Dz. U. 2026 poz. 815

USTAWA

z dnia 29 maja 2026 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 2026 r. poz. 574) wprowadza się następujące zmiany:

1) do tytułu ustawy dodaje się odnośnik 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 uchylającą dyrektywę Rady 2008/114/WE (Dz. Urz. UE L 333 z 27.12.2022, str. 164).”;

2) po tytule ustawy dodaje się oznaczenie i tytuł rozdziału 1 w brzmieniu:

„Rozdział 1

Przepisy ogólne”;

3) art. 1 otrzymuje brzmienie:

„Art. 1. 1. Ustawa określa:

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

---

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 uchylającą dyrektywę Rady 2008/114/WE (Dz. Urz. UE L 333 z 27.12.2022, 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 19 października 1991 r. o gospodarowaniu nieruchomościami rolnymi Skarbu Państwa, ustawę z dnia 22 sierpnia 1997 r. o ochronie osób i mienia, 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 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 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych, 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 24 lipca 2015 r. o kontroli niektórych inwestycji, ustawę z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych, ustawę z dnia 20 lipca 2017 r. – Prawo wodne, 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, ustawę z dnia 11 marca 2022 r. o obronie Ojczyzny, ustawę z dnia 7 października 2022 r. o szczególnych rozwiązaniach służących ochronie odbiorców energii elektrycznej w 2023 roku oraz w 2024 roku w związku z sytuacją na rynku energii elektrycznej, ustawę z dnia 7 lipca 2023 r. o przygotowaniu i realizacji inwestycji w zakresie Krajowego Centrum Przetwarzania Danych, ustawę z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej oraz ustawę z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej.

2. Ustawy w zakresie, o którym mowa w ust. 1:

1) pkt 3 i 4, nie stosuje się do organów oraz jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych;

2) 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 2026 r. poz. 490, 421, 638 i 760).";

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 w obsłudze 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;

1b) dostawcy krytycznym – należy przez to rozumieć podmiot dostarczający produkty, usługi lub technologie, których zakłócenie może spowodować incydent istotny u podmiotu krytycznego;

1c) podmiocie krytycznym o szczególnym znaczeniu europejskim – należy przez to rozumieć podmiot krytyczny świadczący co najmniej jedną usługę kluczową lub świadczący te same lub podobne usługi kluczowe na rzecz co najmniej sześciu państw członkowskich Unii Europejskiej lub w co najmniej sześciu państwach członkowskich Unii Europejskiej, uznany za taki podmiot przez Komisję Europejską;

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;

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

1g) incydencie istotnym – należy przez to rozumieć incydent, który powoduje lub może spowodować istotne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej, spełniający progi uznania incydentu za istotny;",

c) pkt 2 otrzymuje brzmienie:

„2) infrastrukturze krytycznej – należy przez to rozumieć obiekt, urządzenie, instalację, sieć, system lub usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy lub usługi 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) 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 lub usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy lub usługi będące na etapie 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) zapewnienia świadczenia 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 lub usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów lub 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 zarządzania kryzysowego;”,

i) uchyla się pkt 9 i 10,

j) w pkt 11 kropkę zastępuje się średnikiem i dodaje się pkt 12–27 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 wraz z jego skutkami, który określa wartość ryzyka;

14) zarządzaniu ryzykiem – należy przez to rozumieć działania polegające na:

a) ocenie ryzyka,

b) planowaniu postępowania z ryzykiem,

c) wdrażaniu postępowania z ryzykiem,

d) osiąganiu gotowości do reagowania w przypadku wystąpienia sytuacji kryzysowej,

e) okresowej ocenie osiągniętych efektów działań, o których mowa w lit. a–d;

15) module zadaniowym – należy przez to rozumieć zestawienie przedsięwzięć i zadań przewidzianych do realizacji w sytuacji kryzysowej przez podmioty wymienione w siatce bezpieczeństwa, z wykorzystaniem sił i środków, którymi dysponują;

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) Grupie do spraw Odporności Podmiotów Krytycznych – należy przez to rozumieć grupę zapewniającą wsparcie Komisji Europejskiej oraz współpracę państwom członkowskim Unii Europejskiej w zakresie budowania odporności podmiotów krytycznych;

20) misji doradczej – należy przez to rozumieć misję organizowaną przez Komisję Europejską w celu zapewnienia podmiotowi krytycznemu wsparcia w zakresie realizacji zadań, o których mowa w rozdziale 11;

21) zagrożeniu hybrydowym – należy przez to rozumieć kombinację wrogich działań realizowanych przy zastosowaniu środków politycznych, gospodarczych, dyplomatycznych, informacyjnych, militarnych lub innych, które nie stanowią zbrojnej napaści, o której mowa w art. 51 Karty Narodów Zjednoczonych;

22) 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;

23) 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, zmieniającego 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 uchylającego decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE (Dz. Urz. UE L 316 z 14.11.2012, str. 12, z późn. zm.[3)]);

24) 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, zmieniającego 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 uchylającego decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE;

25) 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 2025 r. poz. 568) lub upoważnioną do certyfikacji zgodnie z przepisami ustawy z dnia 12 września 2002 r. o normalizacji (Dz. U. z 2015 r. poz. 1483);

26) certyfikacie – należy przez to rozumieć dokument wydany przez jednostkę certyfikującą, potwierdzający, że wyrób, instalacja, system, proces, usługa lub osoba spełniają wymagania właściwego dokumentu normalizacyjnego, o którym mowa w art. 2 pkt 3 ustawy z dnia 12 września 2002 r. o normalizacji;

27) certyfikacji – należy przez to rozumieć działania jednostki certyfikującej wykazujące, że wyrób, instalacja, system, proces, usługa lub osoba spełniają wymagania właściwego dokumentu normalizacyjnego, o którym mowa w art. 2 pkt 3 ustawy z dnia 12 września 2002 r. o normalizacji.”;

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 2–16 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 na poziomie krajowym zagrożenia:

a) stanowiące katastrofę naturalną w rozumieniu art. 3 ust. 1 pkt 2 ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz. U. z 2025 r. poz. 112) lub awarię techniczną w rozumieniu art. 3 ust. 1 pkt 3 tej ustawy,

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 zagrożeń, o których mowa w pkt 1.

[3)] Zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 323 z 19.12.2022, str. 1 oraz Dz. Urz. UE L 135 z 23.05.2023, str. 1.

3. Przy opracowaniu oceny ryzyka, o której mowa w ust. 2 pkt 3, 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) ocenę ryzyka przeprowadzoną na podstawie art. 6 ust. 1 decyzji Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (Dz. Urz. UE L 347 z 20.12.2013, str. 924, z późn. zm.[4)]);

4) dane o stratach i szkodach spowodowanych przez zagrożenia, o których mowa 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. Przy opracowaniu oceny ryzyka, o której mowa w ust. 2 pkt 3, w odniesieniu do podmiotów krytycznych uwzględnia się dodatkowo:

1) wykaz usług kluczowych, o którym mowa w przepisach wydanych 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, o których mowa w załączniku do ustawy;

5) zależność ciągłości działania usług kluczowych od funkcjonowania podmiotów znajdujących się w innych państwach członkowskich Unii Europejskiej i państwach trzecich;

6) wpływ znaczącego zakłócenia w jednym z sektorów, o których mowa w załączniku do ustawy, na inne sektory, o których mowa w tym załączniku, w tym wszelkie istotne czynniki ryzyka dla obywateli i rynku wewnętrznego;

7) 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 uwzględniające elementy, o których mowa w ust. 3 i 4.

7. Dyrektor Centrum przekazuje wytyczne do opracowania projektu KOR:

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 podmiotom, jeżeli jest to konieczne.

8. W zakresie swojej właściwości organy i podmioty, o których mowa w ust. 7, uwzględniając wytyczne przekazane przez dyrektora Centrum, opracowują propozycje do ujęcia w projekcie KOR.

9. Propozycje do ujęcia w projekcie KOR wraz z danymi stanowiącymi podstawę do ich przygotowania, z wyłączeniem informacji niejawnych, organy i podmioty, o których mowa w ust. 7, przekazują dyrektorowi Centrum we wskazanym przez niego terminie.

10. Dyrektor Centrum może wystąpić do organów i podmiotów, o których mowa w ust. 7, o przekazanie dodatkowych propozycji do ujęcia w projekcie KOR, jeżeli uzna, że ich umieszczenie w KOR jest niezbędne. Wystąpienie wymaga uzasadnienia.

11. Propozycje do ujęcia w projekcie KOR przekazane przez ministra kierującego działem administracji rządowej uwzględniają wkład do propozycji do ujęcia w projekcie KOR 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 temu ministrowi wkład do propozycji do ujęcia w projekcie KOR ministra kierującego działem administracji rządowej.

---

4) Zmiany wymienionej decyzji zostały ogłoszone w Dz. Urz. UE L 250 z 04.10.2018, str. 1, Dz. Urz. UE L 77I z 20.03.2019, str. 1, Dz. Urz. UE L 117 z 15.04.2020, str. 3, Dz. Urz. UE L 185 z 26.05.2021, str. 1 oraz Dz. Urz. UE L 2023/2671 z 28.11.2023.

13. Dyrektor Centrum przedkłada Radzie Ministrów projekt KOR nierzadziej niż raz na 3 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 krajowej oceny ryzyka, o której mowa w art. 6 ust. 1 lit. a decyzji Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności.

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 3 miesięcy od dnia przyjęcia KOR przez Radę Ministrów.

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

2. KSOPK:

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 do spraw podmiotów krytycznych,
   b) ministrów kierujących działami administracji rządowej, którzy identyfikują infrastrukturę krytyczną,
   c) Komisję Nadzoru Finansowego, która identyfikuje infrastrukturę krytyczną,
   d) wojewodów, którzy identyfikują infrastrukturę krytyczną,
   e) inne podmioty zaangażowane we wdrażanie i realizację KSOPK;
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 organy, o których mowa w pkt 2 lit. a–d,
   d) środków mających na celu ułatwienie realizacji zadań, o których mowa w rozdziale 11, przez małe i średnie przedsiębiorstwa, o których mowa w art. 2 ust. 1 załącznika I do rozporządzenia Komisji (UE) nr 651/2014 z dnia 17 czerwca 2014 r. uznającego niektóre rodzaje pomocy za zgodne z rynkiem wewnętrznym w zastosowaniu art. 107 i 108 Traktatu (Dz. Urz. UE L 187 z 26.06.2014, str. 1, z późn. zm.[5)]), 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 art. 41 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20, 252 i 815).

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

4. Dyrektor Centrum przekazuje wytyczne do opracowania projektu KSOPK:

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 podmiotom, jeżeli jest to konieczne.

---

5) Zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 329 z 15.12.2015, str. 28, Dz. Urz. UE L 149 z 07.06.2016, str. 10, Dz. Urz. UE L 156 z 20.06.2017, str. 1, Dz. Urz. UE L 26 z 31.01.2018, str. 53, Dz. Urz. UE L 215 z 07.07.2020, str. 3, Dz. Urz. UE L 89 z 16.03.2021, str. 1, Dz. Urz. UE L 270 z 29.07.2021, str. 39, Dz. Urz. UE L 119 z 05.05.2023, str. 159, Dz. Urz. UE L 167 z 30.06.2023, str. 1 oraz Dz. Urz. UE L 2025/90138 z 13.02.2025.

5. W zakresie swojej właściwości organy i podmioty, o których mowa w ust. 4, uwzględniając wytyczne przekazane przez dyrektora Centrum, opracowują propozycje do ujęcia w projekcie KSOPK.

6. Propozycje do ujęcia w projekcie KSOPK wraz z danymi stanowiącymi podstawę do ich przygotowania, z wyłączeniem informacji niejawnych, organy i podmioty, o których mowa w ust. 4, przekazują dyrektorowi Centrum we wskazanym przez niego terminie.

7. Dyrektor Centrum może wystąpić do organów i podmiotów, o których mowa w ust. 4, o przekazanie dodatkowych propozycji do ujęcia w projekcie KSOPK, jeżeli uzna, że ich umieszczenie w KSOPK jest niezbędne. Wystąpienie wymaga uzasadnienia.

8. Propozycje do ujęcia w projekcie KSOPK przekazane przez ministra kierującego działem administracji rządowej uwzględniają wkład do propozycji do ujęcia w projekcie KSOPK kierownika urzędu centralnego podległego temu ministrowi lub przez niego nadzorowanego.

9. Kierownik urzędu centralnego podległy ministrowi kierującemu działem administracji rządowej lub przez niego nadzorowany opracowuje i przekazuje temu ministrowi wkład do propozycji do ujęcia w projekcie KSOPK ministra kierującego działem administracji rządowej.

10. Dyrektor Centrum udostępnia opracowany projekt KSOPK na stronie podmiotowej Biuletynu Informacji Publicznej Centrum.

11. Dyrektor Centrum kieruje projekt KSOPK do 30-dniowych konsultacji publicznych, z przeprowadzenia których sporządza raport, wskazując główne tezy zawarte w stanowiskach zgłoszonych do projektu KSOPK 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 KSOPK raz na 3 lata.

14. Dyrektor Centrum udostępnia Komisji Europejskiej KSOPK niepóźniej niż w terminie 3 miesięcy od dnia przyjęcia KSOPK przez Radę Ministrów.

15. Przepisy ust. 3–12 i 14 stosuje się do aktualizacji KSOPK.

16. Dyrektor Centrum monitoruje wdrażanie postanowień KSOPK 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 współpracy podmiotów wymienionych w siatce bezpieczeństwa;
3) listę działań na rzecz ograniczenia ryzyka wystąpienia zidentyfikowanych zagrożeń 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,
   f) danych o stratach powstałych na skutek wystąpienia zagrożeń.

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 przez którego jest 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 opracowuje się z uwzględnieniem zagrożeń wskazanych w KOR.

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

5. W planach zarządzania ryzykiem, 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 do opracowania projektu KPZR:

1) ministrom kierującym działami administracji rządowej;

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

3) wojewodom;

4) innym podmiotom, jeżeli jest to konieczne.

3. W zakresie swojej właściwości organy i podmioty, o których mowa w ust. 2, uwzględniając wytyczne przekazane przez dyrektora Centrum, opracowują propozycje do ujęcia w projekcie KPZR.

4. Propozycje do ujęcia w projekcie KPZR wraz z danymi stanowiącymi podstawę do ich przygotowania, z wyłączeniem informacji niejawnych, organy i podmioty, o których mowa w ust. 2, przekazują dyrektorowi Centrum we wskazanym przez niego terminie.

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

6. Propozycje do ujęcia w projekcie KPZR przekazane przez ministra kierującego działem administracji rządowej uwzględniają wkład do propozycji do ujęcia w projekcie KPZR kierownika urzędu centralnego podległego temu ministrowi lub przez niego nadzorowanego.

7. Kierownik urzędu centralnego podległy ministrowi kierującemu działem administracji rządowej lub przez niego nadzorowany opracowuje i przekazuje temu ministrowi wkład do propozycji do ujęcia w projekcie KPZR ministra kierującego działem administracji rządowej.

8. Dyrektor Centrum przedkłada Radzie Ministrów projekt KPZR nierzadziej niż raz na 3 lata. Rada Ministrów przyjmuje KPZR w drodze uchwały.

9. Dyrektor Centrum, na podstawie KPZR, opracowuje i udostępnia Komisji Europejskiej streszczenie istotnych elementów krajowej oceny zdolności zarządzania ryzykiem, o której mowa w art. 6 ust. 1 lit. b decyzji Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności.

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

2. Minister kierujący działem administracji rządowej, w zakresie swojej właściwości, wskazuje kierownika urzędu centralnego podległego temu ministrowi lub przez niego nadzorowanego, który jest obowiązany do opracowania 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 oraz Szef Centralnego Biura Antykorupcyjnego:

1) uzgadniają projekt planu zarządzania ryzykiem z dyrektorem Centrum pod względem spójności z KPZR;

2) zatwierdzają uzgodniony plan zarządzania ryzykiem;

3) przekazują 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 przekazuje:

1) projekt wojewódzkiego planu zarządzania ryzykiem do zatwierdzenia ministrowi właściwemu do spraw administracji publicznej;
2) kopię zatwierdzonego wojewódzkiego planu 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 przez którego jest 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 KOR 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 podmiotów wymienionych w siatce bezpieczeństwa w zakresie reagowania w przypadku wystąpienia sytuacji kryzysowej oraz usuwania jej skutków;
2) opis zasad współpracy podmiotów, o których mowa w pkt 1, w tym wymiany informacji w relacjach krajowych i międzynarodowych;
3) zestawienie pogrupowanych modułów zadaniowych;
4) załączniki określające:
   a) opis organizacji systemu monitorowania zagrożeń, ostrzegania i alarmowania,
   b) opis organizacji 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 organami, o których mowa w art. 6j ust. 1 pkt 2–5, opracowuje projekt KPRK.

3. Na potrzeby opracowania projektu KPRK dyrektor Centrum wydaje wytyczne do jego opracowania obejmujące elementy, o których mowa w ust. 1.

4. Dyrektor Centrum przekazuje wytyczne do opracowania projektu KPRK organom, o których mowa w art. 6j ust. 1 pkt 2–5.

5. W zakresie swojej właściwości organy, o których mowa w art. 6j ust. 1 pkt 2–5, uwzględniając wytyczne przekazane przez dyrektora Centrum, opracowują propozycje do ujęcia w projekcie KPRK.

6. Propozycje do ujęcia w projekcie KPRK wraz z danymi stanowiącymi podstawę do ich przygotowania, z wyłączeniem informacji niejawnych, organy, o których mowa w art. 6j ust. 1 pkt 2–5, przekazują dyrektorowi Centrum we wskazanym przez niego terminie.

7. Dyrektor Centrum może wystąpić do organów, o których mowa w art. 6j ust. 1 pkt 2–5, o przekazanie dodatkowych propozycji do ujęcia w projekcie KPRK, jeżeli uzna, że ich umieszczenie w KPRK jest niezbędne.

8. Propozycje do ujęcia w projekcie KPRK przekazane przez ministra kierującego działem administracji rządowej uwzględniają wkład do propozycji do ujęcia w projekcie KPRK kierownika urzędu centralnego podległego temu ministrowi lub przez niego nadzorowanego.

9. Kierownik urzędu centralnego podległy ministrowi kierującemu działem administracji rządowej lub przez niego nadzorowany opracowuje i przekazuje temu ministrowi wkład do propozycji do ujęcia w projekcie KPRK ministra kierującego działem administracji rządowej.

10. Dyrektor Centrum przedkłada Radzie Ministrów projekt KPRK nierzadziej niż raz na 3 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 podmiotów wymienionych w siatce bezpieczeństwa w zakresie reagowania w przypadku wystąpienia sytuacji kryzysowej oraz usuwania jej skutków;

2) określenie zadań w zakresie monitorowania zagrożeń;

3) zestawienie pogrupowanych modułów zadaniowych wraz z opisem realizacji zadań ujętych w tych modułach;

4) opis zadań z zakresu ochrony infrastruktury krytycznej lub zapewnienia ciągłości świadczenia usług kluczowych.

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

3. Minister kierujący działem administracji rządowej, w zakresie swojej właściwości, wskazuje kierownika urzędu centralnego podległego temu ministrowi lub przez niego nadzorowanego, który jest obowiązany do opracowania 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 oraz Szef Centralnego Biura Antykorupcyjnego:

1) uzgadniają projekt planu reagowania kryzysowego z dyrektorem Centrum pod względem spójności z KPRK;

2) zatwierdzają uzgodniony plan reagowania kryzysowego;

3) przekazują 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, 2 i 4 oraz art. 6l ust. 1 pkt 2 i 3, w odniesieniu do terenu województwa;

2) zestawienie przedsięwzięć minimalizujących skutki zakłócenia funkcjonowania infrastruktury krytycznej dla ludności na terenie województwa wraz z ich opisem.

2. Wojewoda przekazuje:

1) projekt wojewódzkiego planu reagowania kryzysowego do zatwierdzenia ministrowi właściwemu do spraw administracji publicznej;

2) kopię zatwierdzonego wojewódzkiego planu reagowania kryzysowego do wiadomości dyrektorowi Centrum.

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

1) elementy, o których mowa w art. 6k ust. 1 pkt 1, 2 i 4 oraz art. 6l ust. 1 pkt 2 i 3, w odniesieniu do terenu właściwej jednostki samorządu terytorialnego;

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 aktualizacji w cyklu planowania niedłuższym niż 3 lata.

2. Plany zarządzania kryzysowego uzgadnia się z podmiotami wymienionymi w siatce bezpieczeństwa, w zakresie ich dotyczącym.

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 określić, 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 opracowanymi przez tego ministra.

Rozdział 4

Infrastruktura krytyczna

Art. 6p. Zadania dotyczące infrastruktury krytycznej obejmują:

1) identyfikację 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, w zakresie swojej właściwości, są:

1) ministrowie kierujący działami administracji rządowej;

2) wojewodowie;

3) Komisja Nadzoru Finansowego.

2. Organy, o których mowa w ust. 1, w zakresie identyfikacji infrastruktury krytycznej 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 oraz 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 lub 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 w celu zapewnienia:

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

– prowadzi wykaz infrastruktury krytycznej.

2. Wykaz infrastruktury krytycznej zawiera:

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

3. Wykaz infrastruktury krytycznej jest prowadzony w postaci papierowej lub elektronicznej. Wykaz jest dokumentem niejawnym.

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

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

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

d) kryteria skutków społecznych – oceniane w odniesieniu do wpływu na zaufanie opinii publicznej lub zakłócenia codziennego życia obywateli, w tym utraty dostępu do usług kluczowych,

e) kryteria wpływu międzynarodowego – oceniane w odniesieniu do pogorszenia wizerunku kraju na arenie międzynarodowej lub możliwości realizacji zobowiązań międzynarodowych,

f) kryteria unikatowości – oceniane w odniesieniu do braku możliwości zastąpienia lub odtworzenia w akceptowalnym czasie

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

6. Uchwała, o której mowa w ust. 5, jest dokumentem niejawnym.

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;

4) Narodowy Bank Polski.

2. W przypadku Narodowego Banku Polskiego wpis do wykazu infrastruktury krytycznej obejmuje obiekt, urządzenie, instalację, sieć, system lub usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy lub usługi, których Narodowy Bank Polski jest właścicielem lub posiadaczem, niezbędne do wykonywania zadań Narodowego Banku Polskiego, spełniające co najmniej jedno z kryteriów przekrojowych, o których mowa w art. 6r ust. 5 pkt 2. Do wniosku składanego przez Narodowy Bank Polski o wpis do wykazu infrastruktury krytycznej przepisy art. 6t ust. 5 i 6 stosuje się odpowiednio.

3. 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 lub usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy lub usługi mogące stanowić infrastrukturę krytyczną.

2. W przypadku identyfikacji prowadzonej przez ministra kierującego działem administracji rządowej obiekt, urządzenie, instalacja, sieć, system lub usługa lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy lub 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 lub usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów lub usług o udzielenie informacji, które umożliwią ocenę, czy spełniają one odpowiednie kryteria, o których mowa w art. 6r ust. 5, 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 właściciela lub posiadacza obiektu, urządzenia, instalacji, sieci, systemu lub usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów lub usług.

5. Minister kierujący działem administracji rządowej składa dyrektorowi Centrum wniosek o wpis do wykazu infrastruktury krytycznej zawierający:

1) nazwę i lokalizację obiektu, urządzenia, instalacji, sieci, systemu lub usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów lub usług;

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

6. Wniosek sporządza się i składa się w postaci papierowej. Wniosek jest dokumentem niejawnym.

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

2. W przypadku identyfikacji prowadzonej przez wojewodę obiekt, urządzenie, instalacja, sieć, system lub usługa lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy lub 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. Przepisy 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 lub usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy lub usługi mogące stanowić infrastrukturę krytyczną.

2. W przypadku identyfikacji prowadzonej przez Komisję Nadzoru Finansowego obiekt, urządzenie, instalacja, sieć, system lub usługa lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy lub 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 przekrojowych, o których mowa w art. 6r ust. 5 pkt 2. Przepisy art. 6t ust. 3–6 stosuje się odpowiednio.

Art. 6w. 1. Dyrektor Centrum informuje właściciela lub posiadacza obiektu, urządzenia, instalacji, sieci, systemu lub usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów lub usług o dokonaniu wpisu do wykazu infrastruktury krytycznej oraz obowiązkach wynikających z przepisów rozdziału 7, w terminie 30 dni od dnia wpisu do wykazu.

2. Informacje, o których mowa w ust. 1, dyrektor Centrum przekazuje niezwłocznie organowi składającemu wniosek o wpis do wykazu infrastruktury krytycznej.

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

Rozdział 6
Identyfikowanie potencjalnej infrastruktury krytycznej

Art. 6y. 1. Dyrektor Centrum w celu zapewnienia:

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

– prowadzi wykaz potencjalnej infrastruktury krytycznej.

2. Wykaz potencjalnej infrastruktury krytycznej zawiera:

1) nazwę i lokalizację potencjalnej infrastruktury krytycznej;
2) dane inwestora realizującego obowiązki określone w art. 18 ust. 1 ustawy z dnia 7 lipca 1994 r. – Prawo budowlane (Dz. U. z 2026 r. poz. 524, 605 i 646), prowadzącego prace projektowe lub budowlane dotyczące potencjalnej infrastruktury krytycznej, obejmujące siedzibę i adres oraz numer identyfikacji podatkowej (NIP), jeżeli został nadany, zwanego dalej „inwestorem”;
3) wskazanie organu identyfikującego potencjalną infrastrukturę krytyczną.

3. Wykaz potencjalnej infrastruktury krytycznej jest prowadzony w postaci papierowej lub elektronicznej. Wykaz jest dokumentem niejawnym.

4. Obiekt, urządzenie, instalacja, sieć, system lub usługa lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy lub usługi będące na etapie projektowania lub budowy mogą zostać wpisane do wykazu potencjalnej infrastruktury krytycznej, w przypadku gdy z dokumentacji budowy, o której mowa w art. 3 pkt 13 ustawy z dnia 7 lipca 1994 r. – Prawo budowlane, wynika, że spełnią kryteria, o których mowa w przepisach wydanych na podstawie art. 6r ust. 5.

Art. 6z. 1. 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;
4) Narodowy Bank Polski.

2. W przypadku Narodowego Banku Polskiego wpis do wykazu potencjalnej infrastruktury krytycznej obejmuje obiekt, urządzenie, instalację, sieć, system lub usługę lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy lub usługi, w przypadku gdy z dokumentacji budowy, o której mowa w art. 3 pkt 13 ustawy z dnia

7 lipca 1994 r. – Prawo budowlane, wynika, że spełnią kryteria, o których mowa w przepisach wydanych na podstawie art. 6r ust. 5 pkt 2, a których Narodowy Bank Polski jest inwestorem. Do wniosku składanego przez Narodowy Bank Polski o wpis do wykazu potencjalnej infrastruktury krytycznej przepisy art. 6t ust. 5 i 6 stosuje się odpowiednio.

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

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

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

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

Art. 6zb. 1. Dyrektor Centrum informuje inwestora o dokonaniu wpisu do wykazu potencjalnej infrastruktury krytycznej oraz obowiązkach wskazanych w art. 6zc ust. 2, w terminie 30 dni od dnia wpisu do wykazu.

2. Informacje, o których mowa w ust. 1, dyrektor Centrum przekazuje niezwłocznie organowi składającemu wniosek o wpis do wykazu potencjalnej infrastruktury krytycznej.

Art. 6zc. 1. Organy, o których mowa w art. 6z ust. 1, w zakresie swojej właściwości, we współpracy z dyrektorem Centrum, przedstawiają inwestorowi informacje oraz dokumenty pozwalające na uwzględnienie wymogów dotyczących infrastruktury krytycznej w dokumentacji budowy, o której mowa w art. 3 pkt 13 ustawy z dnia 7 lipca 1994 r. – Prawo budowlane, lub podczas realizacji inwestycji oraz zapewniają bieżącą współpracę w zakresie, o którym mowa w art. 6p.

2. Do obowiązków inwestora w zakresie ochrony potencjalnej infrastruktury krytycznej stosuje się przepisy art. 6ze ust. 1 pkt 1, pkt 2 lit. a, pkt 3 lit. a i pkt 4 oraz art. 6zf ust. 2 pkt 1, pkt 3 lit. a i pkt 4 lit. a.

Art. 6zd. Organy, o których mowa w art. 6z ust. 1, oraz dyrektor Centrum prowadzą bieżącą wymianę informacji dotyczących realizacji czynności w zakresie identyfikacji obiektu, urządzenia, instalacji, sieci, systemu lub usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów lub usług będących na etapie projektowania lub budowy, które mogą zostać wpisane do wykazu potencjalnej infrastruktury krytycznej.

Rozdział 7

Obowiązki operatorów infrastruktury krytycznej

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

1) prowadzenie bieżącej analizy zagrożeń dla infrastruktury krytycznej;
2) wdrażanie adekwatnych do wyników przeprowadzonej analizy zagrożeń, o której mowa w pkt 1, rozwiązań w zakresie:
   a) bezpieczeństwa fizycznego w formie ochrony fizycznej lub zabezpieczeń technicznych uwzględniających systemy kontroli 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 funkcjonalność infrastruktury krytycznej do czasu jej pełnego odtworzenia;
3) bieżącą współpracę z organami zarządzania kryzysowego, służbami, strażami i inspekcjami oraz dyrektorem Centrum przez sporządzanie, przekazywanie oraz 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 lub Szefa Agencji Wywiadu;

5) zapewnienie zdolności do ochrony informacji niejawnych rozumianej jako spełnienie wymagań określonych w przepisach ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2025 r. poz. 1209), zwaną dalej „zdolnością do ochrony informacji niejawnych".

2. Operator infrastruktury krytycznej przeprowadza 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 analizy zagrożeń, o której mowa w ust. 1 pkt 1, a następnie stosownie do potrzeb, w zależności od wyników przeprowadzonej analizy zagrożeń.

4. Rada Ministrów określi, 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 potrzebę podejmowania działań zapewniających bezpieczeństwo infrastruktury krytycznej oraz zapewnienia jednolitości rozwiązań.

5. Operator infrastruktury krytycznej w celu zapewnienia wdrażania rozwiązań, o których mowa w ust. 1 pkt 2, może zawierać umowy. Przy zawieraniu umów operator ochrony infrastruktury krytycznej żąda od usługodawców:

1) certyfikatów, uwzględniając dokumenty 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 z dostępem do informacji niejawnych.

6. Minister, o którym mowa w art. 6t ust. 1, właściwy miejscowo 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 2025 r. poz. 98), mogą opracować i udostępnić na stronie podmiotowej Biuletynu Informacji Publicznej zestawienie certyfikatów lub innych dokumentów zapewniających wdrożenie rozwiązań, o których mowa w ust. 1 pkt 2.

7. Minister, o którym mowa w art. 6t ust. 1, właściwy miejscowo wojewoda, Komisja Nadzoru Finansowego lub Narodowy Bank Polski, 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 i na bieżąco aktualizuje dokumentację ochrony infrastruktury krytycznej.

2. Dokumentacja ochrony infrastruktury krytycznej zawiera:

1) opis infrastruktury krytycznej oraz analizę zagrożeń, o której mowa w art. 6ze ust. 1 pkt 1;

2) opis wdrożonych rozwiązań, o których mowa w art. 6ze ust. 1 pkt 2;

3) opis:

a) zasobów umożliwiających podtrzymanie funkcjonowania infrastruktury krytycznej do czasu jej pełnego odtworzenia,

b) współpracy z organami zarządzania kryzysowego, służbami, strażami 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 opis infrastruktury krytycznej.

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

4. Dokumentacja ochrony infrastruktury krytycznej jest dokumentem niejawnym.

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

1) ministrowi, o którym mowa w art. 6t ust. 1;

2) właściwemu miejscowo wojewodzie;

3) Komisji Nadzoru Finansowego.

6. Operator infrastruktury krytycznej może dołączyć do oświadczenia o opracowaniu dokumentacji ochrony infrastruktury krytycznej informację o braku możliwości wdrożenia rozwiązań, o których mowa w art. 6ze ust. 1 pkt 2, wskazując przyczynę tego braku, 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. 5, oraz dyrektora Centrum.

8. Operator infrastruktury krytycznej, będący jednocześnie podmiotem kluczowym lub ważnym w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, w dokumentacji ochrony infrastruktury krytycznej uwzględnia 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, 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 zagrożeń, 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. Raport o stanie ochrony infrastruktury krytycznej jest dokumentem niejawnym.

Art. 6zh. 1. W przypadku pracownika zatrudnionego na stanowisku umożliwiającym dostęp do informacji o bezpieczeństwie infrastruktury krytycznej i osoby ubiegającej się o zatrudnienie na tym stanowisku operator infrastruktury krytycznej żąda od tego 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, o którym mowa w ust. 1, 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 wpisie do wykazu infrastruktury krytycznej.

3. Zastępca koordynatora infrastruktury krytycznej zastępuje koordynatora infrastruktury krytycznej 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 ochrony infrastruktury krytycznej 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.

9. Operator infrastruktury krytycznej, będący jednocześnie podmiotem kluczowym lub ważnym w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, przekazuje do systemu teleinformatycznego, o którym mowa w art. 46 ust. 1 tej ustawy, dane koordynatora ochrony infrastruktury krytycznej oraz zastępcy koordynatora ochrony infrastruktury krytycznej obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej.

Art. 6zj. 1. Operator infrastruktury krytycznej informuje ministra właściwego do spraw wewnętrznych, będącego operatorem Systemu Bezpiecznej Łączności Państwowej, Prezesa Urzędu Komunikacji Elektronicznej oraz kierownika jednostki organizacyjnej podległej Ministrowi Obrony Narodowej właściwej w sprawach zarządzania częstotliwościami o możliwości zastosowania urządzeń uniemożliwiających telekomunikację na określonym obszarze. Informacja, o której mowa w zdaniu pierwszym, zawiera:

1) nazwę i rodzaj planowanych do zastosowania urządzeń uniemożliwiających telekomunikację na określonym obszarze;

2) parametry techniczne urządzeń uniemożliwiających telekomunikację na określonym obszarze, w tym zakresy częstotliwości pracy, moc promieniowaną w poszczególnych zakresach częstotliwości, rodzaje oraz charakterystyki anten wraz z wysokością ich zawieszenia oraz współrzędnymi miejsca ich zainstalowania, a także sektory planowanego oddziaływania urządzeń.

2. W celu zapewnienia ochrony infrastruktury krytycznej operator infrastruktury krytycznej w przypadkach, o których mowa w:

1) art. 156ze ust. 1 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze (Dz. U. z 2025 r. poz. 1431 i 1668 oraz z 2026 r. poz. 176 i 607), lub

2) art. 28a ust. 1 ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2024 r. poz. 597 oraz z 2026 r. poz. 815), lub

3) art. 11 pkt 17 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2026 r. poz. 244, 737 i 815)

– może podjąć decyzję o dopuszczalności zastosowania urządzeń, o których mowa w ust. 1, przez czas niezbędny do wykonywania czynności przez pracowników ochrony specjalistycznych uzbrojonych formacji ochronnych, z uwzględnieniem konieczności minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych.

3. O zastosowaniu urządzeń, o których mowa w ust. 1, operator infrastruktury krytycznej niezwłocznie informuje ministra właściwego do spraw wewnętrznych, będącego operatorem Systemu Bezpiecznej Łączności Państwowej, Prezesa Urzędu Komunikacji Elektronicznej oraz kierownika jednostki organizacyjnej podległej Ministrowi Obrony Narodowej właściwej w sprawach zarządzania częstotliwościami.

4. Jeżeli jest to niezbędne dla zapewnienia funkcjonowania Systemu Bezpiecznej Łączności Państwowej lub zapewnienia bezpieczeństwa wewnętrznego i porządku publicznego państwa, minister właściwy do spraw wewnętrznych może nakazać operatorowi infrastruktury krytycznej zaprzestanie stosowania urządzeń, o których mowa w ust. 1, lub zmianę sposobu ich wykorzystywania, o czym informuje dyrektora Centrum.

5. Jeżeli jest to niezbędne dla zapewnienia obronności i bezpieczeństwa państwa, Minister Obrony Narodowej może nakazać operatorowi infrastruktury krytycznej zaprzestanie stosowania urządzeń, o których mowa w ust. 1, lub zmianę sposobu ich wykorzystywania, o czym informuje dyrektora Centrum oraz właściwego komendanta wojewódzkiego Policji.

6. Minister Obrony Narodowej może powierzyć realizację zadania, o którym mowa w ust. 5, kierownikowi komórki organizacyjnej lub jednostki organizacyjnej podległej Ministrowi Obrony Narodowej lub przez niego nadzorowanej właściwej w sprawach zarządzania częstotliwościami.

Rozdział 8

Organy do spraw podmiotów krytycznych

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

1) 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) transportu:
   a) minister właściwy do spraw transportu w podsektorach:
      – transportu lotniczego,
      – transportu kolejowego,
      – transportu publicznego,
      – transportu drogowego,
   b) minister właściwy do spraw gospodarki morskiej oraz minister właściwy do spraw żeglugi śródlądowej w podsektorze transportu wodnego;

3) bankowości i infrastruktury rynków finansowych – Komisja Nadzoru Finansowego;

4) ochrony zdrowia – minister właściwy do spraw zdrowia;

5) zaopatrzenia w wodę pitną i jej dystrybucji oraz sektora zbiorowego odprowadzania ścieków – minister właściwy do spraw gospodarki wodnej;

6) infrastruktury cyfrowej:

   a) minister właściwy do spraw informatyzacji – w podsektorze infrastruktury cyfrowej, z wyłączeniem komunikacji elektronicznej,

   b) Prezes Urzędu Komunikacji Elektronicznej – w podsektorze komunikacji elektronicznej;

7) administracji publicznej:

   a) minister właściwy do spraw administracji publicznej – w podsektorze podmiotów publicznych,

   b) minister właściwy do spraw finansów publicznych – w podsektorze finansów publicznych;

8) przestrzeni kosmicznej – minister właściwy do spraw gospodarki;

9) produkcji, przetwarzania i dystrybucji żywności – minister właściwy do spraw rolnictwa;

10) zarządzania usługami ICT – minister właściwy do spraw informatyzacji;

11) produkcji, wytwarzania i dystrybucji chemikaliów – minister właściwy do spraw gospodarki;

12) usług pocztowych – Prezes Urzędu Komunikacji Elektronicznej;

13) gospodarowania odpadami – minister właściwy do spraw klimatu.

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 względem uznania ich za podmiot krytyczny w danym sektorze lub podsektorze;

2) prowadzi bieżącą analizę podmiotów krytycznych w danym sektorze lub podsektorze pod względem niespełniania warunków kwalifikujących dany podmiot jako podmiot krytyczny;

3) składa wnioski o dokonanie wpisu do wykazu podmiotów krytycznych oraz wykreślenia z tego wykazu;

4) prowadzi bieżącą wymianę informacji z podmiotami krytycznymi oraz ułatwia dobrowolną wymianę informacji między podmiotami krytycznymi w danym sektorze lub podsektorze;

5) współpracuje z podmiotami krytycznymi w danym sektorze lub podsektorze w zakresie obsługi incydentów;

6) monitoruje stosowanie przepisów ustawy przez podmioty krytyczne;

7) prowadzi kontrole podmiotów krytycznych;

8) prowadzi działania informacyjne dotyczące dobrych praktyk, działań edukacyjnych i kampanii na rzecz poszerzania wiedzy i budowania odporności podmiotów krytycznych;

9) uczestniczy w planowaniu i organizowaniu ćwiczeń podmiotów krytycznych oraz w razie potrzeby bierze w nich udział;

10) współpracuje z innymi organami do spraw podmiotów krytycznych oraz organami właściwymi do spraw cyberbezpieczeństwa, o których mowa w art. 41 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;

11) współpracuje, za pośrednictwem Pojedynczego Punktu Kontaktowego, z odpowiednimi organami państw członkowskich Unii Europejskiej;

12) nakłada kary pieniężne na podmioty krytyczne.

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 2 lata Komisji Europejskiej oraz Grupie do spraw Odporności Podmiotów Krytycznych sprawozdań dotyczących incydentów istotnych zgłaszanych przez podmioty krytyczne mających wpływ na ciągłość świadczonych przez nie usług kluczowych na terytorium Rzeczypospolitej Polskiej oraz ciągłość świadczonych usług kluczowych w państwach członkowskich Unii Europejskiej;

4) zapewnienie reprezentacji Rzeczypospolitej Polskiej w Grupie do spraw Odporności Podmiotów Krytycznych;

5) zapewnienie współpracy z Komisją Europejską w obszarze bezpieczeństwa świadczenia usług kluczowych;

6) koordynacja współpracy między organami do spraw podmiotów krytycznych a 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 Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającej dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80, z późn. zm.[6)]), oraz organów właściwych do spraw cyberbezpieczeństwa, o których mowa w art. 41 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;

8) współpraca z Pojedynczym Punktem Kontaktowym, o którym mowa w art. 4 pkt 18 ustawy 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 Unii Europejskiej;

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 państwach 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) 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 2 lata informacje umożliwiające ocenę wdrażania dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylającej dyrektywę Rady 2008/114/WE (Dz. Urz. UE L 333 z 27.12.2022, str. 164) 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;

6) Zmiana wymienionej dyrektywy została ogłoszona w Dz. Urz. UE L 2025/90884 z 06.11.2025.

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 Unii Europejskiej, w przypadku gdy podmioty krytyczne:

1) korzystają z infrastruktury krytycznej, która jest fizycznie połączona na terytorium co najmniej dwóch państw członkowskich Unii Europejskiej;

2) są częścią struktur przedsiębiorstw połączonych lub powiązanych z podmiotami krytycznymi w innych państwach członkowskich Unii Europejskiej;

3) zostały zidentyfikowane jako podmioty krytyczne w jednym państwie członkowskim Unii Europejskiej i świadczą usługi kluczowe na rzecz innych państw członkowskich Unii Europejskiej lub w innych państwach członkowskich Unii Europejskiej.

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 w celu zapewnienia:

1) identyfikacji podmiotów krytycznych,

2) prowadzenia czynności nadzorczych nad podmiotami krytycznymi

– prowadzi wykaz podmiotów krytycznych.

2. Wykaz podmiotów krytycznych zawiera dane podmiotów krytycznych obejmujące:

1) nazwę (firmę);

2) siedzibę i adres oraz adres do doręczeń elektronicznych;

3) numer identyfikacji podatkowej (NIP), jeżeli został nadany;

4) nazwę świadczonej usługi kluczowej;

5) wskazanie sektora, podsektora i kategorii podmiotu, o których mowa w załączniku do ustawy;

6) dane pełnomocnika bezpieczeństwa usługi kluczowej oraz zastępcy pełnomocnika bezpieczeństwa usługi kluczowej obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej;

7) datę rozpoczęcia świadczenia usługi kluczowej;

8) informację, w których państwach członkowskich Unii Europejskiej podmiot został uznany za podmiot świadczący usługę kluczową;

9) datę zakończenia świadczenia usługi kluczowej;

10) datę wykreślenia z wykazu podmiotów krytycznych.

3. Wykaz podmiotów krytycznych jest prowadzony w systemie, 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 z 2025 r. poz. 1844) oraz ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. z 2023 r. poz. 1524).

5. Dane, o których mowa w ust. 2, organ do spraw podmiotów krytycznych udostępnia, na wniosek:

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 art. 41 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa

– w zakresie niezbędnym do realizacji ich ustawowych zadań.

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

1) prowadzi działalność w sektorze lub podsektorze, o którym mowa w załączniku do ustawy;

2) świadczy co najmniej jedną usługę kluczową;

3) posiada infrastrukturę krytyczną na terytorium Rzeczypospolitej Polskiej lub na obszarach morskich Rzeczypospolitej Polskiej, o których mowa w art. 2 ust. 1 ustawy z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej (Dz. U. z 2024 r. poz. 1125, z 2025 r. poz. 409, 1535 i 1668 oraz z 2026 r. poz. 252);

4) 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 4, jest określana na podstawie progów istotności skutku zakłócającego dla świadczenia usług kluczowych określonych w przepisach wydanych na podstawie ust. 3.

3. Rada Ministrów określi, w drodze rozporządzenia, wykaz usług kluczowych w podziale na sektory, podsektory i kategorie podmiotów, o których mowa w załączniku do ustawy, oraz progi istotności skutku zakłócającego dla świadczenia usług kluczowych, wymienionych w wykazie usług kluczowych, w zależności od:

1) liczby użytkowników zależnych od usługi kluczowej świadczonej przez ten podmiot;

2) stopnia, w jakim inne sektory lub podsektory, o których mowa w załączniku do ustawy, są zależne od usługi świadczonej przez ten podmiot;

3) wpływu, jaki incydent – jeżeli chodzi o jego skalę i czas trwania – mógłby mieć na działalność gospodarczą i społeczną, środowisko naturalne, bezpieczeństwo publiczne lub na zdrowie ludności;

4) udziału tego podmiotu w rynku w odniesieniu do świadczonej usługi kluczowej;

5) obszaru geograficznego, którego mógłby dotyczyć incydent, biorąc pod uwagę wpływ transgraniczny oraz stopień odizolowania geograficznego;

6) znaczenia podmiotu w utrzymywaniu wystarczającego poziomu świadczenia usługi kluczowej przy uwzględnieniu dostępności alternatywnych sposobów jej świadczenia;

7) innych czynników charakterystycznych dla danego sektora lub podsektora, o którym mowa w załączniku do ustawy, jeżeli występują.

4. W rozporządzeniu, o którym mowa w ust. 3, Rada Ministrów określi co najmniej jeden próg istotności skutku zakłócającego dla świadczenia danej usługi kluczowej, 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. Przed dokonaniem wpisu do wykazu podmiotów krytycznych organ do spraw podmiotów krytycznych występuje do operatora infrastruktury krytycznej o:

1) udzielenie informacji, które umożliwią wstępną ocenę, czy ten operator spełnia warunki, o których mowa w art. 6zp ust. 1;

2) wskazanie infrastruktury krytycznej niezbędnej do świadczenia usługi kluczowej, z uwzględnieniem infrastruktury krytycznej innego operatora infrastruktury krytycznej;

3) wskazanie niezbędnego obiektu, urządzenia, instalacji, sieci, systemu lub usługi lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji, sieci, systemów lub usług, których właściciel lub posiadacz nie jest operatorem infrastruktury krytycznej.

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 niekrótszy niż 14 dni, licząc od dnia otrzymania tego wystąpienia przez operatora infrastruktury krytycznej.

3. Operator infrastruktury krytycznej przekazuje organowi do spraw podmiotów krytycznych informacje żądane w wystąpieniu, o którym mowa w ust. 1, w terminie, o którym mowa w ust. 2 pkt 2.

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 1–5 oraz 7 i 8.

2. Wpis operatora infrastruktury krytycznej do wykazu podmiotów krytycznych dokonuje się automatycznie z chwilą złożenia wniosku w systemie, 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, niepóźniej jednak niż w terminie 30 dni, informuje operatora infrastruktury krytycznej o dokonaniu 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, o którym mowa w art. 41 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

5. Dyrektor Centrum może weryfikować dane zawarte we wpisie do wykazu podmiotów krytycznych ze stanem faktycznym z urzędu lub na wniosek organu do spraw podmiotów krytycznych.

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

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 podmiotów krytycznych, zawierający dane, o których mowa w art. 6zo ust. 2 pkt 1–9.

3. Wykreślenie podmiotu krytycznego z wykazu podmiotów krytycznych dokonuje się automatycznie z chwilą złożenia wniosku w systemie, 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, niepóźniej jednak niż w terminie 30 dni, informuje podmiot krytyczny o wykreśleniu z wykazu podmiotów krytycznych 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, o którym mowa w art. 41 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

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

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

Rozdział 11

Obowiązki podmiotów krytycznych

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

1) przeprowadzenie nierzadziej niż raz na 2 lata oceny ryzyka z uwzględnieniem:
   a) zagrożeń i związanych z tym ryzyk wymienionych w KOR oraz innych zagrożeń charakterystycznych dla świadczonej usługi kluczowej, w tym zagrożeń antagonistycznych,
   b) stopnia zależności innych sektorów lub podsektorów, o których mowa 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 uzasadnionych 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 zakresie:
   a) polityk zarządzania ryzykiem,
   b) bezpieczeństwa fizycznego w formie ochrony fizycznej budynków i terenów należących do podmiotu krytycznego lub ich zabezpieczeń technicznych uwzględniających systemy kontroli dostępu,
   c) ochrony infrastruktury krytycznej niezbędnej do świadczenia usługi kluczowej,
   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 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, uwzględniają wymagania określone w normach oraz wytycznych do ich stosowania, wskazanych w przepisach wydanych na podstawie ust. 5.

3. Podmiot krytyczny przeprowadza ocenę ryzyka, o której mowa w ust. 1 pkt 1, w terminie 9 miesięcy od dnia otrzymania informacji o wpisie do wykazu podmiotów krytycznych.

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

5. Rada Ministrów określi, w drodze rozporządzenia, wykaz norm oraz wytycznych do ich stosowania, które podmiot krytyczny uwzględnia przy wdrażaniu rozwiązań organizacyjno-technicznych, o których mowa w ust. 1 pkt 2, w zakresie:

1) zarządzania bezpieczeństwem informacji,

2) zarządzania ciągłością działania usługi kluczowej,

3) zapewnienia bezpieczeństwa fizycznego, w tym ochrony fizycznej infrastruktury służącej do świadczenia usługi kluczowej oraz zabezpieczeń technicznych, uwzględniających systemy kontroli dostępu

– mając na uwadze konieczność zapewnienia bezpieczeństwa świadczenia usług kluczowych oraz zapewnienia jednolitości rozwiązań.

6. Organ do spraw podmiotów krytycznych może opracować, odrębnie dla nadzorowanego sektora lub podsektora, o którym mowa w załączniku do ustawy, 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, które podmiot krytyczny uwzględnia przy wdrażaniu rozwiązań organizacyjno-technicznych, o których mowa 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 dotyczących środków technicznych, środków bezpieczeństwa oraz środków organizacyjnych służących zapewnieniu odporności podmiotów krytycznych.

8. Podmiot krytyczny, w celu zapewnienia wdrażania rozwiązań, o których mowa w ust. 1 pkt 2, może zawierać umowy, w których żąda od usługodawców:

1) certyfikatów, uwzględniając dokumenty 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 z 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, może opracować i udostępnić na stronie podmiotowej Biuletynu Informacji Publicznej zestawienie certyfikatów lub innych dokumentów zapewniających wdrożenie rozwiązań, o których mowa 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 niniejszego rozdziału, uznaje się wymóg prowadzenia oceny ryzyka za spełniony w całości lub w części.

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

2. Dokumentację zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej stanowią:

1) dokumentacja 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) inna dokumentacja niż wskazana w pkt 1–5, biorąc pod uwagę rodzaj świadczonej usługi kluczowej.

3. Dokumentacja jest prowadzona w postaci papierowej lub w postaci elektronicznej.

4. Podmiot krytyczny sporządza dokumentację w terminie 15 miesięcy od dnia otrzymania informacji o wpisie do wykazu 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, licząc od dnia 1 stycznia roku następującego po roku jej wycofania z użytkowania lub zakończenia świadczenia usługi kluczowej. 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 oraz z 2025 r. poz. 1173).

Art. 6zv. 1. Podmiot krytyczny jest obowiązany do zarządzania incydentem w zakresie:

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 wydanych na podstawie ust. 4;
4) zgłaszania incydentu istotnego niezwłocznie, niepóźniej 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) przekazywania sprawozdania z czynności, o których mowa w pkt 1–6, organowi do spraw podmiotów krytycznych oraz dyrektorowi Centrum w terminie niedłuższym niż 30 dni, licząc 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 ust. 1 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 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, zgłoszenie jest przekazywane 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 incydent istotny według zdarzenia w poszczególnych sektorach i podsektorach, o których mowa w załączniku do ustawy, w zależności od:

1) liczby użytkowników dotkniętych zakłóceniem;
2) czasu trwania zakłócenia usługi kluczowej;
3) obszaru geograficznego, którego dotyczy zakłócenie, z uwzględnieniem jego odizolowania geograficznego;
4) innych czynników charakterystycznych dla danego sektora lub podsektora, o którym mowa w załączniku do ustawy, jeżeli występują.

5. W rozporządzeniu, o którym mowa w ust. 4, Rada Ministrów określi co najmniej jeden próg uznania incydentu za incydent istotny dla każdego zdarzenia, 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 krytycznego, o których mowa w art. 6zo ust. 2 pkt 1–5;
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 istotny miał wpływ,
   b) liczbę użytkowników usługi kluczowej, na których incydent istotny 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, o którym mowa w art. 6zv ust. 1 pkt 4, które uzupełnia w trakcie obsługi incydentu istotnego.

3. Organ do spraw podmiotów krytycznych, na podstawie otrzymanych informacji, o których mowa w ust. 1 i 2, 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, na podstawie otrzymanych informacji, o których mowa w ust. 1–3, 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, na podstawie otrzymanych informacji, o których mowa w ust. 1–3, 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 informacji 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 co najmniej raz na 3 lata, na własny koszt, audyt zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej, zwany dalej „audytem”, w zakresie:

1) zarządzania bezpieczeństwem informacji;

2) zarządzania ciągłością działania usługi kluczowej;

3) zapewnienia bezpieczeństwa fizycznego w formie ochrony fizycznej budynków i terenów należących do podmiotu krytycznego lub ich zabezpieczeń technicznych uwzględniających systemy kontroli dostępu.

2. 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. Decyzja nakazująca przeprowadzenie zewnętrznego audytu podlega natychmiastowemu wykonaniu.

Art. 6zza. 1. Audyt może być przeprowadzony 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, spełniających wymogi określone w przepisach wydanych na podstawie 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 ust. 1 pkt 2, w przypadku gdy są oni pracownikami podmiotu krytycznego.

3. Jednostka certyfikująca oraz audytorzy, o których mowa w ust. 1 pkt 2, 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 niepóźniej niż w terminie 2 lat przed dniem rozpoczęcia audytu.

5. Na podstawie zebranych dokumentów i dowodów jednostka certyfikująca oraz audytorzy, o których mowa w ust. 1 pkt 2, sporządzają raport z przeprowadzonego audytu i przekazują je podmiotowi krytycznemu wraz z dokumentacją z przeprowadzonego audytu.

6. Audytu nie przeprowadza się 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, oraz 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 ust. 1 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. 6, za pomocą systemu, o którym mowa w art. 46 ust. 1 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, wymogi dla audytorów, o których mowa w ust. 1 pkt 2, w tym zakres wymaganej wiedzy specjalistycznej oraz wymaganego doświadczenia, mając na względzie zapewnienie skutecznego i rzetelnego przeprowadzania audytu.

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

1) szkoleniach lub ćwiczeniach:
   a) obronnych,
   b) obrony cywilnej,
   c) ochrony ludności,
   d) z zakresu przeciwdziałania zagrożeniom o charakterze terrorystycznym,
   e) zarządzania kryzysowego;
2) testach ciągłości działania w zakresie zapewnienia ciągłości świadczenia usługi kluczowej lub jej przywrócenia.

2. Szkolenia, o których mowa w ust. 1 pkt 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 pkt 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 pkt 1.

5. Testy ciągłości działania, o których mowa w ust. 1 pkt 2, polegają na praktycznym sprawdzeniu, z uwzględnieniem scenariuszy wystąpienia lub możliwości wystąpienia zagrożeń, o których mowa w art. 6e ust. 2 pkt 1 oraz ust. 4 pkt 2, czy podmiot krytyczny potrafi zapewnić ciągłość świadczenia usługi kluczowej lub przywrócić jej świadczenie.

6. Podmiot krytyczny, we współpracy z właściwym organem do spraw podmiotów krytycznych lub dyrektorem Centrum, planuje i organizuje udział w testach ciągłości działania, o których mowa w ust. 1 pkt 2.

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;
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 względem 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 oraz podania nazwiska rodowego i poprzednio noszonego nazwiska, jeżeli było zmieniane, oraz imion, nazwisk, dat i miejsc urodzenia rodziców,
   b) występuje do organu gminy z wnioskiem 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) zwraca się 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 Unii Europejskiej innego niż Rzeczpospolita Polska.

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

1) ważnego dowodu osobistego lub ważnego dokumentu paszportowego oraz podania nazwiska rodowego i poprzednio noszonego nazwiska, jeżeli było zmieniane, oraz imion, nazwisk, dat i miejsc urodzenia rodziców;
2) 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 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 3 lata.

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

8. Sprawdzenia przeszłości nie przeprowadza się w odniesieniu do osoby, o której mowa 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 bezpieczeństwa usługi kluczowej.

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

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

4. Pełnomocnikiem bezpieczeństwa usługi kluczowej może być 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 świadczącego 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 ust. 4–7 stosuje się do zastępcy pełnomocnika bezpieczeństwa usługi kluczowej.

Art. 6zze. Podmioty krytyczne sektora bankowości i infrastruktury rynków finansowych przeprowadzają ocenę ryzyka, o której mowa w art. 6zt ust. 1 pkt 1, w terminie 10 miesięcy od dnia otrzymania informacji o wpisie do wykazu podmiotów krytycznych.

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 świadczeniu co najmniej jednej usługi kluczowej spośród usług kluczowych wskazanych w przepisach rozporządzenia delegowanego Komisji (UE) 2023/2450 z dnia 25 lipca 2023 r. uzupełniającego dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2557 przez ustanowienie wykazu usług kluczowych (Dz. Urz. UE L 2023/2450 z 30.10.2023) lub świadczeniu tych samych lub podobnych usług kluczowych 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 1–5 oraz 7 i 8.

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 Europejską 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.

Art. 6zzh. 1. Organ do spraw podmiotów krytycznych, za pośrednictwem Pojedynczego Punktu Kontaktowego, współpracuje z Komisją Europejską oraz właściwymi organami państwa członkowskiego Unii Europejskiej, na rzecz którego lub w którym jest świadczona usługa kluczowa lub w przypadku gdy podmiot krytyczny o szczególnym

znaczeniu europejskim zidentyfikowany przez państwo członkowskie Unii Europejskiej 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.

2. 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 Komisji Europejskiej wniosek o zorganizowanie misji doradczej;

2) konsultuje z Komisją Europejską 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. 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 przez ten podmiot z nałożonych obowiązków 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 tego podmiotu;

3) informuje Komisję Europejską oraz właściwe organy państwa członkowskiego Unii Europejskiej, na rzecz którego lub w którym jest świadczona usługa kluczowa, o środkach zwiększających odporność tego podmiotu, wprowadzonych z uwzględnieniem opinii, o której mowa w pkt 1, albo informuje 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 za zgodą tego podmiotu, na wniosek organu do spraw podmiotów krytycznych, który zidentyfikował podmiot krytyczny.

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

Rozdział 13

Nadzór nad podmiotami krytycznymi i ich kontrola

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 ich siedzibach, miejscach wykonywania działalności gospodarczej lub zdalnie;

2) zleca audyt na koszt podmiotu krytycznego w przypadku, o którym mowa w art. 6zz ust. 2;

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. 2 pkt 5, obejmujących:

1) wpływ wdrożonych rozwiązań na bezpieczeństwo świadczenia usługi kluczowej;

2) dowody potwierdzające 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 prowadzonej wobec podmiotów krytycznych:

1) będących przedsiębiorcami stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. z 2025 r. poz. 1480, 1795 i 1826 oraz z 2026 r. poz. 507);

2) niebędących przedsiębiorcami stosuje się przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. z 2026 r. poz. 158) określające zasady i tryb przeprowadzania kontroli.

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

1) swobodnego wstępu na teren podmiotu kontrolowanego i poruszania się po tym terenie;

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. Podmioty kontrolowane 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, co odnotowuje 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.

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 datę 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 prowadzącej czynności kontrolne dokonuje ich analizy.

8. Kierownik komórki organizacyjnej prowadzącej czynności kontrolne:

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 prowadzącej czynności kontrolne zasadności zastrzeżeń do protokołu kontroli zmienia lub uzupełnia odpowiednią część protokołu kontroli w formie aneksu do protokołu.

10. Kierownik komórki organizacyjnej prowadzącej czynności kontrolne 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 prowadzącej czynności kontrolne informuje o tym kontrolowany podmiot krytyczny na piśmie.

12. Protokół kontroli w postaci:

1) papierowej sporządza się w dwóch egzemplarzach, z których jeden pozostawia się podmiotowi kontrolowanemu;

2) elektronicznej doręcza się podmiotowi kontrolowanemu.

Art. 6zzn. 1. Jeżeli na podstawie informacji zawartych 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 pokontrolnych.

Rozdział 14

Bezpieczeństwo łańcucha dostaw

Art. 6zzo. Podmiot krytyczny jest obowiązany do identyfikacji dostawców krytycznych, prowadzenia ich rejestru oraz przeprowadzania oceny ryzyka co najmniej raz w roku.

Art. 6zzp. Podmiot krytyczny zapewnia opracowanie planów awaryjnych, możliwość zastąpienia dostawcy krytycznego i minimalne wymagania bezpieczeństwa wobec dostawców krytycznych.

Art. 6zzq. Dostawca krytyczny zgłasza incydenty istotne oraz podlega audytowi za pośrednictwem podmiotu krytycznego.

Rozdział 15

Przepisy o karach pieniężnych dla podmiotów krytycznych

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

1) nie przeprowadza 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 opracowuje lub nie aktualizuje dokumentacji, o której mowa w art. 6zu ust. 1;

4) nie wykonuje obowiązku, o którym mowa w art. 6zv ust. 1 pkt 1, w zakresie obsługi incydentu istotnego;

5) nie wykonuje obowiązku, o którym mowa w art. 6zv ust. 1 pkt 4;

6) nie przeprowadza audytu;

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 przeprowadzanie kontroli, o której mowa w art. 6zzi ust. 2 pkt 1;

9) nie wykonuje w wyznaczonym terminie zaleceń pokontrolnych, o których mowa w art. 6zzn ust. 1;

10) nie wdraża 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 opracowuje 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 ust. 1:

1) pkt 1, wynosi do 100 000 zł;

2) pkt 2, wynosi do 150 000 zł;

3) pkt 3, wynosi do 50 000 zł;

4) pkt 4, wynosi do 20 000 zł za każdy stwierdzony przypadek zaniechania obsługi incydentu istotnego;

5) pkt 5, wynosi do 25 000 zł za każdy stwierdzony przypadek niezgłoszenia incydentu istotnego;

6) pkt 6, wynosi do 200 000 zł;

7) pkt 7, wynosi do 15 000 zł;

8) pkt 8, wynosi do 50 000 zł;

9) pkt 9, wynosi do 200 000 zł;

10) pkt 10, wynosi do 150 000 zł;

11) pkt 11, wynosi do 50 000 zł.

3. Wysokość kary pieniężnej, o której mowa w ust. 1:

1) pkt 4, 5 i 7, nie może być mniejsza niż 2000 zł;

2) pkt 3, 8 i 11, nie może być mniejsza niż 5000 zł;

3) pkt 1, 2, 6, 9 i 10, nie może być mniejsza niż 15 000 zł.

Art. 6zzs. 1. Karę pieniężną, o której mowa w art. 6zzr ust. 1, 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 wywołaniem poważnych utrudnień w świadczeniu usług kluczowych.

3. Wpływy z tytułu kar pieniężnych, o których mowa w art. 6zzr ust. 1, stanowią:

1) w 70 % dochód budżetu państwa;

2) w 30 % 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 2024 r. poz. 1662, z 2025 r. poz. 1017 oraz z 2026 r. poz. 252 i 815).

Art. 6zzt. 1. W przypadku naruszenia przepisów ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa przez podmiot krytyczny będący jednocześnie podmiotem kluczowym w rozumieniu przepisów tej ustawy karę pieniężną na ten podmiot nakłada organ właściwy do spraw cyberbezpieczeństwa, o którym mowa w art. 41 tej ustawy.

2. Do ustalenia wysokości kary pieniężnej w przypadku, o którym mowa w ust. 1, stosuje się przepisy ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

3. Organ właściwy do spraw cyberbezpieczeństwa, o którym mowa w art. 41 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, niezwłocznie informuje organ do spraw podmiotów krytycznych sprawujący nadzór nad podmiotem, o którym mowa w ust. 1, o:

1) wszczęciu wobec tego podmiotu postępowania w sprawie nałożenia kary pieniężnej;

2) naruszeniu dokonanym przez ten podmiot wraz z kwalifikacją prawną;

3) wysokości nałożonej na ten podmiot kary pieniężnej lub odstąpieniu od jej nałożenia.

4. Organ do spraw podmiotów krytycznych nie wszczyna postępowania w sprawie nałożenia kary pieniężnej, o której mowa w art. 6zzr ust. 1, w przypadku, o którym mowa w ust. 1, jeżeli postępowanie w przedmiocie naruszenia prowadzi organ właściwy do spraw cyberbezpieczeństwa, o którym mowa w art. 41 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Art. 6zzu. 1. Organ do spraw podmiotów krytycznych, podejmując decyzję o nałożeniu kary pieniężnej, o której mowa w art. 6zzr ust. 1, i ustalając jej wysokość, bierze pod uwagę:

1) wagę naruszenia i znaczenie naruszonych przepisów ustawy;

2) czas trwania naruszenia;

3) wcześniejsze naruszenia ze strony danego podmiotu krytycznego;

4) spowodowane szkody majątkowe i niemajątkowe, w tym wpływ na użytkowników usługi kluczowej oraz na inne usługi kluczowe;

5) środki zastosowane przez podmiot krytyczny w celu ograniczenia szkód, o których mowa w pkt 4;

6) umyślny lub nieumyślny charakter czynu ze strony podmiotu krytycznego;

7) stopień współpracy podmiotu krytycznego z organem do spraw podmiotów krytycznych.

2. Podejmując decyzję, o której mowa w ust. 1, organ do spraw podmiotów krytycznych uwzględnia również wysokość przychodu uzyskanego z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary pieniężnej, o której mowa w art. 6zzr ust. 1, lub możliwości finansowe podmiotu krytycznego będącego podmiotem publicznym.

3. W związku z toczącym się postępowaniem w sprawie nałożenia kary pieniężnej, o której mowa w art. 6zzr ust. 1, organ do spraw podmiotów krytycznych może żądać od podmiotu krytycznego przekazania we wskazanym terminie, niedłuższym niż 14 dni od dnia otrzymania żądania, informacji niezbędnych do określenia wymiaru kary pieniężnej.

4. W przypadku nieprzekazania informacji, o których mowa w ust. 3, lub przekazania informacji uniemożliwiających ustalenie podstawy wymiaru kary pieniężnej, o której mowa w art. 6zzr ust. 1, 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, o której mowa w art. 6zzr ust. 1, 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 do spraw podmiotów krytycznych w decyzji o wymierzeniu kary pieniężnej.

6. Kara pieniężna, o której mowa w art. 6zzr ust. 1, nieuiszczona w terminie wraz z odsetkami podlega ściągnięciu w trybie określonym w przepisach o postępowaniu egzekucyjnym w administracji.

7. Organ do spraw podmiotów krytycznych może odstąpić od nałożenia kary pieniężnej, o której mowa w art. 6zzr ust. 1, jeżeli waga naruszenia i znaczenie naruszonych przepisów są znikome, a podmiot krytyczny zaprzestał naruszania prawa lub naprawił wyrządzoną szkodę.

Art. 6zzv. W zakresie nieuregulowanym w niniejszym rozdziale stosuje się odpowiednio przepisy działu IVa ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2025 r. poz. 1691).

Rozdział 16

Przepisy szczególne dotyczące niektórych podmiotów krytycznych

Art. 6zzw. Do podmiotów krytycznych z sektora bankowości i infrastruktury rynków finansowych nie stosuje się przepisów rozdziałów 11–15, z wyjątkiem art. 6zt ust. 1 pkt 1, pkt 2 lit. b–d, f, h oraz i, pkt 3 oraz ust. 2–11, art. 6zu ust. 1, ust. 2 pkt 3, 4 i 6 oraz ust. 3–6, art. 6zx, art. 6zy, art. 6zzb oraz art. 6zzd.

Art. 6zzx. Do podmiotów krytycznych z sektora infrastruktury cyfrowej nie stosuje się przepisów rozdziałów 11–15.”;

8) po art. 6zzx dodaje się oznaczenie i tytuł rozdziału 17 w brzmieniu:

„Rozdział 17

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 lub odbudowy infrastruktury krytycznej lub zapewnienia niezakłóconego świadczenia usługi kluczowej;”;

10) w art. 9 w ust. 1 pkt 5 otrzymuje brzmienie:

„5) opiniowanie KPZR oraz KPRK;”;

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

12) w art. 11:

a) 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 (Dz. U. poz. 1907, z 2025 r. poz. 1705 oraz z 2026 r. poz. 646 i 815).”,

b) w ust. 2:

– w pkt 1 lit. b otrzymuje brzmienie:

„b) opracowywanie i aktualizowanie KPZR oraz KPRK,”,

– w pkt 11 wyrazy „oraz europejskiej infrastruktury krytycznej, w tym opracowywanie i aktualizacja załącznika funkcjonalnego do Krajowego Planu Zarządzania Kryzysowego dotyczącego ochrony infrastruktury krytycznej, a także” zastępuje się wyrazami „ , w tym”;

13) 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) zapewnia funkcjonowanie punktu kontaktowego do przekazywania zadań oraz uruchamia procedury wynikające z członkostwa Rzeczypospolitej Polskiej w Organizacji Traktatu Północnoatlantyckiego.”;

14) 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 funkcjonowanie 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 KOR;

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.”;

15) w art. 14 ust. 3 otrzymuje brzmienie:

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

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

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

17) po art. 25d dodaje się oznaczenie i tytuł rozdziału 18 w brzmieniu:

„Rozdział 18

Finansowanie wykonywania zadań zarządzania kryzysowego”;

18) w art. 26 po ust. 4 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 finansowe 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. 26 dodaje się art. 26a w brzmieniu:

„Art. 26a. 1. 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 mu podległej albo przez niego nadzorowanej. Jednostka ta otrzymuje dotację celową na realizację zadania utrzymania tego wykazu.”;

20) po art. 26a dodaje się oznaczenie i tytuł rozdziału 19 w brzmieniu:

„Rozdział 19

Zmiany w przepisach”;

21) po art. 31 dodaje się oznaczenie i tytuł rozdziału 20 w brzmieniu:

„Rozdział 20

Przepisy dostosowujące i przejściowe oraz przepis końcowy”;

22) dodaje się załącznik do ustawy w brzmieniu określonym w załączniku do niniejszej ustawy.

Art. 2. W ustawie z dnia 21 marca 1985 r. o drogach publicznych (Dz. U. z 2025 r. poz. 889) po art. 20h 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. W tym celu właściwy miejscowo wojewoda może nałożyć na zarządcę drogi, zarządzającego ruchem oraz inne organy i podmioty, w zakresie właściwości ich działania, obowiązki zapewniające wykonanie tego rozporządzenia.

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 określa:

1) odcinki dróg publicznych wyznaczone za pomocą współrzędnych geograficznych lub oznakowania umieszczonego na słupkach hektometrowych i kilometrowych, na których wprowadza się czasowe ograniczenia w korzystaniu lub czasowe wyłączenie z ruchu;
2) rodzaj czasowego ograniczenia w korzystaniu z dróg publicznych;
3) okres, na który wprowadza się 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 ogłoszone w drodze obwieszczenia lub za pomocą środków komunikacji elektronicznej, lub w inny sposób zwyczajowo przyjęty na danym terenie.”.

Art. 3. W ustawie z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2025 r. poz. 636, z późn. zm.[7)]) wprowadza się następujące zmiany:

1) 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 2026 r. poz. 244, 737 i 815), 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.”;

2) w art. 18c ust. 1 otrzymuje brzmienie:

„1. Komendant Główny Policji, Komendant CBŚP, Komendant CBZC lub komendant wojewódzki Policji:

1) w celu realizacji zadań, o których mowa w art. 1 ust. 2 pkt 1, 2, 3a i 4a, lub

7) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2025 r. poz. 718 i 1366 oraz z 2026 r. poz. 187, 421, 646 i 760.

2) w przypadkach, o których mowa w:

a) art. 156ze ust. 1 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze (Dz. U. z 2025 r. poz. 1431 i 1668 oraz z 2026 r. poz. 176 i 607), lub

b) art. 28a ust. 1 ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2024 r. poz. 597 oraz z 2026 r. poz. 815), lub

c) art. 11 pkt 17 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, lub

3) po wprowadzeniu trzeciego lub czwartego stopnia alarmowego, o których mowa odpowiednio w art. 15 ust. 5 lub 6 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych

– może podjąć decyzję o dopuszczalności zastosowania przez Policję urządzeń uniemożliwiających telekomunikację na określonym obszarze, przez czas niezbędny do wyeliminowania zagrożenia lub jego skutków, z uwzględnieniem konieczności minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych.”.

Art. 4. W ustawie z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2026 r. poz. 367 i 646) wprowadza się następujące zmiany:

1) w art. 10e ust. 1 otrzymuje brzmienie:

„1. Komendant Główny Straży Granicznej, Komendant BSWSG lub komendant oddziału Straży Granicznej:

1) w celu realizacji zadań, o których mowa w art. 1 ust. 2 pkt 1, 2, 4–5d i 10, lub

2) w przypadkach, o których mowa w:

a) art. 156ze ust. 1 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze, lub

b) art. 28a ust. 1 ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2024 r. poz. 597 oraz z 2026 r. poz. 815), lub

c) art. 11 pkt 17 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2026 r. poz. 244, 737 i 815), lub

3) po wprowadzeniu trzeciego lub czwartego stopnia alarmowego, o których mowa odpowiednio w art. 15 ust. 5 lub 6 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2025 r. poz. 194 oraz z 2026 r. poz. 815)

– może podjąć decyzję o dopuszczalności zastosowania przez Straż Graniczną urządzeń uniemożliwiających telekomunikację na określonym obszarze, przez czas niezbędny do wykonywania czynności przez Straż Graniczną, z uwzględnieniem konieczności minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych.”;

2) w art. 23 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, 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 2026 r. poz. 1).”.

Art. 6. W ustawie z dnia 19 października 1991 r. o gospodarowaniu nieruchomościami rolnymi Skarbu Państwa (Dz. U. z 2025 r. poz. 826 oraz z 2026 r. poz. 318) w art. 39 w ust. 2 w pkt 2a wyrazy „w jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1” zastępuje się wyrazami „w wykazie, o którym mowa w art. 6r ust. 1”.

Art. 7. W ustawie z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2025 r. poz. 532) wprowadza się następujące zmiany:

1) w art. 5:

a) w ust. 2:

– w pkt 1 lit. c otrzymuje brzmienie:

„c) magazyny rezerw strategicznych, o których mowa w art. 15 ustawy z dnia 17 grudnia 2020 r. o rezerwach strategicznych (Dz. U. z 2026 r. poz. 733 i 815);”,

– w pkt 3 lit. a otrzymuje brzmienie:

„a) zakłady, obiekty i urządzenia mające istotne znaczenie dla funkcjonowania powiatów lub miast na prawach powiatu, których zniszczenie lub uszkodzenie może stanowić zagrożenie dla życia i zdrowia ludzi oraz środowiska, w szczególności elektrownie i ciepłownie, ujęcia wody, wodociągi i oczyszczalnie ścieków,”,

– pkt 5 otrzymuje brzmienie:

„5) obiekty, urządzenia lub instalacje lub połączone ze sobą funkcjonalnie obiekty, urządzenia lub 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 2026 r. poz. 574 i 815).”,

b) ust. 3 otrzymuje brzmienie:

„3. Szczegółowe wykazy obszarów, obiektów i urządzeń, o których mowa w ust. 2, sporządzają i na 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 art. 1 ust. 2 ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (Dz. U. z 2025 r. poz. 640 i 1069 oraz z 2026 r. poz. 252 i 644). Umieszczenie w wykazie określonego obszaru, obiektu lub urządzenia następuje w drodze decyzji administracyjnej.”,

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

„3a. Wykazy, o których mowa w ust. 3, są dokumentami niejawnymi.”,

d) ust. 4 otrzymuje brzmienie:

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

e) po ust. 4 dodaje się ust. 4a w brzmieniu:

„4a. Starostowie i prezydenci miast na prawach powiatu informują wojewodę o zakładach, obiektach i urządzeniach, o których mowa w ust. 2 pkt 3 lit. a, znajdujących się na terenie powiatu.”,

f) ust. 5 otrzymuje brzmienie:

„5. Wojewodowie prowadzą ewidencję obszarów, obiektów i urządzeń podlegających obowiązkowej ochronie, znajdujących się na terenie województwa. Ewidencja jest dokumentem niejawnym.”,

g) po ust. 5 dodaje się ust. 5a i 5b w brzmieniu:

„5a. W wykazie, o którym mowa w ust. 3, prowadzonym przez ministra właściwego do spraw energii, może zostać ujęta morska farma wiatrowa, o której mowa w art. 3 pkt 3 ustawy z dnia 17 grudnia 2020 r. o promowaniu wytwarzania energii elektrycznej w morskich farmach wiatrowych (Dz. U. z 2025 r. poz. 498 i 1535 oraz z 2026 r. poz. 516). O umieszczeniu w wykazie morskiej farmy wiatrowej minister właściwy do spraw energii informuje wojewodę właściwego terytorialnie ze względu na umiejscowienie Centrum Bezpieczeństwa Morskiego, o którym mowa w art. 25a ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2024 r. poz. 597 oraz z 2026 r. poz. 815). Wojewoda, o którym mowa w zdaniu drugim, umieszcza morską farmę wiatrową w ewidencji, o której mowa w ust. 5.

5b. 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.”,

h) ust. 6 otrzymuje brzmienie:

„6. Wojewoda, w drodze decyzji administracyjnej, może umieścić w ewidencji, o której mowa w ust. 5, znajdujące się na terenie województwa obszary, obiekty i urządzenia inne niż wpisane do wykazów, o których mowa w ust. 3, lub do wykazu, o którym mowa w art. 6r ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, w tym zakłady, obiekty i urządzenia, o których mowa w ust. 2 pkt 3 lit. a.”,

i) dodaje się ust. 7 i 8 w brzmieniu:

„7. Wojewoda po otrzymaniu wykazów lub ich aktualizacji od organów, 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 zarządza obszarami, obiektami i urządzeniami umieszczonymi w tej ewidencji, oraz odpowiednio organy, 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 i art. 5b w brzmieniu:

„Art. 5a. Środki ochrony fizycznej oraz zabezpieczenie techniczne wykraczające poza granice obszaru, 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 art. 3 ust. 1 pkt 3 ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich;

2) sztucznych wysp, konstrukcji i urządzeń w polskich obszarach morskich, o których mowa w art. 23 ust. 1 ustawy z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej (Dz. U. z 2024 r. poz. 1125, z 2025 r. poz. 409, 1535 i 1668 oraz z 2026 r. poz. 252);

3) kabli i rurociągów układanych i utrzymywanych w obszarach morskich Rzeczypospolitej Polskiej, o których mowa w art. 26 ust. 1 oraz art. 27 ust. 1 ustawy z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej;

4) morskiej farmy wiatrowej, o której mowa w art. 3 pkt 3 ustawy z dnia 17 grudnia 2020 r. o promowaniu wytwarzania energii elektrycznej w morskich farmach wiatrowych.

Art. 5b. Morska farma wiatrowa, o której mowa w art. 3 pkt 3 ustawy z dnia 17 grudnia 2020 r. o promowaniu wytwarzania energii elektrycznej w morskich farmach wiatrowych, może być ochraniana na zasadach określonych w ustawie również poza granicami Rzeczypospolitej Polskiej, na akwenach w polskiej strefie odpowiedzialności Morskiej Służby Poszukiwania i Ratownictwa zgodnie z Międzynarodową konwencją o poszukiwaniu i ratownictwie morskim, sporządzoną w Hamburgu dnia 27 kwietnia 1979 r. (Dz. U. z 1988 r. poz. 184 i 185), i w polskiej wyłącznej strefie ekonomicznej.”;

3) w art. 26 w ust. 1 w pkt 5 w lit. b średnik zastępuje się przecinkiem i dodaje się lit. c w brzmieniu:

„c) w art. 36 ust. 1a–1c;”;

4) w art. 36:

a) w ust. 1 pkt 4 otrzymuje brzmienie:

„4) użycia lub wykorzystania środków przymusu bezpośredniego, o których mowa w art. 12 ust. 1 pkt 1 lit. a, b oraz d, pkt 2 lit. a, pkt 5, 7, 9, 11, pkt 12 lit. a, pkt 13 i 21–23 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2026 r. poz. 244, 737 i 815):

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

b) poza granicami obiektów i obszarów chronionych – w przypadku, o którym mowa w art. 11 pkt 9 tej ustawy;”,

b) ust. 1a otrzymuje brzmienie:

„1a. Środki przymusu bezpośredniego, o których mowa w art. 12 ust. 1 pkt 5 lub 11 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, mogą być wykorzystane wyłącznie zgodnie z art. 156ze ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze (Dz. U. z 2025 r. poz. 1431 i 1668 oraz z 2026 r. poz. 176 i 607),

art. 28a ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich lub art. 11 pkt 17 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej.”,

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

„1b. Pracownik ochrony przy wykonywaniu zadań ochrony obiektów, o których mowa w art. 5 ust. 1, będących jednocześnie obiektami portowymi w rozumieniu art. 3 ust. 1 pkt 3 ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich, w celu zabezpieczenia infrastruktury portowej przed uszkodzeniem może patrolować ten obiekt od strony wody jednostką pływającą.

1c. Wykonując czynności, o których mowa w ust. 1b, pracownik ochrony ma prawo do wezwania osób przebywających w basenie portowym i nieposiadających 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 oraz 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.”;

5) w art. 43 w ust. 2 w pkt 3 po wyrazach „jest prowadzona ochrona,” dodaje się wyrazy „z wyłączeniem morskiej farmy wiatrowej, o której mowa w art. 3 pkt 3 ustawy z dnia 17 grudnia 2020 r. o promowaniu wytwarzania energii elektrycznej w morskich farmach wiatrowych,”;

6) w art. 47 w ust. 2 wprowadzenie do wyliczenia otrzymuje brzmienie:

„Współpracę, o której mowa w ust. 1, specjalistyczne uzbrojone formacje ochronne podejmują odpowiednio z właściwym terytorialnie:”;

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

„Art. 50c. 1. Kto, nie będąc do tego uprawnionym, przebywa na obszarze lub w obiekcie podlegającym obowiązkowej ochronie oraz nie opuszcza takiego obszaru lub obiektu wbrew żądaniu osoby uprawnionej,

podlega grzywnie, karze ograniczenia wolności albo karze pozbawienia wolności do lat 2.

2. Kto, nie będąc do tego uprawnionym, przebywając na obszarze lub w 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. 8. W ustawie z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. z 2026 r. poz. 159) wprowadza się następujące zmiany:

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

„1. W przypadkach, o których mowa w art. 11 pkt 1–6 i 8–16 ustawy z dnia 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, 11, pkt 12 lit. a, c oraz 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 oraz e, pkt 2, 3 i pkt 4 lit. a oraz b oraz 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 oraz d, pkt 13, 17 i 19–23 tej ustawy, lub wykorzystać te środki.

3. W przypadkach, o których mowa w art. 45 pkt 1 lit. a–c oraz e, pkt 2, 3 i pkt 4 lit. a oraz b oraz art. 47 pkt 1–3 i 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. 9. W ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2025 r. poz. 902 i 1366 oraz z 2026 r. poz. 26) 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 2026 r. poz. 574 i 815), 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 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 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 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. 10. W ustawie z dnia 28 marca 2003 r. o transporcie kolejowym (Dz. U. z 2025 r. poz. 1234 oraz z 2026 r. poz. 41) po art. 29f 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. W tym celu właściwy miejscowo wojewoda może nałożyć na zarządcę infrastruktury kolejowej oraz inne organy i podmioty, w zakresie właściwości ich działania, obowiązki zapewniające wykonanie tego rozporządzenia.

2. Rozporządzenie porządkowe określa:

1) linie kolejowe, opisane zgodnie z wykazem linii kolejowych zawartym w regulaminie sieci, o którym mowa w art. 32 ust. 1, wraz ze wskazaniem kilometraża odcinków linii kolejowych, na których wprowadza się czasowe ograniczenia w dostępie do infrastruktury kolejowej, w tym całkowicie wyłącza się dostęp do infrastruktury kolejowej;

2) rodzaj czasowego 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 wprowadza się ograniczenia w dostępie do infrastruktury kolejowej, w tym całkowicie wyłącza się 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;

5) obowiązki zarządcy infrastruktury kolejowej oraz innych organów i podmiotów.

3. Rozporządzenie porządkowe, o którym mowa w ust. 1, może być ogłoszone w drodze obwieszczenia lub za pomocą środków komunikacji elektronicznej, lub w inny sposób zwyczajowo przyjęty na danym terenie.

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. 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 pkt 5 w brzmieniu:

„5) terminalu morskiego przeładunku ropy i paliw ciekłych w Gdańsku.”;

2) po art. 25 dodaje się art. 25a–25e w brzmieniu:

„Art. 25a. 1. Centrum Bezpieczeństwa Morskiego, zwane dalej „CBM”, zapewnia wsparcie 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 polskich obszarach 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 tej ustawy oraz podmorskim sieciom elektroenergetycznym i światłowodowym lub rurociągom, a także związanej z nimi infrastrukturze,

b) telekomunikacji w rozumieniu art. 2 pkt 70 ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej (Dz. U. poz. 1221, z 2025 r. poz. 637 i 820 oraz z 2026 r. poz. 252 i 815),

4) wykorzystywanym w wyłącznej strefie ekonomicznej sztucznym wyspom, konstrukcjom i urządzeniom przeznaczonym do gospodarczego badania i eksploatacji zasobów wyłącznej strefy ekonomicznej

– zwanym dalej „infrastrukturą morską”, oraz statkom, a także zadania w zakresie ochrony granicy państwowej na morzu oraz ochrony życia lub zdrowia ludzi, mienia w znacznych rozmiarach lub środowiska zlokalizowanych na polskich obszarach morskich w rozumieniu ustawy z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej (Dz. U. z 2024 r. poz. 1125, z 2025 r. poz. 409, 1535 i 1668 oraz z 2026 r. poz. 252).

2. Siedziba CBM mieści się we wskazanym przez Komendanta Głównego Straży Granicznej 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 nie działań,

5) opracowywanie raportów dotyczących zagrożeń

– w odniesieniu do żeglugi, infrastruktury morskiej, statków, granicy państwowej na morzu, życia lub zdrowia ludzi, mienia w znacznych rozmiarach lub środowiska na polskich obszarach morskich.

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

6. Koordynację wspólnej realizacji zadań określonych w ust. 4 zapewnia Szef CBM.

Art. 25b. 1. W ramach CBM współdziałają przedstawiciele Ministra Obrony Narodowej, Szefa Służby Kontrwywiadu Wojskowego, Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Agencji Wywiadu, Szefa Służby Wywiadu Wojskowego, Komendanta Głównego Policji, Komendanta Głównego Państwowej Straży Pożarnej, Szefa Krajowej Administracji Skarbowej, Dyrektora Morskiej Służby Poszukiwania i Ratownictwa, dyrektorów urzędów morskich oraz właściwych terytorialnie wojewodów, operatorów infrastruktury krytycznej, o których mowa w art. 3 pkt 3a ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, i kierowników jednostek, o których mowa w art. 7 ust. 1 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia, którzy wspólnie ze Strażą Graniczną realizują zadania określone w art. 25a

ust. 4 na zasadach określonych w porozumieniu zawartym między właściwym organem lub podmiotem a Komendantem Głównym Straży Granicznej.

2. Wspólna realizacja zadań określonych w art. 25a ust. 4 w przypadku przedstawicieli:

1) Ministra Obrony Narodowej, Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Krajowej Administracji Skarbowej, Dyrektora Morskiej Służby Poszukiwania i Ratownictwa oraz dyrektorów urzędów morskich – jest wykonywana w siedzibie CBM;

2) Szefa Agencji Wywiadu, Szefa Służby Kontrwywiadu Wojskowego, Szefa Służby Wywiadu Wojskowego, Komendanta Głównego Policji, Komendanta Głównego Państwowej Straży Pożarnej, właściwych terytorialnie wojewodów, operatorów infrastruktury krytycznej, o których mowa w art. 3 pkt 3a ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, i kierowników jednostek, o których mowa w art. 7 ust. 1 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia – jest wykonywana w siedzibie CBM lub w siedzibie organu lub podmiotu, którego jest przedstawicielem.

3. Komendant Główny Straży Granicznej występuje do organu lub podmiotu, o których mowa w ust. 1, z wnioskiem o wyznaczenie przedstawicieli oraz zawarcie porozumienia.

4. Wniosek, o którym mowa w ust. 3, zawiera w szczególności:

1) zakres zadań i obowiązków 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 przedstawicieli organu lub podmiotu, o których mowa w ust. 1, z uwzględnieniem możliwości jej wykonywania w systemie zmianowym;

4) miejsce wykonywania zadań określonych w art. 25a ust. 4 przez przedstawicieli organu lub podmiotu, o których mowa w ust. 1;

5) liczbę przedstawicieli organu lub podmiotu, o których mowa w ust. 1, niezbędną do wykonywania zadań określonych w art. 25a ust. 4 w celu zapewnienia ciągłości działania CBM.

5. Wniosek, o którym mowa w ust. 3, może zawierać imię i nazwisko przedstawiciela organu lub podmiotu, o których mowa w ust. 1. Organ lub podmiot, o których mowa w ust. 1, może odmówić wyznaczenia osoby, której dotyczy wniosek, jeżeli jest to uzasadnione potrzebami tego organu lub podmiotu.

6. Organ lub podmiot, o których mowa w ust. 1, w terminie 7 dni od dnia otrzymania wniosku, o którym mowa w ust. 3, zawiadamia Komendanta Głównego Straży Granicznej o wyznaczonych przedstawicielach.

7. Porozumienie, o którym mowa w ust. 1, określa w szczególności:

1) datę zawarcia porozumienia;

2) miejsce wykonywania zadań określonych w art. 25a ust. 4 przez przedstawicieli organu lub podmiotu, o których mowa w ust. 1;

3) imiona i nazwiska przedstawicieli organu lub podmiotu, o których mowa w ust. 1;

4) stopnie przedstawicieli organu lub podmiotu, o których mowa w ust. 1, w przypadku gdy są oni funkcjonariuszami albo żołnierzami;

5) numery poświadczeń bezpieczeństwa wydanych przedstawicielom organu lub podmiotu, o których mowa w ust. 1, daty ich wydania i wystawcę takich poświadczeń oraz okres ważności i oznaczenie klauzul upoważniających do przetwarzania informacji niejawnych;

6) zakres zadań i obowiązków przedstawicieli organu lub podmiotu, o których mowa w ust. 1, oraz sposób organizacji wykonywania tych zadań i obowiązków;

7) ustalony czas pracy albo służby przedstawicieli organu lub podmiotu, o których mowa w ust. 1;

8) osobę odpowiedzialną za organizację i koordynację zadań realizowanych w CBM oraz za monitorowanie ich realizacji.

8. W przypadku planowanej zmiany przedstawiciela organ lub podmiot, o których mowa w ust. 1, wskazuje kolejnego przedstawiciela w celu zapewnienia ciągłości działania CBM. W takim przypadku dokonuje się zmiany zawartego porozumienia.

9. Organ lub podmiot, o których mowa w ust. 1, wypłaca swoim przedstawicielom uposażenie albo wynagrodzenie i inne świadczenia oraz należności pieniężne.

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

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

Art. 25d. 1. Organy i podmioty, o których mowa w art. 25b ust. 1, przekazują do CBM informacje na temat zagrożeń, o których mowa w art. 25a ust. 4.

2. Prezes Rady Ministrów określi, w drodze rozporządzenia, katalog i klasyfikację zagrożeń, o których mowa w art. 25a ust. 4, uwzględniając potrzebę zapewnienia skutecznego i kompleksowego przekazywania informacji do CBM.

Art. 25e. 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.”;

3) w art. 27 w ust. 1 w pkt 5 na końcu dodaje się przecinek oraz dodaje się pkt 6 w brzmieniu:

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

4) 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 na 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 2026 r. poz. 244, 737 i 815) 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.

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 2025 r. poz. 470) 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 2026 r. poz. 522, 640 i 644), 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 2026 r. poz. 574 i 815), zwanych dalej „spółkami”.”;

2) w art. 2:

a) ust. 3 i 3a otrzymują 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 niepóźniej niż w terminie 60 dni od dnia ich dokonania.

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.”,

b) ust. 5 otrzymuje brzmienie:

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

c) 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;”;

3) w art. 5:

a) ust. 1 i 1a otrzymują brzmienie:

„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.

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.”,

b) 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.”,

c) dodaje się ust. 6 w brzmieniu:

„6. Do zastępcy pełnomocnika przepisy ust. 2–5 stosuje się odpowiednio.”;

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

„Art. 5a. 1. W przypadku nierealizowania przez pełnomocnika do spraw ochrony infrastruktury krytycznej lub jego zastępcę obowiązków, o których mowa w art. 5 ust. 2, minister właściwy do spraw aktywów państwowych może uznać, że pełnomocnik lub jego zastępca przestał dawać rękojmię prawidłowego wykonywania obowiązków, o czym powiadamia zarząd spółki.

2. Zarząd spółki, w terminie 30 dni od dnia powiadomienia, o którym mowa w ust. 1, odwołuje pełnomocnika do spraw ochrony infrastruktury krytycznej lub jego zastępcę w trybie określonym w art. 5 ust. 1.”;

5) w art. 6:

a) ust. 1 i 2 otrzymują brzmienie:

„1. Zarząd spółki obowiązany 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.

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.”,

b) w ust. 3:

– wprowadzenie do wyliczenia otrzymuje brzmienie:

„Pełnomocnik do spraw ochrony infrastruktury krytycznej lub jego zastępca sporządza dla zarządu spółki oraz rady nadzorczej raport doraźny oraz raporty półroczny i roczny o stanie ochrony infrastruktury krytycznej. Raport półroczny i roczny zawierają informacje dotyczące ochrony infrastruktury krytycznej w zakresie:”,

– w pkt 6 kropkę zastępuje się średnikiem i dodaje się pkt 7–9 w brzmieniu:

„7) stwierdzonych incydentów i podjętych działaniach korygujących;

8) przeprowadzonych kontroli i audytów dotyczących ochrony infrastruktury krytycznej;

9) posiadanych certyfikatów systemów i rozwiązań dotyczących ochrony infrastruktury krytycznej.”,

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

„3a. Raport doraźny jest sporządzany w terminie 24 godzin od zidentyfikowania zagrożenia lub wystąpienia sytuacji stwarzającej rzeczywiste zagrożenie dla funkcjonowania, ciągłości działania oraz integralności infrastruktury krytycznej.”,

d) ust. 4–6 otrzymują brzmienie:

„4. Raporty, o których mowa w ust. 3, 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 obowiązany, 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.

5. Pełnomocnik do spraw ochrony infrastruktury krytycznej lub 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.

6. Pełnomocnik do spraw ochrony infrastruktury krytycznej lub 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.”,

e) ust. 8 otrzymuje brzmienie:

„8. Prezes Rady Ministrów określi, w drodze rozporządzenia:

1) szczegółowy tryb powoływania i odwoływania pełnomocnika do spraw ochrony infrastruktury krytycznej oraz jego zastępcy,

2) sposób wykonywania przez pełnomocnika do spraw ochrony infrastruktury krytycznej i jego zastępcę 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 może podlegać karze pieniężnej za nierealizowanie zadań, o których mowa w:

1) art. 5 ust. 1 – w wysokości do 50 000 zł;

2) art. 6 ust. 1 – w wysokości do 100 000 zł;

3) art. 6 ust. 2 – w wysokości do 50 000 zł.

2. Minister właściwy do spraw aktywów państwowych, w przypadku nierealizowania przez zarząd spółki zadań, o których mowa w art. 5 ust. 1 lub art. 6 ust. 1 lub 2, wzywa zarząd spółki do usunięcia uchybień.

3. Jeżeli zarząd spółki uporczywie narusza przepisy art. 5 ust. 1 lub art. 6 ust. 1 lub 2, może podlegać karze w wysokości do 1 000 000 zł.

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

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

6. Zarząd spółki, w terminie 30 dni od dnia powiadomienia, o którym mowa w ust. 5, obowiązany jest do odwołania pełnomocnika w trybie określonym w art. 5 ust. 1.”.

Art. 13. W ustawie z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych (Dz. U. z 2026 r. poz. 562) w art. 29d ust. 6a otrzymuje brzmienie:

„6a. Na wniosek Prezesa UKE dyrektor Rządowego Centrum Bezpieczeństwa udostępnia Prezesowi UKE, w terminie 14 dni od dnia otrzymania wniosku, wyciągi z wykazu infrastruktury krytycznej, o którym mowa w art. 6r ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, znajdującej się na terenie województw, objętej wojewódzkimi planami zarządzania kryzysowego.”.

Art. 14. W ustawie z dnia 14 grudnia 2012 r. o odpadach (Dz. U. z 2023 r. poz. 1587, z późn. zm.[8)]) 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 2026 r. poz. 574 i 815)”.

Art. 15. W ustawie z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2026 r. poz. 244 i 737) wprowadza się następujące zmiany:

1) w art. 4:

a) w pkt 8 lit. b otrzymuje brzmienie:

„b) obiekty, urządzenia, instalacje, sieci, systemy lub usługi lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje, sieci, systemy lub usługi ujęte w wykazie, o którym mowa w art. 6r ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2026 r. poz. 574 i 815);”,

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;”;

8) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2023 r. poz. 1597, 1688, 1852 i 2029, z 2024 r. poz. 1834, 1911 i 1914, z 2025 r. poz. 1812 oraz z 2026 r. poz. 174.

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

„16) zniszczenia albo 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;

17) zniszczenia albo 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 albo unieruchomienia bezzałogowego obiektu pływającego albo przejęcia nad nim kontroli;

23) środki i urządzenia przeznaczone do zniszczenia albo 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 je 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 je 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 także pocisków niepenetracyjnych zawierających chemiczne środki obezwładniające lub barwiące lub je wykorzystać.”;

5) w art. 33a dodaje się ust. 3 w brzmieniu:

„3. Środki i urządzenia przeznaczone do zniszczenia albo unieruchomienia bezzałogowego statku powietrznego albo przejęcia kontroli nad jego lotem uniemożliwiające telekomunikację na określonym obszarze mogą być zastosowane wyłącznie na zasadach określonych w przepisach odrębnych.”;

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

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

2. Zniszczenie albo 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.

3. Środki i urządzenia przeznaczone do zniszczenia albo unieruchomienia bezzałogowego obiektu pływającego albo przejęcia nad nim kontroli uniemożliwiające telekomunikację na określonym obszarze mogą być zastosowane wyłącznie na zasadach określonych w przepisach odrębnych.

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

2. Zniszczenie albo 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.

3. Środki i urządzenia przeznaczone do zniszczenia albo unieruchomienia bezzałogowego obiektu lądowego albo przejęcia nad nim kontroli uniemożliwiające telekomunikację na określonym obszarze mogą być zastosowane wyłącznie na zasadach określonych w przepisach odrębnych.”;

7) w art. 47 w pkt 7 kropkę zastępuje się średnikiem i dodaje się pkt 8 w brzmieniu:

„8) zniszczenia albo unieruchomienia bezzałogowego obiektu lądowego w przypadkach, o których mowa w art. 11 pkt 17.”.

Art. 16. W ustawie z dnia 24 lipca 2015 r. o kontroli niektórych inwestycji (Dz. U. z 2026 r. poz. 47) w art. 12d w ust. 2 w pkt 1 wyrazy „w jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1” zastępuje się wyrazami „w wykazie, o którym mowa w art. 6r ust. 1”.

Art. 17. W ustawie z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2025 r. poz. 194) wprowadza się następujące zmiany:

1) w art. 2 uchyla się pkt 3;

2) art. 4 otrzymuje brzmienie:

„Art. 4. 1. Organy administracji publicznej, operatorzy infrastruktury krytycznej, o których mowa w art. 3 pkt 3a ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, i kierownicy jednostek, o których mowa w art. 7 ust. 1 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2025 r. poz. 532 oraz z 2026 r. poz. 815), 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. 5 w ust. 1 po wyrazach „Żandarmerię Wojskową” dodaje się wyrazy „ , straż ochrony kolei”;

4) 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 Służby Kontrwywiadu Wojskowego.”,

b) ust. 2 otrzymuje brzmienie:

„2. W przypadku wprowadzenia w trybie art. 16 ust. 1 drugiego stopnia alarmowego lub stopnia wyższego minister właściwy do spraw wewnętrznych, z urzędu lub na wniosek Szefa ABW, może wydać Policji zalecenie szczególnego zabezpieczenia poszczególnych obiektów, urządzeń, instalacji, sieci lub systemów stanowiących infrastrukturę krytyczną lub obszarów, obiektów lub urządzeń wpisanych do ewidencji, o której mowa w art. 5 ust. 5 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia, uwzględniając rodzaj zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym.”,

c) dodaje się ust. 3 i 4 w brzmieniu:

„3. W przypadku wprowadzenia w trybie art. 16 ust. 1 trzeciego lub czwartego stopnia alarmowego minister właściwy do spraw wewnętrznych, z urzędu lub na wniosek Szefa ABW, może wydać Policji zalecenie szczególnego zabezpieczenia innych obiektów, urządzeń, instalacji, sieci, systemów lub obszarów niż określone w ust. 2, uwzględniając rodzaj zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym.

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

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

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

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

7) 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 którego skład 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. 18. W ustawie z dnia 20 lipca 2017 r. – Prawo wodne (Dz. U. z 2025 r. poz. 960 i 1535 oraz z 2026 r. poz. 445 i 605) 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. 19. W ustawie z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (Dz. U. z 2025 r. poz. 34, z późn. zm.[9)]) wprowadza się następujące zmiany:

1) 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 dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2026 r. poz. 244, 737 i 815), 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 oraz 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 oraz 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.”;

2) w art. 39 ust. 1 otrzymuje brzmienie:

„1. Komendant SOP:

1) w celu realizacji zadań, o których mowa w art. 3 pkt 1, lub

2) w przypadkach, o których mowa w:

a) art. 156ze ust. 1 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze (Dz. U. z 2025 r. poz. 1431 i 1668 oraz z 2026 r. poz. 176 i 607), lub

b) art. 28a ust. 1 ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2024 r. poz. 597 oraz z 2026 r. poz. 815), lub

c) art. 11 pkt 17 ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej

– może podjąć decyzję o dopuszczalności zastosowania przez SOP urządzeń uniemożliwiających telekomunikację na określonym obszarze przez czas niezbędny do wykonywania czynności przez SOP, z uwzględnieniem konieczności minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych.”.

Art. 20. W ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20 i 252) wprowadza się następujące zmiany:

1) 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 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym” zastępuje się wyrazami „operatorem infrastruktury krytycznej, o którym mowa w art. 3 pkt 3a ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2026 r. poz. 574 i 815)”;

2) w art. 26:

a) w ust. 3 w pkt 13 wyrazy „części Raportu o zagrożeniach bezpieczeństwa narodowego, o którym mowa w art. 5a ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, dotyczącej cyberbezpieczeństwa” zastępuje się wyrazami „propozycji do ujęcia w projekcie Krajowej Oceny Ryzyka, o której mowa w art. 6e ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, dotyczących cyberbezpieczeństwa”,

b) w ust. 5 w pkt 1 skreśla się wyrazy „ , w tym podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym”,

c) w ust. 7 w pkt 5 i 6 wyrazy „jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym” zastępuje się wyrazami „wykazem, o którym mowa w art. 6r ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym”;

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

„1b. System teleinformatyczny zapewnia wymianę informacji między organami do spraw podmiotów krytycznych, o których mowa w art. 6zk ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, dyrektorem Rządowego Centrum Bezpieczeństwa a podmiotami krytycznymi, o których mowa w art. 3 pkt 1a tej ustawy.”.

---

9) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2024 r. poz. 1871, z 2025 r. poz. 179, 718, 1366 i 1823 oraz z 2026 r. poz. 646.

Art. 21. W ustawie z dnia 17 grudnia 2020 r. o rezerwach strategicznych (Dz. U. z 2026 r. poz. 733) wprowadza się następujące zmiany:

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

„5a) wirtualne środowisko informatyczne – wydzielona przestrzeń wielosystemowa oparta na ograniczonych zasobach fizycznych;”;

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 2026 r. poz. 612 i 791), 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 oraz z 2026 r. poz. 471 i 646), 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:

„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 2025 r. poz. 1691).”;

5) w art. 8:

a) w ust. 2 pkt 5 otrzymuje brzmienie:

„5) ministrem właściwym 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. 3 pkt 16 ustawy o zarządzaniu kryzysowym;

2) wnioski wynikające z wykonania postanowień Strategii Odporności Podmiotów Krytycznych, o której mowa w art. 6f ust. 1 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 w danej 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 strategicznych, wynikające z oceny ryzyka zidentyfikowanych zagrożeń zawartej w Krajowej Ocenie Ryzyka, o której mowa w art. 6e ust. 1 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 dotyczące asortymentów rezerw strategicznych i ich ilości, 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. Przepisy ust. 2 stosuje się do 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 strategicznych utrzymywanych na podstawie umów, o których mowa w art. 17 i art. 18;

5) niezbędnych czynności Agencji i organów, na rzecz których 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;

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 i 5 otrzymują 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 art. 18;

4) może przyjąć określony asortyment w formie darowizny z przeznaczeniem do rezerw strategicznych.

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, tej usługi lub tego 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 do 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 i 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) wskazanie innych szczególnych warunków udostępnienia rezerw strategicznych, w tym dotyczących obowiązku przetransportowania rezerw strategicznych, ich montażu, zainstalowania lub przetworzenia lub obowiązku pokrycia kosztów przeglądów, konserwacji, napraw i demontażu, jeżeli jest to konieczne ze względu na właściwości udostępnionego asortymentu rezerw strategicznych lub uzasadnione innymi względami;”,

– dodaje się pkt 6 i 7 w brzmieniu:

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

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, któremu udostępnione rezerwy strategiczne zostały wydane do użycia, z dniem jego wydania.

10. W przypadku wydania decyzji o udostępnieniu rezerw strategicznych z obowiązkiem zwrotu utrzymanie wydanych rezerw strategicznych w należytym stanie, w tym ich montaż, zainstalowanie lub przetworzenie lub dokonywanie wymaganych przeglądów, konserwacji i napraw, obciąża organ lub podmiot, któremu udostępnione rezerwy strategiczne zostały wydane do użycia.

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 2026 r. poz. 793), jeżeli wartość zamówienia jest mniejsza niż progi unijne, o których mowa w 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 skutkom klęski żywiołowej lub sytuacji kryzysowej lub ich usuwania 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, o których mowa w ust. 1.

3. Specjalistyczny asortyment techniczny rezerw strategicznych 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 wirtualnego środowiska informatycznego oraz fizycznych lub wirtualnych zasobów informatycznych 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, określa w szczególności warunki udostępnienia wirtualnego środowiska informatycznego oraz fizycznych lub wirtualnych zasobów informatycznych oraz ich zwrotu.”;

19) art. 24 otrzymuje brzmienie:

„Art. 24. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, procedurę:

1) udostępnienia rezerw strategicznych, w tym czasowego, zwrotnego udostępnienia specjalistycznego asortymentu technicznego rezerw strategicznych, specjalistycznego asortymentu medycznego rezerw strategicznych oraz udostępnienia wirtualnego środowiska informatycznego oraz fizycznych lub wirtualnych zasobów informatycznych,

2) zwrotu rezerw strategicznych, w tym zwrotu specjalistycznego asortymentu technicznego rezerw strategicznych, specjalistycznego asortymentu medycznego rezerw strategicznych oraz wirtualnego środowiska informatycznego oraz fizycznych lub wirtualnych zasobów informatycznych

– mając na względzie konieczność zapewnienia prawidłowej i efektywnej realizacji zadań Agencji.”;

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

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

21) uchyla się art. 28;

22) w art. 29:

a) ust. 2 otrzymuje brzmienie:

„2. W przypadku, o którym mowa w ust. 1, organ lub podmiot, o którym mowa w art. 8 ust. 2, powierzający Agencji określone zadanie wskazuje rodzaj i ilość asortymentu, zakres jego przechowywania, w tym czas tego

przechowywania, oraz organy lub podmioty, którym dany asortyment zostanie wydany, oraz warunki jego wydania, a także określa wysokość środków przeznaczonych na finansowanie tego zadania.”,

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

„3a. Środki przeznaczone na sfinansowanie zadania oraz na pokrycie kosztów, o których mowa w ust. 3, organ lub podmiot, o którym mowa w art. 8 ust. 2, powierzający Agencji określone zadanie przekazuje Agencji na podstawie zawartego z nią porozumienia.

3b. Środki, 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 wykonywać zadania, o których mowa w ust. 1, po zapewnieniu środków finansowych na ich wykonywanie, 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;”,

– w pkt 13 kropkę zastępuje się średnikiem i dodaje się pkt 14 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 2026 r. poz. 373).”;

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, w porozumieniu z ministrem właściwym do spraw zagranicznych, 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 albo 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.

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 tym 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 Agencji zadania, o których mowa w ust. 1, minister właściwy do spraw wewnętrznych zapewnia jej 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 w 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 asortymentu lub 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.”;

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 na stanowisku:

1) głównego księgowego,

2) zastępcy dyrektora biura lub na stanowisku równorzędnym,

3) kierownika działu lub na stanowisku równorzędnym,

4) 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 (Dz. U. z 2025 r. poz. 499 oraz z 2026 r. poz. 160 i 177) oraz podlegają ograniczeniom w prowadzeniu działalności gospodarczej takim jak pracownicy agencji państwowych, o których mowa w art. 2 pkt 10 tej ustawy.”;

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.[10)]), przez udostępnienie informacji, o których mowa w art. 13 ust. 1 i 2 tego rozporządzenia, 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.”;

[10)] Zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 04.03.2021, str. 35.

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;”,

– w pkt 9 kropkę zastępuje się średnikiem i dodaje się pkt 10 w brzmieniu:

„10) środki pochodzące z budżetu Unii Europejskiej.”,

b) 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.”,

c) 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.”;

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 dnia ogłoszenia ustawy budżetowej na dany rok, przekazuje ministrowi właściwemu do spraw wewnętrznych plan rzeczowy rezerw strategicznych stanowiący załącznik do planu finansowego Agencji.”;

31) 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.”;

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

„1a) minister właściwy do spraw gospodarki surowcami energetycznymi – w odniesieniu do należności i wierzytelności wynikających z wykonywania zadań, o których mowa w art. 31 ust. 1 pkt 8, których wartość należności głównej przekracza kwotę 40 000 zł;”;

33) 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. 22. W ustawie z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1662, z 2025 r. poz. 1017 oraz z 2026 r. poz. 252) w art. 2 w ust. 4 po pkt 1b dodaje się pkt 1c w brzmieniu:

„1c) wpływy z kar pieniężnych, o których mowa w art. 6zzr ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2026 r. poz. 574 i 815);”.

Art. 23. W ustawie z dnia 11 marca 2022 r. o obronie Ojczyzny (Dz. U. z 2025 r. poz. 825, 1014 i 1080 oraz z 2026 r. poz. 26, 426 i 635) w art. 650:

1) w pkt 1 wyrazy „w jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej” zastępuje się wyrazami „w wykazie, o którym mowa w art. 6r ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym”;

2) pkt 2 otrzymuje brzmienie:

„2) przepisach rozdziału 7 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.”.

Art. 24. W ustawie z dnia 7 października 2022 r. o szczególnych rozwiązaniach służących ochronie odbiorców energii elektrycznej w 2023 roku oraz w 2024 roku w związku z sytuacją na rynku energii elektrycznej (Dz. U. z 2024 r. poz. 1288 i 1831 oraz z 2025 r. poz. 565 i 1812) w art. 37 w ust. 6 w pkt 3 wyrazy „w wykazie, o którym mowa w art. 5b ust. 7 pkt 1" zastępuje się wyrazami „w wykazie, o którym mowa w art. 6r ust. 1".

Art. 25. W ustawie z dnia 7 lipca 2023 r. o przygotowaniu i realizacji inwestycji w zakresie Krajowego Centrum Przetwarzania Danych (Dz. U. poz. 1501) w art. 19 w ust. 2 w pkt 5 wyrazy „w jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1" zastępuje się wyrazami „w wykazie, o którym mowa w art. 6r ust. 1".

Art. 26. W ustawie z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej (Dz. U. poz. 1221, z 2025 r. poz. 637 i 820 oraz z 2026 r. poz. 252) uchyla się art. 42.

Art. 27. W ustawie z dnia 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej (Dz. U. poz. 1907, z 2025 r. poz. 1705 oraz z 2026 r. poz. 646) 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. 3 pkt 16 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 ust. 1 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 wprowadzenie do wyliczenia otrzymuje brzmienie:

„Organy ochrony ludności i Dyrektor Rządowego Centrum Bezpieczeństwa uwzględniają w planach zarządzania kryzysowego, o których mowa w art. 3 pkt 16 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym:";

4) art. 40 otrzymuje brzmienie:

„Art. 40. 1. Dyrektor Rządowego Centrum Bezpieczeństwa opracowuje, we współpracy z Szefem Sztabu Generalnego Wojska Polskiego, krajowy plan ewakuacji.

2. Krajowy plan ewakuacji opracowuje się na podstawie wojewódzkich planów ewakuacji ludności.

3. Krajowy plan ewakuacji oraz wojewódzkie plany ewakuacji ludności opracowuje się na okres 3 lat.

4. Krajowy plan ewakuacji oraz wojewódzkie plany ewakuacji ludności są aktualizowane w każdym czasie stosownie do potrzeb.

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, o którym mowa w art. 6j ust. 1 pkt 5 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. Wkłady, o których mowa w art. 43, stanowią załączniki funkcjonalne do planów reagowania kryzysowego odpowiednio gminy i powiatu.".

Art. 28. 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 6 miesięcy od dnia wejścia w życie niniejszej ustawy.

2. Krajową Strategię Odporności Podmiotów Krytycznych, o której mowa w art. 6f ust. 1 ustawy zmienianej w art. 1, Rada Ministrów przyjmuje po raz pierwszy w terminie 6 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 29. 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 12 miesięcy od dnia wejścia w życie niniejszej ustawy.

2. Plany zarządzania ryzykiem, o których mowa w art. 6g ust. 2 pkt 2–5 ustawy zmienianej w art. 1, są zatwierdzane po raz pierwszy w terminie 3 miesięcy od dnia przyjęcia po raz pierwszy Krajowego Planu Zarządzania Ryzykiem, o którym mowa w art. 6g ust. 2 pkt 1 ustawy zmienianej w art. 1.

3. Powiatowe plany zarządzania ryzykiem, o których mowa w art. 6g ust. 2 pkt 6 ustawy zmienianej w art. 1, są zatwierdzane po raz pierwszy w terminie 3 miesięcy od dnia zatwierdzenia po raz pierwszy właściwego wojewódzkiego planu zarządzania ryzykiem, o którym mowa w art. 6g ust. 2 pkt 5 ustawy zmienianej w art. 1.

4. Gminne plany zarządzania ryzykiem, o których mowa w art. 6g ust. 2 pkt 7 ustawy zmienianej w art. 1, są zatwierdzane po raz pierwszy w terminie 3 miesięcy od dnia zatwierdzenia po raz pierwszy właściwego powiatowego planu zarządzania ryzykiem, o którym mowa w art. 6g ust. 2 pkt 6 ustawy zmienianej w art. 1.

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 po raz pierwszy Krajowego Planu Zarządzania Ryzykiem, o którym mowa w art. 6g ust. 2 pkt 1 ustawy zmienianej w art. 1.

6. Plany reagowania kryzysowego, o których mowa w art. 6j ust. 1 pkt 2–5 ustawy zmienianej w art. 1, są zatwierdzane po raz pierwszy w terminie 3 miesięcy od dnia przyjęcia po raz pierwszy Krajowego Planu Reagowania Kryzysowego, o którym mowa w art. 6j ust. 1 pkt 1 ustawy zmienianej w art. 1.

7. Powiatowe plany reagowania kryzysowego, o których mowa w art. 6j ust. 1 pkt 6 ustawy zmienianej w art. 1, są zatwierdzane po raz pierwszy w terminie 3 miesięcy od dnia zatwierdzenia po raz pierwszy właściwego wojewódzkiego planu reagowania kryzysowego, o którym mowa w art. 6j ust. 1 pkt 5 ustawy zmienianej w art. 1.

8. Gminne plany reagowania kryzysowego, o których mowa w art. 6j ust. 1 pkt 7 ustawy zmienianej w art. 1, są zatwierdzane po raz pierwszy w terminie 3 miesięcy od dnia zatwierdzenia po raz pierwszy właściwego powiatowego planu reagowania kryzysowego, o którym mowa w art. 6j ust. 1 pkt 6 ustawy zmienianej w art. 1.

9. Plany zarządzania kryzysowego przyjęte lub zatwierdzone na podstawie ustawy zmienianej w art. 1, w brzmieniu dotychczasowym, pozostają w mocy do dnia przyjęcia lub zatwierdzenia planów, o których mowa w ust. 1–8, i mogą być do tego czasu aktualizowane.

Art. 30. 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, pozostają w mocy do dnia przyjęcia przez Radę Ministrów po raz pierwszy kryteriów, o których mowa w 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, Rada Ministrów przyjmuje po raz pierwszy w terminie 3 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 31. 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, 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, pozostają w mocy do czasu dokonania wpisu infrastruktury krytycznej do wykazu, 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. 32. 1. Właściciele oraz 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, realizują zadania w zakresie ochrony infrastruktury krytycznej na podstawie art. 6 ustawy zmienianej w art. 1, do czasu dokonania wpisu do wykazu, 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 przepisów dotychczasowych do czasu sporządzenia wykazu, o którym mowa w art. 6r ust. 1 ustawy zmienianej w art. 1.

Art. 33. Raport o stanie ochrony infrastruktury krytycznej, o którym mowa w art. 6zg ust. 1 ustawy zmienianej w art. 1, operator infrastruktury krytycznej sporządza po raz pierwszy za rok 2027.

Art. 34. 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, o którym mowa w art. 6zo ust. 1 ustawy zmienianej w art. 1, w terminie 9 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 35. 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 niepóźniej niż w terminie 7 dni od dnia wejścia w życie niniejszej ustawy.

3. Pojedynczy Punkt Kontaktowy, o którym mowa w art. 6zm ust. 1 ustawy zmienianej w art. 1, po raz pierwszy przekazuje Komisji Europejskiej dane kontaktowe wyznaczonych organów do spraw podmiotów krytycznych i Pojedynczego Punktu Kontaktowego oraz wskazuje zakres realizowanych zadań w terminie 3 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 36. 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. 7, w brzmieniu dotychczasowym.

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. 7, w brzmieniu nadanym niniejszą ustawą, 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. 7, w brzmieniu nadanym niniejszą ustawą, 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. 7, w brzmieniu nadanym niniejszą ustawą, Komisja Nadzoru Finansowego niezwłocznie:

1) informuje o tym podmioty umieszczone w tym wykazie oraz Prezesa Narodowego Banku Polskiego;

2) przesyła ten wykaz do właściwych miejscowo 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. 7, w brzmieniu dotychczasowym. Usunięcie podmiotów, o którym mowa w zdaniu pierwszym, nie wymaga decyzji administracyjnej.

Art. 37. 1. Do postępowań w sprawie sprzeciwu wobec uchwał organu spółki lub innych dokonywanych przez zarząd spółki czynności prawnych, o których mowa w art. 2 ust. 1 i 2 ustawy zmienianej w art. 12, wszczętych i niezakończonych przed dniem wejścia w życie niniejszej ustawy, stosuje się przepisy dotychczasowe.

2. Raport półroczny oraz raport roczny o stanie ochrony infrastruktury krytycznej, o których mowa w art. 6 ust. 3 ustawy zmienianej w art. 12, w brzmieniu nadanym niniejszą ustawą, składa się po raz pierwszy odpowiednio za pierwsze półrocze 2027 r. oraz za rok 2027.

Art. 38. Szczegółowa procedura udostępnienia rezerw strategicznych, o której mowa w art. 24 ustawy zmienianej w art. 21, w brzmieniu dotychczasowym, zachowuje moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 24 ustawy zmienianej w art. 21, w brzmieniu nadanym niniejszą ustawą, niedłużej jednak niż przez 6 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 39. W terminie 30 dni od dnia wejścia w życie niniejszej ustawy wojewoda spełnia obowiązek informacyjny, o którym mowa w art. 5 ust. 8 ustawy zmienianej w art. 7, względem dotychczas prowadzonej ewidencji.

Art. 40. 1. Tworzy się Centrum Bezpieczeństwa Morskiego.

2. Centrum Bezpieczeństwa Morskiego zostanie zorganizowane i rozpocznie działanie w terminie 6 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 41. 1. Komendant Główny Straży Granicznej w terminie 7 dni od dnia wejścia w życie niniejszej ustawy wyznacza spośród oficerów Straży Granicznej Pełnomocnika Komendanta Głównego Straży Granicznej do spraw utworzenia Centrum Bezpieczeństwa Morskiego w celu podjęcia czynności przygotowawczych i organizacyjnych niezbędnych do rozpoczęcia funkcjonowania Centrum Bezpieczeństwa Morskiego, w szczególności:

1) wskazania lokalizacji i pomieszczeń;

2) wyposażenia w niezbędny sprzęt;

3) zapewnienia funkcjonalności i komplementarności odpowiednich systemów teleinformatycznych i stanowisk pracy;

4) wspierania procesu wyznaczania przedstawicieli innych organów lub podmiotów do wykonywania zadań Centrum Bezpieczeństwa Morskiego.

2. Czynności, o których mowa w ust. 1, Pełnomocnik Komendanta Głównego Straży Granicznej do spraw utworzenia Centrum Bezpieczeństwa Morskiego realizuje we współpracy z organami lub podmiotami, o których mowa w art. 25b ust. 1 ustawy zmienianej w art. 11, i przy wsparciu tych organów lub podmiotów.

3. Pełnomocnik Komendanta Głównego Straży Granicznej do spraw utworzenia Centrum Bezpieczeństwa Morskiego kończy swoją działalność z dniem rozpoczęcia działania przez Centrum Bezpieczeństwa Morskiego.

Art. 42. Sprawozdanie, o którym mowa w art. 25e ustawy zmienianej w art. 11, przedstawia się po raz pierwszy do dnia 31 marca 2028 r.

Art. 43. Dotychczasowe przepisy wykonawcze wydane na podstawie art. 6 ust. 8 ustawy zmienianej w art. 12, w brzmieniu dotychczasowym, zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 6 ust. 8 ustawy zmienianej w art. 12, w brzmieniu nadanym niniejszą ustawą, jednak niedłużej niż przez 6 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 44. 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. – 586 tys. zł;

2) w 2027 r. – 611 tys. zł;

3) w 2028 r. – 626 tys. zł;

4) w 2029 r. – 642 tys. zł;

5) w 2030 r. – 658 tys. zł;

6) w 2031 r. – 710 tys. zł;

7) w 2032 r. – 691 tys. zł;

8) w 2033 r. – 708 tys. zł;

9) w 2034 r. – 726 tys. zł;

10) w 2035 r. – 744 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 45. 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. – 2 149 tys. zł;

2) w 2027 r. – 2 241 tys. zł;

3) w 2028 r. – 2 297 tys. zł;

4) w 2029 r. – 2 352 tys. zł;

5) w 2030 r. – 2 411 tys. zł;

6) w 2031 r. – 2 603 tys. zł;

7) w 2032 r. – 2 533 tys. zł;

8) w 2033 r. – 2 596 tys. zł;

9) w 2034 r. – 2 661 tys. zł;

10) w 2035 r. – 2 728 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 46. 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. – 586 tys. zł;
2) w 2027 r. – 611 tys. zł;
3) w 2028 r. – 626 tys. zł;
4) w 2029 r. – 642 tys. zł;
5) w 2030 r. – 658 tys. zł;
6) w 2031 r. – 710 tys. zł;
7) w 2032 r. – 691 tys. zł;
8) w 2033 r. – 708 tys. zł;
9) w 2034 r. – 726 tys. zł;
10) w 2035 r. – 744 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 47. 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. – 2 461 tys. zł;
2) w 2027 r. – 1 093 tys. zł;
3) w 2028 r. – 1 123 tys. zł;
4) w 2029 r. – 1 153 tys. zł;
5) w 2030 r. – 1 185 tys. zł;
6) w 2031 r. – 1 253 tys. zł;
7) w 2032 r. – 1 250 tys. zł;
8) w 2033 r. – 1 284 tys. zł;
9) w 2034 r. – 1 319 tys. zł;
10) w 2035 r. – 1 355 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów:

1) nowo powstałych stanowisk pracy;

2) funkcjonowania wykazu podmiotów krytycznych prowadzonego w systemie, o którym mowa w art. 46 ust. 1 ustawy zmienianej w art. 20.

Art. 48. 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. – 586 tys. zł;

2) w 2027 r. – 611 tys. zł;

3) w 2028 r. – 626 tys. zł;

4) w 2029 r. – 642 tys. zł;

5) w 2030 r. – 658 tys. zł;

6) w 2031 r. – 710 tys. zł;

7) w 2032 r. – 691 tys. zł;

8) w 2033 r. – 708 tys. zł;

9) w 2034 r. – 726 tys. zł;

10) w 2035 r. – 744 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 49. 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. – 195 tys. zł;

2) w 2027 r. – 204 tys. zł;

3) w 2028 r. – 209 tys. zł;

4) w 2029 r. – 214 tys. zł;

5) w 2030 r. – 219 tys. zł;

6) w 2031 r. – 237 tys. zł;

7) w 2032 r. – 230 tys. zł;

8) w 2033 r. – 236 tys. zł;

9) w 2034 r. – 242 tys. zł;

10) w 2035 r. – 248 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałego stanowiska pracy.

Art. 50. 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. – 586 tys. zł;

2) w 2027 r. – 611 tys. zł;

3) w 2028 r. – 626 tys. zł;

4) w 2029 r. – 642 tys. zł;

5) w 2030 r. – 658 tys. zł;

6) w 2031 r. – 710 tys. zł;

7) w 2032 r. – 691 tys. zł;

8) w 2033 r. – 708 tys. zł;

9) w 2034 r. – 726 tys. zł;

10) w 2035 r. – 744 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 51. 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. – 10 081 tys. zł;

2) w 2027 r. – 7 444 tys. zł;

3) w 2028 r. – 7 619 tys. zł;

4) w 2029 r. – 7 792 tys. zł;

5) w 2030 r. – 7 975 tys. zł;

6) w 2031 r. – 8 500 tys. zł;

7) w 2032 r. – 8 357 tys. zł;

8) w 2033 r. – 8 554 tys. zł;

9) w 2034 r. – 8 757 tys. zł;

10) w 2035 r. – 8 965 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów:

1) nowo powstałych stanowisk pracy;

2) finansowania działalności Rządowego Centrum Bezpieczeństwa w zakresie prowadzenia:

   a) Pojedynczego Punktu Kontaktowego,

   b) wykazu, o którym mowa w art. 6r ust. 1 ustawy zmienianej w art. 1, oraz wykazu, o którym mowa w art. 6y ust. 1 ustawy zmienianej w art. 1,

   c) wykazu, o którym mowa w art. 6zo ust. 1 ustawy zmienianej w art. 1;

3) finansowania tworzenia i działalności Centrum Bezpieczeństwa Morskiego.

4. Wdrożenie mechanizmu korygującego, o którym mowa w ust. 3 pkt 1 i 2, następuje w uzgodnieniu z Prezesem Rady Ministrów.

Art. 52. 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. – 586 tys. zł;

2) w 2027 r. – 611 tys. zł;

3) w 2028 r. – 626 tys. zł;

4) w 2029 r. – 642 tys. zł;

5) w 2030 r. – 658 tys. zł;

6) w 2031 r. – 710 tys. zł;

7) w 2032 r. – 691 tys. zł;

8) w 2033 r. – 708 tys. zł;

9) w 2034 r. – 726 tys. zł;

10) w 2035 r. – 744 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 53. 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. – 586 tys. zł;

2) w 2027 r. – 611 tys. zł;

3) w 2028 r. – 626 tys. zł;

4) w 2029 r. – 642 tys. zł;

5) w 2030 r. – 658 tys. zł;

6) w 2031 r. – 710 tys. zł;

7) w 2032 r. – 691 tys. zł;

8) w 2033 r. – 708 tys. zł;

9) w 2034 r. – 726 tys. zł;

10) w 2035 r. – 744 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 54. 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. – 586 tys. zł;

2) w 2027 r. – 611 tys. zł;

3) w 2028 r. – 626 tys. zł;

4) w 2029 r. – 642 tys. zł;

5) w 2030 r. – 658 tys. zł;

6) w 2031 r. – 710 tys. zł;

7) w 2032 r. – 691 tys. zł;

8) w 2033 r. – 708 tys. zł;

9) w 2034 r. – 726 tys. zł;

10) w 2035 r. – 744 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 55. 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. – 586 tys. zł;

2) w 2027 r. – 611 tys. zł;

3) w 2028 r. – 626 tys. zł;

4) w 2029 r. – 642 tys. zł;

5) w 2030 r. – 658 tys. zł;

6) w 2031 r. – 710 tys. zł;

7) w 2032 r. – 691 tys. zł;

8) w 2033 r. – 708 tys. zł;

9) w 2034 r. – 726 tys. zł;

10) w 2035 r. – 744 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 56. 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. – 586 tys. zł;

2) w 2027 r. – 611 tys. zł;

3) w 2028 r. – 626 tys. zł;

4) w 2029 r. – 642 tys. zł;

5) w 2030 r. – 658 tys. zł;

6) w 2031 r. – 710 tys. zł;

7) w 2032 r. – 691 tys. zł;

8) w 2033 r. – 708 tys. zł;

9) w 2034 r. – 726 tys. zł;

10) w 2035 r. – 744 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 57. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 85/02 – województwo dolnośląskie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 426 tys. zł;

2) w 2027 r. – 433 tys. zł;

3) w 2028 r. – 444 tys. zł;

4) w 2029 r. – 454 tys. zł;

5) w 2030 r. – 466 tys. zł;

6) w 2031 r. – 513 tys. zł;

7) w 2032 r. – 489 tys. zł;

8) w 2033 r. – 502 tys. zł;

9) w 2034 r. – 514 tys. zł;

10) w 2035 r. – 527 tys. zł.

2. Wojewoda dolnośląski 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 58. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 85/04 – województwo kujawsko-pomorskie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 426 tys. zł;

2) w 2027 r. – 433 tys. zł;

3) w 2028 r. – 444 tys. zł;

4) w 2029 r. – 454 tys. zł;

5) w 2030 r. – 466 tys. zł;

6) w 2031 r. – 513 tys. zł;

7) w 2032 r. – 489 tys. zł;

8) w 2033 r. – 502 tys. zł;

9) w 2034 r. – 514 tys. zł;

10) w 2035 r. – 527 tys. zł.

2. Wojewoda kujawsko-pomorski 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 59. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 85/06 – województwo lubelskie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 426 tys. zł;

2) w 2027 r. – 433 tys. zł;

3) w 2028 r. – 444 tys. zł;

4) w 2029 r. – 454 tys. zł;

5) w 2030 r. – 466 tys. zł;

6) w 2031 r. – 513 tys. zł;

7) w 2032 r. – 489 tys. zł;

8) w 2033 r. – 502 tys. zł;

9) w 2034 r. – 514 tys. zł;

10) w 2035 r. – 527 tys. zł.

2. Wojewoda lubelski 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 60. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 85/08 – województwo lubuskie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 426 tys. zł;

2) w 2027 r. – 433 tys. zł;

3) w 2028 r. – 444 tys. zł;

4) w 2029 r. – 454 tys. zł;

5) w 2030 r. – 466 tys. zł;

6) w 2031 r. – 513 tys. zł;

7) w 2032 r. – 489 tys. zł;

8) w 2033 r. – 502 tys. zł;

9) w 2034 r. – 514 tys. zł;

10) w 2035 r. – 527 tys. zł.

2. Wojewoda lubuski 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 61. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 85/10 – województwo łódzkie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 426 tys. zł;

2) w 2027 r. – 433 tys. zł;

3) w 2028 r. – 444 tys. zł;

4) w 2029 r. – 454 tys. zł;

5) w 2030 r. – 466 tys. zł;

6) w 2031 r. – 513 tys. zł;

7) w 2032 r. – 489 tys. zł;

8) w 2033 r. – 502 tys. zł;

9) w 2034 r. – 514 tys. zł;

10) w 2035 r. – 527 tys. zł.

2. Wojewoda łódzki 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 62. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 85/12 – województwo małopolskie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 426 tys. zł;

2) w 2027 r. – 433 tys. zł;

3) w 2028 r. – 444 tys. zł;

4) w 2029 r. – 454 tys. zł;

5) w 2030 r. – 466 tys. zł;

6) w 2031 r. – 513 tys. zł;

7) w 2032 r. – 489 tys. zł;

8) w 2033 r. – 502 tys. zł;

9) w 2034 r. – 514 tys. zł;

10) w 2035 r. – 527 tys. zł.

2. Wojewoda małopolski 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 63. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 85/14 – województwo mazowieckie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 426 tys. zł;

2) w 2027 r. – 433 tys. zł;

3) w 2028 r. – 444 tys. zł;

4) w 2029 r. – 454 tys. zł;

5) w 2030 r. – 466 tys. zł;

6) w 2031 r. – 513 tys. zł;

7) w 2032 r. – 489 tys. zł;

8) w 2033 r. – 502 tys. zł;

9) w 2034 r. – 514 tys. zł;

10) w 2035 r. – 527 tys. zł.

2. Wojewoda mazowiecki 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 64. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 85/16 – województwo opolskie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 426 tys. zł;
2) w 2027 r. – 433 tys. zł;
3) w 2028 r. – 444 tys. zł;
4) w 2029 r. – 454 tys. zł;
5) w 2030 r. – 466 tys. zł;
6) w 2031 r. – 513 tys. zł;
7) w 2032 r. – 489 tys. zł;
8) w 2033 r. – 502 tys. zł;
9) w 2034 r. – 514 tys. zł;
10) w 2035 r. – 527 tys. zł.

2. Wojewoda opolski 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 65. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 85/18 – województwo podkarpackie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 426 tys. zł;
2) w 2027 r. – 433 tys. zł;
3) w 2028 r. – 444 tys. zł;
4) w 2029 r. – 454 tys. zł;
5) w 2030 r. – 466 tys. zł;
6) w 2031 r. – 513 tys. zł;
7) w 2032 r. – 489 tys. zł;
8) w 2033 r. – 502 tys. zł;
9) w 2034 r. – 514 tys. zł;
10) w 2035 r. – 527 tys. zł.

2. Wojewoda podkarpacki 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 66. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 85/20 – województwo podlaskie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 426 tys. zł;
2) w 2027 r. – 433 tys. zł;
3) w 2028 r. – 444 tys. zł;
4) w 2029 r. – 454 tys. zł;

5) w 2030 r. – 466 tys. zł;

6) w 2031 r. – 513 tys. zł;

7) w 2032 r. – 489 tys. zł;

8) w 2033 r. – 502 tys. zł;

9) w 2034 r. – 514 tys. zł;

10) w 2035 r. – 527 tys. zł.

2. Wojewoda podlaski 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 67. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 85/22 – województwo pomorskie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 426 tys. zł;

2) w 2027 r. – 433 tys. zł;

3) w 2028 r. – 444 tys. zł;

4) w 2029 r. – 454 tys. zł;

5) w 2030 r. – 466 tys. zł;

6) w 2031 r. – 513 tys. zł;

7) w 2032 r. – 489 tys. zł;

8) w 2033 r. – 502 tys. zł;

9) w 2034 r. – 514 tys. zł;

10) w 2035 r. – 527 tys. zł.

2. Wojewoda pomorski 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 68. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 85/24 – województwo śląskie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 426 tys. zł;

2) w 2027 r. – 433 tys. zł;

3) w 2028 r. – 444 tys. zł;

4) w 2029 r. – 454 tys. zł;

5) w 2030 r. – 466 tys. zł;

6) w 2031 r. – 513 tys. zł;

7) w 2032 r. – 489 tys. zł;

8) w 2033 r. – 502 tys. zł;

9) w 2034 r. – 514 tys. zł;

10) w 2035 r. – 527 tys. zł.

2. Wojewoda śląski 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 69. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 85/26 – województwo świętokrzyskie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 426 tys. zł;
2) w 2027 r. – 433 tys. zł;
3) w 2028 r. – 444 tys. zł;
4) w 2029 r. – 454 tys. zł;
5) w 2030 r. – 466 tys. zł;
6) w 2031 r. – 513 tys. zł;
7) w 2032 r. – 489 tys. zł;
8) w 2033 r. – 502 tys. zł;
9) w 2034 r. – 514 tys. zł;
10) w 2035 r. – 527 tys. zł.

2. Wojewoda świętokrzyski 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 70. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 85/28 – województwo warmińsko-mazurskie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 426 tys. zł;
2) w 2027 r. – 433 tys. zł;
3) w 2028 r. – 444 tys. zł;
4) w 2029 r. – 454 tys. zł;
5) w 2030 r. – 466 tys. zł;
6) w 2031 r. – 513 tys. zł;
7) w 2032 r. – 489 tys. zł;
8) w 2033 r. – 502 tys. zł;
9) w 2034 r. – 514 tys. zł;
10) w 2035 r. – 527 tys. zł.

2. Wojewoda warmińsko-mazurski 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 71. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 85/30 – województwo wielkopolskie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 426 tys. zł;
2) w 2027 r. – 433 tys. zł;
3) w 2028 r. – 444 tys. zł;
4) w 2029 r. – 454 tys. zł;
5) w 2030 r. – 466 tys. zł;
6) w 2031 r. – 513 tys. zł;
7) w 2032 r. – 489 tys. zł;
8) w 2033 r. – 502 tys. zł;
9) w 2034 r. – 514 tys. zł;
10) w 2035 r. – 527 tys. zł.

2. Wojewoda wielkopolski 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 72. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 85/32 – województwo zachodniopomorskie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2026 r. – 426 tys. zł;
2) w 2027 r. – 433 tys. zł;
3) w 2028 r. – 444 tys. zł;
4) w 2029 r. – 454 tys. zł;
5) w 2030 r. – 466 tys. zł;
6) w 2031 r. – 513 tys. zł;
7) w 2032 r. – 489 tys. zł;
8) w 2033 r. – 502 tys. zł;
9) w 2034 r. – 514 tys. zł;
10) w 2035 r. – 527 tys. zł.

2. Wojewoda zachodniopomorski 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 oraz odpowiada za wdrożenie mechanizmu korygującego, o którym mowa w ust. 3.

3. W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1, zastosowany zostanie mechanizm korygujący polegający na ograniczeniu kosztów nowo powstałych stanowisk pracy.

Art. 73. Ustawa wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Prezydent Rzeczypospolitej Polskiej: *K. Nawrocki*

Załącznik do ustawy z dnia 29 maja 2026 r.
(Dz. U. poz. 815)

SEKTORY, PODSEKTORY I KATEGORIE PODMIOTÓW

I	II	III
Sektor	Podsektor	Kategoria podmiotu
Energia	Wydobywanie kopalin	Podmioty prowadzące działalność gospodarczą w zakresie wydobywania gazu ziemnego na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze.
		Podmioty prowadzące działalność gospodarczą w zakresie wydobywania ropy naftowej na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze.
		Podmioty prowadzące działalność gospodarczą w zakresie wydobywania węgla brunatnego na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze.
		Podmioty prowadzące działalność gospodarczą w zakresie wydobywania węgla kamiennego na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze.
		Podmioty prowadzące działalność gospodarczą w zakresie wydobywania pozostałych kopalin na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze.
	Energia elektryczna	Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie wytwarzania energii elektrycznej.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 24 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie przesyłania energii elektrycznej.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 25 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie dystrybucji energii elektrycznej.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie obrotu energią elektryczną.
		Podmioty, o których mowa w art. 3 pkt 28b ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne.
		Uczestnicy rynku świadczący usługę, o której mowa w art. 3 pkt 11j ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, świadczące usługę, o której mowa w art. 3 pkt 6e tej ustawy.
		Przedsiębiorcy odpowiedzialni za zarządzanie punktem ładowania i jego obsługę, świadczący usługę ładowania na rzecz użytkowników końcowych, w tym w imieniu i na rzecz dostawcy usług w zakresie mobilności.
		Uczestnicy rynku świadczący usługę, o której mowa w art. 3 pkt 59 i 59a ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne.
	Ciepło	Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie wytwarzania ciepła.

		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie obrotu ciepłem.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie przesyłania ciepła.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie dystrybucji ciepła.
	Ropa i paliwa	Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie wytwarzania paliw ciekłych, o której mowa w art. 32 ust. 1 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne.
		Podmioty prowadzące działalność gospodarczą w zakresie przesyłania ropy naftowej.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie przesyłania paliw ciekłych siecią rurociągów, o której mowa w art. 32 ust. 1 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne.
		Podmiot prowadzący działalność gospodarczą w zakresie magazynowania ropy naftowej, w tym w zakresie bezzbiornikowego podziemnego magazynowania ropy naftowej, o którym mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze.
		Podmioty prowadzące działalność gospodarczą w zakresie przeładunku ropy naftowej.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, wykonujące działalność gospodarczą w zakresie magazynowania paliw ciekłych, o którym mowa w art. 32 ust. 1 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, oraz podmiot prowadzący działalność w zakresie bezzbiornikowego podziemnego magazynowania paliw ciekłych, o którym mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, wykonujące działalność gospodarczą w zakresie przeładunku paliw ciekłych, o którym mowa w art. 32 ust. 1 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, wykonujące działalność gospodarczą w zakresie obrotu paliwami ciekłymi lub w zakresie obrotu paliwami ciekłymi z zagranicą, o którym mowa w art. 32 ust. 1 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne.
		Podmioty prowadzące działalność gospodarczą w zakresie wytwarzania paliw syntetycznych.
		Agencja wykonawcza utworzona na podstawie ustawy z dnia 17 grudnia 2020 r. o rezerwach strategicznych.
	Gaz	Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, prowadzące działalność w zakresie wytwarzania paliw gazowych, o którym mowa w art. 3 pkt 45 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne.

		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie przesyłania paliw gazowych.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie obrotu gazem ziemnym z zagranicą lub na wykonywanie działalności gospodarczej w zakresie obrotu paliwami gazowymi.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 24 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, będące wyznaczonym przez Prezesa Urzędu Regulacji Energetyki operatorem systemu przesyłowego gazowego.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 25 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, będące wyznaczonym przez Prezesa Urzędu Regulacji Energetyki operatorem systemu dystrybucyjnego gazowego.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 26 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, będące wyznaczonym przez Prezesa Urzędu Regulacji Energetyki operatorem systemu magazynowania paliw gazowych.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 27 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, będące wyznaczonym przez Prezesa Urzędu Regulacji Energetyki operatorem systemu skraplania gazu ziemnego.
		Przedsiębiorstwa energetyczne prowadzące działalność gospodarczą w zakresie rafinacji i przetwarzania gazu ziemnego.
	Wodór	Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, prowadzące działalność w zakresie wytwarzania wodoru.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, prowadzące działalność w zakresie magazynowania wodoru.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, prowadzące działalność w zakresie przesyłania wodoru.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, prowadzące działalność w zakresie dystrybucji wodoru.
	Energetyka jądrowa	Podmiot będący operatorem obiektu energetyki jądrowej i inwestorem, określonego w art. 2 pkt 2 ustawy z dnia 29 czerwca 2011 r. o przygotowaniu i realizacji inwestycji w zakresie obiektów energetyki jądrowej oraz inwestycji towarzyszących.
Transport	Transport lotniczy	Przewoźnik lotniczy, o którym mowa w art. 3 pkt 4 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 300/2008 z dnia 11 marca 2008 r. w sprawie wspólnych zasad w dziedzinie ochrony lotnictwa cywilnego i uchylającego rozporządzenie (WE) nr 2320/2002.
		Zarządzający lotniskiem, o którym mowa w art. 2 pkt 7 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze.

		Przedsiębiorca, o którym mowa w art. 177 ust. 2 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze, wykonujący dla przewoźników lotniczych oraz innych użytkowników statków powietrznych jedną lub więcej kategorii usług, o których mowa w art. 176 tej ustawy, oraz przedsiębiorca, o którym mowa w art. 186b ust. 1 pkt 2 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze, wykonujący zadania związane z kontrolą bezpieczeństwa.
		Instytucja zapewniająca służby żeglugi powietrznej, o której mowa w art. 127 ust. 1 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze.
	Transport kolejowy	Zarządca infrastruktury kolejowej w rozumieniu art. 4 pkt 7 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym, z wyłączeniem zarządców wyłącznie infrastruktury nieczynnej, o której mowa w art. 4 pkt 1b tej ustawy, infrastruktury prywatnej, o której mowa w art. 4 pkt 1c tej ustawy, oraz infrastruktury kolei wąskotorowej, o której mowa w art. 4 pkt 1d tej ustawy.
		Przewoźnik kolejowy, o którym mowa w art. 4 pkt 9 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym, którego działalność podlega licencjonowaniu, oraz operator obiektu infrastruktury usługowej, o którym mowa w art. 4 pkt 52 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym, jeżeli przedsiębiorca wykonujący funkcję operatora jest jednocześnie przewoźnikiem kolejowym.
	Transport wodny	Armator w transporcie morskim pasażerów i towarów zgodnie z definicją dla transportu morskiego w załączniku I do rozporządzenia (WE) nr 725/2004 Parlamentu Europejskiego i Rady z dnia 31 marca 2004 r. w sprawie podniesienia ochrony statków i obiektów portowych, z wyłączeniem poszczególnych statków, na których prowadzą działalność ci armatorzy.
		Armator, o którym mowa w art. 5 ust. 1 pkt 2 ustawy z dnia 21 grudnia 2000 r. o żegludze śródlądowej.
		Podmiot zarządzający portem morskim, o którym mowa w art. 3 ust. 1 pkt 2 ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich.
		Podmiot zarządzający obiektem portowym, o którym mowa w art. 2 pkt 11 rozporządzenia (WE) nr 725/2004 Parlamentu Europejskiego i Rady z dnia 31 marca 2004 r. w sprawie podniesienia ochrony statków i obiektów portowych.
		Podmioty prowadzące na terenie portu działalność wspomagającą transport morski.
		VTS (Służba Kontroli Ruchu Statków) – aparat pomocniczy dyrektora urzędu morskiego powołany w celu monitorowania ruchu statków i przekazywania informacji, stanowiący część składową Narodowego Systemu SafeSeaNet, o którym mowa w art. 91 ustawy z dnia 18 sierpnia 2011 r. o bezpieczeństwie morskim.
	Transport publiczny	Podmioty, o których mowa w art. 4 ust. 1 pkt 8 ustawy z dnia 16 grudnia 2010 r. o publicznym transporcie zbiorowym.
	Transport drogowy	Organy, o których mowa w art. 19 ust. 2, 5 i 5a ustawy z dnia 21 marca 1985 r. o drogach publicznych, z wyłączeniem podmiotów publicznych, dla których zarządzanie ruchem lub obsługa inteligentnych systemów transportowych stanowią inną niż istotna część ich ogólnej działalności.
		Podmioty, o których mowa w art. 43a ust. 1 ustawy z dnia 21 marca 1985 r. o drogach publicznych.
Bankowość i infrastruktura rynków finansowych		Bank krajowy, o którym mowa w art. 4 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe.
		Oddział banku zagranicznego, o którym mowa w art. 4 ust. 1 pkt 20 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe.
		Spółdzielcze kasy oszczędnościowo-kredytowe w rozumieniu ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych.

		Podmiot prowadzący rynek regulowany, o którym mowa w art. 14 ust. 1 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi.
		Podmiot, o którym mowa w art. 3 pkt 49 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi.
		Podmiot, o którym mowa w art. 48 ust. 7 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi.
		Administratorzy kluczowych wskaźników referencyjnych.
		Centralny depozyt papierów wartościowych, o którym mowa w art. 3 pkt 21a ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi, mający siedzibę na terytorium Rzeczypospolitej Polskiej.
		Podmiot prowadzący ASO w rozumieniu art. 3 pkt 2 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi.
		Podmiot prowadzący OTF w rozumieniu art. 3 pkt 10b ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi.
		Giełda towarowa w rozumieniu art. 2 pkt 1 ustawy z dnia 26 października 2000 r. o giełdach towarowych.
		Izba rozliczeniowa, o której mowa w art. 67 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe.
		Giełdowa izba rozrachunkowa w rozumieniu art. 2 pkt 4 ustawy z dnia 26 października 2000 r. o giełdach towarowych.
		Izba rozliczeniowa w rozumieniu art. 68a ust. 1 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi.
		Izba rozrachunkowa w rozumieniu art. 68a ust. 2 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi.
Ochrona zdrowia	Udzielanie świadczeń zdrowotnych i zdrowie publiczne	Podmiot leczniczy, o którym mowa w art. 4 ust. 1 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej.
		Laboratoria referencyjne UE, o których mowa w art. 15 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2371 z dnia 23 listopada 2022 r. w sprawie poważnych transgranicznych zagrożeń zdrowia oraz uchylenia decyzji nr 1082/2013/UE.
		Jednostki organizacyjne publicznej służby krwi, o których mowa w art. 4 ust. 3 pkt 2 ustawy z dnia 22 sierpnia 1997 r. o publicznej służbie krwi.
		Podmioty udzielające świadczeń opieki zdrowotnej w rozumieniu art. 133 ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych.
		Jednostki organizacyjne podległe lub nadzorowane przez ministra kierującego działem administracji rządowej – zdrowie.
		Urzędy obsługujące centralne organy nadzorowane przez ministra właściwego do spraw zdrowia.
	Produkcja, dystrybucja, obrót i magazynowanie substancji czynnych, produktów leczniczych i wyrobów medycznych	Urzędy obsługujące organy Państwowej Inspekcji Farmaceutycznej.
		Podmioty prowadzące działalność badawczo-rozwojową w zakresie produktów leczniczych zdefiniowanych w art. 1 pkt 2 dyrektywy 2001/83/WE Parlamentu Europejskiego i Rady z dnia 6 listopada 2001 r. w sprawie wspólnotowego kodeksu odnoszącego się do produktów leczniczych stosowanych u ludzi.
		Podmioty produkujące podstawowe substancje farmaceutyczne oraz leki i pozostałe wyroby farmaceutyczne, o których mowa w sekcji C dział 21 klasyfikacji NACE Rev. 2.

		Podmioty produkujące wyroby medyczne uznane za mające krytyczne znaczenie podczas danego stanu zagrożenia zdrowia publicznego („wykaz wyrobów medycznych o krytycznym znaczeniu w przypadku stanu zagrożenia zdrowia publicznego”) w rozumieniu art. 22 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/123 z dnia 25 stycznia 2022 r. w sprawie wzmocnienia roli Europejskiej Agencji Leków w zakresie gotowości na wypadek sytuacji kryzysowej i zarządzania kryzysowego w odniesieniu do produktów leczniczych i wyrobów medycznych.
		Przedsiębiorca prowadzący działalność polegającą na prowadzeniu hurtowni farmaceutycznej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.
		Przedsiębiorca lub podmiot prowadzący działalność gospodarczą w państwie członkowskim Unii Europejskiej lub państwie członkowskim Europejskiego Porozumienia o Wolnym Handlu (EFTA) – stronie umowy o Europejskim Obszarze Gospodarczym, który uzyskał pozwolenie na dopuszczenie do obrotu produktu leczniczego.
		Wytwórca lub importer produktu leczniczego w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.
		Wytwórca, importer lub dystrybutor substancji czynnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.
		Importer równoległy w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.
		Przedsiębiorca prowadzący działalność w formie apteki ogólnodostępnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.
		Jednostki organizacyjne podległe lub nadzorowane przez ministra kierującego działem administracji rządowej – zdrowie.
		Urzędy obsługujące centralne organy nadzorowane przez ministra właściwego do spraw zdrowia.
		Jednostki notyfikowane, jednostki oceniające zgodność, producenci, o których mowa w ustawie z dnia 7 kwietnia 2022 r. o wyrobach medycznych.
Zaopatrzenie w wodę pitną i jej dystrybucja		Podmiot dostarczający wodę przeznaczoną do spożycia przez ludzi, w tym przedsiębiorstwo wodociągowo-kanalizacyjne, o którym mowa w art. 2 pkt 4 ustawy z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków, z wyłączeniem podmiotów, dla których dostarczanie wody przeznaczonej do spożycia przez ludzi jest inną niż istotną częścią ich ogólnej działalności.
Zbiorowe odprowadzanie ścieków		Podmiot odprowadzający lub oczyszczający ścieki, w tym przedsiębiorstwo wodociągowo-kanalizacyjne, o którym mowa w art. 2 pkt 4 ustawy z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków, z wyłączeniem podmiotów, dla których odprowadzanie lub oczyszczanie ścieków jest inną niż istotną częścią ich ogólnej działalności.
Infrastruktura cyfrowa	Infrastruktura cyfrowa, z wyłączeniem komunikacji elektronicznej	Dostawca punktu wymiany ruchu internetowego.
		Dostawca usług DNS, z wyłączeniem operatorów głównych serwerów nazw.
		Rejestr nazw domen najwyższego poziomu (TLD).
		Dostawca usług chmurowych.
		Dostawca usług ośrodka przetwarzania danych.
		Dostawca sieci dostarczania treści.
		Dostawca usług zaufania.
		Podmiot świadczący usługę rejestracji nazw domen.
	Komunikacja elektroniczna	Przedsiębiorca komunikacji elektronicznej.

Administracja publiczna	Podmioty publiczne	Jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, oraz urzędy je obsługujące, z wyłączeniem jednostek organizacyjnych podległych ministrowi właściwemu do spraw budżetu, finansów publicznych i instytucji finansowych lub przez niego nadzorowanych, urzędu obsługującego tego ministra oraz spółki celowej utworzonej do wykonywania niektórych zadań dotyczących informatyzacji w zakresie działów administracji rządowej – budżet i finanse publiczne.
		Jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 3, 5, 6, 8, 9, 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, z wyłączeniem jednostek organizacyjnych obsługujących jednostki samorządu terytorialnego.
		Podmiot, o którym mowa w art. 96 ust. 1 ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych.
		Instytuty badawcze.
		Urząd Dozoru Technicznego.
		Polska Agencja Żeglugi Powietrznej.
		Polskie Centrum Akredytacji.
		Urząd Komisji Nadzoru Finansowego.
		Polska Agencja Prasowa.
		Polska Wytwórnia Papierów Wartościowych.
		Państwowe Gospodarstwo Wodne Wody Polskie, o którym mowa w ustawie z dnia 20 lipca 2017 r. – Prawo wodne.
		Polski Fundusz Rozwoju i inne instytucje rozwoju, o których mowa w art. 2 ust. 1 pkt 1 i 3–6 ustawy z dnia 4 lipca 2019 r. o systemie instytucji rozwoju.
		Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej.
		Wojewódzkie fundusze ochrony środowiska i gospodarki wodnej.
		Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych.
		Zakład Unieszkodliwiania Odpadów Promieniotwórczych z siedzibą w Otwocku Świerku.
		Podmioty zarządzające lub odpowiedzialne za stan techniczny oraz sprawność infrastruktury przeciwpowodziowej, budowli hydrotechnicznych i pozostałych obiektów o charakterze inżynierskim.
		Spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej.
	Finanse publiczne	Centrum Informatyki Resortu Finansów.
		Spółka celowa, o której mowa w art. 2 ust. 1 ustawy z dnia 29 kwietnia 2016 r. o szczególnych zasadach wykonywania niektórych zadań dotyczących informatyzacji w zakresie działów administracji rządowej budżet i finanse publiczne.
		Urząd obsługujący ministra właściwego do spraw budżetu, finansów publicznych i instytucji finansowych.
Przestrzeń kosmiczna		Operator infrastruktury naziemnej, który wspiera świadczenie usług kosmicznych, z wyjątkiem operatora, o którym mowa w art. 2 pkt 40 lit. b ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej.
		Polska Agencja Kosmiczna.

Produkcja, przetwarzanie i dystrybucja żywności		Przedsiębiorstwa spożywcze w rozumieniu art. 3 pkt 2 rozporządzenia (WE) nr 178/2002 Parlamentu Europejskiego i Rady z dnia 28 stycznia 2002 r. ustanawiającego ogólne zasady i wymagania prawa żywnościowego, powołującego Europejski Urząd ds. Bezpieczeństwa Żywności oraz ustanawiającego procedury w zakresie bezpieczeństwa żywności, zajmujące się dystrybucją hurtową oraz przemysłowymi produkcją i przetwarzaniem.
Zarządzanie usługami ICT		Dostawca usług zarządzanych.
Produkcja, wytwarzanie i dystrybucja chemikaliów		Przedsiębiorstwo zajmujące się produkcją substancji oraz wytwarzaniem i dystrybucją substancji lub mieszanin, o których mowa w art. 3 pkt 9 i 14 rozporządzenia (WE) nr 1907/2006 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2006 r. w sprawie rejestracji, oceny, udzielania zezwoleń i stosowanych ograniczeń w zakresie chemikaliów (REACH) i utworzenia Europejskiej Agencji Chemikaliów, zmieniającego dyrektywę 1999/45/WE oraz uchylającego rozporządzenie Rady (EWG) nr 793/93 i rozporządzenie Komisji (WE) nr 1488/94, jak również dyrektywę Rady 76/769/EWG i dyrektywy Komisji 91/155/EWG, 93/67/EWG, 93/105/WE i 2000/21/WE.
		Przedsiębiorstwa zajmujące się wytwarzaniem z substancji lub mieszanin wyrobów, o których mowa w art. 3 pkt 3 rozporządzenia (WE) nr 1907/2006 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2006 r. w sprawie rejestracji, oceny, udzielania zezwoleń i stosowanych ograniczeń w zakresie chemikaliów (REACH) i utworzenia Europejskiej Agencji Chemikaliów, zmieniającego dyrektywę 1999/45/WE oraz uchylającego rozporządzenie Rady (EWG) nr 793/93 i rozporządzenie Komisji (WE) nr 1488/94, jak również dyrektywę Rady 76/769/EWG i dyrektywy Komisji 91/155/EWG, 93/67/EWG, 93/105/WE i 2000/21/WE.
Usługi pocztowe		Operator pocztowy, o którym mowa w art. 3 pkt 12 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe.
Gospodarowanie odpadami	Zbieranie odpadów	Przedsiębiorstwa świadczące usługi w rozumieniu ustawy z dnia 14 grudnia 2012 r. o odpadach, polegające na zbieraniu odpadów, zobowiązane do uzyskania wpisu w rejestrze, o którym mowa w art. 49 ust. 1 ustawy z dnia 14 grudnia 2012 r. o odpadach, z wyłączeniem przedsiębiorstw, dla których usługi te nie stanowią podstawowej działalności gospodarczej określonej zgodnie z przepisami wydanymi na podstawie art. 40 ust. 7 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej.
	Transport odpadów	Przedsiębiorstwa świadczące usługi w rozumieniu ustawy z dnia 14 grudnia 2012 r. o odpadach, polegające na transporcie odpadów, zobowiązane do uzyskania wpisu w rejestrze, o którym mowa w art. 49 ust. 1 ustawy z dnia 14 grudnia 2012 r. o odpadach, z wyłączeniem przedsiębiorstw, dla których usługi te nie stanowią podstawowej działalności gospodarczej określonej zgodnie z przepisami wydanymi na podstawie art. 40 ust. 7 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej.
	Przetwarzanie odpadów, wraz z nadzorem nad wymienionymi działaniami, a także późniejsze postępowanie z miejscami unieszkodliwiania odpadów	Przedsiębiorstwa świadczące usługi w rozumieniu ustawy z dnia 14 grudnia 2012 r. o odpadach, polegające na przetwarzaniu odpadów, wraz z nadzorem nad wymienionymi działaniami, a także podmioty świadczące usługi z późniejszym postępowaniem z miejscami unieszkodliwiania odpadów, zobowiązane do uzyskania wpisu w rejestrze, o którym mowa w art. 49 ust. 1 ustawy z dnia 14 grudnia 2012 r. o odpadach, z wyłączeniem przedsiębiorstw, dla których usługi te nie stanowią podstawowej działalności gospodarczej określonej zgodnie z przepisami wydanymi na podstawie art. 40 ust. 7 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej.

	Działania wykonywane w charakterze sprzedawcy odpadów lub pośrednika w obrocie odpadami	Przedsiębiorstwa świadczące usługi w rozumieniu ustawy z dnia 14 grudnia 2012 r. o odpadach, polegające na działaniach wykonywanych w charakterze sprzedawcy odpadów lub pośrednika w obrocie odpadami, zobowiązane do uzyskania wpisu w rejestrze, o którym mowa w art. 49 ust. 1 ustawy z dnia 14 grudnia 2012 r. o odpadach, z wyłączeniem przedsiębiorstw, dla których usługi te nie stanowią podstawowej działalności gospodarczej określonej zgodnie z przepisami wydanymi na podstawie art. 40 ust. 7 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej.