosek.

8. Kopię raportu z przeprowadzonego audytu lub certyfikatu, o którym mowa w ust. 6, przekazuje się za pomocą systemu, o którym mowa w art. 46 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

9. W przypadku braku możliwości przekazania kopii audytu lub certyfikatu, o którym mowa w ust. 7, za pomocą systemu, o którym mowa w art. 46 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, przekazanie następuje na piśmie utrwalonym w postaci elektronicznej, opatrzonym kwalifikowanym podpisem

elektronicznym, podpisem osobistym, podpisem zaufanym albo kwalifikowaną pieczęcią elektroniczną.

10. Rada Ministrów określi, w drodze rozporządzenia, wykaz certyfikatów uprawniających do przeprowadzenia audytów, uwzględniając zakres wiedzy specjalistycznej wymaganej od osób lub podmiotów legitymujących się poszczególnymi certyfikatami oraz wymagane doświadczenie.

Art. 6zzb. 1. Podmiot krytyczny zapewnia udział struktur organizacyjnych lub pracowników niezbędnych do zapewnienia niezakłóconego świadczenia usługi kluczowej w szkoleniach lub ćwiczeniach:

1) obronnych;
2) obrony cywilnej;
3) ochrony ludności;
4) z zakresu przeciwdziałania zagrożeniom o charakterze terrorystycznym;
5) zarządzania kryzysowego.

2. Szkolenia, o których mowa w ust. 1, polegają na nabywaniu lub aktualizacji wiedzy i umiejętności niezbędnych do realizacji przedsięwzięć w zakresie, o którym mowa w ust. 1.

3. Ćwiczenia, o których mowa w ust. 1, polegają na nabywaniu przez ćwiczących umiejętności praktycznej realizacji zadań w zakresie, o którym mowa w ust. 1.

4. Podmiot krytyczny we współpracy z właściwym organem do spraw podmiotów krytycznych lub dyrektorem Centrum planuje i organizuje udział w szkoleniach i ćwiczeniach, o których mowa w ust. 1.

Art. 6zzc. 1. Podmiot krytyczny, w celu zapewnienia ochrony ciągłości świadczenia usługi kluczowej, może prowadzić sprawdzenie przeszłości w odniesieniu do:

1) pracownika podmiotu krytycznego lub kandydata na pracownika:
   a) pełniącego newralgiczną rolę bezpośrednio w strukturze organizacyjnej podmiotu krytycznego lub działając na jego rzecz, w tym:
      - reprezentującego podmiot krytyczny samodzielnie lub łącznie z innymi osobami na podstawie statutu, umowy lub innego aktu założycielskiego,
      - pełniącego funkcje kierownicze lub koordynacyjne,

b) posiadającego bezpośredni lub zdalny dostęp do budynków i terenów podmiotu krytycznego, obiegu informacji lub systemów kontroli, w szczególności związanych z bezpieczeństwem podmiotu krytycznego,

c) realizującego audyt, o którym mowa w art. 6zz ust. 1;

2) osoby świadczącej usługę na rzecz podmiotu krytycznego, niebędącej pracownikiem podmiotu krytycznego, posiadającej bezpośredni lub zdalny dostęp do budynków i terenów podmiotu krytycznego, obiegu informacji lub systemów kontroli, w szczególności związanych z bezpieczeństwem podmiotu krytycznego.

2. Sprawdzenie przeszłości osób, o których mowa w ust. 1, obejmuje:

1) potwierdzenie tożsamości;

2) ocenę informacji pozyskanych z rejestrów karnych pod kątem przestępstw, które mogą mieć znaczenie dla zajmowanego stanowiska, ubiegania się o to stanowisko lub świadczenia usług na rzecz podmiotu krytycznego.

3. Podmiot krytyczny, w odniesieniu do osoby, o której mowa w ust. 1 pkt 1, w celu:

1) potwierdzenia tożsamości:

a) żąda przedłożenia ważnego dowodu osobistego lub ważnego dokumentu paszportowego tej osoby oraz podania nazwiska rodowego i poprzednio noszonego nazwiska, jeżeli było zmieniane, oraz nazwisk, imion, dat i miejsc urodzenia rodziców,

b) wnioskuje do organu dowolnej gminy o udostępnienie danych jednostkowych zawartych w rejestrze PESEL oraz o udostępnienie danych w trybie jednostkowym z Rejestru Dowodów Osobistych;

2) dokonania oceny informacji pozyskanych z rejestrów karnych:

a) pozyskuje informację z Krajowego Rejestru Karnego w zakresie skazań za przestępstwa umyślne ścigane z oskarżenia publicznego oraz umyślne przestępstwa skarbowe,

b) występuje do Biura Informacyjnego Krajowego Rejestru Karnego z wnioskiem o wystąpienie do organów centralnych państw członkowskich Unii Europejskiej państwa obywatelstwa osoby podlegającej sprawdzeniu przeszłości z zapytaniem o udzielenie informacji o osobie, w przypadku gdy osoba podlegająca sprawdzeniu ma obywatelstwo państwa członkowskiego innego niż Rzeczpospolita Polska.

4. Podmiot krytyczny, w odniesieniu do osoby, o której mowa w ust. 1 pkt 2, ma prawo żądać:

1) przedłożenia przez tę osobę ważnego dowodu osobistego lub ważnego dokumentu paszportowego tej osoby oraz podania nazwiska rodowego i poprzednio noszonego nazwiska, jeżeli było zmieniane, oraz nazwisk, imion, dat i miejsc urodzenia rodziców;
2) przedłożenia przez tę osobę informacji z Krajowego Rejestru Karnego w zakresie skazań za przestępstwa umyślne ścigane z oskarżenia publicznego oraz umyślne przestępstwa skarbowe.

5. Podmiot krytyczny uwzględnia negatywny wynik sprawdzenia przeszłości w zakresie powierzania zadań osobom, o których mowa w ust. 1, w szczególności w przypadku skazania prawomocnym wyrokiem na karę pozbawienia wolności za przestępstwo umyślne ścigane z oskarżenia publicznego, także popełnione za granicą, lub umyślne przestępstwo skarbowe, jeżeli czyn, za który nastąpiło skazanie wywołuje uzasadnione wątpliwości w zakresie powierzenia realizacji tych zadań.

6. Sprawdzenie przeszłości przeprowadza się co najmniej raz na trzy lata.

7. Podmiot krytyczny przetwarza dane osobowe w zakresie realizacji czynności, o których mowa w ust. 1, w zakresie i w celu niezbędnym do ich realizacji.

8. Sprawdzenia przeszłości nie prowadzi się w odniesieniu do osoby wskazanej w ust. 1 pkt 1, która samodzielnie przedłożyła wymagane dokumenty albo posiada co najmniej poświadczenie bezpieczeństwa o klauzuli "poufne".

Art. 6zzd. 1. W celu realizacji zadań, o których mowa w art. 6zt ust. 1, art. 6zu ust. 1, art. 6zv ust. 1, art. 6zzb ust. 1 oraz art. 6zzc ust. 1, podmiot krytyczny wyznacza pełnomocnika bezpieczeństwa usługi kluczowej oraz zastępcę pełnomocnika usługi kluczowej.

2. Podmiot krytyczny wyznacza pełnomocnika bezpieczeństwa usługi kluczowej oraz zastępcę pełnomocnika usługi kluczowej w terminie 30 dni od dnia otrzymania informacji o ujęciu w wykazie podmiotów krytycznych.

3. Zastępca pełnomocnika bezpieczeństwa usługi kluczowej zastępuje pełnomocnika w czasie jego nieobecności lub czasowej niemożności wykonywania przez niego obowiązków.

4. Pełnomocnik bezpieczeństwa usługi kluczowej jest osoba, która:

1) jest pracownikiem podmiotu krytycznego albo żołnierzem lub funkcjonariuszem pełniącym służbę w jednostce organizacyjnej będącej podmiotem krytycznym;
2) korzysta z pełni praw publicznych;
3) posiada wiedzę, umiejętności i doświadczenie w zakresie zarządzania bezpieczeństwem, z uwzględnieniem przedmiotu działalności podmiotu świadczące usługę kluczową;
4) nie była skazana prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe;
5) spełnia wymagania bezpieczeństwa osobowego w zakresie dostępu do informacji niejawnych o klauzuli „poufne”.

5. Pełnomocnik bezpieczeństwa usługi kluczowej podlega bezpośrednio organowi zarządzającemu podmiotu krytycznego.

6. O wyznaczeniu pełnomocnika bezpieczeństwa usługi kluczowej podmiot krytyczny informuje niezwłocznie właściwy organ do spraw podmiotów krytycznych oraz dyrektora Centrum, przekazując dane tej osoby obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej.

7. Podmiot krytyczny zapewnia pełnomocnikowi bezpieczeństwa usługi kluczowej organizacyjne i techniczne warunki realizacji zadań, w tym dostęp do niezbędnych dokumentów i informacji.

8. Przepisy, o których mowa w ust. 4-7, stosuje się do zastępcy pełnomocnika bezpieczeństwa usługi kluczowej.

Art. 6zze. 1. Do podmiotów krytycznych z sektora bankowego i infrastruktury rynków finansowych nie stosuje się przepisów rozdziału 11-14 ustawy, z wyjątkiem art. 6zt ust. 1 pkt 1, art. 6zt ust. 1 pkt 2 lit. b-d, f, h, i, art. 6zt pkt 3, art. 6zt ust. 2-11, art. 6zu ust. 1 i ust. 2 pkt 3, 4, 6, art. 6zu ust. 3-6, art. 6zx, art. 6zy, art. 6zzb, art. 6zzd.

2. Do podmiotów krytycznych z sektora infrastruktury cyfrowej nie stosuje się przepisów rozdziału 11-14 ustawy.

3. Podmioty krytyczne sektora bankowego i infrastruktury rynków finansowych przeprowadzają po raz pierwszy ocenę ryzyka, o której mowa w art. 6zt ust. 1 pkt 1, w terminie 10 miesięcy od otrzymania informacji o ujęciu w wykazie podmiotów krytycznych.

4. Do Narodowego Banku Polskiego nie stosuje się przepisów rozdziału 13 i 14 ustawy.

Rozdział 12

Podmiot krytyczny o szczególnym znaczeniu europejskim i misje doradcze

Art. 6zzf. 1. Podmiot krytyczny informuje właściwy organ do spraw podmiotów krytycznych oraz Pojedynczy Punkt Kontaktowy o fakcie świadczenia co najmniej jednej usługi kluczowej spośród usług kluczowych wskazanych w przepisach rozporządzenia delegowanego wydanego na podstawie art. 5 ust. 1 dyrektywy 2022/2557 na rzecz co najmniej sześciu państw członkowskich Unii Europejskiej lub w co najmniej sześciu państwach członkowskich Unii Europejskiej.

2. W przypadku, o którym mowa w ust. 1, właściwy organ do spraw podmiotów krytycznych, za pośrednictwem Pojedynczego Punktu Kontaktowego informuje Komisję Europejską o potencjalnym podmiocie krytycznym o szczególnym znaczeniu europejskim, przekazując dane, o których mowa w art. 6zo ust. 2 pkt 1-7.

Art. 6zzg. 1. 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.

2. W przypadku uznania przez Komisję Europejska podmiotu krytycznego, o którym mowa w art. 6zzf ust. 1, za podmiot krytyczny o szczególnym znaczeniu europejskim, organ do spraw podmiotów krytycznych informuje niezwłocznie podmiot krytyczny, o tym fakcie oraz obowiązkach, o których mowa w przepisach rozdziału 11 ustawy.

Art. 6zzh. 1. Organ do spraw podmiotów krytycznych, za pośrednictwem Pojedynczego Punktu Kontaktowego, zapewnia współpracę z Komisją Europejską oraz właściwymi organami państwa członkowskiego, na rzecz którego lub w którym jest świadczona usługa kluczowa lub w przypadku gdy podmiot krytyczny o szczególnym znaczeniu europejskim zidentyfikowany przez państwo członkowskie świadczy usługę kluczową na rzecz Rzeczypospolitej Polskiej lub na jej terytorium, w tym prowadzi wymianę informacji w zakresie:

1) oceny ryzyka podmiotu krytycznego o szczególnym znaczeniu europejskim;

2) wdrażania odpowiednich i proporcjonalnych do wyników oceny ryzyka rozwiązań organizacyjno-technicznych służących zapewnieniu odporności tego podmiotu;
3) działań z zakresu nadzoru oraz egzekwowania przepisów ustawy przez właściwy organ do spraw podmiotów krytycznych.

2. Właściwy organ do spraw podmiotów krytycznych, za pośrednictwem Pojedynczego Punktu Kontaktowego, współpracuje z Komisją Europejską w zakresie organizowania i zapewnienia obsługi misji doradczej, w tym:

1) przedkłada wniosek o zorganizowanie misji doradczej;
2) konsultuje program misji doradczej, w tym proponuje kandydatów do uczestnictwa w misji doradczej;
3) koordynuje realizację czynności związanych z dostępem przedstawicieli misji doradczej do informacji oraz budynków, terenów i infrastruktury krytycznej podmiotu krytycznego o szczególnym znaczeniu europejskim;
4) przeprowadza analizę sprawozdania z ustaleń misji doradczej.

3. Właściwy organ do spraw podmiotów krytycznych za pośrednictwem Pojedynczego Punktu Kontaktowego:

1) 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;
2) przekazuje opinię, o której mowa w pkt 1, podmiotowi krytycznemu o szczególnym znaczeniu europejskim oraz zapewnia wsparcie w przypadku konieczności wdrożenia dodatkowych środków zwiększających odporność;
3) informuje Komisję Europejską oraz właściwe organy państwa członkowskiego, na rzecz którego lub w którym jest świadczona usługa kluczowa, o środkach zwiększających odporność, wprowadzonych z uwzględnieniem opinii, o której mowa w pkt 1, albo informację o braku konieczności wprowadzania tych środków.

4. Przepisy ust. 2 i 3 stosuje się odpowiednio do misji doradczej organizowanej dla podmiotu krytycznego niebędącego podmiotem krytycznym o szczególnym znaczeniu

europejskim, na wniosek organu do spraw podmiotów krytycznych, który zidentyfikował podmiot krytyczny i za zgoda tego podmiotu.

5. Przepis ust. 2 stosuje się odpowiednio do wniosku o organizację misji doradczej, w przypadku gdy podmiot krytyczny o szczególnym znaczeniu europejskim zidentyfikowany przez państwo członkowskie świadczy usługę kluczową na rzecz Rzeczypospolitej Polskiej lub na jej terytorium.

Rozdział 13

Nadzór i kontrola podmiotów krytycznych

Art. 6zzi. 1. 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 wynikających z ustawy dotyczących przeciwdziałania zagrożeniom dla świadczonych usług kluczowych i zgłaszania incydentów istotnych.

2. W ramach nadzoru, o którym mowa w ust. 1, organ do spraw podmiotów krytycznych:

1) prowadzi kontrole podmiotów krytycznych, w siedzibie podmiotu, miejscu wykonywania działalności gospodarczej lub zdalnie;
2) zleca audyt zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej na koszt podmiotu krytycznego, w przypadku, o którym mowa w art. 6zz ust. 3;
3) nakłada kary pieniężne na podmioty krytyczne.

3. Organ do spraw podmiotów krytycznych może żądać od podmiotu krytycznego informacji w zakresie wdrożenia rozwiązań zawartych w dokumentacji cyberbezpieczeństwa, o której mowa w art. 6zu ust. 3 pkt 5, obejmujących:

1) wpływ wdrożonych rozwiązań na bezpieczeństwo świadczenia usługi kluczowej,
2) dowodów potwierdzających wdrożone rozwiązania, w tym wyniki audytów przeprowadzonych przez podmiot krytyczny.

4. Organ do spraw podmiotów krytycznych wskazuje cel i uzasadnienie żądania, o którym mowa w ust. 3.

Art. 6zzj. Do kontroli realizowanej wobec podmiotów:

1) będących przedsiębiorcami stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. - Prawo przedsiębiorców (Dz. U. z 2024 r. poz. 236 i 1222);
2) niebędących przedsiębiorcami stosuje się przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. z 2020 r. poz. 224) określające zasady i tryb przeprowadzania kontroli.

Art. 6zzk. Osoba prowadząca czynności kontrolne wobec podmiotów będących przedsiębiorcami ma prawo do:

1) swobodnego wstępu i poruszania się po terenie podmiotu kontrolowanego;
2) wglądu do dokumentów dotyczących działalności podmiotu kontrolowanego, pobierania za pokwitowaniem oraz zabezpieczania dokumentów związanych z zakresem kontroli, z zachowaniem przepisów o tajemnicy prawnie chronionej;
3) sporządzania, a w razie potrzeby żądania sporządzenia, niezbędnych do kontroli kopii, odpisów lub wyciągów z dokumentów oraz zestawień lub obliczeń;
4) przetwarzania danych osobowych w zakresie niezbędnym do realizacji celu kontroli;
5) żądania złożenia ustnych lub pisemnych wyjaśnień w sprawach dotyczących zakresu kontroli;
6) przeprowadzania oględzin urządzeń, nośników oraz systemów informacyjnych.

Art. 6zzl. 1. Kontrolowane podmioty zapewniają osobie prowadzącej czynności kontrolne warunki niezbędne do sprawnego przeprowadzenia kontroli, w szczególności przez zapewnienie niezwłocznego przedstawienia żądanych dokumentów, terminowego udzielania ustnych i pisemnych wyjaśnień w sprawach objętych kontrolą, udostępniania niezbędnych urządzeń technicznych, a także sporządzania we własnym zakresie kopii lub wydruków dokumentów oraz informacji zgromadzonych na nośnikach, w urządzeniach lub w systemach informacyjnych.

2. Podmiot kontrolowany dokonuje potwierdzenia za zgodność z oryginałem sporządzonych kopii lub wydruków, o których mowa w ust. 1. W przypadku odmowy potwierdzenia za zgodność z oryginałem potwierdza je osoba prowadząca czynności kontrolne, o czym czyni wzmiankę w protokole kontroli.

Art. 6zzm. 1. Osoba prowadząca czynności kontrolne wobec podmiotów krytycznych ustala stan faktyczny na podstawie dowodów zebranych w toku kontroli, w szczególności dokumentów, przedmiotów, oględzin oraz ustnych lub pisemnych wyjaśnień i oświadczeń.

2. Osoba prowadząca czynności kontrolne wobec podmiotów krytycznych będących przedsiębiorcami przedstawia przebieg przeprowadzonej kontroli w protokole kontroli.

3. Protokół kontroli zawiera:

1) wskazanie nazwy oraz adresu podmiotu kontrolowanego;
2) imię i nazwisko osoby reprezentującej podmiot kontrolowany lub nazwę organu reprezentującego ten podmiot;
3) imię i nazwisko oraz stanowisko służbowe osoby prowadzącej czynności kontrolne;
4) datę rozpoczęcia i zakończenia czynności kontrolnych;
5) określenie przedmiotu, zakresu oraz okresu kontroli;
6) opis stanu faktycznego ustalonego w toku kontroli;
7) ocenę kontrolowanej działalności, w tym zakres, przyczyny i skutki stwierdzonych nieprawidłowości;
8) wyszczególnienie załączników.

4. Protokół kontroli podpisują osoba prowadząca czynności kontrolne oraz osoba reprezentująca podmiot kontrolowany.

5. W przypadku zastrzeżeń dotyczących ustaleń zawartych w protokole kontroli podmiot krytyczny ma prawo odmówić podpisania protokołu kontroli oraz złożyć umotywowane pisemne zastrzeżenia do tego protokołu w terminie 7 dni od dnia przedstawienia mu protokołu do podpisu.

6. Odmowę podpisania protokołu kontroli osoba prowadząca czynności kontrolne odnotowuje w protokole wraz ze wskazaniem daty tej odmowy.

7. W razie złożenia zastrzeżeń do protokołu kontroli kierownik komórki organizacyjnej do spraw kontroli dokonuje ich analizy.

8. Kierownik komórki organizacyjnej do spraw kontroli:

1) odrzuca zastrzeżenia do protokołu kontroli wniesione przez osobę nieuprawnioną lub wniesione po upływie terminu i informuje o tym na piśmie zgłaszającego zastrzeżenia, podając przyczyny, albo
2) uwzględnia zastrzeżenia do protokołu kontroli w całości albo w części lub je oddala.

9. W razie potrzeby, osoba prowadząca czynności kontrolne podejmuje dodatkowe czynności kontrolne, a w przypadku stwierdzenia przez kierownika komórki organizacyjnej do spraw kontroli zasadności zastrzeżeń do protokołu kontroli zmienia lub uzupełnia odpowiednią część protokołu kontroli w formie aneksu do protokołu.

10. Kierownik komórki organizacyjnej do spraw kontroli, po rozpatrzeniu zastrzeżeń do protokołu kontroli, sporządza stanowisko wobec tych zastrzeżeń.

11. W przypadku nieuwzględnienia zastrzeżeń do protokołu kontroli w całości albo w części kierownik komórki organizacyjnej do spraw kontroli informuje kontrolowany podmiot krytyczny na piśmie.

12. Protokół kontroli:

1) w postaci papierowej sporządza się w dwóch egzemplarzach, z których jeden pozostawia się podmiotowi kontrolowanemu;
2) w postaci elektronicznej doręcza się podmiotowi kontrolowanemu.

Art. 6zzn. 1. 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, wskazując jednocześnie termin ich usunięcia. Przy określaniu terminu usunięcia nieprawidłowości, organ do spraw podmiotów krytycznych bierze pod uwagę zakres i rodzaj stwierdzonych naruszeń.

2. Od zaleceń pokontrolnych nie przysługują środki odwoławcze.

3. Podmiot kontrolowany, w wyznaczonym terminie, informuje organ do spraw podmiotów krytycznych o sposobie wykonania zaleceń.

Rozdział 14

Przepisy o karach pieniężnych dla podmiotów krytycznych

Art. 6zzo. 1. Karze pieniężnej podlega podmiot krytyczny, który:

1) nie przeprowadza systematycznej oceny ryzyka, o której mowa w art. 6zt ust. 1 pkt 1;
2) nie wdraża rozwiązań organizacyjno-technicznych, o których mowa w art. 6zt ust. 1 pkt 2;
3) nie prowadzi dokumentacji, o której mowa w art. 6zu ust. 1;
4) nie wykonuje obowiązku, o których mowa w art. 6zv ust. 1 pkt 1, w zakresie obsługi incydentu istotnego;
5) nie wykonuje obowiązku, o których mowa w art. 6zv ust. 1 pkt 4;
6) nie przeprowadza audytu, o którym mowa w art. 6zz ust. 1;
7) nie wyznacza pełnomocnika bezpieczeństwa usługi kluczowej lub zastępcy pełnomocnika bezpieczeństwa usługi kluczowej, o których mowa w art. 6zzd ust. 1;

8) uniemożliwia lub utrudnia wykonywanie kontroli, o której mowa w art. 6zzi ust. 2 pkt 1;
9) nie wykonał w wyznaczonym terminie zaleceń pokontrolnych, o których mowa w art. 6zzn ust. 1;
10) nie wdrożył rozwiązań dotyczących ochrony infrastruktury krytycznej, o których mowa w art. 6ze ust. 1 pkt 2, w odniesieniu do infrastruktury krytycznej niezbędnej do świadczenia usługi kluczowej;
11) nie opracował dokumentacji ochrony infrastruktury krytycznej, o której mowa w art. 6zf ust. 1, w odniesieniu do infrastruktury krytycznej niezbędnej do świadczenia usługi kluczowej.

2. Wysokość kary pieniężnej, o której mowa w:
1) ust. 1 pkt 1, wynosi do 100 000 zł;
2) ust. 1 pkt 2, wynosi do 150 000 zł;
3) ust. 1 pkt 3, wynosi do 50 000 zł;
4) ust. 1 pkt 4, wynosi do 20 000 zł za każdy stwierdzony przypadek zaniechania obsługi incydentu istotnego;
5) ust. 1 pkt 5, wynosi do 25 000 zł za każdy stwierdzony przypadek niezgłoszenia incydentu istotnego;
6) ust. 1 pkt 6, wynosi do 200 000 zł;
7) ust. 1 pkt 7, wynosi do 15 000 zł:
8) ust. 1 pkt 8, wynosi do 50 000 zł;
9) ust. 1 pkt 9, wynosi do 200 000 zł;
10) ust. 1 pkt 10, wynosi do 150 000 zł;
11) ust. 1 pkt 11, wynosi do 50 000 zł.

3. Kara, o której mowa w:
1) ust. 1 pkt 4,5 i 7, nie może być niższa niż 2000 zł;
2) ust. 1 pkt 3, 8 i 11, nie może być niższa niż 5000 zł;
3) ust. 1 pkt 1, 2, 6, 9 i 10, nie może być niższa niż 15 000 zł.

Art. 6zzp. 1. Karę pieniężną, o której mowa w art. 6zzo, nakłada w drodze decyzji, organ do spraw podmiotów krytycznych.

2. Organ do spraw podmiotów krytycznych może decyzji, o której mowa w ust. 1, nadać rygor natychmiastowej wykonalności w całości albo w części, jeżeli wymaga tego

ochrona bezpieczeństwa lub porządku publicznego oraz zagrożenie wywołania poważnych utrudnień w świadczeniu usług.

3. Wpływy z tytułu kar pieniężnych, o których mowa w art. 6zzo, stanowią 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 (Dz. U. z 2023 r. poz. 677 oraz z 2024 r. poz. 834).

4. W przypadku niewykonywania zadań w zakresie cyberbezpieczeństwa przez podmiot krytyczny karę na ten podmiot nakłada organ właściwy do spraw cyberbezpieczeństwa w trybie i na zasadach, o których mowa w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Art. 6zzq. 1. Organ do spraw podmiotów krytycznych, podejmując decyzję o nałożeniu kary pieniężnej i ustalając jej wysokość bierze pod uwagę:

1) wagę naruszenie i znaczenie naruszonych przepisów ustawy;
2) czasu trwania naruszenia;
3) wcześniejszych naruszeń ze strony danego podmiotu krytycznego;
4) spowodowane szkody majątkowe i niemajątkowe, w tym wpływ na użytkowników usługi oraz na inne usługi kluczowe;
5) środki zastosowane przez podmiot w celu ograniczenia szkód, o których mowa w pkt 4;
6) umyślny lub nieumyślny charakter czynu ze strony sprawcy naruszenia;
7) stopień współpracy podmiotu krytycznego z organem do spraw podmiotów krytycznych.

2. Podejmując decyzję organ uwzględnia również wysokość przychodu uzyskanego z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary pieniężnej lub możliwości finansowe podmiotu krytycznego będącego podmiotem publicznym.

3. W związku z toczącym się postępowaniem w sprawie nałożenia kary pieniężnej, organ do spraw podmiotów krytycznych może żądać od podmiotu krytycznego przekazania we wskazanym terminie, nie dłuższym niż 14 dni od dnia otrzymania żądania, informacji niezbędnych do określenia wymiaru kary pieniężnej.

4. W przypadku nieprzekazania informacji, o których mowa w ust. 2, lub przekazania informacji uniemożliwiających ustalenie podstawy wymiaru kary pieniężnej, organ do spraw podmiotów krytycznych ustala podstawę wymiaru kary pieniężnej w

sposób szacunkowy uwzględniając wielkość podmiotu krytycznego, specyfikę działalności tego podmiotu oraz ogólnodostępne dane finansowe.

5. Karę pieniężną uiszcza się w terminie 14 dni, od dnia, w którym decyzja o jej wymierzeniu stała się ostateczna lub od dnia doręczenia decyzji z rygorem natychmiastowej wykonalności, na odrębny rachunek bankowy wskazany przez organ właściwy do spraw podmiotów krytycznych w decyzji o wymierzeniu kary pieniężnej.

6. Kara pieniężna nieuiszczona w terminie wraz z odsetkami podlega ściągnięciu w trybie określonym w przepisach o postępowaniu egzekucyjnym w administracji.

7. Organ właściwy do spraw podmiotów krytycznych może odstąpić od nałożenia kary pieniężnej, jeżeli waga naruszenia i znaczenie naruszonych przepisów jest znikome, a podmiot krytyczny zaprzestał naruszania prawa lub naprawił wyrządzoną szkodę.

Art. 6zzr. W zakresie nieuregulowanym w niniejszym rozdziale stosuje się odpowiednio przepisy działu IVa ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego.

8) po art. 6zzr dodaje się oznaczenie „Rozdział 15 Organy właściwe w sprawach zarządzania kryzysowego i ich zadania";

9) w art. 7a w ust. 3 pkt 2 otrzymuje brzmienie:

"2) zapewnienia właściwego funkcjonowania, ochrony, wzmocnienia oraz odbudowy infrastruktury krytycznej lub zapewnienia niezakłóconego świadczenia usługi kluczowej;";

10) w art. 10 w ust. 1 skreśla się wyrazy „, zwane dalej „Centrum”,”;

11) w art. 11:

a) w pkt 1 lit. b otrzymuje brzmienie:

"b) opracowywanie i aktualizowanie Krajowego Planu Zarządzania Ryzykiem oraz Krajowego Planu Reagowania Kryzysowego,”,

b) po ust. 1a dodaje się ust. 1b w brzmieniu:

"1b. Centrum realizuje zadania, o których mowa w art. 22 ustawy z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej.";

12) po art. 11a dodaje się art. 11b w brzmieniu:

"Art. 11b. W celu realizacji zadań planowania cywilnego wynikających z członkostwa Rzeczypospolitej Polskiej w Organizacji Traktatu Północnoatlantyckiego, Centrum:

1) koordynuje:

a) udział przedstawicieli Rzeczypospolitej Polskiej w pracach Komitetu do spraw Odporności Organizacji Traktatu Północnoatlantyckiego oraz zapewnia wsparcie merytoryczne prowadzonych prac,

b) opracowywanie stanowisk Rzeczypospolitej Polskiej na potrzeby procesów planowania cywilnego Organizacji Traktatu Północnoatlantyckiego;

2) zapewnienia funkcjonowanie punktu kontaktowego do przekazywania zadań oraz uruchamiania procedur wynikających z członkostwa Rzeczypospolitej Polskiej w Organizacji Traktatu Północnoatlantyckiego.";

13) w art. 12:

a) ust. 1 otrzymuje brzmienie:

„1. Ministrowie kierujący działami administracji rządowej oraz kierownicy urzędów centralnych realizują, w zakresie swojej właściwości, zadania dotyczące zarządzania kryzysowego, w tym:

1) opracowują plany zarządzania kryzysowego;

2) organizują, prowadzą i koordynują szkolenia i ćwiczenia z zakresu zarządzania kryzysowego oraz biorą udział w ćwiczeniach krajowych i międzynarodowych;

3) współpracują z operatorami infrastruktury krytycznej lub podmiotami krytycznymi w zakresie realizacji zadań ochrony infrastruktury krytycznej oraz zapewnienia niezakłóconego świadczenia usług kluczowych;

4) zapewniają funkcjonowania stałego dyżuru w ramach podwyższania gotowości obronnej państwa.",

b) uchyla się ust. 2 i 2a,

c) ust. 2c otrzymuje brzmienie:

„2c. Do zadań zespołów, o których mowa w ust. 2b, należy:

1) dokonywanie okresowej oceny ryzyka na potrzeby Krajowej Oceny Ryzyka;

2) dokonywanie okresowej oceny gotowości do reagowania w przypadku wystąpienia sytuacji kryzysowej w zakresie organizacyjnym, technicznym i finansowym;

3) opiniowanie projektów planów zarządzania kryzysowego;

4) wypracowywanie wniosków i propozycji dotyczących zapobiegania i przeciwdziałania zagrożeniom.”;

14) w art. 14 ust. 3 otrzymują brzmienie:

„3. Minister właściwy do spraw administracji publicznej w uzgodnieniu z ministrem właściwym do spraw wewnętrznych oraz po zasięgnięciu opinii dyrektora Centrum, wydaje, w drodze zarządzenia, wojewodom wytyczne do wojewódzkich planów zarządzania kryzysowego. Wytyczne do wojewódzkich planów zarządzania kryzysowego mogą zostać wydane w każdym czasie, niezależnie od cyklu planowania.";

15) w art. 25 w ust. 3 pkt 13 otrzymuje brzmienie:

"13) wspieranie w wykonywaniu zadań związanych z naprawą i odbudową infrastruktury technicznej;";

16) uchyla się art. 25a-25d;

17) po art. 25d dodaje się oznaczenie „Rozdział 16 Finansowanie zadań zarządzania kryzysowego";

18) w art. 26 dodaje się ust. 4a i 4b w brzmieniu:

„4a. Środki finansowe z rezerwy celowej, o której mowa w ust. 4, mogą być przeznaczone na realizację przedsięwzięć związanych z zarządzaniem ryzykiem, reagowaniem w przypadku wystąpienia sytuacji kryzysowej oraz usuwaniem jej skutków i odtwarzaniem zasobów, z uwzględnieniem planowanych działań z zakresu ochrony ludności i obrony cywilnej.

4b. Środki z rezerwy celowej, o której mowa w ust. 4, mogą być przeznaczane na pomoc finansową udzielaną innym jednostkom samorządu terytorialnego na realizację przez te jednostki przedsięwzięć, o których mowa w ust. 4a."

19) po art. 31 dodaje się oznaczenie „Rozdział 17 Przepisy dostosowujące, przejściowe i końcowe".

Art. 2. W ustawie z dnia 21 marca 1985 r. o drogach publicznych (Dz. U. z 2024 r. poz. 320 i 1222) dodaje się art. 20i w brzmieniu:

"Art. 20i 1. W sytuacji kryzysowej, jeżeli wymagają tego potrzeby obronności lub istotny interes bezpieczeństwa państwa, właściwy miejscowo wojewoda może, w drodze rozporządzenia porządkowego, po zasięgnięciu opinii zarządcy drogi, wprowadzić czasowe ograniczenia w korzystaniu z dróg publicznych, w tym czasowo wyłączyć je z ruchu;

2. Czasowe ograniczenia w korzystaniu z dróg publicznych, w tym ich czasowe wyłączenie z ruchu wprowadza się w sposób, który umożliwia przemieszczanie się w określonych kierunkach za pomocą innych dróg niepodlegających ograniczeniom w korzystaniu i niewyłączonych z ruchu.

3. Rozporządzenie porządkowe w zakresie, o którym mowa w ust. 1, określa:

1) odcinki dróg publicznych wyznaczone za pomocą współrzędnych geograficznych lub oznakowania umieszczonego na słupkach hektometrowych i kilometrowych, na których wprowadzono czasowe ograniczenia w korzystaniu lub czasowo zamknięte dla ruchu;
2) rodzaj ograniczenia w korzystaniu z dróg publicznych;
3) okres, na który wprowadzono ograniczenia w korzystaniu z dróg publicznych lub czasowe wyłączenie z ruchu;
4) obowiązki zarządcy drogi, zarządzającego ruchem oraz innych organów i podmiotów w zakresie, o którym mowa w ust. 1.

4. Rozporządzenie porządkowe, o którym mowa w ust. 1, może być publikowane w drodze obwieszczenia lub za pomocą środków komunikacji elektronicznej, lub w inny sposób zwyczajowo przyjęty na danym terenie. Dzień takiego opublikowania jest dniem ogłoszenia.".

Art. 3. W ustawie z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2024 r. poz. 145, 1006, 1089, 1222, 1248, 1473 i 1562) w art. 16 ust. 1 otrzymuje brzmienie:

„1. W przypadkach, o których mowa w art. 11 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2024 r. poz. 383), policjanci mogą użyć środków przymusu bezpośredniego, o których mowa w art. 12 ust. 1 pkt 1−13 i 17−23 tej ustawy, lub wykorzystać te środki.”.

Art. 4. W ustawie z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2024 r. poz. 915, 1089, 1222, 1248, 1473 i 1562) wprowadza się następujące zmiany:

1) w art. 1 po ust. 3b dodaje się ust. 3c w brzmieniu:

„3c. Straż Graniczna zapewnia koordynację działań podejmowanych przez podmioty realizujące zadania w ramach CBM, o którym mowa w art. 25a ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich.";

2) w art. 23 ust. 1 otrzymuje brzmienie:

„1. W przypadkach, o których mowa w art. 11 ustawy z 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2024 r. poz. 383), funkcjonariusze mogą użyć środków przymusu bezpośredniego, o których mowa w art. 12 ust. 1 pkt 1−13 i 16−23 tej ustawy, lub wykorzystać te środki.”

Art. 5. W ustawie z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (Dz. U. z 2025 r. poz. 188) w art. 14fa ust. 3 otrzymuje brzmienie:

"3. Plany ratownicze w zakresie zdarzeń z dużą liczbą poszkodowanych oraz działań ratowniczych i działań pomocowych podczas katastrof, klęsk żywiołowych i zdarzeń nadzwyczajnych są skorelowane z planami reagowania kryzysowego, o których mowa w art. 6j ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, oraz z planami postępowania awaryjnego, o których mowa w art. 84 ust.1 ustawy z dnia 29 listopada 2000 r. - Prawo atomowe (Dz.U. z 2024 r. poz. 1277, 1897 i 1907).".

Art. 6. W ustawie z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2021 r. poz. 1995) wprowadza się następujące zmiany:

1) w art. 5:

a) w ust. 2 pkt 5 otrzymuje brzmienie:

„5) obiekt, urządzenie, instalację lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje ujęte w wykazie , o którym mowa w art. 6r ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz.122 oraz z 2024 r. poz. 834, 1222 i 1473).”,

b) ust. 3 otrzymuje brzmienie:

„3. Szczegółowe wykazy obszarów, obiektów i urządzeń, o których mowa w ust. 2, sporządzają i bieżąco aktualizują: Prezes Narodowego Banku Polskiego, Krajowa Rada Radiofonii i Telewizji, ministrowie, kierownicy urzędów centralnych i wojewodowie w stosunku do podległych, podporządkowanych lub nadzorowanych jednostek organizacyjnych, oraz Komisja Nadzoru Finansowego w stosunku do podmiotów podlegających nadzorowi Komisji Nadzoru Finansowego w rozumieniu ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (Dz. U. z 2024 r. poz. 135). Umieszczenie w wykazie określonego obszaru, obiektu lub urządzenia następuje w drodze decyzji administracyjnej.”,

c) po ust. 3 dodaje się ust. 3a w brzmieniu:

3a. Do wykazów, o których mowa w ust. 3 , stosuje się przepisy ustawy z dnia 5 sierpnia 2010 r o ochronie informacji niejawnych.”,

d) ust. 4 i 5 otrzymują brzmienie:

„4. Podmioty, o których mowa w ust. 3 , przekazują wykazy oraz ich aktualizacje właściwym terytorialnie wojewodom w terminie 14 dni odpowiednio od ich sporządzenia lub aktualizacji.

5. Wojewodowie prowadzą ewidencję obszarów, obiektów i urządzeń podlegających obowiązkowej ochronie, znajdujących się na terenie województwa. Do ewidencji stosuje się przepisy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.”,

e) po ust. 5 dodaje się ust. 5a w brzmieniu:

"5a. Ewidencja, o której mowa w ust. 5, zawiera dane dotyczące w szczególności:

1) numeru wpisu;
2) nazwy obszaru, obiektu lub urządzenia;
3) adresu obszaru, obiektu lub urządzenia;
4) nazwy stanowiska kierownika jednostki, która zarządza obszarem, obiektem lub urządzeniem;
5) organu, o którym mowa w ust. 3 , właściwego w stosunku do obszaru, obiektu lub urządzenia.",

f) dodaje się ust. 7 i 8 w brzmieniu:

„7. Wojewoda, po otrzymaniu wykazów lub ich aktualizacji od podmiotów, o których mowa w ust. 3, niezwłocznie aktualizuje ewidencję, o której mowa w ust. 5.

8. Wojewoda, niezwłocznie po umieszczeniu obszaru, obiektu lub urządzenia w ewidencji, o której mowa w ust. 5, informuje o tym kierownika jednostki, który bezpośrednio zarządza obszarami, obiektami i urządzeniami umieszczonymi w ewidencji oraz odpowiednio podmioty, o których mowa w ust. 3 , a także właściwego terytorialnie komendanta wojewódzkiego Policji oraz właściwego terytorialnie dyrektora delegatury Agencji Bezpieczeństwa Wewnętrznego.”;

2) po art. 5 dodaje się art. 5a w brzmieniu:

„Art. 5a. Środki ochrony fizycznej oraz zabezpieczenia techniczne wykraczające poza granice obiektu lub urządzenia podlegającego obowiązkowej ochronie mogą być stosowane od strony wody w odniesieniu do:

1) obiektów, o których mowa w art. 5 ust. 1, będących jednocześnie obiektami portowymi w rozumieniu ustawy z 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2024 r. poz. 597);
2) sztucznych wysp, konstrukcji i urządzeń w obszarach morskich Rzeczypospolitej Polskiej, o których mowa w art. 23 ust. 1 ustawy z dnia

21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej;

3) kabli i rurociągów układanych i utrzymywanych w obszarach morskich Rzeczypospolitej Polskiej, o których mowa w art. 26 ust. 1 ustawy z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej.”;

3) w art. 26 w ust. 1 w pkt 5 dodaje się lit. c w brzmieniu:

"c) w art. 36 ust. 1a-1c;";

4) w art. 36:

a) w ust. 1 w pkt 4 wprowadzenie do wyliczenia i lit. a otrzymują brzmienie:

„użycia lub wykorzystania środków przymusu bezpośredniego, o których mowa w art. 12 ust. 1 pkt 1 lit. a, b i d, pkt 2 lit. a, pkt 5, 7, 9, 11, pkt 12 lit. a oraz pkt 13 i 21-23 ustawy z 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2024 r. poz. 383 i 1248):

a) w granicach chronionych obiektów i obszarów − w przypadkach, o których mowa w art. 11 pkt 2, 5, 8, 10, 13,15-17 tej ustawy,”,

b) po ust. 1 dodaje się ust. 1b–1d w brzmieniu:

„1b. Pracownik ochrony przy wykonywaniu zadań ochrony obiektów, o których mowa w art. 5a pkt 1, w celu zabezpieczenia infrastruktury portowej przed uszkodzeniem, może patrolować ten obiekt jednostką pływającą od strony wody.

1c. Wykonując czynności, o których mowa w ust. 1b, pracownik ochrony ma prawo do wezwania osób przebywających w basenie portowym, a niemających do tego uprawnień, do jego opuszczenia, a także do podjęcia interwencji wobec tych osób, w tym ujęcia ich oraz użycia środków przymusu bezpośredniego określonych w art. 12 ust. 1 pkt 1 lit. a, b i d, pkt 2 lit. a, pkt 11, 13 i 21-23 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej w przypadkach, o których mowa w art. 11 pkt 2, 5, 8, 10,13 i 15-17 tej ustawy.

1d. Środki przymusu bezpośredniego, o których mowa w art. 12 ust. 1 pkt 11 ustawy z 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, mogą być wykorzystane wyłącznie w przypadkach, o których mowa w art. 11 pkt 15 tej ustawy.”;

5) w art. 47 w ust. 2 wstęp do wyliczenia otrzymuje brzmienie:

"2. Współpracę, o której mowa w ust. 1, specjalistyczne uzbrojone formacje ochronne podejmują odpowiednio z właściwymi terytorialnie:";

6) po art. 50b dodaje się art. 50c w brzmieniu:

"Art. 50c. 1.Kto nie będąc do tego uprawnionym, przebywa na obszarze lub obiekcie podlegającym obowiązkowej ochronie oraz takiego obszaru lub obiektu wbrew żądaniu osoby uprawnionej nie opuszcza, podlega grzywnie, karze ograniczenia wolności albo karze pozbawienia wolności do lat 2.

2. Kto nie będąc do tego uprawnionym, przebywając na obszarze lub obiekcie podlegającym obowiązkowej ochronie, utrudnia lub uniemożliwia korzystanie z tych obszarów, obiektów lub znajdujących się na ich terenie urządzeń lub instalacji, podlega grzywnie, karze ograniczenia wolności albo karze pozbawienia wolności do lat 5.".

Art. 7. W ustawie z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. z 2023 r. poz. 1266, 1860 oraz z 2024 r. poz. 1222 i 1248) wprowadza się następujące zmiany:

1) w art. 42 ust. 1 i 2 otrzymują brzmienie:

„Art. 42. 1. W przypadkach, o których mowa w art. 11 pkt 1−6 i 8−16 ustawy z 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, żołnierze Żandarmerii Wojskowej mogą użyć środków przymusu bezpośredniego, o których mowa w art. 12 ust. 1 pkt 1−9, pkt 11, pkt 12 lit. a, c i d, pkt 13-14 i 17−23 tej ustawy, lub wykorzystać te środki.

2. W przypadkach, o których mowa w art. 45 pkt 1 lit. a-c i e, pkt 2-3 i pkt 4 lit. a i b oraz w art. 47 pkt 1-3 i 5-8 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, żołnierze Żandarmerii Wojskowej mogą użyć broni palnej lub ją wykorzystać.”;

2) w art. 51 ust. 2 i 3 otrzymują brzmienie:

"2. W przypadkach, o których mowa w art. 11 pkt 1-6 i 8-14 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, żołnierze wojskowych organów porządkowych wchodzących w skład służby garnizonowej i służby wewnętrznej jednostki wojskowej w związku z wykonywaniem czynności służbowych mogą użyć środków przymusu bezpośredniego, o których mowa w art. 12 ust. 1 pkt 1-5, 7-9, 11, pkt 12 lit. a, c i d, pkt 13, 17, 19-23 tej ustawy, lub wykorzystać te środki.

3. W przypadkach, o których mowa w art. 45 pkt 1 lit. a-c i e, pkt 2, 3, pkt 4 lit. a i b oraz w art. 47 pkt 1-3, 5-8 ustawy z dnia 24 maja 2013 r. o środkach przymusu

bezpośredniego i broni palnej, żołnierze wojskowych organów porządkowych wchodzących w skład służby garnizonowej i służby wewnętrznej jednostki wojskowej w związku z wykonywaniem czynności służbowych mogą użyć broni palnej lub ją wykorzystać.”.

Art. 8. W ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2024 r. poz. 812, 1222 i 1562) wprowadza się następujące zmiany:

1) w art. 5 w ust. 1 pkt 2a otrzymuje brzmienie:

„2a) rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych objętych wykazem, o którym mowa w art. 6r ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122 oraz z 2024 r. poz. 834, 1222 i 1473), a także systemów teleinformatycznych operatorów infrastruktury krytycznej, o których mowa w art. 3 pkt 3a tej ustawy;”;

2) w art. 32a ust. 1 otrzymuje brzmienie:

„1. W celu zapobiegania, przeciwdziałania i zwalczania zdarzeń o charakterze terrorystycznym lub uprawdopodabniających popełnienie przestępstwa szpiegostwa, dotyczących istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub sieci teleinformatycznych objętych wykazem, o którym mowa w art. 6r ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, a także systemów teleinformatycznych operatorów infrastruktury krytycznej, o których mowa w art. 3 pkt 3a tej ustawy, lub danych przetwarzanych w tych systemach oraz rozpoznawania, zapobiegania i wykrywania przestępstw o charakterze terrorystycznym w lub przestępstwa szpiegostwa w tym obszarze oraz ścigania ich sprawców, ABW może przeprowadzać ocenę bezpieczeństwa tych systemów teleinformatycznych, zwaną dalej „oceną bezpieczeństwa”.”;

3) w art. 32aa ust. 1 otrzymuje brzmienie:

„1. W celu zapobiegania, przeciwdziałania i zwalczania zdarzeń o charakterze terrorystycznym lub uprawdopodabniających popełnienie przestępstwa szpiegostwa, dotyczących istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub sieci teleinformatycznych objętych wykazem, o których mowa w art. 6r ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, a także systemów teleinformatycznych operatorów

infrastruktury krytycznej, o których mowa w art. 3 pkt 3a tej ustawy, lub danych przetwarzanych w tych systemach oraz rozpoznawania, zapobiegania i wykrywania przestępstw o charakterze terrorystycznym lub przestępstwa szpiegostwa w tym obszarze oraz ścigania ich sprawców, ABW wdraża w tych podmiotach system wczesnego ostrzegania o zagrożeniach występujących w sieci Internet, zwany dalej „systemem ostrzegania", prowadzi go i koordynuje jego funkcjonowanie.".

Art. 9. W ustawie z dnia 28 marca 2003 r. o transporcie kolejowym (Dz. U. z 2024 r. poz. 697 i 731) dodaje się art. 29g w brzmieniu:

"Art. 29g. 1. W sytuacji kryzysowej, jeżeli wymagają tego potrzeby obronności lub istotny interes bezpieczeństwa państwa, właściwy miejscowo wojewoda może, w drodze rozporządzenia porządkowego, po zasięgnięciu opinii zarządcy infrastruktury kolejowej, wprowadzić czasowe ograniczenia w dostępie do infrastruktury kolejowej, w tym całkowicie wyłączyć dostęp do infrastruktury kolejowej.

2. Rozporządzenie porządkowe w zakresie, o którym mowa w ust. 1 określa:

1) linie kolejowe, opisane zgodnie z wykazem linii kolejowych zawartym w regulaminie sieci, wraz ze wskazaniem kilometraża odcinków linii kolejowych, na których wprowadzono czasowe ograniczenia w dostępie do infrastruktury kolejowej, w tym całkowicie wyłączono dostęp do infrastruktury kolejowej;
2) rodzaj ograniczenia w dostępie do infrastruktury kolejowej, w tym wskazuje przewozy priorytetowe lub ładunki z pierwszeństwem dostępu do infrastruktury kolejowej oraz przejazdu;
3) okres, na który wprowadzono ograniczenia w dostępie do infrastruktury kolejowej, w tym całkowicie wyłączono dostęp do infrastruktury kolejowej;
4) koordynatora przewozów priorytetowych lub ładunków z pierwszeństwem dostępu do infrastruktury kolejowej oraz przejazdu na liniach kolejowych, o których mowa w pkt 1.

3. Rozporządzenie porządkowe, o którym mowa w ust. 1, może być publikowane w drodze obwieszczenia lub za pomocą środków komunikacji elektronicznej, lub w inny sposób zwyczajowo przyjęty na danym terenie. Dzień takiego opublikowania jest dniem ogłoszenia.

4. Operatorzy obiektów infrastruktury usługowej zapewniają pierwszeństwo w obsłudze przewozom priorytetowym lub ładunkom z pierwszeństwem dostępu do

infrastruktury kolejowej oraz przejazdu, w zakresie wskazanym przez koordynatora, o którym mowa w ust. 2 pkt 4.

5. Jeżeli w opinii, o której mowa w ust. 1, zarządca infrastruktury kolejowej wskazuje na konieczność wprowadzenia czasowego ograniczenia w dostępie do infrastruktury kolejowej, w tym całkowitego wyłączenia dostępu do infrastruktury kolejowej zlokalizowanej poza obszarem właściwości wojewody wydającego rozporządzenie porządkowe, wojewoda przekazuje tę opinię pozostałym właściwym miejscowo wojewodom.".

Art. 10. W ustawie z dnia 11 marca 2004 r. o ochronie zdrowia zwierząt oraz zwalczaniu chorób zakaźnych zwierząt (Dz. U. z 2023 r. poz. 1075) dodaje się art. 47d-47g w brzmieniu:

"Art. 47d. 1. W przypadku nakazu odstrzału, o którym mowa w art. 46 ust. 3 pkt 8 ustawy, jeżeli jest to niezbędne ze względu na rodzaj i skalę zagrożenia, minister właściwy do spraw wewnętrznych, na wniosek wojewody, może przekazać do jego dyspozycji doraźne zgrupowanie zadaniowe sformowane z policjantów, funkcjonariuszy Straży Granicznej lub funkcjonariuszy Państwowej Straży Pożarnej, którzy posiadają uprawnienia do wykonywania polowania, celem ich użycia do odstrzału sanitarnego zwierząt wolno żyjących (dzikich) na określonych obszarach.

2. Dowodzenie doraźnymi zgrupowaniami zadaniowymi, o których mowa w ust. 1, powierzane jest odpowiednio policjantowi, funkcjonariuszowi Straży Granicznej lub funkcjonariuszowi Państwowej Straży Pożarnej wskazanemu przez właściwego miejscowo komendanta odpowiednio Policji, Straży Granicznej lub Państwowej Straży Pożarnej, a w przypadku stworzenia doraźnego zgrupowania zadaniowego złożonego z policjantów, funkcjonariuszy Straży Granicznej lub funkcjonariuszy Państwowej Straży Pożarnej – policjantowi wskazanemu przez właściwego miejscowo komendanta Policji.

Art. 47e. 1. Jeżeli w sytuacji kryzysowej użycie innych sił i środków jest niemożliwe lub może okazać się niewystarczające, Minister Obrony Narodowej, na wniosek wojewody, może przekazać do jego dyspozycji doraźne zgrupowanie zadaniowe sformowane z żołnierzy, którzy posiadają uprawnienia do wykonywania polowania, celem użycia ich do odstrzału, o którym mowa w art. 46 ust. 3 pkt 8 ustawy z dnia 11 marca 2004 r. o ochronie zdrowia zwierząt oraz zwalczaniu chorób zakaźnych zwierząt, zwierząt wolno żyjących (dzikich) na określonych obszarach.

2. Dowodzenie doraźnymi zgrupowaniami zadaniowymi, o których mowa w ust. 1, odbywa się na zasadach określonych w regulaminach wojskowych i według procedur obowiązujących w Siłach Zbrojnych Rzeczypospolitej Polskiej.

3. Użycie doraźnych zgrupowań zadaniowych w sytuacji kryzysowej nie może zagrozić zdolności Sił Zbrojnych do realizacji zadań wynikających z Konstytucji Rzeczypospolitej Polskiej i ratyfikowanych umów międzynarodowych.

Art. 47f. 1. W przypadkach, o których mowa w art. 47d i art. 47e, odpowiednio policjanci, funkcjonariusze Straży Granicznej, funkcjonariusze Państwowej Straży Pożarnej i żołnierze używają broni myśliwskiej prywatnej lub użyczonej zgodnie z przepisami ustawy z dnia 21 maja 1999 r. o broni i amunicji (Dz. U. z 2024 r. poz. 485).

2. Odpowiedzialność za szkody wyrządzone przez policjantów, funkcjonariuszy Straży Granicznej, funkcjonariuszy Państwowej Straży Pożarnej i żołnierzy realizujących zadania, o których mowa w ust. 1, ponosi wojewoda.

3. W przypadkach, o których mowa w art. 47d i art. 47e:

1) nie stosuje się przepisów ustawy dotyczących ryczałtu;
2) policjanci, funkcjonariusze Straży Granicznej, funkcjonariusze Państwowej Straży Pożarnej i żołnierze współpracują z zarządcą lub dzierżawcą obwodu łowieckiego.

Art. 47g. W przypadkach, o których mowa w art. 47d i art. 47e, do obowiązków wojewody należy:

1) zapewnienie amunicji do broni, o której mowa w art. 47f ust. 1;
2) zwrot kosztów transportu, zakwaterowania i wyżywienia doraźnych zgrupowań zadaniowych; zwrot kosztów zakwaterowania lub wyżywienia nie przysługuje w przypadku zapewnienia w miejscu wykonywania czynności bezpłatnego zakwaterowania lub wyżywienia.

Art. 11. W ustawie z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2024 r. poz. 597) wprowadza się następujące zmiany:

1) w art. 1 w ust. 3 w pkt 4 kropkę zastępuje się średnikiem i dodaje się punkt 5 w brzmieniu: „5) terminalu morskiego przeładunku ropy i paliw ciekłych w Gdańsku.";
2) w art. 24 ust. 5 otrzymuje brzmienie:

„5. W przypadku wprowadzenia poziomu ochrony 3 stosuje się odpowiednio art. 21 i art. 25 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U z 2023 r. poz. 122 oraz z 2024 r. poz. 834, 1222 i 1473).”;

3) po art. 25 dodaje się art. 25a-25d w brzmieniu:

„Art. 25a. 1 W celu zapewnienia wsparcia wymiany informacji pomiędzy organami lub podmiotami realizującymi zadania w zakresie zapobiegania, ograniczania lub usuwania poważnego niebezpieczeństwa grożącego:

1) obiektom portowym i portom morskim oraz związanej z nimi infrastrukturze;
2) obiektom, urządzeniom i instalacjom wchodzącym w skład infrastruktury zapewniającej dostęp do portów o podstawowym znaczeniu dla gospodarki narodowej;
3) zlokalizowanym na terenie polskich obszarów morskich obiektom, urządzeniom i instalacjom wchodzącym w skład infrastruktury służącej do:
   a) wytwarzania lub przesyłania źródeł energii lub surowców energetycznych, w tym morskim farmom wiatrowym w rozumieniu art. 3 pkt 3 ustawy o promowaniu i zespołom urządzeń służącym do wyprowadzenia mocy w rozumieniu art. 3 pkt 13 ustawy o promowaniu, oraz podmorskim sieciom elektroenergetycznym i światłowodowym lub rurociągom, a także związanej z nimi infrastrukturze,
   b) telekomunikacji w rozumieniu ustawy z dnia 12 lipca 2024 r. Prawo komunikacji elektronicznej (Dz. U. poz. 1221),
4) wykorzystywanym w wyłącznej strefie ekonomicznej sztucznym wyspom, konstrukcjom i urządzeniom przeznaczonym do gospodarczego badania i eksploatacji zasobów wyłącznej strefy ekonomicznej

- zwanych dalej „infrastrukturą morską” oraz statkom, a także zadania w zakresie ochrony granicy państwa na morzu oraz ochrony życia lub zdrowia ludzi, mienia w znacznych rozmiarach lub środowiska zlokalizowanych na polskich obszarów morskich w rozumieniu ustawy z dnia 21 marca 19912 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej, tworzy się Centrum Bezpieczeństwa Morskiego, zwane dalej „CBM”.

2. Funkcję CBM pełni komórka organizacyjna Straży Granicznej utworzona przez Komendanta Głównego Straży Granicznej w wybranym oddziale Straży Granicznej.

3. CBM kieruje wyznaczony przez Komendanta Głównego Straży Granicznej komendant oddziału Straży Granicznej lub jego zastępca, zwany dalej „Szefem CBM”.

4. Do zadań CBM należy:

1) bieżące monitorowanie zagrożeń,
2) wspieranie wymiany informacji pomiędzy organami lub podmiotami, o których mowa w art. 25b ust. 1,

3) wspieranie współpracy z właściwymi organami innych państw,
4) wspieranie procesu decyzyjnego właściwych organów lub podmiotów oraz podejmowanych przez nich działań,
5) opracowywanie raportów dotyczących zagrożeń

- w odniesieniu do żeglugi, infrastruktury morskiej, statków, granicy państwa na morzu, życia lub zdrowia ludzi, mienia w znacznych rozmiarach lub ochrony środowiska na polskich obszarach morskich

5. CBM realizuje zadania w systemie całodobowym przez 7 dni w tygodniu.

6. Realizację zadań CBM zapewnia komendant oddziału Straży Granicznej właściwego ze względu na umiejscowienie CBM.

Art. 25b. 1. W celu realizacji zadań, o których mowa w art. 25a ust. 4, na wniosek Komendanta Głównego Straży Granicznej, Minister Obrony Narodowej, Szef Służby Kontrwywiadu Wojskowego, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Agencji Wywiadu, Komendant Główny Policji, Komendant Główny Państwowej Straży Pożarnej, Dyrektor Morskiej Służby Poszukiwania i Ratownictwa (Służby SAR), dyrektorzy urzędów morskich, wojewodowie oraz operatorzy infrastruktury krytycznej mogą oddelegować swoich przedstawicieli do Straży Granicznej do wykonywania zadań CBM na zasadach określonych w porozumieniu zawartym między każdym z nich a Komendantem Głównym Straży Granicznej.

2. Wniosek, o którym mowa w ust. 1, zwany dalej „wnioskiem” zawiera:
1) zakres wykonywanych zadań oraz kwalifikacje, uprawnienia lub umiejętności wymagane do ich wykonywania;
2) wymagania w zakresie posiadania poświadczenia bezpieczeństwa upoważniającego do dostępu do informacji niejawnych i okresu jego ważności;
3) proponowany czas pracy albo służby, z uwzględnieniem możliwości wykonywania pracy albo pełnienia służby w systemie zmianowym;
4) proponowany okres oddelegowania;
5) planowany dzień rozpoczęcia oddelegowania;
6) liczbę godzin pracy albo służby na stanowiskach wyposażonych w monitory ekranowe;
7) proponowane stanowisko pracy lub stanowisko służbowe dla oddelegowanego.

3. Wniosek może zawierać imię i nazwisko oddelegowanego.

4. Komendant Główny Straży Granicznej występuje z wnioskiem do właściwego organu lub podmiotu oddelegowującego, o którym mowa w ust. 1, nie później niż 14 dni od planowanego dnia rozpoczęcia oddelegowania .

5. Organ lub podmiot, o którym mowa w ust. 1, w terminie 7 dni od dnia otrzymania wniosku, zawiadamia Komendanta Głównego Straży Granicznej o decyzji w sprawie oddelegowania i w przypadku uwzględnienia tego wniosku, w terminie kolejnych 7 dni wyznacza oddelegowanego.

6. Porozumienie, o którym mowa w ust. 1, zawiera w szczególności:

1) datę porozumienia;
2) okres oddelegowania;
3) imię i nazwisko oddelegowanego;
4) stopień oddelegowanego, w przypadku gdy jest on funkcjonariuszem albo żołnierzem;
5) numer poświadczenia bezpieczeństwa wydanego oddelegowanemu, datę jego wydania i wystawcę takiego poświadczenia oraz okres ważności i oznaczenie klauzuli upoważniających do przetwarzania informacji niejawnych;
6) zakres zadań i obowiązków oddelegowanego oraz sposób organizacji wykonywania tych zadań i obowiązków;
7) rozkład czasu pracy albo służby oddelegowanego.

7. Komendant Główny Straży Granicznej, zgodnie z porozumieniem, o którym mowa w ust. 1, wyznacza oddelegowanemu w formie pisemnej, w postaci papierowej lub elektronicznej:

1) zadania, które będzie wykonywał w CBM;
2) osobę odpowiedzialną za organizację wykonywanych przez niego zadań i rozliczanie go z nich;
3) rozkład jego czasu pracy albo służby.

8. Podmiot oddelegowujący odwołuje swojego oddelegowanego do Straży Granicznej do wykonywania zadań CBM przed upływem terminu oddelegowania, na wniosek Komendanta Głównego Straży Granicznej albo z własnej inicjatywy, po uprzednim zawiadomieniu Komendanta Głównego Straży Granicznej o planowanym terminie odwołania oddelegowanego.

9. W przypadku odwołania z własnej inicjatywy, kierownik podmiotu oddelegowującego, o którym mowa w ust. 1, niezwłocznie wskazuje kolejnego

oddelegowanego w celu zapewnienia ciągłości wykonywania pracy lub pełnienia służby. Przepisy ust 2 - 8 i ust. 10 stosuje się odpowiednio.

10. W okresie oddelegowania podmiot oddelegowujący wypłaca przedstawicielowi oddelegowanemu do Straży Granicznej do wykonywania zadań w CBM uposażenie albo wynagrodzenie i inne świadczenia oraz należności pieniężne.

Art. 25c. 1. W szczególnie uzasadnionych przypadkach związanych z zagrożeniem wystąpienia poważnego niebezpieczeństwa, Szef CBM powołuje sztab koordynacyjny, w skład którego wchodzą przedstawiciele wyznaczeni przez organy lub podmioty, o których mowa w art. 25b ust. 1.

2. Do zadań sztabu koordynacyjnego należy dokonywanie aktualnej oceny stopnia zagrożenia infrastruktury morskiej, statków lub granicy państwa na morzu oraz wydawania rekomendacji zmierzających do odpowiedniego zabezpieczenia tej infrastruktury, statków lub granicy.

Art. 25d. Komendant Główny Straży Granicznej, w terminie do dnia 31 marca każdego roku kalendarzowego, przedstawia ministrowi właściwemu do spraw wewnętrznych sprawozdanie z działania CBM w poprzednim roku kalendarzowym.”.

4) w art. 27 w ust. 1 po pkt 5 dodaje się pkt 6 w brzmieniu:

"6) terminalowi morskiego przeładunku ropy i paliw ciekłych w Gdańsku";

5) po rozdziale 6 dodaje się rozdział 6a w brzmieniu:

„Rozdział 6a

Zapobieganie bezprawnemu wykonywaniu operacji z użyciem bezzałogowych obiektów pływających

Art. 28a. 1. Bezzałogowy obiekt pływający może zostać zniszczony, unieruchomiony albo może nad nim zostać przejęta kontrola, w przypadku gdy:

1) przebieg operacji lub działanie bezzałogowego obiektu pływającego:
   a) zagraża lub może zagrozić życiu lub zdrowiu ludzi lub zwierząt,
   b) stwarza lub może stworzyć zagrożenie dla chronionych obiektów, urządzeń lub obszarów,
   c) stwarza lub może stworzyć uzasadnione podejrzenie, że może zostać użyty jako środek ataku terrorystycznego,
   d) stwarza lub może stworzyć zagrożenie bezpieczeństwa jednostki pływającej lub życia lub zdrowia załogi lub pasażerów znajdujących się na jej pokładzie,

e) utrudnia lub może utrudnić ruch w portach morskich lub powoduje lub może spowodować jego wstrzymanie lub ograniczenie;

2) bezzałogowy obiekt pływający wbrew zakazowi wykonuje operację w polskich obszarach morskich.

2. Do zniszczenia, unieruchomienia bezzałogowego obiektu pływającego albo przejęcia nad nim kontroli, w związku z realizacją zadań ustawowych, są uprawnieni na zasadach określonych w ustawie z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2024 r. poz. 383 i 1248) funkcjonariusze Policji, Straży Granicznej, Służby Ochrony Państwa oraz, zgodnie z zakresem właściwości miejscowej, pracownicy ochrony specjalistycznych uzbrojonych formacji ochronnych, , o których mowa w art. 2 pkt 7 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2021 r. poz. 1995).

3. Do zniszczenia, unieruchomienia bezzałogowego obiektu pływającego albo przejęcia nad nim kontroli, w związku z realizacją zadań ustawowych, na terenie chronionych obiektów Sił Zbrojnych Rzeczypospolitej Polskiej oraz jednostek organizacyjnych podległych, podporządkowanych lub nadzorowanych przez Ministra Obrony Narodowej są uprawnieni na zasadach określonych w ustawie z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej żołnierze Żandarmerii Wojskowej oraz Sił Zbrojnych Rzeczypospolitej Polskiej.

4. Za szkody powstałe w wyniku zniszczenia, unieruchomienia albo przejęcia kontroli nad bezzałogowym obiektem pływającym w przypadkach, o których mowa w ust. 1, odpowiada właściciel lub operator lub armator bezzałogowego obiektu pływającego zniszczonego, unieruchomionego albo nad którym przejęto kontrolę.”.

Art. 12. W ustawie 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) wprowadza się następujące zmiany:

1) w art. 1 ust. 1 otrzymuje brzmienie:

„1. Ustawa określa szczególne uprawnienia przysługujące ministrowi właściwemu do spraw aktywów państwowych w spółkach kapitałowych lub grupach kapitałowych, w rozumieniu art. 3 ust. 1 pkt 44 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120, 295 i 1598 oraz z 2024 r. poz. 619), prowadzących działalność

w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych, których mienie zostało ujawnione w wykazie, o którym mowa w art. 6r ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122 oraz z 2024 r. poz. 834, 1222 i 1473), zwanych dalej „spółkami”.”;

2) w art. 2:

a) ust. 3 otrzymuje brzmienie:

„3. Sprzeciw jest wyrażany w formie decyzji administracyjnej, w terminie 45 dni od dnia otrzymania przez ministra właściwego do spraw aktywów państwowych od pełnomocnika do spraw ochrony infrastruktury krytycznej, o którym mowa w art. 5, informacji o podjęciu przez organy spółki uchwały lub dokonaniu przez zarząd spółki czynności prawnej, o której mowa w ust. 1 i 2, jednak nie później niż w terminie 60 dni od dnia ich dokonania.",

b) po ust. 3 dodaje się ust. 3a w brzmieniu:

"3a. Sprzeciw jest wyrażany po zasięgnięciu opinii odpowiednio ministra właściwego do spraw energii lub ministra właściwego do spraw gospodarki surowcami energetycznymi. Opinię wydaje się w terminie 10 dni od dnia otrzymania wniosku o jej wydanie. Niewyrażenie opinii w tym terminie uważa się za brak uwag.”,

c) ust. 5 otrzymuje brzmienie:

„5. W przypadku złożenia wniosku o ponowne rozpatrzenie sprawy termin na jej załatwienie wynosi 30 dni od dnia otrzymania wniosku.”,

d) w ust. 6 pkt 1 otrzymuje brzmienie:

„1) minister właściwy do spraw aktywów państwowych przekazuje skargę do właściwego sądu administracyjnego wraz z aktami sprawy i odpowiedzią na skargę w terminie 30 dni od dnia jej wniesienia przez stronę;”,

e) ust. 8 otrzymuje brzmienie:

„8. W sprawach nieuregulowanych w ust. 1-7 do postępowania w sprawie sprzeciwu stosuje się przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2024 r. poz. 572).",

3) w art. 4 ust. 2 otrzymuje brzmienie:

„2. Minister właściwy do spraw aktywów państwowych, po otrzymaniu od dyrektora Rządowego Centrum Bezpieczeństwa informacji o ujęciu spółki w wykazie lub wyciągu,

o którym mowa w ust. 1, powiadamia spółkę o ujęciu w wykazie składników jej mienia, o których mowa w art. 1 ust. 1 i 2.”;

4) w art. 5 wprowadza się następujące zmiany:

a) ust. 1

„1. Zarząd spółki, w porozumieniu z ministrem właściwym do spraw aktywów państwowych oraz dyrektorem Rządowego Centrum Bezpieczeństwa, powołuje i odwołuje pełnomocnika do spraw ochrony infrastruktury krytycznej oraz jego zastępcę, przy czym powołanie pełnomocnika następuje w terminie 30 dni, a powołanie jego zastępcy w terminie 60 dni od dnia otrzymania powiadomienia, o którym mowa w art. 4 ust. 2.",

b) po ust. 1 dodaje się ust. 1a w brzmienie:

„1a. Minister właściwy do spraw aktywów państwowych niezwłocznie informuje odpowiednio ministra właściwego do spraw energii lub ministra właściwego do spraw gospodarki surowcami energetycznymi o powołaniu lub odwołaniu pełnomocnika do spraw infrastruktury krytycznej oraz jego zastępcy.”,

c) ust. 4 otrzymuje brzmienie:

„4. Pełnomocnik do spraw ochrony infrastruktury krytycznej może jednocześnie pełnić funkcję koordynatora ochrony infrastruktury krytycznej lub pełnomocnika bezpieczeństwa usługi kluczowej, o których mowa odpowiednio w art. 6zi ust. 1 i art. 6zzd ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.",

d) po ust. 5 dodaje się ust. 6 w brzmieniu:

„6. Do zastępcy pełnomocnika postanowienia art. 5 ust. 2-5 stosuje się odpowiednio.”,

5) art. 6 wprowadza się następujące zmiany:

a) ust. 1 otrzymuje brzmienie:

„1. Zarząd spółki zobowiązany jest do przekazywania pełnomocnikowi do spraw ochrony infrastruktury krytycznej lub jego zastępcy, dokumentów lub informacji o podjęciu uchwały lub o dokonaniu przez organy spółki czynności prawnych, o których mowa w art. 2 ust. 1 i 2, w terminie 3 dni od dnia ich podjęcia lub dokonania.",

b) ust. 2 otrzymuje brzmienie:

"2. Zarząd spółki powiadamia pełnomocnika do spraw ochrony infrastruktury krytycznej lub jego zastępcę o każdym planowanym posiedzeniu dotyczącym spraw, o których mowa w art. 2 ust. 1 i 2.",

c) w ust. 3 wstęp do wyliczenia otrzymuje brzmienie:

„3. Pełnomocnik do spraw ochrony infrastruktury krytycznej albo jego zastępca, sporządza dla zarządu spółki oraz rady nadzorczej raport doraźny, okresowy, raport półroczny i roczny o stanie ochrony infrastruktury krytycznej. Raport doraźny sporządzany jest w terminie 1 dnia od zidentyfikowania zagrożenia lub wystąpienia sytuacji stwarzającej zagrożenie dla funkcjonowania, ciągłości działania oraz integralności infrastruktury krytycznej. Raport okresowy jest sporządzany, co kwartał lub na żądanie zarządu spółki lub rady nadzorczej. Raport powinien zawierać informacje dotyczące ochrony infrastruktury krytycznej w zakresie:”,

d) po ust. 3 dodaje się ust. 3a w brzmieniu:

"3a. Raport roczny i półroczny zawiera informację, o których mowa w ust. 3, poszerzone o:

1) rejestr stwierdzonych incydentów wraz z informacją o przeprowadzonych działaniach korygujących;
2) informację o przeprowadzonych kontrolach i audytach dotyczących ochrony infrastruktury krytycznej;
3) informację o posiadanych certyfikatach systemów i rozwiązań dotyczących ochrony infrastruktury krytycznej;",

e) ust. 4 otrzymuje brzmienie:

„4. Raport doraźny oraz raport półroczny i roczny są przekazywane ministrowi właściwemu do spraw aktywów państwowych, dyrektorowi Rządowego Centrum Bezpieczeństwa oraz odpowiednio ministrowi właściwemu do spraw energii lub ministrowi właściwemu do spraw gospodarki surowcami energetycznymi. Jeżeli raporty są niepełne, zawierają nieścisłości lub nie przedstawiają dokładnie stanu faktycznego w zakresie spraw w nim zawartych, pełnomocnik do spraw ochrony infrastruktury krytycznej lub jego zastępca jest zobowiązany, na wezwanie ministra właściwego do spraw aktywów państwowych lub dyrektora Rządowego Centrum Bezpieczeństwa, lub odpowiednio ministra właściwego do spraw energii lub ministra

właściwego do spraw gospodarki surowcami energetycznymi, do uzupełnienia raportów we wskazanym zakresie i terminie.”,

f) ust. 5 otrzymuje brzmienie:

„5. Pełnomocnik do spraw ochrony infrastruktury krytycznej lub w razie jego nieobecności jego zastępca, sporządza sprawozdania półroczne i roczne z wykonanych obowiązków, które składa ministrowi właściwemu do spraw aktywów państwowych, dyrektorowi Rządowego Centrum Bezpieczeństwa oraz odpowiednio ministrowi właściwemu do spraw energii lub ministrowi właściwemu do spraw gospodarki surowcami energetycznymi.”,

g) ust. 6 otrzymuje brzmienie:

„6. Pełnomocnik do spraw ochrony infrastruktury krytycznej lub w razie jego nieobecności jego zastępca, w terminie 4 dni od dnia otrzymania dokumentów lub informacji o podjęciu uchwały lub o dokonaniu przez organy spółki czynności prawnych, o których mowa w art. 2 ust. 1 i 2, przekazuje ministrowi właściwemu do spraw aktywów państwowych, dyrektorowi Rządowego Centrum Bezpieczeństwa oraz odpowiednio ministrowi właściwemu do spraw energii lub ministrowi właściwemu do spraw gospodarki surowcami energetycznymi pisemną informację w tej sprawie oraz stanowisko odnośnie do wniesienia sprzeciwu, wraz z jego uzasadnieniem. Stanowisko powinno zawierać informacje dotyczące faktów i okoliczności podjętych przez spółkę czynności prawnych, o których mowa w art. 2 ust. 1 i 2 wraz ze wskazaniem motywów podejmowanych działań i tła historycznego”,

h) ust. 8 otrzymuje brzmienie:

"8. Prezes Rady Ministrów określi, w drodze rozporządzenia, szczegółowy tryb powoływania i odwoływania pełnomocnika do spraw ochrony infrastruktury krytycznej oraz jego zastępcy, sposób wykonywania obowiązku monitorowania działalności spółki w zakresie, o którym mowa w art. 2 ust. 1 i 2, uwzględniając konieczność efektywnego wykonywania szczególnych uprawnień ministra właściwego do spraw aktywów państwowych w spółkach kapitałowych lub grupach kapitałowych.";

6) po art. 7 dodaje się art. 7a w brzmieniu:

„Art. 7a. 1. Zarząd spółki za nierealizowanie obowiązków wskazanych w ustawie może podlegać karze pieniężnej.

1) za nierealizowanie zadań, o których mowa w art. 5 ust. 1 – do 50 000 zł;

2) za nierealizowanie zadań, o których mowa w art. 6 ust. 1 – do 100 000 zł;

3) za nierealizowanie zadań, o których mowa w art. 6 ust. 2 – do 50 000 zł.

2. Jeżeli zarząd spółki uporczywie narusza przepisy ustawy, może podlegać karze w wysokości do 1 000 000 zł.

3. Kary pieniężne nakłada w drodze decyzji minister właściwy do spraw aktywów państwowych.

4. W przypadku nierealizowania przez pełnomocnika do spraw ochrony infrastruktury krytycznej, lub jego zastępcę, obowiązków wskazanych w art. 5 ust. 2 ustawy, minister właściwy do spraw aktywów państwowych może uznać, że pełnomocnik przestał dawać rękojmię prawidłowego wykonywania obowiązków, o czym powiadamia zarząd spółki.

5. Zarząd spółki w terminie 30 dni od powiadomienia, o którym mowa w art. 7a ust. 4 zobowiązany jest do odwołania pełnomocnika w trybie określonym w art. 5 ust. 1 ustawy.";

Art. 13. W ustawie z dnia 14 grudnia 2012 r. o odpadach (Dz. U. z 2023 r. poz. 1587, 1597, 1688, 1852 i 2029) w art. 25 w ust. 6i pkt 2 otrzymuje brzmienie:

„2) stanowiącego element infrastruktury krytycznej ujętej w wykazie, o którym mowa w art. 6r ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122 oraz z 2024 r. poz. 834, 1222 i 1473);”.

Art. 14. W ustawie z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2024 r. poz. 383) wprowadza się następujące zmiany:

1) w art. 4:

a) w pkt 8 lit. b otrzymuje brzmienie:

„b) obiekty, urządzenia, instalacje, sieci, systemy oraz usługi lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy oraz usługi ujęte w wykazie infrastruktury krytycznej, o którym mowa w art. 6r ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122 oraz z 2024 r. poz. 834, 1222 i 1473),",

b) pkt 9 otrzymuje brzmienie:

„9) wykorzystaniu środka przymusu bezpośredniego – należy przez to rozumieć zastosowanie środka przymusu bezpośredniego:

a) wobec zwierzęcia,

b) w celu zatrzymania, zablokowania lub unieruchomienia pojazdu lub pokonania przeszkody,

c) w przypadku bezzałogowego statku powietrznego – w celu jego zniszczenia, unieruchomienia albo przejęcia kontroli nad jego lotem,

d) w przypadku bezzałogowego obiektu pływającego – w celu jego zniszczenia, unieruchomienia albo przejęcia nad nim kontroli,

e) w przypadku bezzałogowego obiektu lądowego – w celu jego zniszczenia, unieruchomienia albo przejęcia nad nim kontroli;”;

2) w art. 11 w pkt 15 kropkę zastępuje się średnikiem i dodaje się pkt 16 i 17 w brzmieniu:

„16) zniszczenia, unieruchomienia bezzałogowego obiektu pływającego albo przejęcia nad nim kontroli, w przypadkach, o których mowa w art. 28a ust. 1 ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2024 r. poz. 597);

17) zniszczenia, unieruchomienia bezzałogowego obiektu lądowego albo przejęcia nad nim kontroli, w przypadku gdy:

a) zagraża lub może zagrozić życiu lub zdrowiu ludzi lub zwierząt,

b) stwarza lub może stworzyć zagrożenie dla chronionych obiektów, urządzeń lub obszarów,

c) zakłóca lub może zakłócić przebieg zgromadzenia lub imprezy masowej albo zagraża bezpieczeństwu ich uczestników,

d) stwarza lub może stworzyć uzasadnione podejrzenie, że może zostać użyty jako środek ataku o charakterze terrorystycznym.”;

3) w art. 12 w ust. 1 w pkt 21 kropkę zastępuje się średnikiem i dodaje się pkt 22 i 23 w brzmieniu:

„22) środki i urządzenia przeznaczone do zniszczenia, unieruchomienia bezzałogowego obiektu pływającego albo przejęcia nad nim kontroli;

23) środki i urządzenia przeznaczone do zniszczenia, unieruchomienia bezzałogowego obiektu lądowego albo przejęcia nad nim kontroli.”;

4) art. 23 otrzymuje brzmienie:

„Art. 23.1. Pocisków niepenetracyjnych miotanych z broni palnej, broni pneumatycznej lub urządzeń do tego przeznaczonych można użyć lub wykorzystać w przypadkach, o których mowa w art. 11 pkt 2–5, 7–11, 13 i 15–17.

2. W przypadku zbiorowego zakłócenia porządku publicznego użycie pocisków niepenetracyjnych poprzedza się strzałem ostrzegawczym lub salwą ostrzegawczą w bezpiecznym kierunku, z wyjątkiem sytuacji, gdy miałoby to nastąpić w pomieszczeniach, obiektach aresztu śledczego, zakładu karnego, strzeżonego ośrodka lub aresztu dla cudzoziemców.

3. Pocisków niepenetracyjnych używa się w celu obezwładnienia osób lub wykorzystuje się w celu obezwładnienia zwierzęcia przez zadanie bólu fizycznego, przy czym nie celuje się w głowę lub szyję, oraz w celu zniszczenia albo unieruchomienia bezzałogowego statku powietrznego, bezzałogowego obiektu pływającego lub bezzałogowego obiektu lądowego.

4. Można użyć lub wykorzystać także pociski niepenetracyjne zawierające chemiczne środki obezwładniające lub barwiące.”;

5) po art. 33a dodaje się art. 33b i 33c w brzmieniu:

„Art. 33b. 1. Środki i urządzenia przeznaczone do zniszczenia, unieruchomienia bezzałogowego obiektu pływającego albo przejęcia nad nim kontroli można wykorzystać w przypadku, o którym mowa w art. 11 pkt 16.

2. Zniszczenie, unieruchomienie bezzałogowego obiektu pływającego albo przejęcie nad nim kontroli może nastąpić przez wykorzystanie:

1) bezzałogowych statków powietrznych;
2) pocisków niepenetracyjnych lub innych przedmiotów miotanych za pomocą przeznaczonych do tego urządzeń oraz za pomocą broni palnej i broni pneumatycznej;
3) urządzeń emitujących skumulowaną wiązkę energii lub fal elektromagnetycznych;
4) urządzeń zakłócających działanie systemów pozycjonowania obiektu pływającego;
5) urządzeń zakłócających komunikację pomiędzy operatorem a obiektem pływającym;
6) urządzeń technicznych przymocowanych do dna morskiego i służących do ochrony fizycznej;
7) bezzałogowych obiektów pływających.

Art. 33c. 1. Środki i urządzenia przeznaczone do zniszczenia, unieruchomienia bezzałogowego obiektu lądowego albo przejęcia nad nim kontroli można wykorzystać w przypadku, o którym mowa w art. 11 pkt 17.

2. Zniszczenie, unieruchomienie bezzałogowego obiektu lądowego albo przejęcie nad nim kontroli może nastąpić przez wykorzystanie:

1) bezzałogowych statków powietrznych;
2) pocisków niepenetracyjnych lub innych przedmiotów miotanych za pomocą przeznaczonych do tego urządzeń oraz za pomocą broni palnej i broni pneumatycznej;
3) urządzeń emitujących skumulowaną wiązkę energii lub fal elektromagnetycznych;
4) urządzeń zakłócających działanie systemów pozycjonowania obiektu lądowego;
5) urządzeń zakłócających komunikację pomiędzy operatorem a obiektem lądowym;
6) bezzałogowych obiektów lądowych.”;

6) w art. 47 w pkt 7 kropkę zastępuje się średnikiem i dodaje się pkt 8 w brzmieniu:
„8) zniszczenia lub unieruchomienia bezzałogowego obiektu lądowego, w przypadkach, o których mowa w art. 11 pkt 17.”.

Art. 15. W ustawie z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2024 r. poz. 92 i 1248) wprowadza się następujące zmiany:

1) w art. 2 uchyla się pkt 3;
2) art. 4 otrzymuje brzmienie:

„Art. 4. 1. Organy administracji publicznej lub operatorzy infrastruktury krytycznej współpracują z organami, służbami i instytucjami właściwymi w sprawach bezpieczeństwa i zarządzania kryzysowego przy realizacji działań antyterrorystycznych.

2. Organy i podmioty, o których mowa w ust. 1, przekazują niezwłocznie Szefowi ABW będące w ich posiadaniu informacje dotyczące zagrożeń o charakterze terrorystycznym, w tym zagrożeń dla funkcjonowania systemów i sieci energetycznych, wodno-kanalizacyjnych, ciepłowniczych oraz teleinformatycznych istotnych z punktu widzenia bezpieczeństwa państwa.

3. W przypadku powzięcia informacji o możliwości wystąpienia zdarzenia o charakterze terrorystycznym zagrażającego infrastrukturze krytycznej, życiu lub zdrowiu ludzi, mieniu w znacznych rozmiarach, dziedzictwu narodowemu lub środowisku, Szef ABW może wydawać polecenia organom i podmiotom, o których mowa w ust. 1, z wyłączeniem podmiotów, o których mowa w art. 7, zagrożonym tymi zdarzeniami, mające na celu przeciwdziałanie zagrożeniom, ich usunięcie albo minimalizację, oraz przekazywać im informacje niezbędne do tego celu. Organy i

podmioty, o których mowa w zdaniu pierwszym, informują Szefa ABW o podjętych działaniach w tym zakresie.

4. Szef ABW o podjętych działaniach, o których mowa w ust. 3, informuje niezwłocznie Ministra Koordynatora Służb Specjalnych, jeżeli został powołany.”;

3) w art. 12:

a) w ust. 1 pkt 1 i 2 otrzymują brzmienie:

„1) Policja – w obiektach infrastruktury krytycznej wskazanych przez Komendanta Głównego Policji w uzgodnieniu z Szefem ABW;

2) Żandarmeria Wojskowa – w obiektach stanowiących siedzibę urzędu obsługującego Ministra Obrony Narodowej oraz w obiektach należących do komórek i jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych albo administrowanych przez te komórki i jednostki organizacyjne wskazanych przez Ministra Obrony Narodowej w uzgodnieniu z Szefem SKW.”,

b) po ust. 2 dodaje się ust. 3 w brzmieniu:

„3. Komendant Główny Policji i Szef ABW, określą w drodze porozumienia, tryb wskazywania obiektów infrastruktury krytycznej, o których mowa w ust.1 pkt 1. ”;

4) w art. 15 w ust. 9 wyraz „zadania” zastępuje się wyrazem „przedsięwzięcia”;

5) w art. 16 w ust. 1 pkt 4 otrzymuje brzmienie:

„4) dla określonych obiektów jednostek organizacyjnych administracji publicznej, prokuratury, sądów lub obiektów infrastruktury krytycznej;”;

6) w art. 17:

a) ust. 1 otrzymuje brzmienie:

„1. W przypadku wprowadzenia pierwszego lub drugiego stopnia alarmowego lub pierwszego lub drugiego stopnia alarmowego CRP w trybie art. 16 ust. 1, Szef ABW może powołać sztab koordynacyjny, w skład którego wchodzą przedstawiciele wyznaczeni przez podmioty, o których mowa w art. 5 ust. 1.”,

b) po ust. 1 dodaje się ust. 1a w brzmieniu:

„1a. W przypadku wprowadzenia trzeciego lub czwartego stopnia alarmowego lub trzeciego lub czwartego stopnia alarmowego CRP, w trybie art. 16 ust. 1, Szef ABW powołuje sztab koordynacyjny, o którym mowa w ust. 1.”,

c) ust. 3 otrzymuje brzmienie:

„3. Do zadań sztabu koordynacyjnego należy:

1) rekomendowanie zmiany lub odwołania stopnia alarmowego lub stopnia alarmowego CRP;
2) dokonywanie oceny stopnia zagrożenia infrastruktury krytycznej zlokalizowanej na obszarze objętym obowiązywaniem stopnia alarmowego lub stopnia alarmowego CRP oraz wydawanie rekomendacji zmierzających do jej odpowiedniego zabezpieczenia;
3) rekomendowanie form i zakresu współdziałania podmiotów wchodzących w skład sztabu koordynacyjnego i biorących udział w jego pracach.”.

Art. 16. W ustawie z dnia 20 lipca 2017 r. - Prawo wodne (Dz. U. z 2024 r. poz. 1087) w art. 240 w ust. 3 pkt 24 otrzymuje brzmienie:

"24) współdziałają z wojewodami w zakresie opracowywania wojewódzkiego planu zarządzania ryzykiem oraz wojewódzkiego planu reagowania kryzysowego;".

Art. 17. W ustawie z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (Dz. U. z 2024 r. poz. 325 i 1222) w art. 37 ust. 1 i 2 otrzymują brzmienie:

„1. W przypadkach, o których mowa w art. 11 pkt 1–6 i 9–16 ustawy z 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2024 r. poz. 383), funkcjonariusz może użyć środków przymusu bezpośredniego, o których mowa w art. 12 ust. 1 pkt 1, pkt 2 lit. a, pkt 5, 7, 9, 11, pkt 12 lit. a, c i d, pkt 13 i 17–23 tej ustawy, lub wykorzystać te środki.

2. W przypadkach, o których mowa w art. 45 pkt 1 lit. a-c i e, pkt 2 i pkt 3 lit. a z wyłączeniem pościgu za osobą, o której mowa w art. 45 pkt 1 lit. d, oraz w art. 47 pkt 1, pkt 2 lit. a i pkt 3-8 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, funkcjonariusz może użyć broni palnej lub ją wykorzystać.”.

Art. 18. W ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913, 1703 oraz z 2024 r. poz. 834) wprowadza się następujące zmiany:

1) w art. 10 w ust. 4 wyrazy „właścicielem, posiadaczem samoistnym albo posiadaczem zależnym obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1” zastępuje się wyrazami „operatorem infrastruktury krytycznej, o którym mowa w art. 3 pkt 3a”;
2) w art. 15 w ust. 7 w pkt 2 wyrazy „właścicielem, posiadaczem samoistnym albo posiadaczem zależnym obiektów, instalacji, urządzeń lub usług wchodzących w skład

infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1” zastępuje się wyrazami ,,operatorem infrastruktury krytycznej, o którym mowa w art. 3 pkt 3a”;

3) w art. 26:

a) w ust. 2 wyrazy ,,właścicieli, posiadaczy samoistnych albo posiadaczy zależnych obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1” zastępuje się wyrazami „operatorów infrastruktury krytycznej, o których mowa w art. 3 pkt 3a”,

b) w ust. 5 pkt 1 otrzymuje brzmienie:

„1) podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, w tym podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są wykazem, o których mowa w art. 6r ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;”,

c) w ust. 7 pkt 5 i 6 otrzymują brzmienie:

„5) inne niż wymienione w pkt 1–4 oraz ust. 5 podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są wykazem, o którym mowa w art. 6i ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;

6) podmioty, o których mowa w ust. 6, jeżeli incydent dotyczy systemów teleinformatycznych lub sieci teleinformatycznych objętych wykazami, o których mowa w art. 6i ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.”,

d) w art. 46 po ust. 1 dodaje się ust. 1a w brzmieniu:

"1a. System, o którym mowa w ust. 1, zapewnia wymianę informacji między organami do spraw podmiotów krytycznych, o których mowa w art. 6v ustawy z dnia 27 kwietnia 2007 r. o zarządzaniu kryzysowym, dyrektorem Rządowego Centrum Bezpieczeństwa a podmiotami krytycznymi, o których mowa w art. art. 3 pkt 1a tej ustawy.".

Art. 19. W ustawie z dnia 17 grudnia 2020 r. o rezerwach strategicznych (Dz. U. z 2024 r. poz. 1598) wprowadza się następujące zmiany:

1) w art. 2:

a) pkt 1 otrzymuje brzmienie:

"1) infrastruktura krytyczna - infrastrukturę, o której mowa w art. 3 pkt 2 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122 oraz z 2024 r. poz. 834, 1222 i 1473),

b) dodaje się pkt 1a i 1b w brzmieniu:

"1a) podmiot krytyczny - podmiot, o którym mowa w art. 3 pkt 1a ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;

1b) usługa kluczowa - usługa, o której mowa w art. 3 pkt 1d ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;",

c) po pkt 4 dodaje się pkt 4a w brzmieniu:

„4a) wirtualne środowisko informatyczne – wydzielona przestrzeń wielosystemowa oparta o ograniczone zasoby fizyczne;”;

2) art. 4 otrzymuje brzmienie:

„Art. 4. Rezerwy strategiczne mogą stanowić surowce, materiały, urządzenia, maszyny, konstrukcje, elementy infrastruktury krytycznej, moc produkcyjna, moc usługowa, wirtualne środowisko informatyczne, fizyczne i wirtualne zasoby teleinformatyczne, produkty naftowe, produkty rolne i rolno–spożywcze, środki spożywcze i ich składniki, wyroby medyczne, produkty lecznicze, produkty lecznicze weterynaryjne oraz substancje czynne w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne (Dz. U. z 2024 r. poz. 686), materiały wybuchowe, broń, amunicja oraz ich istotne części, ładunki miotające oraz wyroby i technologie o przeznaczeniu wojskowym lub policyjnym w rozumieniu ustawy z dnia 13 czerwca 2019 r. o wykonywaniu działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym (Dz. U. z 2023 r. poz. 1743), produkty biobójcze, a także inne produkty – niezbędne do realizacji celów, o których mowa w art. 3.";

3) w art. 5 dotychczasową treść oznacza się jako ust. 2 i dodaje się ust. 1 w brzmieniu:

„Art. 5. 1. Agencja w imieniu własnym dokonuje zakupu asortymentu, o którym mowa w art. 4, z przeznaczeniem do rezerw strategicznych oraz zawiera umowy, o których mowa w art. 17 i art. 18 w celu utworzenia rezerw strategicznych.”;

4) art. 7 otrzymuje brzmienie:

„Art. 7. Do decyzji wydawanych przez ministra właściwego do spraw wewnętrznych w zakresie rezerw strategicznych oraz decyzji, o której mowa w art. 32 ust. 1, a także do decyzji wydawanych przez organy i podmioty, o których mowa w art. 8

ust. 2, w przypadku, o którym mowa w art. 29, nie stosuje się przepisów ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2024 r. poz. 572).”;

5) w art. 8:

a) w ust. 2 pkt 5 otrzymuje brzmienie:

„5) minister właściwy do spraw gospodarki surowcami energetycznymi;”,

b) w ust. 4 pkt 1-3 otrzymują brzmienie:

"1) ocenę ryzyka zidentyfikowanych zagrożeń, uwzględniającą sposoby i środki reagowania na te zagrożenia, zawartą w opracowanych planach zarządzania kryzysowego, o których mowa w art. 2 pkt 16 ustawy o zarządzaniu kryzysowym;

2) wnioski wynikające z wykonania postanowień Strategii Oporności Podmiotów Krytycznych, o której mowa w art. 6f ustawy o zarządzaniu kryzysowym, w zakresie sprawowania nadzoru nad infrastrukturą krytyczną oraz podmiotami krytycznymi zapewniającymi świadczenie usług kluczowych;

3) wykazy potrzeb wynikających z oceny ryzyka, dotyczących utworzenia rezerw strategicznych w danym asortymencie i ilości, w podziale na poszczególne lata wraz z uzasadnieniem;”,

6) w art. 9 w ust. 1 pkt 1 i 2 otrzymują brzmienie:

„1) wnioski dotyczące tworzenia, utrzymywania i likwidacji rezerw wynikające z oceny ryzyka zidentyfikowanych zagrożeń zawartej w Krajowej Ocenie Ryzyka, o której mowa w art. 6e ustawy o zarządzaniu kryzysowym, oraz wnioski, o których mowa w art. 8 ust. 4 pkt 2;

2) dane dotyczące asortymentów rezerw strategicznych i ich ilości, jakie należy utworzyć w poszczególnych latach wraz z uzasadnieniem;”;

7) w art. 10:

a) ust. 2 otrzymuje brzmienie:

„2. Minister właściwy do spraw wewnętrznych, po przyjęciu Programu przez Radę Ministrów, niezwłocznie przekazuje:

1) Program – Agencji i organom, o których mowa w art. 8 ust. 2 pkt 1–3;

2) wyciąg z Programu, zawierający informacje o rodzaju i ilości rezerw strategicznych ujętych w Programie, z podziałem na poszczególne lata – organom i podmiotom, o których mowa w art. 8 ust. 2 pkt 4–22.”;

b) dodaje się ust. 3 w brzmieniu:

„3. Przepis ust. 2 stosuje się odpowiednio w przypadku aktualizacji Programu.”;

8) w art. 11 w ust. 2 w pkt 1 lit. a i b otrzymują brzmienie:

„a) zakupu asortymentu w celu utworzenia rezerw strategicznych oraz odtworzenia udostępnionych rezerw strategicznych,

b) utrzymywania i przechowywania rezerw strategicznych, w tym ich zamiany, wymiany i konserwacji,”;

9) w art. 12 ust. 1 otrzymuje brzmienie:

„1. W budżecie państwa tworzy się rezerwę celową z przeznaczeniem na finansowanie działań ministra właściwego do spraw wewnętrznych w sytuacjach zagrożeń, o których mowa w art. 3, na skutek zdarzeń, których nie można było przewidzieć ani im przeciwdziałać, w szczególności na finansowanie kosztów:

1) udostępnienia rezerw strategicznych, w tym wydawania, przetransportowania i dystrybucji udostępnionych rezerw strategicznych do ostatecznych odbiorców;

2) innych usług niezbędnych do udostępnienia rezerw strategicznych ostatecznym odbiorcom;

3) przetworzenia i przetrzymania udostępnionych rezerw strategicznych, jeżeli jest to konieczne;

4) zakupu danego asortymentu rezerw lub usług w ramach udostępnienia rezerw utrzymywanych na podstawie umów, o których mowa w art. 17 i art. 18;

5) niezbędnych czynności Agencji i organów, na których rzecz rezerwy strategiczne udostępniono, oraz podmiotów, którym je wydano, w zakresie organizacji i realizacji udostępnienia rezerw strategicznych, na zasadach określonych w ustawie;

6) utworzenia i utrzymywania rezerw strategicznych nieobjętych Programem, o których mowa w art. 14;

7) odtworzenia udostępnionych rezerw strategicznych objętych Programem, o których mowa w art. 13;

8) realizacji zadań, o których mowa w art. 32.”;

10) w art. 13:

a) ust. 2 otrzymuje brzmienie:

„2. Decyzja o utworzeniu rezerw strategicznych określa w szczególności:

1) sposób utworzenia rezerw strategicznych przez Agencję;
2) rodzaj i ilość asortymentu rezerw strategicznych.”,

b) ust. 4 otrzymuje brzmienie:

„4. Wykonując decyzję o utworzeniu rezerw strategicznych, Agencja:
1) dokonuje nabycia określonej ilości asortymentu rezerw strategicznych;
2) przechowuje zakupiony asortyment rezerw strategicznych;
3) zawiera umowy, o których mowa w art. 17 lub w art. 18;
4) może przyjąć określony asortyment w formie darowizny z przeznaczeniem do rezerw strategicznych.”,

c) ust. 5 otrzymuje brzmienie:

„5. W przypadkach, w których nie mają zastosowania przepisy o zamówieniach publicznych, Agencja, dokonując zakupu asortymentu rezerw strategicznych lub usług związanych z utrzymywaniem rezerw strategicznych, lub zawierając umowy, o których mowa w art. 17 i art. 18, stosuje przejrzyste, niedyskryminacyjne i konkurencyjne warunki wyłaniania sprzedawcy tego asortymentu, usługi lub podmiotu, z którym zostanie zawarta umowa, o której mowa w art. 17 i art. 18, w szczególności:
1) przesyła zapytania ofertowe do podmiotów wykonujących działalność gospodarczą w zakresie produkcji, handlu, świadczenia określonych usług, w tym przechowywania oraz dysponujących odpowiednią bazą magazynową i gwarantujących odpowiednią jakość poszukiwanego asortymentu rezerw strategicznych, a także zapewniających ochronę informacji niejawnych, zgodnie z odrębnymi przepisami;
2) zaprasza do negocjacji podmioty oferujące najkorzystniejsze ekonomicznie warunki sprzedaży, świadczenia usług i przechowywania asortymentu rezerw strategicznych, biorąc pod uwagę relację ceny do jakości;
3) przeprowadza negocjacje cenowe z uwzględnieniem cen rynkowych w zakresie zakupu określonej ilości asortymentu rezerw strategicznych lub zakupu określonych usług.”;

11) w art. 14 dodaje się ust. 3 w brzmieniu:

„3. Do decyzji, o której mowa w ust. 1, przepisy art. 13 ust. 2–6 stosuje się odpowiednio.”;

12) w art. 17 w ust. 2 pkt 1–3 otrzymują brzmienie:

„1) wysokość wynagrodzenia za utrzymywanie rezerw z możliwością ich zakupu lub najmu na rzecz Agencji;

2) zobowiązanie podmiotu, z którym zawarto umowę, do stałej gotowości sprzedaży lub najmu na rzecz Agencji asortymentu przechowywanych rezerw;

3) tryb i warunki, w tym cenę sprzedaży asortymentu będącego przedmiotem umowy na rzecz Agencji lub wysokość czynszu najmu tego asortymentu, do którego uiszczenia będzie zobowiązana Agencja w przypadku wydania, przez upoważniony organ, decyzji o udostępnieniu rezerw strategicznych.”;

13) w art. 19:

a) w ust. 5:

– pkt 4–5 otrzymują brzmienie:

„4) wskazanie czy udostępnienie rezerw strategicznych następuje bez obowiązku zwrotu, z obowiązkiem zwrotu lub z obowiązkiem zwrotu niewykorzystanej części udostępnionych rezerw strategicznych;

5) inne szczególne warunki udostępnienia rezerw strategicznych, w tym w szczególności dotyczące obowiązku przetransportowania rezerw, montażu, zainstalowania lub ich przetworzenia lub obowiązku pokrycia kosztów przeglądów, demontażu, jeżeli jest to konieczne ze względu na właściwości udostępnionego asortymentu rezerw strategicznych lub jest uzasadnione innymi względami;”,

– w pkt 5 kropkę zastępuje się średnikiem i dodaje się pkt 6 i 7 w brzmieniu:

„6) określenie, czy udostępnione bez obowiązku zwrotu rezerwy strategiczne podlegają odtworzeniu wraz ze wskazaniem ilości oraz źródeł finansowania;

7) określenie źródła finansowania kosztów udostępnienia.”,

b) dodaje się ust. 9–11 w brzmieniu:

„9. W przypadku wydania decyzji o udostępnieniu rezerw strategicznych bez obowiązku zwrotu własność asortymentu rezerw strategicznych przechodzi na organ lub podmiot, na którego rzecz rezerwy strategiczną są udostępnione z chwilą jego wydania.

10. W przypadku wydania decyzji o udostępnieniu rezerw strategicznych z obowiązkiem zwrotu utrzymanie wydanych rezerw strategicznych w należytym

stanie, w tym dokonywanie wymaganych przeglądów, konserwacji i napraw, obciąża, podmiot lub organ, któremu rezerwy strategiczne zostały wydane.

11. Do zakupu usług transportowych oraz innych usług logistycznych związanych z wykonaniem decyzji o udostępnieniu rezerw strategicznych nie stosuje się przepisów ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2024 r. poz. 1320), jeżeli wartość zamówienia jest mniejsza niż progi unijne, o których mowa art. 3 ust. 1 tej ustawy.";

14) w art. 20 w ust. 2 pkt 6 otrzymuje brzmienie:

„6) zwraca Agencji niewykorzystaną część udostępnionych rezerw strategicznych, jeżeli zostały udostępnione z obowiązkiem zwrotu niewykorzystanej części;”;

15) w art. 21:

a) ust. 1 otrzymuje brzmienie:

„1. Minister właściwy do spraw wewnętrznych może, w drodze decyzji, udostępnić określony specjalistyczny asortyment techniczny rezerw strategicznych, mając na względzie potrzebę przeciwdziałania lub usuwania skutków klęski żywiołowej lub sytuacji kryzysowej lub wsparcia realizacji celów społecznych lub przedsięwzięć gospodarczych, w szczególności związanych z odtworzeniem, budową, modernizacją lub remontem infrastruktury. Przepisy art. 19 ust. 2 i 4 oraz ust. 5 pkt 1–3 stosuje się odpowiednio.”,

b) ust. 3 otrzymuje brzmienie:

„3. Udostępnienie specjalistycznego asortymentu technicznego rezerw strategicznych, jest dokonywane nieodpłatnie na rzecz państwowych jednostek organizacyjnych, jednostek samorządu terytorialnego lub utworzonych przez nie jednostek organizacyjnych w przypadku wystąpienia klęski żywiołowej lub sytuacji kryzysowej lub w celu zaspokojenia potrzeb społecznych lub gospodarczych, w szczególności związanych z odtworzeniem, budową, modernizacją lub remontem infrastruktury.”;

16) art. 22 otrzymuje brzmienie:

„Art. 22. 1. Agencja może odpłatnie udostępnić określony specjalistyczny asortyment techniczny rezerw strategicznych na rzecz jednostek samorządu terytorialnego, utworzonych przez nie jednostek organizacyjnych, służb, inspekcji lub innych jednostek, o których mowa w art. 8 ust. 2 pkt 22, oraz na rzecz przedsiębiorców

mając na względzie potrzebę wsparcia w realizacji celów społecznych lub przedsięwzięć gospodarczych.

2. Udostępnienie specjalistycznego asortymentu technicznego rezerw strategicznych, jest dokonywane na wniosek podmiotów określonych w ust. 1.

3. Specjalistyczny asortyment techniczny rezerw strategicznych, o którym mowa w ust. 1 jest udostępniany na podstawie umowy zawartej na czas oznaczony między Agencją a podmiotem, o którym mowa w ust. 1.

4. Umowa, o której mowa w ust. 3, określa w szczególności warunki udostępnienia specjalistycznego asortymentu technicznego rezerw strategicznych oraz jego zwrotu.”;

17) w art. 23 ust. 5 otrzymuje brzmienie:

„5. Umowa, o której mowa w ust. 4, określa w szczególności warunki udostępnienia specjalistycznego asortymentu medycznego rezerw strategicznych oraz jego zwrotu.”;

18) po art. 23 dodaje się art. 23a w brzmieniu:

„Art. 23a. 1. Minister właściwy do spraw wewnętrznych może, w drodze decyzji, udostępnić wirtualne środowisko informatyczne oraz fizyczne lub wirtualne zasoby informatyczne mając na względzie potrzebę wsparcia realizacji celów związanych z cyberbezpieczeństwem państwa oraz konieczność odtworzenia zasobów cyfrowych. Przepisy art. 19 ust. 2 i 4 oraz ust. 5 pkt 1–3 stosuje się odpowiednio.

2. Decyzję, o której mowa w ust. 1, wykonuje Agencja.

3. Udostępnienie, o którym mowa w ust. 1, jest dokonywane odpłatnie na rzecz państwowych jednostek organizacyjnych, jednostek samorządu terytorialnego lub utworzonych przez nie jednostek organizacyjnych w przypadku wystąpienia zagrożenia cyberbezpieczeństwa państwa lub konieczności odtworzenia zasobów cyfrowych.

4. Wirtualne środowisko informatyczne oraz fizyczne lub wirtualne zasoby informatyczne są udostępniane na podstawie umowy zawartej na czas oznaczony pomiędzy Agencją a podmiotem, o którym mowa w ust. 3.

5. Umowa, o której mowa w ust. 4, w szczególności warunki udostępnienia asortymentu określonego w ust. 1 oraz jego zwrotu.”;

19) art. 24 otrzymuje brzmienie:

„Art. 24. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, szczegółową procedurę udostępnienia rezerw strategicznych, w tym czasowego, zwrotnego udostępnienia specjalistycznego asortymentu technicznego rezerw strategicznych oraz specjalistycznego asortymentu medycznego rezerw strategicznych,

procedurę zwrotu asortymentu rezerw strategicznych, oraz szczegółowe czynności przy udostępnieniu lub wydaniu rezerw strategicznych, uwzględniając konieczność zapewnienia prawidłowej i efektywnej realizacji zadań Agencji.”;

20) w art. 27a w ust. 1 wprowadzenie do wyliczenia otrzymuje brzmienie:

„1. Minister właściwy do spraw wewnętrznych może zlikwidować, w drodze decyzji, określony asortyment rezerw strategicznych, ze względu na konieczność:”;

21) uchyla się art. 28;

22) art. 29:

a) ust. 2 otrzymuje brzmienie:

"2. W przypadkach, o których mowa w ust. 1, organ lub podmiot powierzający Agencji określone zadanie wskazuje, rodzaj i ilość asortymentu, zakres jego przechowania, w tym czas tego przechowania, oraz organy lub podmioty, którym dany asortyment zostanie wydany oraz warunki wydania, a także określa wysokość środków finansowych przeznaczonych na finansowanie zadania.",

b) po ust. 3 dodaje się ust. 3a i 3b w brzmieniu:

3a. Środki finansowe na realizację powierzonego zadania oraz na pokrycie kosztów, o których mowa w ust. 3, organ lub podmiot powierzający Agencji określone zadanie przekazuje Agencji na podstawie zawartego z nią porozumienia.

3b. Środki finansowe, o których mowa w ust. 3a, nie stanowią przychodu Agencji, a ich przekazanie nie wymaga dokonywania zmian w planie finansowym Agencji.";

23) po art. 29 dodaje się art. 29a w brzmieniu:

„Art. 29a. 1. Agencja, za zgodą ministra właściwego do spraw wewnętrznych, może wykonywać zadania związane z:

1) przeciwdziałaniem wystąpieniu zagrożenia bezpieczeństwa i obronności państwa, porządku i zdrowia publicznego, klęski żywiołowej lub sytuacji kryzysowej;
2) udzielaniem pomocy humanitarnej ludności znajdującej się w sytuacji zagrożenia życia lub zdrowia

– na podstawie przepisów prawa międzynarodowego publicznego, procedur organizacji międzynarodowych oraz porozumień tworzących wiążące zobowiązanie wobec Agencji.

2. Agencja może realizować zadania, o których mowa w ust. 1, po zapewnieniu środków finansowych na ich realizację, w tym na pokrycie wydatków niekwalifikowanych, zgodnie z ustawą o finansach publicznych.”;

24) w art. 31:

a) w ust. 1

– pkt 3 otrzymuje brzmienie:

„3) wykonywanie decyzji organów lub podmiotów, o których mowa w art. 8 ust. 2, dotyczących zakupu, przechowywania, dystrybucji i wydawania określonych asortymentów towarów zgodnie z zasadami określonymi w rozdziale 6;”,

– po pkt 8 dodaje się pkt 8a w brzmieniu:

„8a) wykonywanie zadań, o których mowa w art. 29a ust. 1;”,

– pkt 10 i 11 otrzymują brzmienie:

„10) opracowywanie informacji o asortymencie rezerw strategicznych, ilości i wartości rezerw strategicznych oraz ich finansowaniu, wykorzystaniu i rozmieszczeniu, w terminach do dnia 15 września każdego roku za I półrocze i do dnia 31 marca każdego roku za rok poprzedni;

11) przekazywanie Ministrowi Obrony Narodowej, ministrowi właściwemu do spraw transportu, ministrowi właściwemu do spraw wewnętrznych i Szefowi Agencji Bezpieczeństwa Wewnętrznego informacji o ilości i rozmieszczeniu rezerw strategicznych, ujętych w Programie w terminach do dnia 15 września każdego roku za I półrocze i do dnia 31 marca każdego roku za rok poprzedni;”

- po pkt 13 kropkę zastępuje się średnikiem i dodaje się pkt 13 w brzmieniu:

„14) prowadzenie działalności informacyjnej, promocyjnej i edukacyjnej w zakresie zadań Agencji.”,

b) ust. 2 otrzymuje brzmienie:

„2. Do czynności realizowanych przez Agencję w ramach zadań, o których mowa w ust. 1 pkt 5, nie stosuje się przepisów art. 38–41 ustawy z dnia 16 grudnia 2016 r. o zasadach zarządzania mieniem państwowym (Dz. U. z 2024 r. poz. 125 i 834).”;

25) art. 32 otrzymuje brzmienie:

„Art. 32. 1. Minister właściwy do spraw wewnętrznych może powierzyć Agencji, w drodze decyzji, realizację innych zadań niż określone w art. 31, na terytorium Rzeczypospolitej Polskiej lub poza jej granicami, związanych z:

1) wystąpieniem zagrożenia bezpieczeństwa i obronności państwa, porządku i zdrowia publicznego, klęski żywiołowej lub sytuacji kryzysowej;

2) wypełnieniem zobowiązania międzynarodowego lub udzieleniem pomocy lub wsparcia:
   a) podmiotowi prawa międzynarodowego publicznego,
   b) podmiotowi krajowemu, zagranicznemu lub międzynarodowemu podejmującemu działania w zakresie niesienia pomocy humanitarnej lub usuwania skutków sytuacji kryzysowej

– w szczególności w przypadkach określonych w pkt 1.

2. Realizując zadania, o których mowa w ust. 1, Agencja jest uprawniona w szczególności do:

1) nabywania, zbywania, transportowania, przechowywania, wydawania oraz do wywozu poza terytorium Rzeczypospolitej Polskiej i przywozu z terytorium innego państwa określonego asortymentu;
2) nabywania oraz świadczenia usług, w szczególności usług o charakterze logistycznym, transportowym i magazynowym, na terytorium Rzeczypospolitej Polskiej lub poza jej granicami;
3) zlecania wykonania robót budowlanych oraz usług związanych z ich wykonaniem;
4) przyjmowania i przekazywania darowizn.

3. Powierzając zadania, o których mowa w ust. 1, minister właściwy do spraw wewnętrznych zapewnia Agencji na ten cel odpowiednie środki finansowe.

4. Wydając decyzję, o której mowa w ust. 1, minister właściwy do spraw wewnętrznych może nadać jej rygor natychmiastowej wykonalności. Decyzja nie wymaga uzasadnienia.

5. Do udzielania zamówień niezbędnych do realizacji decyzji, o której mowa w ust. 1, nie stosuje się przepisów ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych, jeżeli wartość zamówienia jest mniejsza niż progi unijne, o których mowa art. 3 ust. 1 tej ustawy.

6. Agencja, w terminie 30 dni od dnia udzielenia zamówienia, o którym mowa w ust. 5, zamieszcza w Biuletynie Zamówień Publicznych informację o udzieleniu tego zamówienia, w której podaje:

1) datę i miejsce zawarcia umowy lub informację o zawarciu umowy drogą elektroniczną;
2) opis przedmiotu umowy, z wyszczególnieniem odpowiednio ilości rzeczy lub innych dóbr oraz zakresu usług;

3) cenę albo cenę maksymalną, jeżeli cena nie jest znana w chwili zamieszczenia ogłoszenia;
4) wskazanie okoliczności faktycznych uzasadniających udzielenie zamówienia bez zastosowania przepisów ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych;
5) nazwę (firmę) podmiotu albo imię i nazwisko osoby, z którymi została zawarta umowa

– z wyłączeniem przypadków, w których udzielenie zamówienia wiąże się z korzystaniem z informacji niejawnych.”;

26) w art. 36 dodaje się ust. 5 w brzmieniu:

„5. Przepisów ust. 1–4 nie stosuje się do naboru wewnętrznego spośród pracowników Agencji do zatrudnienia na wolne stanowiska pracy w Agencji.”;

27) art. 40 otrzymuje brzmienie:

„Art. 40. Pracownicy Agencji zatrudnieni:
1) na stanowisku głównego księgowego,
2) na stanowisku zastępcy dyrektora biura lub na stanowisku równorzędnym,
3) na stanowisku kierownika działu lub na stanowisku równorzędnym,
4) na stanowisku kierownika składnicy lub na stanowisku równorzędnym

– składają Prezesowi Agencji oświadczenia o stanie majątkowym na zasadach, w trybie i w terminach określonych w przepisach ustawy z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne oraz podlegają ograniczeniom w prowadzeniu działalności gospodarczej, takim jak pracownicy agencji państwowych, o których mowa w art. 2 pkt 10 ustawy z dnia 21 sierpnia 1997 r. o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne (Dz. U. z 2023 r. poz. 1090).”;

28) po art. 40 dodaje się art. 40a w brzmieniu:

„Art. 40a. Agencja wykonuje obowiązek, o którym mowa w art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.), zwanego dalej „rozporządzeniem 2016/679”, przez udostępnienie informacji, o których mowa w art. 13 ust. 1 i 2 rozporządzenia 2016/679, na swojej

stronie internetowej lub w Biuletynie Informacji Publicznej na stronie podmiotowej Agencji. W takim przypadku Agencja, podczas pozyskiwania danych osobowych, informuje osobę, której dane dotyczą, o miejscu udostępnienia tych informacji.”;

29) w art. 41:

a) w ust. 2 pkt 2 otrzymuje brzmienie:

„2) dotacje celowe na realizację zadań, o których mowa w art. 12 ust. 1;”

b) w ust. 2 w pkt 9 kropkę zastępuje się średnikiem i dodaje się pkt 10 w brzmieniu:

„10) środki pochodzące z budżetu Unii Europejskiej.”

c) ust. 3 otrzymuje brzmienie:

„3. Przychody, o których mowa w ust. 2 pkt 4–7, przeznacza się na realizację zadań Agencji, o których mowa w art. 31 i art. 32, oraz na bieżącą działalność Agencji, w tym wynagrodzenia jej pracowników.”;

d) po ust. 3a dodaje się ust. 3b w brzmieniu:

„3b. Przychody Agencji, o których mowa w ust. 2 pkt 10, przeznacza się na realizację zadań Agencji, o których mowa w art. 31 ust. 1, w szczególności w pkt 8a.”;

30) w art. 42:

a) w ust. 1 w pkt 3 lit. b otrzymuje brzmienie:

„b) realizacji zadań określonych w ustawie oraz w ustawie o zapasach ropy naftowej, produktów naftowych i gazu ziemnego, z uwzględnieniem:

– kosztów realizacji tych zadań przez inne podmioty,

– zakupu towarów i usług;”,

b) ust. 3 otrzymuje brzmienie:

„3. Agencja w terminie 30 dni od ogłoszenia ustawy budżetowej na dany rok, przekazuje ministrowi właściwemu do spraw wewnętrznych plan rzeczowy rezerw strategicznych stanowiący załącznik do planu finansowego Agencji.”,

c) po ust. 3 dodaje się ust. 3a i 3b w brzmieniu:

„3a. W przypadku gdy:

1) wystąpiło zagrożenie bezpieczeństwa i obronności państwa, bezpieczeństwa, porządku i zdrowia publicznego lub wystąpiła klęska żywiołowa lub sytuacja kryzysowa,

2) zaistniała konieczność wypełnienia zobowiązania międzynarodowego lub potrzeba udzielenia pomocy lub wsparcia:

a) podmiotowi prawa międzynarodowego publicznego,

b) podmiotowi krajowemu, zagranicznemu lub międzynarodowemu podejmującemu działania w zakresie niesienia pomocy humanitarnej lub usuwania skutków sytuacji kryzysowej

– w szczególności w przypadkach określonych w pkt 1,

– zmiany planu finansowego Agencji dokonywane zgodnie z art. 21 ust. 5 pkt 2 ustawy o finansach publicznych, dotyczące realizacji zadań związanych z tworzeniem, utrzymywaniem, udostępnianiem i likwidacją rezerw strategicznych oraz realizowanych na podstawie art. 32, nie wymagają uzyskania opinii sejmowej komisji właściwej do spraw budżetu.

3b. W przypadkach, o których mowa w ust. 3a, przepisów art. 21 ust. 6 oraz art. 52 ust. 2 pkt 2 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych nie stosuje się.”,

d) ust. 4 otrzymuje brzmienie:

„4. Agencja sporządza i przekazuje ministrowi właściwemu do spraw wewnętrznych sprawozdania finansowe i związane z nimi informacje, w trybie i na zasadach określonych w ustawie o finansach publicznych oraz ustawie o rachunkowości.”;

31) po art. 42 dodaje się art. 42a w brzmieniu:

„Art. 42a. 1.W celu zapewnienia ciągłości realizacji zadań Agencji w przypadkach, o których mowa w art. 42 ust. 3a, minister właściwy do spraw wewnętrznych nie później niż do dnia 10 listopada przekazuje ministrowi właściwemu do spraw finansów publicznych informację o zapotrzebowaniu na środki na realizację wydatków niewygasających w terminie nie dłuższym niż do dnia 30 czerwca następnego roku budżetowego.

2. Do dnia 15 grudnia danego roku budżetowego Rada Ministrów może określić, w drodze rozporządzenia, po uzyskaniu opinii sejmowej komisji właściwej do spraw budżetu, rodzaj i wysokość wydatków Agencji, do których nie stosuje się przepisów art. 181 ust. 1 ustawy o finansach publicznych, i ostateczny termin ich dokonania, nie dłuższy niż 30 czerwca następnego roku budżetowego.

3. Wydając rozporządzenie, o którym mowa w ust. 2, Rada Ministrów uwzględni konieczność zapewnienia ciągłości realizacji zadań Agencji, w przypadkach o których mowa w art. 42 ust. 3a.”;

32) w art. 44 ust. 1 otrzymuje brzmienie:

„1. Należności i wierzytelności Agencji mające charakter cywilnoprawny, w szczególności z tytułu wykonywania zadań, o których mowa w art. 31 ust. 1 pkt 1, 2, 4–8 i 13, mogą być umarzane w całości albo w części lub ich spłata może być odraczana, lub rozkładana na raty.”;

33) w art. 46 w ust. 1 dodaje się pkt 1a w brzmieniu:

„1a) minister właściwy do spraw gospodarki surowcami energetycznymi – w zakresie należności i wierzytelności wynikających z wykonywania zadań, o których mowa w art. 31 ust. 1 pkt 8, z zastrzeżeniem pkt 1;”;

34) po art. 46 dodaje się art. 46a w brzmieniu:

„Art. 46a. Przepisów art. 44–46 nie stosuje się do zawarcia ugody na podstawie art. 54a ustawy o finansach publicznych.”.

Art. 20. W ustawie z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. poz. 1662) w art. 2 w ust. 4 po pkt 1 dodaje się pkt 1a w brzmieniu:

"1a) wpływy z kar pieniężnych, o których mowa w art. 6zzo ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122 oraz z 2024 r. poz. 834, 1222, 1473, 1572 i 1907);".

Art. 21. W ustawie z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz. U. poz. 1907) wprowadza się następujące zmiany:

1) w art. 5 ust. 2 otrzymuje brzmienie:

„2. Podmioty ochrony ludności i obrony cywilnej są obowiązane do współpracy z organami ochrony ludności i obrony cywilnej, stosownie do swoich możliwości, kompetencji, obszaru działania oraz zakresu działania ujętego w planach zarządzania kryzysowego, o których mowa w art. 6g ust. 2 oraz art. 6j ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, i planach ciągłości działania.”;

2) w art. 15 w ust. 1 pkt 6 otrzymuje brzmienie:

„6) analizowanie wniosków z ocen ryzyka mających wpływ na bezpieczeństwo i ochronę ludności i obronę cywilną, o których mowa w Krajowej Ocenie Ryzyka, o której mowa w art. 6e ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, i informacji pochodzących z raportów Rządowego Centrum Bezpieczeństwa oraz

centrów służb podległych mu i nadzorowanych przez niego, a także przedstawianie propozycji rozwiązań w tym zakresie;”;

3) w art. 38, wstęp do wyliczenia otrzymuje brzmienie:

"Organy ochrony ludności i Dyrektor Rządowego Centrum Bezpieczeństwa uwzględniają w planach, o których mowa w art. 6g ust. 2 oraz art. 6j ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym:”;

4) art. 40 otrzymuje brzmienie:

„Art. 40. 1. Dyrektor Rządowego Centrum Bezpieczeństwa opracowuje krajowy plan ewakuacji ludności we współpracy z Szefem Sztabu Generalnego Wojska Polskiego.

2. Krajowy plan ewakuacji opracowuje się na podstawie wojewódzkich planów ewakuacji ludności.

3. Krajowy plan ewakuacji oraz wojewódzkie plany ewakuacji opracowuje się na okres 3 lat.

4. Plany, o których mowa w ust. 3 mogą być aktualizowane w przypadku zmian dotyczących sytuacji, o których mowa w art. 39 ust. 1.

5. Krajowy plan ewakuacji jest zatwierdzany przez ministra właściwego do spraw wewnętrznych.”;

5) art. 44 otrzymuje brzmienie:

„Art. 44 Wojewódzki plan ewakuacji ludności stanowi załącznik funkcjonalny do wojewódzkiego planu reagowania kryzysowego. Wkłady, o których mowa w art. 43, stanowią załącznik funkcjonalny do planów reagowania kryzysowego odpowiednio gminy i powiatu.”

Art. 22. 1. Krajową Ocenę Ryzyka, o której mowa w art. 6e ust. 1 ustawy zmienianej w art. 1, Rada Ministrów przyjmuje po raz pierwszy w terminie do dnia 17 stycznia 2026 r.

2. Strategia odporności podmiotów krytycznych, o której mowa w art. 6f ust. 1 ustawy zmienianej w art. 1, Rada Ministrów przyjmuje po raz pierwszy w terminie do dnia 17 stycznia 2026 r.

Art. 23. 1.Krajowy Plan Zarządzania Ryzykiem, o którym mowa w art. 6g ust. 2 pkt 1 ustawy zmienianej w art. 1 Rada Ministrów przyjmuje po raz pierwszy w terminie do 31 grudnia 2026 r.

2. Plany zarządzania ryzykiem, o których mowa w art. 6g ust. 2 pkt 2-5 ustawy zmienianej w art. 1 są przyjmowane po raz pierwszy w terminie 3 miesięcy od dnia przyjęcia Krajowego Planu Zarządzania Ryzykiem.

3. Plany zarządzania ryzykiem, o których mowa w art. 6g ust. 2 pkt 6 ustawy zmienianej w art. 1 są przyjmowane po raz pierwszy w terminie 3 miesięcy od dnia przyjęcia planu zarządzania ryzykiem właściwego wojewody.

4. Plany zarządzania ryzykiem, o których mowa w art. 6g ust. 2 pkt 7 ustawy zmienianej w art. 1 są przyjmowane po raz pierwszy w terminie 3 miesięcy od dnia przyjęcia planu zarządzania ryzykiem właściwego starosty.

5. Krajowy Plan Reagowania Kryzysowego, o którym mowa w art. 6j ust. 1 pkt 1 ustawy zmienianej w art. 1 Rada Ministrów przyjmuje po raz pierwszy w terminie 9 miesięcy od dnia przyjęcia Krajowego Planu Zarządzania Ryzykiem.

6. Plany reagowania kryzysowego, o których mowa w art. 6j ust. 1 pkt 2-5 ustawy zmienianej w art. 1 są przyjmowane po raz pierwszy w terminie 3 miesięcy od dnia przyjęcia Krajowego Planu Reagowania Kryzysowego.

7. Plany reagowania kryzysowego, o których mowa w art. 6j ust. 1 pkt 6 ustawy zmienianej w art. 1 są przyjmowane po raz pierwszy w terminie 3 miesięcy od dnia przyjęcia planu reagowania kryzysowego właściwego wojewody.

8. Plany reagowania kryzysowego, o których mowa w art. 6j ust. 1 pkt 7 ustawy zmienianej w art. 1 są przyjmowane po raz pierwszy w terminie 3 miesięcy od dnia przyjęcia planu reagowania kryzysowego właściwego starosty.

9. Plany zarządzania kryzysowego sporządzone i zatwierdzone na podstawie ustawy zmienianej w art. 1 w brzmieniu dotychczasowym pozostają w mocy do czasu sporządzenia planów, o których mowa w ust. 1-8 i mogą być w tym czasie aktualizowane.

Art. 24. 1. Szczegółowe kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi, o których mowa w art. 5b ust. 2 pkt 3 ustawy zmienianej w art. 1 w brzmieniu dotychczasowym, pozostają w mocy do czasu sporządzenia kryteriów, wydanych na podstawie art. 6r ust. 5 ustawy zmienianej w art. 1 i mogą być w tym czasie aktualizowane.

2. Kryteria, o których mowa w art. 6r ust. 5 ustawy zmienianej w art. 1 zostaną sporządzone po raz pierwszy w terminie do dnia 17 stycznia 2026 r.

Art. 25. 1. Jednolity wykaz obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy zmienianej w art. 1

w brzmieniu dotychczasowym, pozostaje w mocy do czasu sporządzenia wykazu, o którym mowa w art. 6r ust. 1 ustawy zmienianej w art. 1, i może być w tym czasie aktualizowany.

2. Plany ochrony infrastruktury krytycznej, o których mowa w art. 6 ust. 5 ustawy zmienianej w art. 1 w brzmieniu dotychczasowym, pozostają w mocy do czasu ujęcia infrastruktury krytycznej w wykazie, o którym mowa w art. 6r ust. 1 ustawy zmienianej w art. 1 oraz opracowania dokumentacji ochrony infrastruktury krytycznej, o której mowa w art. 6zf ust. 1 ustawy zmienianej w art. 1 i mogą być w tym czasie aktualizowane.

Art. 26. 1. Właściciele, posiadacze samoistni i zależni obiektów instalacji, urządzeń i usług ujętych w jednolitym wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy zmienianej w art. 1 w brzmieniu dotychczasowym, realizują zadania w zakresie ochrony infrastruktury krytycznej na podstawie art. 6 ustawy zmienianej w art. 1 w brzmieniu dotychczasowym do czasu ujęcia w wykazie infrastruktury krytycznej, o którym mowa w art. 6r ust. 1 ustawy zmienianej w art. 1.

2. Ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych oraz wojewodowie, w zakresie swoich właściwości, realizują zadania w zakresie ochrony infrastruktury krytycznej ujętej w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy zmienianej w art. 1, na podstawie dotychczasowych przepisów do czasu sporządzenia wykazu infrastruktury krytycznej, o którym mowa w art. 6r ust. 1 ustawy zmienianej w art. 1.

Art. 27. Organy do spraw podmiotów krytycznych, o których mowa w art. 6zk ust. 1 ustawy zmienianej w art. 1 po raz pierwszy identyfikują podmioty krytyczne i wpisują je do wykazu podmiotów krytycznych w terminie do dnia 17 lipca 2026 r.

Art. 28. 1. Pojedynczy Punkt Kontaktowy, o którym mowa w art. 6zm ust. 1 ustawy zmienianej w art. 1 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.

2. Pojedynczy Punkt Kontaktowy, o którym mowa w art. 6zm ust. 1 ustawy zmienianej w art. 1 po raz pierwszy przekazuje Komisji Europejskiej informacje o przepisach dotyczących kar pieniężnych nie później niż w ciągu 7 dni od dnia wejścia w życie ustawy.

3. Pojedynczy Punkt Kontaktowy, o którym mowa w art. 6zm ust. 1 ustawy zmienianej w art. 1 przekazuje Komisji Europejskiej dane kontaktowe wyznaczonych organów do spraw podmiotów krytycznych, Pojedynczego Punktu Kontaktowego oraz wskazuje zakres realizowanych zadań, w terminie trzech miesięcy od dnia wejścia w życie ustawy.

Art. 29. Utrzymanie wykazu podmiotów krytycznych prowadzonego w systemie, o którym mowa w art. 46 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa jest finansowane z części budżetowej , której dysponentem jest minister właściwy do spraw informatyzacji.

2. Minister właściwy do spraw informatyzacji może powierzyć realizację zadania utrzymania wykazu podmiotów krytycznych jednostce podległej albo przez niego nadzorowanej. Jednostka ta otrzymuje dotację celową na realizację zadania utrzymania wykazu podmiotów krytycznych.

Art. 30. 1. W terminie 30 dni od dnia wejścia w życie niniejszej ustawy Prezes Narodowego Banku Polskiego przekazuje Komisji Nadzoru Finansowego zestawienie podmiotów podlegających nadzorowi Komisji Nadzoru Finansowego umieszczonych w prowadzonym przez siebie wykazie, o którym mowa w art. 5 ust. 3 ustawy zmienianej w art. 5.

2. W terminie 45 dni od dnia wejścia w życie niniejszej ustawy w wykazie, o którym mowa w art. 5 ust. 3 ustawy zmienianej w art. 5, prowadzonym przez Komisję Nadzoru Finansowego umieszcza się podmioty zgodnie z zestawieniem, o którym mowa w ust. 1.

3. W przypadku, o którym mowa w ust. 2, umieszczenie podmiotu w wykazie, o którym mowa w art. 5 ust. 3 ustawy zmienianej w art. 5, prowadzonym przez Komisję Nadzoru Finansowego nie wymaga decyzji administracyjnej.

4. Po umieszczeniu podmiotów w prowadzonym przez siebie wykazie, o którym mowa w art. 5 ust. 3 ustawy zmienianej w art. 5, Komisji Nadzoru Finansowego niezwłocznie:

1) informuje o tym umieszczone podmioty oraz Prezesa Narodowego Banku Polskiego;
2) przesyła ten wykaz do właściwych terytorialnie wojewodów.

5. Po otrzymaniu informacji, o której mowa w ust. 4 pkt 1, Prezes Narodowego Banku Polskiego usuwa podmioty umieszczone w wykazie prowadzonym przez Komisję Nadzoru Finansowego z prowadzonego przez siebie wykazu, o którym mowa w art. 5 ust. 3 ustawy zmienianej w art. 5. Usunięcie podmiotów, o którym mowa w zdaniu pierwszym nie wymaga decyzji administracyjnej.

Art. 31. Dotychczasowa szczegółowa procedura udostępnienia rezerw strategicznych, o której mowa w art. 24 ustawy zmienianej w art. 17, zachowuje moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 24 ustawy zmienianej w art. 17, jednak nie dłużej niż przez 6 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 32. W terminie 30 dni od dnia wejścia w życie niniejszej ustawy wojewoda wypełnia obowiązek informacyjny, o którym mowa w art. 5 ust. 8 ustawy zmienianej w art. 5, względem dotychczas prowadzonej ewidencji.

Art 33. Komendant Główny Straży Granicznej w terminie 7 dni od dnia wejścia w życie ustawy wyznacza spośród oficerów Straży Granicznej Pełnomocnika Komendanta Głównego Straży Granicznej do spraw utworzenia Centrum Bezpieczeństwa Morskiego, zwanego dalej „Pełnomocnikiem”, w celu podjęcia czynności przygotowawczych i organizacyjnych niezbędnych do rozpoczęcia funkcjonowania Centrum Bezpieczeństwa Morskiego, w szczególności:

1) wskazania lokalizacji i pomieszczeń;
2) wyposażenia w niezbędny sprzęt;
3) zapewnienia funkcjonalności i komplementarności odpowiednich systemów teleinformatycznych i stanowisk pracy;
4) wspierania procesu oddelegowania przedstawicieli innych podmiotów do Straży Granicznej do wykonywania zadań CBM.

2. Czynności, o których mowa w ust.1, Pełnomocnik realizuje we współpracy i przy wsparciu podmiotów, o których mowa w art. 25b ust. 1 i 2 ustawy zmienianej w art. 1 .

3. Pełnomocnik kończy swoją działalność z dniem utworzenia Centrum Bezpieczeństwa Morskiego.

Art. 34. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 17 – administracja publiczna, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 553 tys. zł;
2) w 2027 r. – 591 tys. zł;
3) w 2028 r. – 622 tys. zł;
4) w 2029 r. – 655 tys. zł;
5) w 2030 r. – 690 tys. zł;
6) w 2031 r. – 762 tys. zł;

7) w 2032 r. – 763 tys. zł;
8) w 2033 r. – 801 tys. zł;
9) w 2034 r. – 842 tys. zł;
10) w 2035 r. – 884 tys. zł.

2. Minister właściwy do spraw administracji publicznej monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw administracji publicznej wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności organu do spraw podmiotów krytycznych dla sektora administracji publicznej.

Art. 35. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 19 – budżet, finanse publiczne, instytucje finansowe, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:
1) w 2026 r. – 553 tys. zł;
2) w 2027 r. – 591 tys. zł;
3) w 2028 r. – 622 tys. zł;
4) w 2029 r. – 655 tys. zł;
5) w 2030 r. – 690 tys. zł;
6) w 2031 r. – 762 tys. zł;
7) w 2032 r. – 763 tys. zł;
8) w 2033 r. – 801 tys. zł;
9) w 2034 r. – 842 tys. zł;
10) w 2035 r. – 884 tys. zł.

2. Minister właściwy do spraw finansów publicznych monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw gospodarki wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności organu do spraw podmiotów krytycznych dla sektora finansów publicznych.

Art. 36. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 20 – gospodarka, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 553 tys. zł;
2) w 2027 r. – 591 tys. zł;
3) w 2028 r. – 622 tys. zł;
4) w 2029 r. – 655 tys. zł;
5) w 2030 r. – 690 tys. zł;
6) w 2031 r. – 762 tys. zł;
7) w 2032 r. – 763 tys. zł;
8) w 2033 r. – 801 tys. zł;
9) w 2034 r. – 842 tys. zł;
10) w 2035 r. – 884 tys. zł.

2. Minister właściwy do spraw gospodarki monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw gospodarki wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności organu do spraw podmiotów krytycznych dla sektora przestrzeni kosmicznej oraz sektora produkcji, wytwarzania i dystrybucji chemikaliów.

Art. 37. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 21 – gospodarka morska, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 2.028 tys. zł;
2) w 2027 r. – 2.167 tys. zł;
3) w 2028 r. – 2.282 tys. zł;
4) w 2029 r. – 2.403 tys. zł;
5) w 2030 r. – 2.531 tys. zł;
6) w 2031 r. – 2.795 tys. zł;
7) w 2032 r. – 2.799 tys. zł;
8) w 2033 r. – 2.939 tys. zł;
9) w 2034 r. – 3.086 tys. zł;
10) w 2035 r. – 3.240 tys. zł.

2. Minister właściwy do spraw gospodarki morskiej monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw gospodarki morskiej wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności organu do spraw podmiotów krytycznych podsektora transportu wodnego oraz realizacji zadań Centrum Bezpieczeństwa Morskiego.

Art. 38. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 22 – gospodarka wodna, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 553 tys. zł;
2) w 2027 r. – 591 tys. zł;
3) w 2028 r. – 622 tys. zł;
4) w 2029 r. – 655 tys. zł;
5) w 2030 r. – 690 tys. zł;
6) w 2031 r. – 762 tys. zł;
7) w 2032 r. – 763 tys. zł;
8) w 2033 r. – 801 tys. zł;
9) w 2034 r. – 842 tys. zł;
10) w 2035 r. – 884 tys. zł.

2. Minister właściwy do spraw gospodarki wodnej monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw gospodarki wodnej wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności organu do spraw podmiotów krytycznych dla sektora wody pitnej oraz sektora ścieków.

Art. 39. 1.Maksymalny limit wydatków z budżetu państwa dla części budżetowej 27 – informatyzacja, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 2.797 tys. zł;
2) w 2027 r. – 1.467 tys. zł;
3) w 2028 r. – 1.534 tys. zł;

4) w 2029 r. – 1.603 tys. zł;
5) w 2030 r. – 1.677 tys. zł;
6) w 2031 r. – 1.813 tys. zł;
7) w 2032 r. – 1.831 tys. zł;
8) w 2033 r. – 1.912 tys. zł;
9) w 2034 r. – 1.996 tys. zł;
10) w 2035 r. – 2.085 tys. zł.

2. Minister właściwy do spraw informatyzacji monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw informatyzacji wdraża mechanizm korygujący polegający na:

1) ograniczeniu finansowania organu do spraw podmiotów krytycznych dla sektora infrastruktura cyfrowa oraz sektora zarządzanie usługami ICT;
2) wykazu podmiotów krytycznych prowadzonego w systemie, o którym mowa w art. 46 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Art. 40. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 32 – rolnictwo, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 553 tys. zł;
2) w 2027 r. – 591 tys. zł;
3) w 2028 r. – 622 tys. zł;
4) w 2029 r. – 655 tys. zł;
5) w 2030 r. – 690 tys. zł;
6) w 2031 r. – 762 tys. zł;
7) w 2032 r. – 763 tys. zł;
8) w 2033 r. – 801 tys. zł;
9) w 2034 r. – 842 tys. zł;
10) w 2035 r. – 884 tys. zł.

2. Minister właściwy do spraw rolnictwa monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok

budżetowy limitu wydatków minister właściwy do spraw rolnictwa wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności organu do spraw podmiotów krytycznych dla sektora produkcji, przetwarzania i dystrybucji żywności.

Art. 41. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 37 – sprawiedliwość, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 184 tys. zł;
2) w 2027 r. – 197 tys. zł;
3) w 2028 r. – 207 tys. zł;
4) w 2029 r. – 218 tys. zł;
5) w 2030 r. – 230 tys. zł;
6) w 2031 r. – 254 tys. zł;
7) w 2032 r. – 254 tys. zł;
8) w 2033 r. – 267 tys. zł;
9) w 2034 r. – 281 tys. zł;
10) w 2035 r. – 295 tys. zł.

2. Minister Sprawiedliwości monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków Minister Sprawiedliwości wdraża mechanizm korygujący polegający na ograniczeniu finansowania realizacja zadań.

Art. 42. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 39 – transport, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 553 tys. zł;
2) w 2027 r. – 591 tys. zł;
3) w 2028 r. – 622 tys. zł;
4) w 2029 r. – 655 tys. zł;
5) w 2030 r. – 690 tys. zł;
6) w 2031 r. – 762 tys. zł;
7) w 2032 r. – 763 tys. zł;
8) w 2033 r. – 801 tys. zł;
9) w 2034 r. – 842 tys. zł;

10) w 2035 r. – 884 tys. zł.

2. Minister właściwy do spraw transportu monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw transportu wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności organu do spraw podmiotów krytycznych dla sektora transportu z wyłączeniem podsektora transportu wodnego.

Art. 43. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 42 – sprawy wewnętrzne, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 10.835 tys. zł;
2) w 2027 r. – 8.412 tys. zł;
3) w 2028 r. – 8.837 tys. zł;
4) w 2029 r. – 9.282 tys. zł;
5) w 2030 r. – 9.751 tys. zł;
6) w 2031 r. – 10.655 tys. zł;
7) w 2032 r. – 10.735 tys. zł;
8) w 2033 r. – 11.251 tys. zł;
9) w 2034 r. – 11.791 tys. zł;
10) w 2035 r. – 12.358 tys. zł;

2. Minister właściwy do spraw wewnętrznych monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw wewnętrznych wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności Centrum w zakresie:

1) prowadzenia Pojedynczego Punktu Kontaktowego;
2) prowadzenia wykazu infrastruktury krytycznej oraz wykazu potencjalnej infrastruktury krytycznej;
3) prowadzenia wykazu podmiotów krytycznych.

Wdrożenie mechanizmu korygującego następuje w uzgodnieniu z Prezesem Rady Ministrów.

Art. 44. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 46 – zdrowie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 553 tys. zł;
2) w 2027 r. – 591 tys. zł;
3) w 2028 r. – 622 tys. zł;
4) w 2029 r. – 655 tys. zł;
5) w 2030 r. – 690 tys. zł;
6) w 2031 r. – 762 tys. zł;
7) w 2032 r. – 763 tys. zł;
8) w 2033 r. – 801 tys. zł;
9) w 2034 r. – 842 tys. zł;
10) w 2035 r. – 884 tys. zł.

2. Minister właściwy do spraw zdrowia monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw zdrowia wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności organu do spraw podmiotów krytycznych dla sektora ochrony zdrowia.

Art. 45. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 47 – energia, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 553 tys. zł;
2) w 2027 r. – 591 tys. zł;
3) w 2028 r. – 622 tys. zł;
4) w 2029 r. – 655 tys. zł;
5) w 2030 r. – 690 tys. zł;
6) w 2031 r. – 762 tys. zł;
7) w 2032 r. – 763 tys. zł;
8) w 2033 r. – 801 tys. zł;
9) w 2034 r. – 842 tys. zł;
10) w 2035 r. – 884 tys. zł.

2. Minister właściwy do spraw energii monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec

każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw energii wdraża mechanizm korygujący polegający na ograniczeniu finansowania organu do spraw podmiotów krytycznych dla sektora energii z wyłączeniem podsektorach wydobywania kopalin, ropy i paliw, gazu, energetyki jądrowej oraz wodoru.

Art. 46. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 48 – gospodarka surowcami energetycznymi, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 553 tys. zł;
2) w 2027 r. – 591 tys. zł;
3) w 2028 r. – 622 tys. zł;
4) w 2029 r. – 655 tys. zł;
5) w 2030 r. – 690 tys. zł;
6) w 2031 r. – 762 tys. zł;
7) w 2032 r. – 763 tys. zł;
8) w 2033 r. – 801 tys. zł;
9) w 2034 r. – 842 tys. zł;
10) w 2035 r. – 884 tys. zł.

2. Minister właściwy do spraw gospodarki surowcami energetycznymi monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw gospodarki surowcami energetycznymi energii wdraża mechanizm korygujący polegający na ograniczeniu finansowania organu do spraw podmiotów krytycznych w podsektorach wydobywania kopalin, ropy i paliw, gazu, energetyki jądrowej oraz wodoru.

Art. 47. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 51 – klimat, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 553 tys. zł;
2) w 2027 r. – 591 tys. zł;
3) w 2028 r. – 622 tys. zł;

4) w 2029 r. – 655 tys. zł;
5) w 2030 r. – 690 tys. zł;
6) w 2031 r. – 762 tys. zł;
7) w 2032 r. – 763 tys. zł;
8) w 2033 r. – 801 tys. zł;
9) w 2034 r. – 842 tys. zł;
10) w 2035 r. – 884 tys. zł.

2. Minister właściwy do spraw klimatu monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw klimatu wdraża mechanizm korygujący polegający na ograniczeniu finansowania organu do spraw podmiotów krytycznych dla sektora gospodarowania odpadami.

Art. 48. 1.Maksymalny limit wydatków z budżetu państwa dla części budżetowej 69 – żegluga śródlądowa, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:
1) w 2026 r. – 553 tys. zł;
2) w 2027 r. – 591 tys. zł;
3) w 2028 r. – 622 tys. zł;
4) w 2029 r. – 655 tys. zł;
5) w 2030 r. – 690 tys. zł;
6) w 2031 r. – 762 tys. zł;
7) w 2032 r. – 763 tys. zł;
8) w 2033 r. – 801 tys. zł;
9) w 2034 r. – 842 tys. zł;
10) w 2035 r. – 884 tys. zł.

2. Minister właściwy do spraw żeglugi śródlądowej monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw klimatu wdraża mechanizm korygujący polegający na ograniczeniu finansowania organu do spraw podmiotów krytycznych dla podsektora transportu wodnego.

Art. 49. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 76 – Urząd Komunikacji Elektronicznej, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 553 tys. zł;
2) w 2027 r. – 591 tys. zł;
3) w 2028 r. – 622 tys. zł;
4) w 2029 r. – 655 tys. zł;
5) w 2030 r. – 690 tys. zł;
6) w 2031 r. – 762 tys. zł;
7) w 2032 r. – 763 tys. zł;
8) w 2033 r. – 801 tys. zł;
9) w 2034 r. – 842 tys. zł;
10) w 2035 r. – 884 tys. zł.

2. Prezes Urzędu Komunikacji Elektronicznej monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków Prezes Urzędu Komunikacji Elektronicznej wdraża mechanizm korygujący polegający na ograniczeniu finansowania organu do spraw podmiotów krytycznych dla sektora usług pocztowych.

Art. 50. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej:

1) 85/02 – województwo dolnośląskie,
2) 85/04 – województwo kujawsko-pomorskie,
3) 85/06 – województwo lubelskie,
4) 85/08 – województwo lubuskie,
5) 85/10 – województwo łódzkie,
6) 85/12 – województwo małopolskie,
7) 85/14 – województwo mazowieckie,
8) 85/16 – województwo opolskie,
9) 85/18 – województwo podkarpackie,
10) 85/20 – województwo podlaskie,
11) 85/22 – województwo pomorskie,
12) 85/24 – województwo śląskie,

13) 85/26 – województwo świętokrzyskie,
14) 85/28 – województwo warmińsko-mazurskie,
15) 85/30 – województwo wielkopolskie,
16) 85/32 – województwo zachodniopomorskie

- będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 6.436 tys. zł;
2) w 2027 r. – 6.697 tys. zł;
3) w 2028 r. – 7.055 tys. zł;
4) w 2029 r. – 7.429 tys. zł;
5) w 2030 r. – 7.823 tys. zł;
6) w 2031 r. – 8.806 tys. zł;
7) w 2032 r. – 8.650 tys. zł;
8) w 2033 r. – 9.083 tys. zł;
9) w 2034 r. – 9.538 tys. zł;
10) w 2035 r. – 10.014 tys. zł.

2. Właściwy wojewoda monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków właściwy wojewoda wdraża mechanizm korygujący polegający na ograniczeniu finansowania realizacji zadań w zakresie realizacji zadań związanych z identyfikacją infrastruktury krytycznej na terenie województwa oraz wsparciem operatorów infrastruktury krytycznej w zakresie jej ochrony.

Art. 51. Ustawa wchodzi w życie po upływie 14 dni od dnia ogłoszenia.