

Opracowano na
podstawie: t.j.
Dz. U. z 2026 r.
poz. 574, 815.

U S T A W A

z dnia 26 kwietnia 2007 r.

o zarządzaniu kryzysowym¹⁾

Rozdział 1

Przepisy ogólne

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.

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).

Art. 2. Zarządzanie kryzysowe to działalność organów administracji publicznej będąca elementem kierowania bezpieczeństwem narodowym, która polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku

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).

wystąpienia sytuacji kryzysowych, usuwaniu ich skutków oraz odtwarzaniu zasobów i infrastruktury krytycznej.

Art. 3. Ilećroć w ustawie jest mowa o:

- 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;
- 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 incydem realizowanej w drodze zaplanowanych działań, z wykorzystaniem posiadanych zasobów, reagowania w przypadku wystąpienia incydem i jego absorbowania oraz adaptacji i usuwania skutków incydem, 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;
- 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;
- 2a) (uchylony)
- 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;
- 3) ochronie infrastruktury krytycznej – należy przez to rozumieć wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działania oraz integralności infrastruktury krytycznej;
- 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;
- 4) planowaniu cywilnym – należy przez to rozumieć:

- a) całokształt przedsięwzięć organizacyjnych mających na celu przygotowanie administracji publicznej do zarządzania kryzysowego,
 - b) planowanie w zakresie wspierania Sił Zbrojnych Rzeczypospolitej Polskiej w razie ich użycia oraz planowanie wykorzystania Sił Zbrojnych Rzeczypospolitej Polskiej do realizacji zadań z zakresu zarządzania kryzysowego;
- 5) (uchylony)
- 6) powiecie – należy przez to rozumieć również miasto na prawach powiatu;
- 7) cyklu planowania – należy przez to rozumieć okresowe realizowanie etapów: analizowania, programowania, opracowywania planu lub programu, jego wdrażanie, testowanie i uruchamianie;
- 8) siatce bezpieczeństwa – należy przez to rozumieć zestawienie potencjalnych zagrożeń ze wskazaniem podmiotu wiodącego oraz podmiotów współpracujących w realizacji działań zarządzania kryzysowego;
- 9) (uchylony)
- 10) (uchylony)
- 11) zdarzeniu o charakterze terrorystycznym – należy przez to rozumieć sytuację, o której mowa w art. 2 pkt 7 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2025 r. poz. 194);
- 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) osiągnięciu 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.²⁾);
- 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.

²⁾ 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.

Art. 4. 1. Zadania z zakresu planowania cywilnego obejmują:

- 1) przygotowanie planów zarządzania kryzysowego;
- 1a) prowadzenie oceny ryzyka;
- 2) przygotowanie struktur uruchamianych w sytuacjach kryzysowych;
- 3) przygotowanie i utrzymywanie zasobów niezbędnych do wykonania zadań ujętych w planie zarządzania kryzysowego;
- 4) utrzymywanie baz danych niezbędnych w procesie zarządzania kryzysowego;
- 5) przygotowanie rozwiązań na wypadek zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej;
- 6) zapewnienie spójności między planami zarządzania kryzysowego a innymi planami sporządzanymi w tym zakresie przez właściwe organy administracji publicznej, których obowiązek wykonania wynika z odrębnych przepisów.

2. Zadania, o których mowa w ust. 1, powinny uwzględniać:

- 1) zapewnienie funkcjonowania administracji publicznej w sytuacji kryzysowej;
- 2) zapewnienie funkcjonowania i możliwości odtworzenia infrastruktury krytycznej;
- 3) zapewnienie ciągłego monitorowania zagrożeń;
- 4) racjonalne gospodarowanie siłami i środkami w sytuacjach kryzysowych;
- 5) pomoc udzielaną ludności w zapewnieniu jej warunków przetrwania w sytuacjach kryzysowych.

Art. 5. (uchylony)

Art. 5a. (uchylony)

Art. 5b. (uchylony)

Art. 6. (uchylony)

Art. 6a. (uchylony)

Art. 6b. (uchylony)

Art. 6c. (uchylony)

Art. 6d. (uchylony)

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. 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.³⁾);

³⁾ Zmiany wymienionej decyzji zostały ogłoszone w Dz. Urz. UE L 250 z 04.10.2018, str. 1, Dz. Urz. UE L 771 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.

- 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.

13. Dyrektor Centrum przedkłada Radzie Ministrów projekt KOR nie częściej 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 osiągnięciu 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.⁴⁾), 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. 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.

⁴⁾ 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.

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 nie później 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 nie rzadziej 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 nie rzadziej 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 nie dłuższym 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 spełniają 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 wiąże 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 uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80, z późn. zm.⁵⁾), 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:

⁵⁾ Zmiana wymienionej dyrektywy została ogłoszona w Dz. Urz. UE L 2025/90884 z 06.11.2025.

- 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;
- 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) Prokuraturii 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 wnioski 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, nie później 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, nie później 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 nie rzadziej 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 wiąże 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 incydemem 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, nie później niż w terminie 24 godzin od momentu jego wystąpienia lub wykrycia:
 - a) właściwemu organowi do spraw podmiotów krytycznych oraz dyrektorowi Centrum,
 - b) Szefowi Agencji Bezpieczeństwa Wewnętrznego,
 - c) podmiotowi, w ramach którego funkcjonuje Zespół Reagowania na Incydynty 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 nie dłuższym 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. 6zv. 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 przeprowadzaniem audytu, 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. 6zsz. 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 dokonany 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, nie dłuższym niż 14 dni od dnia otrzymania żądania, informacji niezbędnych do określenia wymiaru kary pieniężnej.

4. W przypadku nieprzekazania informacji, o których mowa w ust. 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 rygiorem 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.

Rozdział 17

Organy właściwe w sprawach zarządzania kryzysowego i ich zadania

Art. 7. 1. Rada Ministrów sprawuje zarządzanie kryzysowe na terytorium Rzeczypospolitej Polskiej.

2. W przypadkach niecierpiących zwłoki zarządzanie kryzysowe sprawuje minister właściwy do spraw wewnętrznych, zawiadamiając niezwłocznie o swoich działaniach Prezesa Rady Ministrów.

3. Decyzje podjęte przez ministra właściwego do spraw wewnętrznych podlegają rozpatrzeniu na najbliższym posiedzeniu Rady Ministrów.

4. Prezes Rady Ministrów, z zachowaniem przepisów o ochronie informacji niejawnych, określa, w drodze zarządzenia, wykaz przedsięwzięć i procedur systemu zarządzania kryzysowego z uwzględnieniem zobowiązań wynikających z członkostwa w Organizacji Traktatu Północnoatlantyckiego oraz organy odpowiedzialne za ich uruchamianie.

Art. 7a. 1. W sytuacji kryzysowej Prezes Rady Ministrów może, z własnej inicjatywy albo na wniosek ministra wydawać polecenia obowiązujące:

- 1) organy administracji rządowej;
- 2) państwowe osoby prawne oraz państwowe jednostki organizacyjne posiadające osobowość prawną;
- 3) organy samorządu terytorialnego, samorządowe osoby prawne oraz samorządowe jednostki organizacyjne nieposiadające osobowości prawnej;
- 4) osoby prawne, inne niż określone w pkt 2, i jednostki organizacyjne nieposiadające osobowości prawnej oraz przedsiębiorców.

2. W sytuacji kryzysowej minister kierujący działem administracji rządowej, zwany dalej „ministrem wydającym polecenie”, może wydawać w zakresie swojego działania, określonego zgodnie z przepisami ustawy z dnia 4 września 1997 r. o działach administracji rządowej (Dz. U. z 2025 r. poz. 1275 i 1846 oraz z 2026 r. poz. 160 i 187), polecenia obowiązujące:

- 1) podległe mu lub przez niego nadzorowane organy administracji rządowej;
- 2) podległe mu lub przez niego nadzorowane państwowe osoby prawne oraz państwowe jednostki organizacyjne posiadające osobowość prawną;
- 3) spółki, w których prawa z akcji Skarbu Państwa wykonuje:
 - a) minister wydający polecenie,
 - b) państwowa osoba prawna lub państwowa jednostka organizacyjna posiadająca osobowość prawną, która jest podległa ministrowi wydającemu polecenie lub jest przez niego nadzorowana,
 - c) inna spółka, w której prawa z akcji Skarbu Państwa wykonuje minister wydający polecenie.

3. Polecenia, o których mowa w ust. 1 i 2, mogą być wydawane w celu:

- 1) przejęcia kontroli nad sytuacją kryzysową, której wpływ na poziom bezpieczeństwa ludzi, mienia lub środowiska, jest szczególnie negatywny;
- 2) zapewnienia właściwego funkcjonowania, ochrony, wzmocnienia lub odbudowy infrastruktury krytycznej lub zapewnienia niezakłóconego świadczenia usługi kluczowej;
- 3) usunięcia skutków sytuacji kryzysowej, o której mowa w pkt 1.

4. Polecenia, o których mowa w ust. 1 i 2, nie mogą dotyczyć rozstrzygnięć co do istoty sprawy załatwianej w drodze decyzji administracyjnej, a także nie

mogą dotyczyć czynności operacyjno-rozpoznawczych, dochodzeniowo-śledczych oraz czynności z zakresu ścigania wykroczeń i przestępstw.

5. Wykonywanie poleceń, o których mowa w ust. 1, może być finansowane z budżetu państwa lub innych źródeł określonych na podstawie odrębnych przepisów. Polecenia, o których mowa w ust. 2, są finansowane z części budżetowej, której dysponentem jest minister wydający polecenie.

6. W przypadku wydania polecenia, o którym mowa w ust. 1, minister właściwy do spraw finansów publicznych może utworzyć w celu finansowania nową rezerwę celową i przenieść do tej rezerwy kwoty wydatków zablokowanych na podstawie art. 177 ust. 1 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2025 r. poz. 1483, 1844 i 1846 oraz z 2026 r. poz. 426).

7. Wniosek, o którym mowa w ust. 1, zawiera co najmniej:

- 1) wskazanie podmiotu, wobec którego ma być wydane polecenie;
- 2) określenie zakresu przedmiotowego polecenia;
- 3) szczegółowe uzasadnienie wniosku, w tym określenie celu, o którym mowa w ust. 3;
- 4) określenie szacunkowych kosztów wykonania polecenia;
- 5) wskazanie źródeł finansowania wykonania polecenia;
- 6) określenie okresu, w jakim ma obowiązywać polecenie;
- 7) wskazanie ministra właściwego w sprawach wykonania oraz nadzorowania wykonania polecenia.

8. W przypadku, gdy wniosek nie spełnia wymogów, o których mowa w ust. 7, Prezes Rady Ministrów może wystąpić do ministra składającego wniosek o jego uzupełnienie lub wyjaśnienie treści.

9. Polecenia, o których mowa w ust. 1 i 2, są wydawane po uzyskaniu opinii Prezesa Prokuratury Generalnej Rzeczypospolitej Polskiej i podlegają natychmiastowemu wykonaniu z chwilą ich doręczenia.

10. Prezes Prokuratury Generalnej Rzeczypospolitej Polskiej wydaje opinię o projekcie polecenia niezwłocznie, niepóźniej jednak niż po upływie 3 dni od dnia przekazania projektu polecenia.

11. W uzasadnionych przypadkach polecenia, o których mowa w ust. 1, mogą być wydane bez wystąpienia o opinię, o której mowa w ust. 9, lub przed jej uzyskaniem.

12. Do wydawania poleceń, o których mowa w ust. 1 i 2, ich zmiany oraz uchylenia, nie stosuje się przepisów ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2025 r. poz. 1691), z wyjątkiem przepisów dotyczących doręczeń oraz sprostowań.

13. Polecenia, o których mowa w ust. 1 i 2, zawierają w szczególności:

- 1) podstawę prawną wydania polecenia;
- 2) wskazanie na czyj wniosek polecenie jest wydawane, w przypadku poleceń wydawanych na wniosek;
- 3) wskazanie podmiotu, wobec którego polecenie jest wydawane;
- 4) określenie zakresu przedmiotowego polecenia;
- 5) wskazanie źródeł finansowania wykonania polecenia;
- 6) określenie okresu, w jakim ma obowiązywać polecenie;
- 7) wskazanie ministra właściwego w sprawach wykonania oraz nadzorowania wykonania polecenia, w przypadku poleceń, o których mowa w ust. 1.

14. Do zmiany i uchylenia poleceń, o których mowa w ust. 1 i 2, stosuje się odpowiednio przepisy dotyczące wydawania poleceń.

15. Polecenia, o których mowa w ust. 1, mogą być uchylone lub zmieniane, przez Prezesa Rady Ministrów, z własnej inicjatywy, na wniosek ministra lub innego podmiotu objętego poleceniem, o którym mowa w ust. 1.

16. Wniosek podmiotu, o którym mowa w ust. 15, o zmianę lub uchylenie polecenia składany jest za pośrednictwem właściwego ministra, o którym mowa w ust. 1.

17. Prezes Rady Ministrów może wystąpić o opinię w sprawie wniosku o uchylenie lub zmianę polecenia do ministra, o którym mowa w ust. 1 oraz w ust. 13 pkt 7.

18. Od poleceń, o których mowa w ust. 1 i 2, oraz od ich uchylenia lub zmiany przysługuje prawo wniesienia do sądu administracyjnego skargi na zasadach i w trybie określonych dla aktów lub czynności, o których mowa w art. 3 § 2 pkt 4 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. z 2026 r. poz. 143). Stronami postępowania mogą być skarżący, podmiot objęty poleceniem lub minister, który złożył wniosek o wydanie, zmianę lub uchylenie polecenia.

19. Do ministra, który złożył wniosek o wydanie polecenia, stosuje się przepisy ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi dotyczące organu, którego działanie jest przedmiotem skargi.

20. Zadania nałożone w trybie, o którym mowa w ust. 1, są realizowane przez jednostki samorządu terytorialnego jako zadania zlecone z zakresu administracji rządowej.

21. Minister wydający polecenie niezwłocznie informuje o wydaniu polecenia Prezesa Rady Ministrów, wskazując co najmniej:

- 1) adresata polecenia;
- 2) treść polecenia;
- 3) datę wydania polecenia;
- 4) treść opinii Prezesa Prokuratury Generalnej Rzeczypospolitej Polskiej.

Art. 7b. 1. Wykonywanie zadań objętych poleceniem, o którym mowa w art. 7a ust. 1, wydanym w stosunku do podmiotów, o których mowa w art. 7a ust. 1 pkt 4 oraz innych podmiotów, o ile przewiduje to polecenie, następuje na podstawie umowy zawartej z podmiotem wskazanym w poleceniu przez ministra wskazanego w poleceniu i jest finansowane z budżetu państwa lub innych źródeł wskazanych w poleceniu.

2. Wykonywanie zadań objętych poleceniem, o którym mowa w art. 7a ust. 2, wydanym w stosunku do podmiotów, o których mowa w art. 7a ust. 2 pkt 3, następuje na podstawie umowy zawartej z podmiotem wskazanym w poleceniu przez ministra wydającego polecenie.

3. W przypadku niezawarcia umowy, o której mowa w ust. 1 lub 2, zadania objęte poleceniem są wykonywane na podstawie polecenia, o którym mowa w art. 7a ust. 1 lub 2.

Art. 7ba. (uchylony)

Art. 7bb. (uchylony)

Art. 7bc. 1. Jeżeli w stosunku do tego samego podmiotu wydano polecenie zarówno na podstawie art. 7a ust. 1, jak i 2, a wykonanie ich obu jest niemożliwe, znacząco utrudnione lub uniemożliwiłoby prawidłowe funkcjonowanie podmiotu będącego adresatem polecenia, wiążące wobec podmiotu jest polecenie wydane na podstawie art. 7a ust. 1.

2. W sytuacji, o której mowa w ust. 1, Prezes Rady Ministrów, z własnej inicjatywy lub na wniosek podmiotu będącego adresatem poleceń, uchyla polecenie wydane na podstawie art. 7a ust. 2.

Art. 7c. 1. Do zamówień na usługi lub dostawy niezbędne do realizacji poleceń, o których mowa w art. 7a ust. 1 oraz 2, nie stosuje się przepisów ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2024 r. poz. 1320, z późn. zm.⁶⁾).

2. Zamawiający, w terminie 7 dni od dnia udzielenia zamówienia, o którym mowa w ust. 1, zamieszcza w Biuletynie Zamówień Publicznych informację o udzieleniu tego zamówienia, w której podaje:

- 1) nazwę (firmę) i adres siedziby zamawiającego;
- 2) datę i miejsce zawarcia umowy lub informację o zawarciu umowy drogą elektroniczną;
- 3) opis przedmiotu umowy, z wyszczególnieniem odpowiednio ilości rzeczy lub innych dóbr oraz zakresu usług;
- 4) cenę albo cenę maksymalną, jeżeli cena nie jest znana w chwili zamieszczenia ogłoszenia;
- 5) wskazanie okoliczności faktycznych uzasadniających udzielenie zamówienia bez zastosowania przepisów ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych;
- 6) nazwę (firmę) podmiotu albo imię i nazwisko osoby, z którymi została zawarta umowa.

Art. 8. 1. Przy Radzie Ministrów tworzy się Rządowy Zespół Zarządzania Kryzysowego, zwany dalej „Zespołem”, jako organ opiniodawczo-doradczy właściwy w sprawach inicjowania i koordynowania działań podejmowanych w zakresie zarządzania kryzysowego.

2. W skład Zespołu wchodzi:

- 1) Prezes Rady Ministrów – przewodniczący;
- 2) Minister Obrony Narodowej i minister właściwy do spraw wewnętrznych – zastępcy przewodniczącego;

⁶⁾ Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2025 r. poz. 620, 769, 794, 1165, 1173 i 1235 oraz z 2026 r. poz. 252.

- 2a) minister właściwy do spraw administracji publicznej;
- 3) Minister Spraw Zagranicznych;
- 4) Minister Koordynator Służb Specjalnych – jeżeli został powołany.

3. W posiedzeniach Zespołu, na prawach członka, biorą udział wyznaczone przez przewodniczącego, w zależności od potrzeb, następujące organy administracji rządowej:

- 1) ministrowie kierujący działami administracji rządowej:
 - a) (uchylona)
 - aa) aktywa państwowe,
 - b) budownictwo, planowanie i zagospodarowanie przestrzenne oraz mieszkalnictwo,
 - c) finanse publiczne,
 - d) gospodarka,
 - e) gospodarka morska,
 - f) gospodarka wodna,
 - g) instytucje finansowe,
 - h) informatyzacja,
 - i) kultura i ochrona dziedzictwa narodowego,
 - j) łączność,
 - k) oświata i wychowanie,
 - l) rolnictwo,
 - m) sprawiedliwość,
 - n) środowisko,
 - o) transport,
 - p) zdrowie,
 - q) praca,
 - r) zabezpieczenie społeczne,
 - s) (uchylona)
 - t) energia,
 - u) gospodarka surowcami energetycznymi,
 - v) żegluga śródlądowa,
 - w) klimatu;
- 2) Główny Geodeta Kraju;

- 2a) Główny Inspektor Ochrony Środowiska;
- 3) Główny Inspektor Sanitarny;
- 4) Główny Lekarz Weterynarii;
- 5) Komendant Główny Państwowej Straży Pożarnej;
- 6) Komendant Główny Policji;
- 7) Komendant Główny Straży Granicznej;
- 7a) (uchylony)
- 8) Prezes Państwowej Agencji Atomistyki;
- 9) Prezes Urzędu Lotnictwa Cywilnego;
- 10) Szef Agencji Bezpieczeństwa Wewnętrznego;
- 11) Szef Agencji Wywiadu;
- 12) Szef Obrony Cywilnej;
- 13) Szef Służby Kontrwywiadu Wojskowego;
- 14) Szef Służby Wywiadu Wojskowego;
- 15) Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa.

4. Prezydent Rzeczypospolitej Polskiej może skierować do prac Zespołu, na prawach członka, Szefa Biura Bezpieczeństwa Narodowego lub innego przedstawiciela.

5. Przewodniczący może zapraszać do udziału w posiedzeniach Zespołu, na prawach członka, inne osoby.

6. W przypadku nieobecności przewodniczącego, pracami Zespołu kieruje wyznaczony przez niego zastępca albo członek Zespołu, w którego właściwości – wynikającej z kierowania danym działem administracji rządowej – pozostaje rodzaj zaistniałej sytuacji kryzysowej.

7. Członkowie Zespołu mogą wyznaczać do udziału w jego pracach swoich przedstawicieli:

- 1) Prezes Rady Ministrów – wiceprezesa Rady Ministrów;
- 2) ministrowie – sekretarza lub podsekretarza stanu;
- 3) organy, o których mowa w ust. 3 pkt 2–14 – swojego zastępcę.

8. (uchylony)

Art. 9. 1. Do zadań Zespołu należy:

- 1) przygotowywanie propozycji użycia sił i środków niezbędnych do opanowania sytuacji kryzysowych;

- 2) doradzanie w zakresie koordynacji działań organów administracji rządowej, instytucji państwowych i służb w sytuacjach kryzysowych;
- 3) opiniowanie sprawozdań końcowych z działań podejmowanych w związku z zarządzaniem kryzysowym;
- 4) opiniowanie potrzeb w zakresie odtwarzania infrastruktury lub przywrócenia jej pierwotnego charakteru;
- 5) opiniowanie KPZR oraz KPRK;
- 6) (uchylony)
- 7) opiniowanie projektu zarządzenia Prezesa Rady Ministrów, o którym mowa w art. 7 ust. 4.
- 8) (uchylony)
- 9) (uchylony)
2. (uchylony)

3. Prezes Rady Ministrów określi, w drodze zarządzenia, organizację i tryb pracy Zespołu, z uwzględnieniem rozwiązań pozwalających na niezwłoczne zebranie się Zespołu i zapewnienie uzyskania pełnej informacji o zdarzeniach będących przedmiotem posiedzenia.

Art. 10. 1. Tworzy się Rządowe Centrum Bezpieczeństwa będące państwową jednostką budżetową podległą Prezesowi Rady Ministrów.

2. Centrum kieruje dyrektor powoływany i odwoływany przez Prezesa Rady Ministrów.

2a. Dyrektor Centrum pełni funkcję sekretarza Zespołu, o którym mowa w art. 8 ust. 1.

3. Zastępców dyrektora Centrum powołuje i odwołuje Prezes Rady Ministrów, na wniosek dyrektora Centrum.

4. Prezes Rady Ministrów określi, w drodze rozporządzenia, organizację i tryb działania Centrum, uwzględniając potrzebę ciągłości funkcjonowania Centrum.

Art. 11. 1. Centrum zapewnia obsługę Rady Ministrów, Prezesa Rady Ministrów, Zespołu i ministra właściwego do spraw wewnętrznych w sprawach zarządzania kryzysowego oraz pełni funkcję krajowego centrum zarządzania kryzysowego.

1a. Centrum zapewnia obsługę Zespołu do spraw Incydentów Krytycznych, o którym mowa w art. 36 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

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).

2. Do zadań Centrum należy:

- 1) planowanie cywilne, w tym:
 - a) przedstawianie szczegółowych sposobów i środków reagowania na zagrożenia oraz ograniczania ich skutków,
 - b) opracowywanie i aktualizowanie KPZR oraz KPRK,
 - c) analiza i ocena możliwości wystąpienia zagrożeń lub ich rozwoju,
 - d) gromadzenie informacji o zagrożeniach i analiza zebranych materiałów,
 - e) wypracowywanie wniosków i propozycji zapobiegania i przeciwdziałania zagrożeniom,
 - f) planowanie wykorzystania Sił Zbrojnych Rzeczypospolitej Polskiej do wykonywania zadań, o których mowa w art. 25 ust. 3,
 - g) planowanie wsparcia przez organy administracji publicznej realizacji zadań Sił Zbrojnych Rzeczypospolitej Polskiej;
- 2) monitorowanie potencjalnych zagrożeń;
- 2a) uzgadnianie planów zarządzania kryzysowego sporządzanych przez ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych;
- 3) przygotowanie uruchamiania, w przypadku zaistnienia zagrożeń, procedur związanych z zarządzaniem kryzysowym;
- 4) przygotowywanie projektów opinii i stanowisk Zespołu;
- 5) przygotowywanie i obsługa techniczno-organizacyjna prac Zespołu;
- 5a) zapewnienie koordynacji polityki informacyjnej organów administracji publicznej w czasie sytuacji kryzysowej;
- 6) współdziałanie z podmiotami, komórkami i jednostkami organizacyjnymi Organizacji Traktatu Północnoatlantyckiego i Unii Europejskiej oraz innych organizacji międzynarodowych, odpowiedzialnymi za zarządzanie kryzysowe i ochronę infrastruktury krytycznej;

- 7) organizowanie, prowadzenie i koordynacja szkoleń i ćwiczeń z zakresu zarządzania kryzysowego oraz udział w ćwiczeniach krajowych i międzynarodowych;
- 8) zapewnienie obiegu informacji między krajowymi i zagranicznymi organami i strukturami zarządzania kryzysowego;
- 9) realizacja zadań stałego dyżuru w ramach gotowości obronnej państwa;
- 10) realizacja zadań z zakresu zapobiegania, przeciwdziałania i usuwania skutków zdarzeń o charakterze terrorystycznym;
- 10a) współdziałanie z Szefem Agencji Bezpieczeństwa Wewnętrznego w zakresie zapobiegania, przeciwdziałania i usuwania skutków zdarzeń o charakterze terrorystycznym;
- 11) realizacja zadań planistycznych i programowych z zakresu ochrony infrastruktury krytycznej, w tym współpraca, jako krajowy punkt kontaktowy, z instytucjami Unii Europejskiej i Organizacji Traktatu Północnoatlantyckiego oraz ich krajami członkowskimi w zakresie ochrony infrastruktury krytycznej;
- 12) (uchylony)
- 13) przygotowanie projektu zarządzenia Prezesa Rady Ministrów, o którym mowa w art. 7 ust. 4;
- 14) informowanie, zgodnie z właściwością, podmiotów, o których mowa w art. 8 ust. 2 i 3, o potencjalnych zagrożeniach oraz działaniach podjętych przez właściwe organy;
- 15) współdziałanie z centrami zarządzania kryzysowego organów administracji publicznej.

2a. Koszty związane z funkcjonowaniem Centrum są pokrywane z budżetu państwa z części, której dysponentem jest minister właściwy do spraw wewnętrznych.

3. Rada Ministrów lub Prezes Rady Ministrów mogą zlecić Centrum dodatkowe zadania związane z zarządzaniem kryzysowym.

Art. 11a. Centrum informuje Komisję Europejską i państwa członkowskie Unii Europejskiej o środkach zastosowanych w sytuacji kryzysowej w celu zabezpieczenia prawidłowego działania publicznej sieci telekomunikacyjnej oraz

stacji nadawczych i odbiorczych używanych do zapewnienia bezpieczeństwa, w zakresie dotyczącym systemu łączności i sieci teleinformatycznych.

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.

Art. 12. 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.

2. (uchylony)

2a. (uchylony)

2b. Ministrowie i kierownicy, o których mowa w ust. 1, na potrzeby realizacji zadań z zakresu zarządzania kryzysowego tworzą zespoły zarządzania kryzysowego, w skład których wchodzi kierujący właściwymi komórkami

organizacyjnymi urzędu obsługującego ministra lub kierownika, o których mowa w ust. 1, a także inne osoby przez nich wskazane.

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.

3. (uchylony)

4. Ministrowie i kierownicy, o których mowa w ust. 1, określają, w drodze zarządzenia, organizację, skład oraz miejsce i tryb pracy zespołów zarządzania kryzysowego.

Art. 12a. (uchylony)

Art. 13. 1. Ministrowie i centralne organy administracji rządowej, do których zakresu działania należą sprawy związane z zapewnieniem bezpieczeństwa narodowego, w tym ochrony ludności lub gospodarczych podstaw bezpieczeństwa państwa, tworzą centra zarządzania kryzysowego.

2. Do zadań centrów, o których mowa w ust. 1, należy:

- 1) pełnienie całodobowego dyżuru w celu zapewnienia przepływu informacji na potrzeby zarządzania kryzysowego;
- 2) współdziałanie z centrami zarządzania kryzysowego organów administracji publicznej;
- 3) nadzór nad funkcjonowaniem systemu wykrywania i alarmowania oraz systemu wczesnego ostrzegania ludności;
- 4) współpraca z podmiotami realizującymi monitoring środowiska;
- 5) współdziałanie z podmiotami prowadzącymi akcje ratownicze, poszukiwawcze i humanitarne;
- 6) dokumentowanie działań podejmowanych przez centrum;
- 7) realizacja zadań stałego dyżuru na potrzeby podwyższania gotowości obronnej państwa;

- 8) współdziałanie na wszystkich szczeblach administracji rządowej w zakresie informowania i przekazywania poleceń do wykonania w systemie całodobowym dla jednostek ochrony zdrowia w przypadkach awaryjnych, losowych, jak również zaburzeń funkcjonowania systemu.

2a. Obowiązek utworzenia centrum zarządzania kryzysowego uznaje się za spełniony jeżeli organ, o którym mowa w ust. 1, utworzył komórkę organizacyjną w urzędzie go obsługującym lub jednostkę organizacyjną jemu podległą lub nadzorowaną, odpowiedzialną za pełnienie całodobowych dyżurów i stwarzającą gwarancję realizacji zadań, o których mowa w ust. 2.

3. Rada Ministrów, w drodze rozporządzenia, określi organy administracji rządowej, które utworzą centra zarządzania kryzysowego, oraz sposób ich funkcjonowania, uwzględniając w szczególności warunki techniczne i standardy ich wyposażenia oraz procedury współpracy z Rządowym Centrum Bezpieczeństwa i innymi organami administracji publicznej.

Art. 14. 1. Organem właściwym w sprawach zarządzania kryzysowego na terenie województwa jest wojewoda.

2. Do zadań wojewody w sprawach zarządzania kryzysowego należy:

- 1) kierowanie monitorowaniem, planowaniem, reagowaniem i usuwaniem skutków zagrożeń na terenie województwa;
- 2) realizacja zadań z zakresu planowania cywilnego, w tym:
 - a) wydawanie starostom zaleceń do powiatowych planów zarządzania kryzysowego,
 - b) zatwierdzanie powiatowych planów zarządzania kryzysowego,
 - c) przygotowywanie i przedkładanie do zatwierdzenia ministrowi właściwemu do spraw administracji publicznej wojewódzkiego planu zarządzania kryzysowego,
 - d) realizacja wytycznych do wojewódzkich planów zarządzania kryzysowego;
- 3) zarządzanie, organizowanie i prowadzenie szkoleń, ćwiczeń i treningów z zakresu zarządzania kryzysowego;
- 4) wnioskowanie o użycie pododdziałów lub oddziałów Sił Zbrojnych Rzeczypospolitej Polskiej do wykonywania zadań, o których mowa w art.

25 ust. 3, oraz doraźnych zgrupowań zadaniowych do wykonywania zadań, o których mowa w art. 25b ust. 1;

- 4a) wnioskowanie o użycie Policji, Straży Granicznej lub Państwowej Straży Pożarnej do wykonywania zadań, o których mowa w art. 25a;
- 5) wykonywanie przedsięwzięć wynikających z dokumentów planistycznych wykonywanych w ramach planowania operacyjnego realizowanego w województwie;
- 6) zapobieganie, przeciwdziałanie i usuwanie skutków zdarzeń o charakterze terrorystycznym;
- 6a) współdziałanie z Szefem Agencji Bezpieczeństwa Wewnętrznego w zakresie zapobiegania, przeciwdziałania i usuwania skutków zdarzeń o charakterze terrorystycznym;
- 7) organizacja wykonania zadań z zakresu ochrony infrastruktury krytycznej.
- 8) (uchylony)

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.

4. Minister właściwy do spraw administracji publicznej w uzgodnieniu z ministrem właściwym do spraw wewnętrznych zatwierdza wojewódzkie plany zarządzania kryzysowego i ich aktualizacje, po zasięgnięciu opinii dyrektora Centrum.

5. Zadania, o których mowa w ust. 2, wykonuje wojewoda we współpracy z właściwymi organami administracji publicznej.

6. Do zadań komórki organizacyjnej właściwej w sprawach zarządzania kryzysowego w urzędzie wojewódzkim należy w szczególności:

- 1) gromadzenie i przetwarzanie danych oraz ocena zagrożeń występujących na obszarze województwa;
- 2) monitorowanie, analizowanie i prognozowanie rozwoju zagrożeń na obszarze województwa;

- 3) dostarczanie niezbędnych informacji dotyczących aktualnego stanu bezpieczeństwa dla wojewódzkiego zespołu zarządzania kryzysowego, zespołu zarządzania kryzysowego działającego w urzędzie obsługującym ministra właściwego do spraw wewnętrznych oraz Centrum;
- 4) współpraca z powiatowymi zespołami zarządzania kryzysowego;
- 5) zapewnienie funkcjonowania wojewódzkiego zespołu zarządzania kryzysowego, w tym dokumentowanie jego prac;
- 6) realizacja zadań stałego dyżuru w ramach gotowości obronnej państwa;
- 7) opracowywanie i aktualizacja wojewódzkiego planu zarządzania kryzysowego;
- 8) przygotowywanie, w oparciu o analizę zagrożeń w poszczególnych powiatach, zaleceń wojewody do powiatowych planów zarządzania kryzysowego;
- 9) opiniowanie oraz przedkładanie do zatwierdzenia wojewodzie powiatowych planów zarządzania kryzysowego;
- 10) gromadzenie i przetwarzanie informacji dotyczących infrastruktury krytycznej zlokalizowanej na terenie województwa;
- 11) planowanie wsparcia innych organów właściwych w sprawach zarządzania kryzysowego;
- 12) planowanie użycia pododdziałów lub oddziałów Sił Zbrojnych Rzeczypospolitej Polskiej do wykonywania zadań, o których mowa w art. 25 ust. 3;
- 13) planowanie wsparcia przez organy administracji publicznej realizacji zadań Sił Zbrojnych Rzeczypospolitej Polskiej.

7. Organem pomocniczym wojewody w zapewnieniu wykonywania zadań zarządzania kryzysowego jest wojewódzki zespół zarządzania kryzysowego, powoływany przez wojewodę, który określa jego skład, organizację, siedzibę oraz tryb pracy, zwany dalej „zespołem wojewódzkim”.

8. Do zadań zespołu wojewódzkiego należy w szczególności:

- 1) ocena występujących i potencjalnych zagrożeń mogących mieć wpływ na bezpieczeństwo publiczne i prognozowanie tych zagrożeń;

- 2) przygotowywanie propozycji działań i przedstawianie wojewodzie wniosków dotyczących wykonania, zmiany lub zaniechania działań ujętych w wojewódzkim planie zarządzania kryzysowego;
- 3) przekazywanie do wiadomości publicznej informacji związanych z zagrożeniami;
- 4) opiniowanie wojewódzkiego planu zarządzania kryzysowego.
- 5) (uchylony)

9. W skład zespołu wojewódzkiego wchodzi wojewoda jako przewodniczący, kierownik komórki organizacyjnej właściwej w sprawach zarządzania kryzysowego w urzędzie wojewódzkim jako zastępca przewodniczącego, a także inne osoby wskazane przez przewodniczącego w zależności od potrzeb spośród:

- 1) kierowników zespolonych służb, inspekcji i straży wojewódzkich;
- 2) osób zatrudnionych w urzędzie wojewódzkim lub w jednostkach organizacyjnych służb, inspekcji i straży wojewódzkich;
- 3) osób zatrudnionych w Państwowym Gospodarstwie Wodnym Wody Polskie oraz Instytucie Meteorologii i Gospodarki Wodnej.

10. W skład zespołu wojewódzkiego wchodzi również wyznaczeni przez Ministra Obrony Narodowej przedstawiciele Sił Zbrojnych Rzeczypospolitej Polskiej.

11. W skład zespołu wojewódzkiego może wchodzić przedstawiciel samorządu województwa, wyznaczony przez marszałka województwa.

12. W skład zespołu wojewódzkiego mogą wchodzić inne osoby zaproszone przez przewodniczącego.

Art. 15. Zarząd województwa uczestniczy w realizacji zadań z zakresu zarządzania kryzysowego, w tym planowania cywilnego, wynikających z jego kompetencji.

Art. 16. 1. Tworzy się wojewódzkie centra zarządzania kryzysowego, których obsługę zapewniają komórki organizacyjne właściwe w sprawach zarządzania kryzysowego w urzędach wojewódzkich.

2. Do zadań wojewódzkich centrów zarządzania kryzysowego należy:

- 1) pełnienie całodobowego dyżuru w celu zapewnienia przepływu informacji na potrzeby zarządzania kryzysowego;
- 2) współdziałanie z centrami zarządzania kryzysowego organów administracji publicznej;
- 3) nadzór nad funkcjonowaniem systemu wykrywania i alarmowania oraz systemu wczesnego ostrzegania ludności;
- 4) współpraca z podmiotami realizującymi monitoring środowiska;
- 5) współdziałanie z podmiotami prowadzącymi akcje ratownicze, poszukiwawcze i humanitarne;
- 6) dokumentowanie działań podejmowanych przez centrum;
- 7) realizacja zadań stałego dyżuru na potrzeby podwyższania gotowości obronnej państwa.
- 8) (uchylony)

3. Wojewódzkie centra zarządzania kryzysowego wykonują zadania określone w art. 22 ust. 1 i 2 ustawy z dnia 24 lipca 2015 r. – Prawo o zgromadzeniach (Dz. U. z 2022 r. poz. 1389).

4. Wojewódzkie centra zarządzania kryzysowego wykonują zadania określone w art. 92 ust. 1d i art. 93 ust. 1 ustawy z dnia 27 kwietnia 2001 r. – Prawo ochrony środowiska.

Art. 17. 1. Organem właściwym w sprawach zarządzania kryzysowego na obszarze powiatu jest starosta jako przewodniczący zarządu powiatu.

2. Do zadań starosty w sprawach zarządzania kryzysowego należy:

- 1) kierowanie monitorowaniem, planowaniem, reagowaniem i usuwaniem skutków zagrożeń na terenie powiatu;
- 2) realizacja zadań z zakresu planowania cywilnego, w tym:
 - a) opracowywanie i przedkładanie wojewodzie do zatwierdzenia powiatowego planu zarządzania kryzysowego,
 - b) realizacja zaleceń do powiatowych planów zarządzania kryzysowego,
 - c) wydawanie organom gminy zaleceń do gminnego planu zarządzania kryzysowego,
 - d) zatwierdzanie gminnego planu zarządzania kryzysowego;
- 3) zarządzanie, organizowanie i prowadzenie szkoleń, ćwiczeń i treningów z zakresu zarządzania kryzysowego;

- 4) wykonywanie przedsięwzięć wynikających z planu operacyjnego funkcjonowania powiatów i miast na prawach powiatu;
- 5) zapobieganie, przeciwdziałanie i usuwanie skutków zdarzeń o charakterze terrorystycznym;
- 5a) współdziałanie z Szefem Agencji Bezpieczeństwa Wewnętrznego w zakresie przeciwdziałania, zapobiegania i usuwania skutków zdarzeń o charakterze terrorystycznym;
- 6) organizacja i realizacja zadań z zakresu ochrony infrastruktury krytycznej.

3. Zadania, o których mowa w ust. 2, starosta wykonuje przy pomocy powiatowej administracji zespolonej i jednostek organizacyjnych powiatu.

4. Starosta wykonuje zadania zarządzania kryzysowego przy pomocy powiatowego zespołu zarządzania kryzysowego powołanego przez starostę, który określa jego skład, organizację, siedzibę oraz tryb pracy, zwanego dalej „zespołem powiatowym”.

5. Zespół powiatowy wykonuje na obszarze powiatu zadania przewidziane dla zespołu wojewódzkiego.

6. W skład zespołu powiatowego, którego pracami kieruje starosta, wchodzi osoby powołane spośród:

- 1) osób zatrudnionych w starostwie powiatowym, powiatowych jednostkach organizacyjnych lub jednostkach organizacyjnych stanowiących aparat pomocniczy kierowników zespolonych służb, inspekcji i straży powiatowych;
- 2) przedstawicieli społecznych organizacji ratowniczych.

7. W skład zespołu powiatowego mogą wchodzić inne osoby zaproszone przez starostę.

Art. 18. 1. Tworzy się powiatowe centra zarządzania kryzysowego.

2. Powiatowe centra zarządzania kryzysowego zapewniają przepływ informacji na potrzeby zarządzania kryzysowego oraz wykonują odpowiednio zadania, o których mowa w art. 16 ust. 2.

3. Organizację, siedzibę oraz tryb pracy powiatowego centrum zarządzania kryzysowego, w tym sposób całodobowego alarmowania członków zespołu zarządzania kryzysowego oraz sposób zapewnienia całodobowego obiegu informacji w sytuacjach kryzysowych, określa starosta.

3a. Starosta może powierzyć wykonywanie zadań powiatowego centrum zarządzania kryzysowego komendantowi powiatowemu (miejskiemu) Państwowej Straży Pożarnej.

4. W miejscowościach będących jednocześnie siedzibami powiatów i miast na prawach powiatu, na podstawie porozumienia zawartego między tymi jednostkami samorządu terytorialnego, może być tworzone wspólne centrum zarządzania kryzysowego obejmujące zasięgiem działania obszar obu jednostek samorządu terytorialnego.

Art. 19. 1. Organem właściwym w sprawach zarządzania kryzysowego na terenie gminy jest wójt, burmistrz, prezydent miasta.

2. Do zadań wójta, burmistrza, prezydenta miasta w sprawach zarządzania kryzysowego należy:

- 1) kierowanie monitorowaniem, planowaniem, reagowaniem i usuwaniem skutków zagrożeń na terenie gminy;
- 2) realizacja zadań z zakresu planowania cywilnego, w tym:
 - a) realizacja zaleceń do gminnego planu zarządzania kryzysowego,
 - b) opracowywanie i przedkładanie staroście do zatwierdzenia gminnego planu zarządzania kryzysowego;
- 3) zarządzanie, organizowanie i prowadzenie szkoleń, ćwiczeń i treningów z zakresu zarządzania kryzysowego;
- 4) wykonywanie przedsięwzięć wynikających z planu operacyjnego funkcjonowania gmin i gmin o statusie miasta;
- 5) zapobieganie, przeciwdziałanie i usuwanie skutków zdarzeń o charakterze terrorystycznym;
- 5a) współdziałanie z Szefem Agencji Bezpieczeństwa Wewnętrznego w zakresie przeciwdziałania, zapobiegania i usuwania skutków zdarzeń o charakterze terrorystycznym;
- 6) organizacja i realizacja zadań z zakresu ochrony infrastruktury krytycznej.

3. Zadania, o których mowa w ust. 2, wójt, burmistrz, prezydent miasta wykonuje przy pomocy komórki organizacyjnej urzędu gminy (miasta) właściwej w sprawach zarządzania kryzysowego.

4. Organem pomocniczym wójta, burmistrza, prezydenta miasta w zapewnieniu wykonywania zadań zarządzania kryzysowego jest gminny zespół

zarządzania kryzysowego powoływany przez wójta, burmistrza, prezydenta miasta, który określa jego skład, organizację, siedzibę oraz tryb pracy, zwany dalej „zespołem gminnym”.

5. Zespół gminny wykonuje na obszarze gminy zadania przewidziane dla zespołu wojewódzkiego.

6. W skład zespołu gminnego, którego pracami kieruje wójt, burmistrz, prezydent miasta, wchodzi osoby powołane spośród:

- 1) osób zatrudnionych w urzędzie gminy, gminnych jednostkach organizacyjnych lub jednostkach pomocniczych;
- 2) pracowników zespolonych służb, inspekcji i straży, skierowanych przez przełożonych do wykonywania zadań w tym zespole na wniosek wójta, burmistrza, prezydenta miasta;
- 3) przedstawicieli społecznych organizacji ratowniczych.

7. W skład zespołu gminnego mogą wchodzić inne osoby zaproszone przez wójta, burmistrza, prezydenta miasta.

Art. 20. 1. Wójt, burmistrz, prezydent miasta zapewnia na obszarze gminy (miasta) realizację następujących zadań:

- 1) całodobowe alarmowanie członków gminnego zespołu zarządzania kryzysowego, a w sytuacjach kryzysowych zapewnienie całodobowego dyżuru w celu zapewnienia przepływu informacji oraz dokumentowania prowadzonych czynności;
- 2) współdziałanie z centrami zarządzania kryzysowego organów administracji publicznej;
- 3) nadzór nad funkcjonowaniem systemu wykrywania i alarmowania oraz systemu wczesnego ostrzegania ludności;
- 4) współpracę z podmiotami realizującymi monitoring środowiska;
- 5) współdziałanie z podmiotami prowadzącymi akcje ratownicze, poszukiwawcze i humanitarne;
- 6) realizację zadań stałego dyżuru na potrzeby podwyższania gotowości obronnej państwa.

2. W celu realizacji zadań, o których mowa w ust. 1, wójt, burmistrz, prezydent miasta może tworzyć gminne (miejskie) centra zarządzania kryzysowego.

2a. W przypadku utworzenia, gminne (miejskie) centrum zarządzania kryzysowego wykonuje zadania określone w art. 22 ust. 1 i 2 ustawy z dnia 24 lipca 2015 r. – Prawo o zgromadzeniach.

3. Art. 18 ust. 4 stosuje się odpowiednio.

Art. 20a. Organy właściwe w sprawach zarządzania kryzysowego mają prawo żądania udzielenia informacji, gromadzenia i przetwarzania danych niezbędnych do realizacji zadań określonych w ustawie.

Art. 20b. Ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych, wojewodowie, starostowie, wójtowie, burmistrzowie, prezydenci miast, właściciele oraz posiadacze samoistni i zależni obiektów, instalacji, urządzeń i usług infrastruktury krytycznej są obowiązani do udzielania dyrektorowi Centrum, w wyznaczonym terminie, żądanych przez niego informacji i wyjaśnień niezbędnych do realizacji zadań Centrum określonych w ustawie.

Art. 21. Obowiązek podjęcia działań w zakresie zarządzania kryzysowego spoczywa na tym organie właściwym w sprawach zarządzania kryzysowego, który pierwszy otrzymał informację o wystąpieniu zagrożenia. Organ ten niezwłocznie informuje o zaistniałym zdarzeniu organy odpowiednio wyższego i niższego szczebla, przedstawiając jednocześnie swoją ocenę sytuacji oraz informację o zamierzonych działaniach.

Art. 21a. 1. Ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych oraz wojewodowie niezwłocznie informują dyrektora Centrum o zagrożeniu, które może skutkować wystąpieniem na wskazanym obszarze sytuacji kryzysowej, oraz o konieczności powiadomienia ludności o zagrożeniu.

2. Właściciele oraz posiadacze samoistni i zależni obiektów, instalacji, urządzeń i usług infrastruktury krytycznej niezwłocznie informują dyrektora Centrum oraz właściwe terytorialnie wojewódzkie centrum zarządzania kryzysowego o zakłóceniu funkcjonowania tej infrastruktury, które może skutkować wystąpieniem na wskazanym obszarze sytuacji kryzysowej.

3. Operator ruchomej publicznej sieci telekomunikacyjnej w rozumieniu przepisów 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), zwany dalej

„operatorem”, jest obowiązany, na żądanie dyrektora Centrum, do niezwłocznego, nieodpłatnego wysłania lub wysyłania, komunikatów do wszystkich lub określonych przez dyrektora Centrum grup użytkowników końcowych, w szczególności przebywających na określonym przez niego obszarze, jednorazowo lub przez wskazany przez dyrektora Centrum okres.

3a. Obowiązek, o którym mowa w ust. 3, nie obejmuje wysyłania komunikatu użytkownikom końcowym, których karty SIM są zainstalowane i wykorzystywane w urządzeniach używanych wyłącznie do świadczenia usług komunikacji maszyno-maszyna.

4. Rada Ministrów określi, w drodze rozporządzenia, sposób i tryb współpracy dyrektora Centrum z operatorem w celu realizacji obowiązku, o którym mowa w ust. 3, niezbędne elementy komunikatu oraz sposób jego przekazywania użytkownikom końcowym, mając na uwadze konieczność:

- 1) zapewnienia efektywnego i niezakłóconego przepływu informacji między Centrum a operatorem;
- 2) zapewnienia sprawnej dystrybucji komunikatu na obszarze zagrożonym wystąpieniem sytuacji kryzysowej oraz łatwości zrozumienia treści zawartych w komunikacie i zastosowania się do nich.

Art. 21b. 1. Na potrzeby zapewnienia ochrony lokalnej społeczności w sytuacji kryzysowej lub możliwości wystąpienia sytuacji kryzysowej wójt, burmistrz, prezydent miasta określa szczególne formy udzielania pomocy dla lokalnej społeczności.

2. Wójt, burmistrz, prezydent miasta sporządza wykaz szczególnych form udzielania pomocy dla lokalnej społeczności oraz informuje, w sposób zwyczajowo przyjęty oraz w tłumaczeniu na język migowy, mieszkańców o warunkach korzystania z pomocy.

3. Uwzględnienie w wykazie, o którym mowa w ust. 2, następuje na wniosek osoby wymagającej wsparcia lub jej opiekuna prawnego.

Art. 22. Ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych, wojewodowie, starostowie i wójtowie, burmistrzowie, prezydenci miast mogą powoływać ekspertów do udziału w pracach właściwych zespołów zarządzania kryzysowego.

Art. 23. (uchylony)**Art. 24.** (uchylony)

Art. 25. 1. Jeżeli w sytuacji kryzysowej użycie innych sił i środków jest niemożliwe lub może okazać się niewystarczające, o ile inne przepisy nie stanowią inaczej, Minister Obrony Narodowej, na wniosek wojewody, może przekazać do jego dyspozycji pododdziały lub oddziały Sił Zbrojnych Rzeczypospolitej Polskiej, zwane dalej „oddziałami Sił Zbrojnych”, wraz ze skierowaniem ich do wykonywania zadań z zakresu zarządzania kryzysowego.

2. W realizacji zadań z zakresu zarządzania kryzysowego mogą uczestniczyć oddziały Sił Zbrojnych, stosownie do ich przygotowania specjalistycznego, zgodnie z wojewódzkim planem zarządzania kryzysowego.

3. Do zadań, o których mowa w ust. 2, należy:

- 1) współudział w monitorowaniu zagrożeń;
- 2) wykonywanie zadań związanych z oceną skutków zjawisk zaistniałych na obszarze występowania zagrożeń;
- 3) wykonywanie zadań poszukiwawczo-ratowniczych;
- 4) ewakuowanie poszkodowanej ludności i mienia;
- 5) wykonywanie zadań mających na celu przygotowanie warunków do czasowego przebywania ewakuowanej ludności w wyznaczonych miejscach;
- 6) współudział w ochronie mienia pozostawionego na obszarze występowania zagrożeń;
- 7) izolowanie obszaru występowania zagrożeń lub miejsca prowadzenia akcji ratowniczej;
- 8) wykonywanie prac zabezpieczających, ratowniczych i ewakuacyjnych przy zagrożonych obiektach budowlanych i zabytkach;
- 9) prowadzenie prac wymagających użycia specjalistycznego sprzętu technicznego lub materiałów wybuchowych będących w zasobach Sił Zbrojnych Rzeczypospolitej Polskiej;
- 10) usuwanie materiałów niebezpiecznych i ich unieszkodliwianie, z wykorzystaniem sił i środków będących na wyposażeniu Sił Zbrojnych Rzeczypospolitej Polskiej;
- 11) likwidowanie skażeń chemicznych oraz skażeń i zakażeń biologicznych;

- 12) usuwanie skażeń promieniotwórczych;
- 13) wspieranie w wykonywaniu zadań związanych z naprawą i odbudową infrastruktury technicznej;
- 14) współudział w zapewnieniu przejezdności szlaków komunikacyjnych;
- 15) udzielanie pomocy medycznej i wykonywanie zadań sanitarnohigienicznych i przeciwepidemicznych.
- 16) (uchylony)

4. Plan, o którym mowa w ust. 2, podlega uzgodnieniu z właściwymi organami wskazanymi przez Ministra Obrony Narodowej.

5. Oddziały Sił Zbrojnych mogą być przekazane do dyspozycji wojewody w składzie etatowym albo jako tworzone doraźnie zgrupowania zadaniowe.

6. Koordynowanie udziału oddziałów Sił Zbrojnych w realizacji zadań, o których mowa w ust. 3, w zależności od obszaru występowania zagrożeń, zapewniają odpowiednio organy, o których mowa w art. 14 ust. 1, art. 17 ust. 1 i art. 19 ust. 1. Obejmuje ono przedsięwzięcia mające na celu sprawne włączenie oddziałów Sił Zbrojnych do realizacji zadań, z uwzględnieniem czasu i miejsca ich użycia oraz sposobu współdziałania z innymi podmiotami.

7. Zadania dla oddziałów Sił Zbrojnych organy, o których mowa w art. 14 ust. 1, art. 17 ust. 1 i art. 19 ust. 1, przekazują wyłącznie ich dowódcom.

8. Dowodzenie oddziałami Sił Zbrojnych odbywa się na zasadach określonych w regulaminach wojskowych i według procedur obowiązujących w Siłach Zbrojnych Rzeczypospolitej Polskiej.

9. Użycie oddziałów Sił Zbrojnych w sytuacji kryzysowej nie może zagrozić ich zdolności do realizacji zadań wynikających z Konstytucji Rzeczypospolitej Polskiej i ratyfikowanych umów międzynarodowych.

Art. 25a. 1. W przypadku nakazu wykonania odstrzału, o którym mowa w art. 28 ust. 4 pkt 12 ustawy z dnia 21 listopada 2025 r. o zdrowiu zwierząt (Dz. U. poz. 1795), jeżeli jest to niezbędne ze względu na rodzaj i skalę zagrożenia, minister właściwy do spraw wewnętrznych, na wniosek wojewody, może przekazać do dyspozycji wojewody doraźne zgrupowanie zadaniowe sformowane z policjantów, funkcjonariuszy Straży Granicznej lub funkcjonariuszy Państwowej Straży Pożarnej, którzy posiadają uprawnienia do wykonywania polowania, celem ich

użycia do wykonania tego odstrzału w odniesieniu do zwierząt dzikich na określonych obszarach.

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

Art. 25b. 1. Jeżeli w sytuacji kryzysowej użycie innych sił i środków jest niemożliwe lub niewystarczające, Minister Obrony Narodowej, na wniosek wojewody, może przekazać do dyspozycji wojewody doraźne zgrupowanie zadaniowe sformowane z żołnierzy, którzy posiadają uprawnienia do wykonywania polowania, celem ich użycia do wykonania odstrzału, o którym mowa w art. 28 ust. 4 pkt 12 ustawy z dnia 21 listopada 2025 r. o zdrowiu zwierząt, w odniesieniu do zwierząt dzikich na określonych obszarach.

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

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

Art. 25c. 1. W przypadkach, o których mowa w art. 25a i art. 25b, odpowiednio policjanci, funkcjonariusze Straży Granicznej, funkcjonariusze Państwowej Straży Pożarnej i żołnierze używają broni myśliwskiej prywatnej lub użyczonej zgodnie z przepisami ustawy z dnia 21 maja 1999 r. o broni i amunicji (Dz. U. z 2024 r. poz. 485, z 2025 r. poz. 1795 oraz z 2026 r. poz. 187).

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

3. W przypadkach, o których mowa w art. 25a i art. 25b:

- 1) nie stosuje się przepisów ustawy z dnia 21 listopada 2025 r. o zdrowiu zwierząt dotyczących ryczałtu;
- 2) policjanci, funkcjonariusze Straży Granicznej, funkcjonariusze Państwowej Straży Pożarnej i żołnierze współpracują z zarządcą lub dzierżawcą obwodu łowieckiego.

Art. 25d. W przypadkach, o których mowa w art. 25a i art. 25b, do obowiązków wojewody należy:

- 1) zapewnienie amunicji do broni, o której mowa w art. 25c ust. 1;
- 2) zwrot kosztów transportu, zakwaterowania i wyżywienia doraźnych zgrupowań zadaniowych; zwrot kosztów zakwaterowania lub wyżywienia nie przysługuje w przypadku zapewnienia w miejscu wykonywania czynności bezpłatnego zakwaterowania lub wyżywienia.

Rozdział 18

Finansowanie wykonywania zadań zarządzania kryzysowego

Art. 26. 1. Finansowanie wykonywania zadań własnych z zakresu zarządzania kryzysowego na poziomie gminnym, powiatowym i wojewódzkim planuje się w ramach budżetów odpowiednio gmin, powiatów i samorządów województw.

2. Finansowanie wykonywania zadań z zakresu zarządzania kryzysowego na poziomie krajowym planuje się w ramach budżetu państwa w częściach, którymi dysponują wojewodowie, minister właściwy do spraw wewnętrznych i inni ministrowie kierujący działami administracji rządowej oraz centralne organy administracji rządowej.

3. Na finansowanie zadań zleconych z zakresu administracji rządowej, o których mowa w ust. 2, jednostki samorządu terytorialnego otrzymują z budżetu państwa dotacje celowe w wysokości zapewniającej realizację tych zadań.

4. W budżecie jednostki samorządu terytorialnego tworzy się rezerwę celową na realizację zadań własnych z zakresu zarządzania kryzysowego w wysokości nie mniejszej niż 0,5 % wydatków budżetu jednostki samorządu terytorialnego, pomniejszonych o wydatki inwestycyjne, wydatki na wynagrodzenia i pochodne oraz wydatki na obsługę długu.

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.

5. Na dofinansowanie zadań własnych z zakresu zarządzania kryzysowego jednostki samorządu terytorialnego mogą otrzymywać dotacje celowe z budżetu państwa.

6. Zasady otrzymywania i rozliczania dotacji, o których mowa w ust. 3 i 5, określają przepisy ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2025 r. poz. 1483, 1844 i 1846 oraz z 2026 r. poz. 426) i ustawy z dnia 1 października 2024 r. o dochodach jednostek samorządu terytorialnego (Dz. U. poz. 1572 i 1717 oraz z 2025 r. poz. 1659).

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.

Rozdział 19

Zmiany w przepisach

Art. 27. (pominięty)

Art. 28. (pominięty)

Art. 29. (pominięty)

Art. 30. (pominięty)

Art. 31. (pominięty)

Rozdział 20

Przepisy dostosowujące i przejściowe oraz przepis końcowy

Art. 32. Gminne zespoły reagowania, powiatowe zespoły reagowania kryzysowego i wojewódzkie zespoły reagowania kryzysowego, utworzone na podstawie ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej, stają się z dniem wejścia w życie niniejszej ustawy odpowiednio gminnymi zespołami zarządzania kryzysowego, powiatowymi zespołami zarządzania kryzysowego i wojewódzkimi zespołami zarządzania kryzysowego.

Art. 33. Prezes Rady Ministrów powoła, w drodze zarządzenia, Pełnomocnika Rządu do spraw organizacji Rządowego Centrum Bezpieczeństwa.

Art. 34. 1. Plany, o których mowa w art. 5 ust. 1 i art. 6 ust. 2, są sporządzane w terminie 12 miesięcy od dnia wejścia w życie ustawy.

2. Plany sporządzane w terminie, o którym mowa w ust. 1, mogą nie zawierać map, o których mowa w art. 5 ust. 2 pkt 1 lit. a.

Art. 35. Ustawa wchodzi w życie po upływie 3 miesięcy od dnia ogłoszenia⁷⁾, z wyjątkiem art. 33, który wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Ó

⁷⁾ Ustawa została ogłoszona w dniu 21 maja 2007 r.

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		Bank krajowy, o którym mowa w art. 4 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe.

rynków finansowych		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 uchylecia 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	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.

	leczniczych i wyrobów medycznych	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.