Projekt, 03.07.2024 r. wersja - uzgodnienia międzyresortowe

U S T A W A

z dnia

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

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

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

2) art. 1 otrzymuje brzmienie:

„Art. 1. Ustawa określa:

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

2) usługi kluczowe oraz zadania i obowiązki podmiotów krytycznych;

3) organy właściwe do spraw podmiotów krytycznych oraz zadania i obowiązki tych organów;

4) zasady sprawowania nadzoru nad podmiotami krytycznymi oraz ich kontroli;

5) zasady finansowania zadań, o których mowa w pkt 1-4.”,

3) w art. 3:

a) pkt 1 otrzymuje brzmienie:

„1) sytuacji kryzysowej – należy przez to rozumieć sytuację wpływającą negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach, środowiska lub dziedzictwa kulturowego, wywołującą znaczne ograniczenia w działaniu właściwych organów administracji publicznej ze względu na

---

1) Niniejsza ustawa wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz. Urz. UE L 333 z 27.12.2022 r. str. 164).

2) Niniejszą ustawą zmienia się ustawy: ustawę z dnia 22 sierpnia 1997 r. o ochronie osób i mienia, ustawę z dnia 29 listopada 2000 r. - Prawo atomowe, ustawę z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, ustawę z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich, ustawę z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw aktywów państwowych oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych, ustawę z dnia 14 grudnia 2012 r. o odpadach, ustawę z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej, ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, ustawę z dnia 17 grudnia 2020 r. o rezerwach strategicznych, ustawę z dnia 27 stycznia 2023 r. o kontroli niektórych inwestycji oraz ustawę z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej.

nieadekwatność posiadanych sił i środków lub zakłócenia obsługi tych organów;”,

b) po pkt 1 dodaje się pkt 1a - 1f w brzmieniu:

„1a) podmiocie krytycznym - należy przez to rozumieć operatora infrastruktury krytycznej ujętego w wykazie podmiotów krytycznych, realizującego usługę kluczową, prowadzącego działalność w sektorze lub podsektorze wymienionym w załączniku do ustawy i prowadzącego działalność na terytorium Rzeczypospolitej Polskiej lub na obszarach morskich Rzeczypospolitej Polskiej, o których mowa w ustawie z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej (Dz. U. z 2023 r. poz. 960, 1688, 2029 oraz z 2024 r. poz. 731 i 834);

1b) podmiocie krytycznym o szczególnym znaczeniu europejskim - należy przez to rozumieć podmiot krytyczny świadczący usługę kluczową na rzecz co najmniej sześciu państw członkowskich Unii Europejskiej lub w co najmniej sześciu państwach członkowskich Unii Europejskiej;

1c) odporności podmiotów krytycznych - należy przez to rozumieć zapewnienie zdolności do zapobiegania incydentom, przejmowania nad nimi kontroli w drodze zaplanowanych działań, zapewnienia zasobów niezbędnych do reagowania w przypadku występowania incydentów, konieczności usuwania skutków incydentów oraz odtwarzania infrastruktury krytycznej niezbędnej do świadczenia usługi kluczowej;

1d) 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, świadczoną w sektorze lub podsektorze wymienionym w załączniku do ustawy;

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

1f) incydent istotny – incydent, który powoduje lub może spowodować istotne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej;”,

c) pkt 2 otrzymuje brzmienie:

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

a) zapewnieniu funkcjonowania organów administracji publicznej,

b) zapewnieniu funkcjonowania przedsiębiorców,

c) zaspokajaniu potrzeb obywateli

- w tym zapewniające świadczenie usług kluczowych;”,

d) uchyla się pkt 2a,

e) pkt 3 otrzymuje brzmienie:

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

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

"3a) operatorze infrastruktury krytycznej – należy przez to rozumieć właściciela lub posiadacza obiektu, urządzenia oraz instalacji lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji oraz sieci systemu lub usługi, które zostały ujęte w wykazie infrastruktury krytycznej;",

g) uchyla się pkt 9 i 10,

h) w pkt 11 kropkę zastępuje się średnikiem i dodaje się pkt 12-23 w brzmieniu:

„12) ryzyku – należy przez to rozumieć prawdopodobieństwo wystąpienia zagrożenia wraz z jego skutkami, z uwzględnieniem odporności środowiska w którym zagrożenie występuje;

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

a) planowaniu działań ograniczających ryzyko,

b) wdrażaniu działań ograniczających ryzyko,

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

d) okresowej ocenie osiągniętych efektów;

14) ocenie ryzyka - należy przez to rozumieć proces identyfikacji prawdopodobieństwa wystąpienia zagrożenia, podatności na zagrożenie oraz szacowania jego skutków. Wynikiem oceny jest wartość ryzyka;

15) module zadaniowym – należy przez to rozumieć zestawienie przedsięwzięć i zadań przewidzianych do realizacji w sytuacji kryzysowej przez podmioty wskazane w siatce bezpieczeństwa, z wykorzystaniem własnych sił i środków, a także możliwego, zaplanowanego i uzgodnionego wsparcia ze strony innych podmiotów wskazanych w siatce bezpieczeństwa;
16) jednostce certyfikującej – należy przez to rozumieć jednostkę oceniającą zgodność akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 1854) lub upoważnioną do certyfikacji zgodnie z przepisami ustawy z dnia 12 września 2002 r. o normalizacji (Dz.U. 2015 poz. 1483);
17) certyfikacie - należy przez to rozumieć dokument wydany przez jednostkę certyfikującą potwierdzający, że wyrób, instalacja, system, proces, usługa lub osoba spełniają odpowiednie wymagania;
18) certyfikacji - należy przez to rozumieć działania jednostki certyfikującej, wykazujące, że wyrób, instalacja, system, proces, usługa lub osoba spełniają odpowiednie wymagania;
19) decyzji 1313/2013/UE – należy przez to rozumieć decyzję Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (Dz. Urz. UE L 347 z 20.12.2013, str. 924, z późn. zm.[3)]);
20) Grupie do spraw Podmiotów Krytycznych - należy przez to rozumieć grupę, o której mowa w art. 19 dyrektywy 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 r. str. 164), zwanej dalej "dyrektywą 2022/2557";
21) misji doradczej – należy przez to rozumieć misję doradczą, o której mowa w art. 18 ust. 1 dyrektywy 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;
22) zagrożeniu antagonistycznym - należy przez to rozumieć działania ukierunkowane przeciw osobom, grupom społecznym, państwu i jego

---

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

instytucjom oraz usługom kluczowym i infrastrukturze zapewniającej te usługi, realizowane w sposób celowy i świadomy przez niezidentyfikowanych sprawców, terrorystów, siły nieregularne, organizacje przestępcze, podmioty państwowe lub niepaństwowe, bez względu na motywacje ich postępowania;

23) zagrożeniu hybrydowym – należy przez to rozumieć zaplanowane i skoordynowane działania prowadzone przez podmioty państwowe lub niepaństwowe w sposób utrudniający przypisanie odpowiedzialności za nie sprawcy, które zmierzają do osiągnięcia celów politycznych, strategicznych lub wojskowych oraz mogą łączyć różne środki wywierania nacisku i uzależniania od potencjalnego agresora, takie jak polityczne, militarne, ekonomiczne, społeczne, prawne oraz informacyjne.";

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

„1a) prowadzenie oceny ryzyka;”,

5) uchyla się art. 5-5b,

6) po art. 5b dodaje się rozdziały 2 i 3 w brzmieniu:

„Rozdział 2

Dokumenty strategiczne

Art. 5c 1. W celu dokonania oceny ryzyka zidentyfikowanych zagrożeń opracowuje się Krajową Ocenę Ryzyka”. Rada Ministrów przyjmuje Krajową Ocenę Ryzyka w drodze uchwały.

2. Krajowa Ocena Ryzyka Ocena zawiera:

1) zidentyfikowane istotne zagrożenia, w szczególności:
   a) naturalne mogące spowodować klęskę żywiołową,
   b) techniczne mogące spowodować katastrofę,
   c) spowodowane niedostępnością usług o kluczowym znaczeniu dla państwa i jego obywateli,
   d) antagonistyczne, w tym zagrożenia hybrydowe, o charakterze terrorystycznym oraz zagrożenia cyberbezpieczeństwa,
   e) inne możliwe do zidentyfikowania zagrożenia mogące wystąpić w przyszłości.
2) ocenę ryzyka wynikającego ze zidentyfikowanych zagrożeń;
3) streszczenie istotnych elementów oceny ryzyka w rozumieniu decyzji 1313/2013/EU.

3. Przy opracowaniu oceny ryzyka uwzględnia się w szczególności:

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

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

1) wykaz usług kluczowych, o którym mowa w art. 6u;
2) istotne ryzyka wynikające ze stopnia wzajemnej zależności między sektorami określonymi w załączniku do ustawy;
3) zależność ciągłości działania usług kluczowych od podmiotów znajdujących się w innych państwach członkowskich i państwach trzecich;
4) wpływ, jaki znaczące zakłócenie w jednym sektorze może mieć wpływ na inne sektory, w tym wszelkie istotne czynniki ryzyka dla obywateli i rynku wewnętrznego;
5) informacje dotyczące incydentów zgłaszanych przez podmioty krytyczne świadczące usługi kluczowe.

5. Projekt Krajowej Oceny Ryzyka opracowuje Szef Rządowego Centrum Bezpieczeństwa, zwanego dalej „Centrum”.

6. Na potrzeby opracowania projektu Krajowej Oceny Ryzyka Szef Centrum opracowuje wytyczne do jego opracowania i przekazuje:

1) ministrom kierującym działami administracji rządowej;
2) wojewodom;
3) innym niż wymienione w pkt 1 i 2 podmiotom, jeżeli jest to konieczne.

7. Organy i podmioty, o których mowa w ust. 6, w zakresie swojej właściwości, przekazują Szefowi Centrum we wskazanym terminie propozycje do ujęcia w Krajowej Ocenie Ryzyka, obejmujące elementy, o których mowa w ust. 2 pkt 1 i 2, oraz uwzględniając elementy, o których mowa w ust. 3 i 4.

8. Organy i podmioty, o których mowa w ust. 6, przekazują Szefowi Centrum propozycje wraz z danymi stanowiącymi podstawę do ich przygotowania.

9. Szef Centrum może wystąpić o przekazanie dodatkowych propozycji, jeżeli uzna, że ich umieszczenie w Krajowej Ocenie Ryzyka jest niezbędne.

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

11. Szef Centrum przedkłada Radzie Ministrów projekt Krajowej Oceny Ryzyka nie rzadziej niż raz na trzy lata.

12. Szef Centrum udostępnia Komisji Europejskiej streszczenie istotnych elementów oceny ryzyka, o której mowa w ust. 2 pkt 3.

Art. 5d. Krajową Ocena Ryzyka uwzględnia się w:

1) Krajowym Planie Zarządzania Kryzysowego oraz planach zarządzania kryzysowego, o których mowa w rozdziale 3 ustawy;
2) procesach identyfikacji podmiotów krytycznych;
3) opracowywaniu ocen ryzyka dla 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.

Art. 5e. 1. W celu realizacji zadań z zakresu planowania cywilnego opracowuje się Krajowy Plan Zarządzania Kryzysowego. Rada Ministrów przyjmuje Krajowy Plan Zarządzania Kryzysowego, w drodze uchwały.

2. Krajowy Plan Zarządzania Kryzysowego zawiera:

1) część dotyczącą zarządzania ryzykiem;
2) część dotyczącą reagowania kryzysowego;
3) streszczenie istotnych elementów krajowej oceny zdolności zarządzania ryzykiem w rozumieniu decyzji 1313/2013/EU.

3. W części dotyczącej zarządzania ryzykiem Krajowy Plan Zarządzania Kryzysowego zawiera:

1) cele strategiczne;
2) opis zasad współdziałania między podmiotami wskazanymi w siatce bezpieczeństwa;

3) uporządkowaną listę działań na rzecz ograniczenia ryzyka katastrof 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.

4. W części dotyczącej reagowania kryzysowego Krajowy Plan Zarządzania Kryzysowego zawiera:

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

5. Przepisy art. 5c ust. 5-11stosuje się odpowiednio do opracowywania Krajowego Plany Zarządzania Kryzysowego.

6. Szef Centrum udostępnia Komisji Europejskiej streszczenie istotnych elementów krajowej oceny zdolności zarządzania ryzykiem, o której mowa w ust. 2 pkt 3.

Art. 5f. 1. W celu zwiększenia odporności podmiotów krytycznych opracowuje się Strategię Odporności Podmiotów Krytycznych, zwaną dalej „Strategią”. Rada Ministrów przyjmuje Strategię, w drodze uchwały.

2. Strategia:

1) określa cele strategiczne i priorytety w zakresie zapewnienia niezakłóconego świadczenia usług kluczowych przez podmioty krytyczne oraz niezakłóconego funkcjonowania infrastruktury krytycznej;
2) określa zakresy działań oraz formy działań służące osiąganiu celów strategicznych i priorytetów przez:
   a) organy właściwe w sprawach podmiotów krytycznych,
   b) ministrów, którzy identyfikują infrastrukturę krytyczną,
   c) podmioty niewymienione w lit. a i b, zaangażowane we wdrażanie i realizację Strategii;
3) zawiera opisy:
   a) procesów identyfikujących podmioty krytyczne,
   b) środków niezbędnych do zwiększenia ogólnej odporności podmiotów krytycznych,
   c) procesów wspierania podmiotów krytycznych przez podmioty, o których mowa w pkt 2 lit. a-c.
   d) środków mających na celu ułatwienie wypełniania obowiązków wynikających z rozdziału III dyrektywy 2022/2557 przez małe i średnie przedsiębiorstwa, w rozumieniu załącznika do zalecenia Komisji 2003/361/W, które zostały zidentyfikowane jako podmioty krytyczne;
4) określa zakres koordynacji działań właściwych organów w sprawach podmiotów krytycznych i podmiotów właściwych w sprawach cyberbezpieczeństwa, o których mowa w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 i 1703 oraz z 2024 r. poz. 834).

3. Przepisy art. 5c ust. 5-11 stosuje się odpowiednio do opracowywania Strategii.

4. Szef Centrum monitoruje wdrażanie Strategii oraz co roku przedkłada Radzie Ministrów sprawozdanie z jej wdrażania.";

„Rozdział 3

Plany zarządzania kryzysowego

Art. 5g. 1. Plan zarządzania 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 składa się z części dotyczącej:

1) zarządzania ryzykiem;
2) reagowania kryzysowego.

2. W części dotyczącej zarządzania ryzykiem plan zawiera elementy, o których mowa w art. 5e ust. 3.

3. W części dotyczącej reagowania kryzysowego plan zawiera:

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

4. Plan zarządzania kryzysowego, o którym mowa w ust. 1, opracowuje i wdraża minister kierujący działem administracji rządowej, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Agencji Wywiadu, Szef Centralnego Biura Antykorupcyjnego oraz kierownik urzędu centralnego podległego ministrowi kierującemu działem administracji rządowej lub przez niego nadzorowany.

5. Minister kierujący działem administracji rządowej, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Agencji Wywiadu, Szef Centralnego Biura Antykorupcyjnego oraz kierownik urzędu centralnego podległego ministrowi kierującemu działem administracji rządowej lub przez niego nadzorowany przekazuje plan zarządzania kryzysowego, o którym mowa w ust. 1, Szefowi Centrum.

6. Minister kierujący działem administracji rządowej, po zasięgnięciu opinii Szefa Centrum, może wydać, w drodze zarządzenia, wytyczne do opracowania planów

zarządzania kryzysowego kierowników urzędów centralnych podległych temu ministrowi oraz przez niego nadzorowanych.

Art. 5h. 1. Wojewódzki plan zarządzania kryzysowego składa się z części dotyczącej:

1) zarządzania ryzykiem;
2) reagowania kryzysowego.

2. W części dotyczącej zarządzania ryzykiem plan zawiera elementy, o których mowa w art. 5e ust. 3.

3. W części dotyczącej reagowania kryzysowego plan zawiera:

1) elementy, o których mowa w art. 5e ust. 4 pkt 1–3 i 5 oraz art. 5g ust. 3 pkt 2 i 3;
2) wykaz działań określonych planami działań krótkoterminowych, o których mowa w art. 92 ustawy z dnia 27 kwietnia 2001 r. – Prawo ochrony środowiska, wraz z ich opisem;
3) wykaz przedsięwzięć minimalizujących skutki zakłócenia funkcjonowania infrastruktury krytycznej dla ludności na terenie województwa wraz z ich opisem;

4. Wojewoda opracowuje projekt wojewódzkiego planu zarządzania kryzysowego i przekazuje do zatwierdzenia ministrowi właściwemu do spraw administracji publicznej.

5. Wojewoda wdraża zatwierdzony wojewódzki plan zarządzania kryzysowego oraz przekazuje go do wiadomości Szefowi Centrum.

Art. 5i. 1. Powiatowy plan zarządzania kryzysowego składa się z części dotyczącej:

1) zarządzania ryzykiem;
2) reagowania kryzysowego.

2. W części dotyczącej zarządzania ryzykiem plan zawiera elementy, o których mowa w art. 5e ust. 3.

3. W części dotyczącej reagowania kryzysowego plan zawiera:

1) elementy, o których mowa w art. 5e ust. 4 pkt 1–3 i 5 oraz art. 5g ust. 3 pkt 2 i 3;
2) wykaz przedsięwzięć minimalizujących skutki zakłócenia funkcjonowania infrastruktury krytycznej dla ludności na terenie właściwej jednostki samorządu terytorialnego, wraz z ich opisem;

4. Starosta opracowuje projekt powiatowego planu zarządzania kryzysowego i przekazuje do zatwierdzenia właściwemu wojewodzie.

5. Starosta wdraża zatwierdzony powiatowy plan zarządzania kryzysowego.

Art. 5j. 1. Gminy plany zarządzania kryzysowego:

1) może składać się z części dotyczącej zarządzania ryzykiem, zawierającej elementy, o których mowa w art. 5e ust. 3;
2) składa się z części dotyczącej reagowania kryzysowego zawierającej:
   a) elementy, o których mowa w art. 5e ust. 4 pkt 1–3 i 5 oraz art. 5g ust. 3 pkt 2 i 3,
   b) wykaz przedsięwzięć minimalizujących skutki zakłócenia funkcjonowania usług kluczowych lub infrastruktury krytycznej dla ludności na terenie właściwej jednostki samorządu terytorialnego, wraz z ich opisem,

2. Wójt (burmistrz, prezydent miasta) opracowuje i wdraża gminny plan zarządzania kryzysowego.

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

4. Wójt (burmistrz, prezydent miasta) wdraża zatwierdzony gminny plan zarządzania kryzysowego.

Art. 5k. 1. Plany zarządzania kryzysowego podlegają systematycznej aktualizacji w cyklu planowania nie dłuższym niż trzy lata.

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

3. Plany postępowania na wypadek wystąpienia sytuacji kryzysowej, opracowane na podstawie odrębnych przepisów, z wyłączeniem planów sporządzanych na czas zewnętrznego zagrożenia bezpieczeństwa państwa i na czas wojny, stanowią załączniki do planu zarządzania kryzysowego właściwego organu administracji publicznej.";

7) uchyla się art. 6-6d;
8) dodaje się rozdziały 4-11 w brzmieniu:

„Rozdział 4

Identyfikowanie infrastruktury krytycznej i potencjalnej infrastruktury krytycznej

Art. 6e. Zadania w zakresie infrastruktury krytycznej obejmują:

1) identyfikację oraz wyznaczanie infrastruktury krytycznej;
2) gromadzenie i przetwarzanie informacji dotyczących zagrożeń infrastruktury krytycznej;

2) opracowywanie i wdrażanie procedur na wypadek wystąpienia zagrożeń infrastruktury krytycznej;
3) odtwarzanie infrastruktury krytycznej;
4) współpracę między organami administracji publicznej a operatorami infrastruktury krytycznej w zakresie ochrony infrastruktury krytycznej.

Art. 6f. 1. Rada Ministrów określi, w drodze uchwały, kryteria pozwalające zidentyfikować obiekty, urządzenia oraz instalacje lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje oraz sieci, systemy lub usługi jako infrastrukturę krytyczną, w tym:

1) kryteria sektorowe – progi liczbowe charakteryzujące parametry obiektu, urządzenia oraz instalacji lub połączonych ze sobą funkcjonalnie obiektów, urządzeń oraz instalacji, sieci, systemu lub usługi, warunkujące identyfikację infrastruktury krytycznej,
2) kryteria przekrojowe – progi odnoszące się do znaczenia obiektu, urządzenia oraz instalacji lub połączonych ze sobą funkcjonalnie obiektów, urządzeń oraz instalacji, sieci, systemu lub usługi obejmujące:
   a) kryteria ofiar w ludziach – oceniane w odniesieniu do ewentualnej liczby ofiar śmiertelnych lub liczby rannych,
   b) kryteria ewakuacji - oceniane w odniesieniu do liczby osób ewakuowanych lub czasu ewakuacji,
   c) kryteria skutków ekonomicznych – oceniane w odniesieniu do znaczenia strat ekonomicznych lub pogorszenia świadczenia jakości usług kluczowych,
   d) kryteria skutków społecznych – oceniane w odniesieniu do wpływu na zaufanie opinii publicznej lub zakłócenia codziennego życia obywateli, w tym utraty usług kluczowych,
   e) kryteria wpływu międzynarodowego – oceniane w odniesieniu do pogorszenia wizerunku kraju na arenie międzynarodowej lub możliwości realizacji zobowiązań międzynarodowych,
   f) kryteria unikatowości - oceniane w odniesieniu do braku możliwości zastąpienia lub odtworzenia w akceptowalnym czasie

- uwzględniając znaczenie obiektów, urządzeń oraz instalacji lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji oraz sieci, systemu lub usługi dla funkcjonowania

państwa i zaspokajania potrzeb obywateli, w tym potrzeb lokalnych społeczności oraz świadczenia usług kluczowych.

2. Uchwała, o której mowa w ust. 1, ma charakter niejawny.

Art. 6g. 1. Obiekt, urządzenie oraz instalacja lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje oraz sieć, system lub usługa mogą zostać wpisane do wykazu infrastruktury krytycznej, jeżeli spełniają łącznie kryterium sektorowe, o którym mowa w art. 6f ust. 1 pkt 1, oraz co najmniej jedno z kryteriów, o których mowa w art. 6f ust. 1 pkt 2.

2. W przypadku infrastruktury krytycznej identyfikowanej przez wojewodów stosuje się kryteria, o których mowa w art. 6f ust. 1 pkt 2.

Art. 6h. 1. Minister kierujący działem administracji rządowej lub właściwy miejscowo wojewoda we współpracy z Szefem Centrum identyfikuje obiekt, urządzenie, instalację lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje oraz sieć, system lub usługę mogące stanowić infrastrukturę krytyczną.

2. Minister kierujący działem administracji rządowej lub właściwy miejscowo wojewoda może wystąpić do ich właściciela lub posiadacza o udzielenie informacji, które umożliwią ocenę, czy spełniają one warunki do uznania ich za infrastrukturę krytyczną, przekazując dokumenty niezbędne do udzielenia informacji.

3. Minister kierujący działem administracji rządowej lub właściwy miejscowo wojewoda w wystąpieniu wskazuje termin udzielenia informacji. Wyznaczony termin nie może być krótszy niż 14 dni, licząc od dnia otrzymania wystąpienia przez podmiot.

4. Minister kierujący działem administracji rządowej oraz właściwy miejscowo wojewoda prowadzą bieżącą wymianę informacji w zakresie realizacji czynności, o których mowa w ust. 1-3.

5. W sytuacjach niecierpiących zwłoki Szef Centrum identyfikuje obiekt, urządzenie, instalację lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje oraz sieć, system lub usługę mogące stanowić infrastrukturę krytyczną. Przepisy ust. 2-4, art. 6j ust. 3-6 oraz art. 6k stosuje się odpowiednio.

6. Komisja Nadzoru Finansowego, w zakresie swojej właściwości, identyfikuje obiekt, urządzenie, instalację lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje oraz sieć, system lub usługę mogące stanowić infrastrukturę krytyczną. Przepisy ust. 2-4, art. 6j oraz art. 6k stosuje się odpowiednio.

Art. 6i. 1. Szef Centrum prowadzi wykaz infrastruktury krytycznej, który zawiera:

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

2. Wykaz ma charakter niejawny.

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

Art. 6j. 1. Minister kierujący działem administracji rządowej lub właściwy miejscowo wojewoda, składa do Szefa Centrum wniosek o wpis obiektu, urządzenia, instalacji lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji oraz sieci, systemu lub usługi do wykazu infrastruktury krytycznej. Wniosek zawiera informacje, o których mowa w art. 6i.

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

3. Szef Centrum, na podstawie wniosku złożonego przez ministra kierującego działem administracji rządowej dokonuje wpisu do wykazu. Wpis do wykazu jest czynnością materialno-techniczną.

4. Szef Centrum informuje właściciela lub posiadacza obiektu, urządzenia, instalacji lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji oraz sieci, systemu lub usługi o ujęciu w wykazie infrastruktury krytycznej oraz obowiązkach z tym związanych w terminie 30 dni od wpisu do wykazu.

5. Informację, o której mowa w ust. 4, Szef Centrum przekazuje ministrowi kierującemu działem administracji rządowej lub właściwemu miejscowo wojewodzie.

6. Ministrowie kierujący działami administracji rządowej, wojewodowie oraz Szef Centrum w zakresie swojej właściwości zapewniają bieżącą współpracę dotyczącą wyłanianej infrastruktury krytycznej, w tym:
1) prowadzą bieżącą wymianę informacji na temat bieżących zagrożeń;
2) organizują fora ochrony infrastruktury krytycznej;
3) udzielają wsparcia merytorycznego operatorom infrastruktury krytycznej w zakresie wdrażania dobrych praktyk dotyczących ochrony infrastruktury krytycznej.

Art. 6k. 1. Minister kierujący działem administracji rządowej lub właściwy miejscowo wojewoda, we współpracy z Szefem Centrum oraz operatorem infrastruktury krytycznej rozpoznaje obiekty, urządzenia, instalacje lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje oraz sieci, systemy lub usługi będące w fazie projektowania lub budowy, mogące potencjalnie spełniać kryteria, o których mowa w art. 6f ust. 1, zwane dalej „potencjalną infrastrukturą krytyczną”. Przepisy art. 6h ust. 2 i 3 stosuje się odpowiednio.

2. Szef Centrum prowadzi wykaz potencjalnej infrastruktury krytycznej. Przepis art. 6i stosuje się odpowiednio.

3. Minister kierujący działem administracji rządowej lub właściwy miejscowo wojewoda składa do Szefa Centrum wniosek o wpis obiektu, urządzenia, instalacji lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji oraz sieci, systemu lub usługi do wykazu potencjalnej infrastruktury krytycznej. Wniosek zawiera informacje, o których mowa w art. 6i. Przepisy art. 6j ust. 2-4 stosuje się odpowiednio.

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

Rozdział 5

Obowiązki operatora infrastruktury krytycznej

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

1) prowadzenie systematycznej analizy zagrożeń dla infrastruktury krytycznej;
2) wdrażanie adekwatnych do przeprowadzonej analizy zagrożeń rozwiązań w zakresie:
   a) bezpieczeństwa fizycznego, w tym ochrony fizycznej oraz zabezpieczeń technicznych,
   b) bezpieczeństwa osobowego dotyczącego pracowników i dostawców zewnętrznych,
   c) bezpieczeństwa teleinformatycznego,
   d) bezpieczeństwa prawnego,

e) ciągłości działania i odtwarzania, w tym utrzymywania własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie infrastruktury krytycznej do czasu jej pełnego odtworzenia;

3) bieżącą współpracę z organami administracji publicznej oraz Szefem Centrum przez przekazywanie i odbieranie informacji o:
   a) zagrożeniach zakłócających lub mogących zakłócić funkcjonowanie infrastruktury krytycznej,
   b) spodziewanych przerwach lub zakłóceniach w funkcjonowaniu infrastruktury krytycznej;

4) sporządzanie i przekazywanie informacji w zakresie zapewnienia ochrony infrastruktury krytycznej odpowiednio na żądanie:
   a) ministra, o którym mowa w art. 6h, oraz Szefa Centrum,
   b) właściwego miejscowo wojewody;

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

2. Operator infrastruktury krytycznej wdraża rozwiązania, o których mowa w ust. 1 pkt 2, z uwzględnieniem minimalnych standardów określonych w przepisach wykonawczych wydanych na podstawie ust. 4 w terminie 6 miesięcy od dnia ujęcia w wykazie infrastruktury krytycznej.

3. Operator infrastruktury krytycznej może, w celu zapewnienia wdrożenia rozwiązań, o których mowa w ust. 1 pkt 1, żądać od usługodawców w postępowaniach przetargowych lub zamówieniach:

1) zdolności do ochrony informacji niejawnych oraz stosowania tych przepisów przy projektowaniu i wykonywaniu obiektów, urządzeń instalacji i innych systemów będących elementami infrastruktury krytycznej;
2) certyfikatów potwierdzających posiadanie właściwych kompetencji i uprawnień wskazanych w akcie wykonawczym wydanym na podstawie art. 6zf ust. 9.

4. Rada Ministrów określi, w drodze rozporządzenia minimalne standardy ochrony infrastruktury krytycznej, uwzględniając bezpieczeństwo fizyczne, techniczne, osobowe, teleinformatyczne, prawne oraz ciągłość działania z uwzględnieniem lokalizacji i charakterystyki infrastruktury krytycznej.

Art. 6m. 1. Operator infrastruktury krytycznej opracowuje, stosuje i aktualizuje dokumentację ochrony infrastruktury krytycznej.

2. Dokumentacja, o której mowa w ust. 1, zawiera:

1) charakterystykę infrastruktury krytycznej oraz analizę zagrożeń, o której mowa w art. 6l ust. 1 pkt 1;
2) opis zastosowanych, adekwatnie do rodzaju zagrożeń środków bezpieczeństwa w zakresie zapewnienia:
   a) bezpieczeństwa fizycznego, w tym opis organizacji i wykonywania ochrony fizycznej infrastruktury krytycznej, w tym dane specjalistycznej uzbrojonej formacji ochronnej chroniącej infrastrukturę krytyczną, o której mowa w art. 2 pkt 7 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2021 r. poz. 1995) – jeżeli występuje,
   b) bezpieczeństwa technicznego,
   c) bezpieczeństwa osobowego,
   d) bezpieczeństwa teleinformatycznego,
   e) bezpieczeństwa prawnego,
   f) ciągłości działania i odtwarzania;
3) opis:
   a) zasobów umożliwiających podtrzymanie funkcjonowania infrastruktury krytycznej do czasu jej pełnego odtworzenia,
   b) współpracy z właściwymi podmiotami administracji publicznej dotyczący wymiany informacji o zdarzeniu zakłócającym lub mogącym zakłócić funkcjonowanie infrastruktury krytycznej oraz sposobu postępowania w przypadku takiego zdarzenia;
4) procedury:
   a) działania w sytuacji zagrożenia lub zakłócenia funkcjonowania infrastruktury krytycznej,
   b) zapewnienia ciągłości funkcjonowania infrastruktury krytycznej,
   c) odtwarzania infrastruktury krytycznej;
5) inne elementy niż wskazane w pkt 1-4, biorąc pod uwagę charakterystykę infrastruktury krytycznej.

3. Operator infrastruktury krytycznej uzgadnia z właściwymi podmiotami administracji publicznej zakres współpracy, o której mowa w ust. 2 pkt 4 lit. a.

4. Do dokumentacji ochrony infrastruktury krytycznej stosuje się przepisy o ochronie informacji niejawnych lub o ochronie tajemnicy przedsiębiorstwa.

5. Operator infrastruktury krytycznej w terminie 6 miesięcy od uzyskania informacji o ujęciu w wykazie infrastruktury krytycznej przedkłada oświadczenie o opracowaniu dokumentacji ochrony infrastruktury krytycznej oraz wdrożeniu minimalnych wymagań, o których mowa w art. 6l ust. 4, odpowiednio:

1) ministrowi, o którym mowa w art. 6h, lub Szefowi Centrum;
2) właściwemu miejscowo wojewodzie.

6. W przypadku braku możliwości wdrożenia rozwiązań, o których mowa w art. 6l ust. 1 pkt 2, z uwzględnieniem minimalnych standardów określonych w przepisach wykonawczych wydanych na podstawie art. 6l ust. 4, dokumentacja, o której mowa w art. 6m podlega uzgodnieniu odpowiednio z:

1) ministrem, o którym mowa w art. 6h lub Szefem Centrum;
2) właściwym miejscowo wojewodą.

7. Minister, o którym mowa w art. 6h, Szef Centrum oraz m miejscowo wojewoda mogą wskazać podmioty administracji publicznej, od których operator ma uzyskać opinię na temat sporządzonej dokumentacji oraz określają termin do zasięgnięcia opinii. Wyznaczony termin nie może być krótszy niż 14 dni, licząc od dnia otrzymania informacji przez operatora infrastruktury krytycznej o konieczności zasięgnięcia opinii.

8. Operator infrastruktury krytycznej będący jednocześnie operatorem usługi kluczowej w rozumieniu art. 5 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa uwzględnia w dokumentacji, o której mowa w ust. 1, dokumentację dotyczącą cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych, określoną w przepisach wykonawczych wydanych na podstawie art. 10 ust. 5 tej ustawy.

Art. 6n. 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) bezpieczeństwa teleinformatycznego;
5) bezpieczeństwa prawnego;
6) ciągłości działania i odtwarzania.

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

1) analizy zagrożeń dla infrastruktury krytycznej, o której mowa w art. 6l ust. 1 pkt 1;
2) wdrożonych rozwiązań, o których mowa w art. 6l ust. 1 pkt 2;
3) zagrożeń, które zakłóciły lub mogły zakłócić funkcjonowanie infrastruktury krytycznej, a nie były uwzględnione w analizie, o której mowa w art. 6l ust. 1 pkt 1;
4) wyników przeprowadzonych kontroli i audytów odnoszących się do wdrożonych rozwiązań, o których mowa w art. 6l 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. 6h, oraz Szefowi Centrum;
2) właściwemu miejscowo wojewodzie.

5. Raport o stanie ochrony infrastruktury krytycznej sporządza się z zachowaniem przepisów o ochronie informacji niejawnych.

Art. 6o. 1. W celu realizacji zadań, o których mowa w art. 6l–6n, operator infrastruktury krytycznej wyznacza koordynatora do spraw ochrony infrastruktury krytycznej, zwanego dalej „koordynatorem”.

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

3. Koordynatorem 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 co najmniej „poufne”.

4. Koordynator podlega bezpośrednio organowi zarządzającemu operatora infrastruktury krytycznej.

5. O wyznaczeniu koordynatora operator infrastruktury krytycznej informuje odpowiednio:

1) ministra, o którym mowa w art. 6h, oraz Szefa Centrum;

2) właściwego miejscowo wojewodę.

6. Operator infrastruktury krytycznej zapewnia koordynatorowi organizacyjne i techniczne warunki realizacji zadań, o których mowa w art. 6l–6n, w tym dostęp do niezbędnych dokumentów i informacji.

Art. 6p. 1. W przypadku pracownika zatrudnionego na stanowisku umożliwiającym dostęp do informacji o bezpieczeństwie obiektu infrastruktury krytycznej i osoby ubiegającej się o zatrudnienie na tym stanowisku, operator infrastruktury krytycznej żąda od pracownika i tej osoby przedłożenia informacji dotyczących karalności, w tym informacji, czy ich dane osobowe są zgromadzone w Krajowym Rejestrze Karnym.

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

3. Operator infrastruktury krytycznej przechowuje informacje i dane, o których mowa w ust. 1 i 2, wyłącznie przez okres zatrudnienia pracownika, którego te dane dotyczą.

Rozdział 6

Identyfikowanie podmiotów krytycznych

Art. 6q. 1. Organ do spraw podmiotów krytycznych ujmuje operatora infrastruktury krytycznej w wykazie podmiotów krytycznych, jeżeli:

1) świadczy co najmniej jedną usługę kluczową;

2) incydent miałby istotny skutek zakłócający dla świadczenia usługi kluczowej.

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

3. Przy dokonywaniu wpisu do wykazu organ do spraw podmiotów krytycznych uwzględnia wyniki Krajowej Oceny Ryzyka oraz postanowienia Strategii.

Art. 6r. 1. Organ do spraw podmiotów krytycznych może wystąpić do operatora o udzielenie informacji, które umożliwią wstępną ocenę, czy spełnia warunki do uznania go za podmiot krytyczny, w szczególności w zakresie spełniania warunków, o których mowa w art. 6q ust. 1 oraz wskazania infrastruktury krytycznej niezbędnej do świadczenia usługi kluczowej.

2. Organ do spraw podmiotów krytycznych przekazuje operatorowi dokumenty w zakresie niezbędnym do udzielenia informacji.

3. Organ do spraw podmiotów krytycznych w wystąpieniu, o którym mowa w ust. 1, wskazuje termin udzielenia informacji. Wyznaczony termin nie może być krótszy niż 14 dni, licząc od dnia otrzymania wystąpienia przez podmiot.

4. Operator infrastruktury krytycznej przekazuje organowi do spraw podmiotów krytycznych żądane informacje oraz wskazujące infrastrukturę krytyczną niezbędną do świadczenia usługi kluczowej.

Art. 6s. 1. Organ do spraw podmiotów krytycznych prowadzi wykaz podmiotów krytycznych, który zawiera:

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

2. Wpisu do wykazu podmiotów krytycznych dokonuje organ do spraw podmiotów krytycznych. Wpis do wykazu jest czynnością materialno-techniczną.

3. Dane z wykazu podmiotów krytycznych, w zakresie niezbędnym do realizacji ich ustawowych zadań, organ właściwy do spraw podmiotów krytycznych udostępnia, na wniosek, następującym podmiotom:

1) Agencji Bezpieczeństwa Wewnętrznego;

2) Agencji Wywiadu;
3) Centralnemu Biuru Antykorupcyjnemu;
4) organom Krajowej Administracji Skarbowej;
5) Policji;
6) Pełnomocnikowi Rządu do spraw Cyberbezpieczeństwa;
7) Prezesowi Urzędu Ochrony Danych Osobowych;
8) Prokuratorii Generalnej Rzeczypospolitej Polskiej;
9) prokuraturze;
10) sądom;
11) Służbie Kontrwywiadu Wojskowego;
12) Służbie Ochrony Państwa;
13) Służbie Wywiadu Wojskowego;
14) Straży Granicznej;
15) Żandarmerii Wojskowej;
16) Szefowi Centrum;
17) wojewodom.

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

5. Informację, o których mowa w ust. 4, organ do spraw podmiotów krytycznych przekazuje Szefowi Centrum.

Art. 6t. 1. W przypadku zakończenia świadczenia usługi kluczowej przez podmiot krytyczny organ do spraw podmiotów krytycznych dokonuje wykreślenia tego podmiotu z wykazu podmiotów krytycznych. Wykreślenie z wykazu jest czynnością materialno-techniczną.

2. Organ do spraw podmiotów krytycznych niezwłocznie informuje podmiot krytyczny o wykreśleniu z wykazu i dacie wykreślenia.

3. Informację, o której mowa w ust. 2, organ do spraw podmiotów krytycznych przekazuje Szefowi Centrum.

Art. 6u. Rada Ministrów określi, w drodze rozporządzenia:

1) wykaz usług kluczowych w podziale na sektory, podsektory i kategorie podmiotów wymienionych w załączniku do ustawy, uwzględniając znaczenie danej usługi dla

utrzymania niezbędnych funkcji społecznych, niezbędnej działalności gospodarczej, zdrowia i bezpieczeństwa publicznego lub środowiska naturalnego,

2) progi istotności skutku zakłócającego dla świadczenia usług kluczowych, wymienionych w wykazie usług kluczowych, z uwzględnieniem:
   a) liczby użytkowników zależnych od usługi kluczowej świadczonej przez dany podmiot,
   b) stopnia, w jakim inne sektory lub podsektory, o których mowa w załączniku do ustawy, są zależne od usługi świadczonej przez ten podmiot,
   c) wpływu, jaki incydent - jeżeli chodzi o jego skalę i czas trwania - mógłby mieć na działalność gospodarczą i społeczną, środowisko, bezpieczeństwo publicznej lub na zdrowie ludności,
   d) udziału podmiotu krytycznego w rynku w odniesieniu do świadczonej usługi kluczowej,
   e) obszaru geograficzny, którego mógłby dotyczyć incydent,
   f) znaczenia podmiotu w utrzymywaniu wystarczającego poziomu świadczenia usługi kluczowej przy uwzględnieniu dostępności alternatywnych sposobów jej świadczenia,
   g) innych czynników charakterystycznych dla danego sektora lub podsektora jeżeli występują

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

Rozdział 7

Organy do spraw podmiotów krytycznych i Pojedynczy Punkt Kontaktowy"

Art. 6v. Organami do spraw podmiotów krytycznych są:

1) dla sektora energii - minister właściwy do spraw energii;
2) dla sektora transportu z wyłączeniem podsektora transportu wodnego - minister właściwy do spraw transportu;
3) dla podsektora transportu wodnego - minister właściwy do spraw gospodarki morskiej oraz minister właściwy do spraw żeglugi śródlądowej;
4) dla sektora bankowości i infrastruktury rynków finansowych - Komisja Nadzoru Finansowego;
5) dla sektora zdrowia - minister właściwy do spraw zdrowia;

6) dla sektora wody pitnej oraz sektora ścieków - minister właściwy do spraw gospodarki wodnej;
7) dla sektora infrastruktury cyfrowa - minister właściwy do spraw informatyzacji;
8) dla sektora administracji publicznej – Prezes Rady Ministrów;
9) dla sektora przestrzeni kosmicznej - minister właściwy do spraw gospodarki;
10) dla sektora produkcji, przetwarzania i dystrybucji żywności - minister właściwy do spraw rolnictwa;
11) dla sektora zarządzanie usługami ICT - minister właściwy do spraw informatyzacji;
12) dla sektora produkcji, wytwarzania i dystrybucji chemikaliów i innych produktów przemysłowych – minister właściwy do spraw zdrowia;
13) dla sektora usług pocztowych i kurierskich - minister właściwy do spraw łączności;
14) dla sektora gospodarowania odpadami – minister właściwy do spraw klimatu.

Art. 6w. 1. Organ do spraw podmiotów krytycznych:

1) prowadzi bieżącą analizę operatorów infrastruktury krytycznej pod kątem uznania ich za podmiot krytyczny w danym sektorze lub podsektorze;
2) prowadzi bieżącą analizę podmiotów krytycznych w danym sektorze lub podsektorze pod kątem niespełniania warunków kwalifikujących dany podmiot jako podmiot krytyczny;
3) prowadzi wykaz podmiotów krytycznych w danym sektorze lub podsektorze, w tym dokonuje wpisu do wykazu oraz wykreślenia z wykazu;
4) prowadzi bieżącą wymianę informacji oraz współpracę w zakresie obsługi incydentów;
5) monitoruje stosowanie przepisów ustawy przez podmioty krytyczne;
6) prowadzi kontrole podmiotów krytycznych;
7) prowadzi działania informacyjne dotyczące dobrych praktyk, działań edukacyjnych i kampanii na rzecz poszerzania wiedzy i budowania odporności podmiotów krytycznych;
8) uczestniczy w planowaniu i organizowaniu ćwiczeń podmiotów krytycznych oraz w razie potrzeby bierze w nich udział;
9) współpracuje z innymi organami do spraw podmiotów krytycznych oraz organami właściwymi do spraw cyberbezpieczeństwa, o których mowa w ustawie o ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa w zakresie realizacji zadań wskazanych w pkt 1-8.

2. Organ do spraw podmiotów krytycznych może powierzyć realizację, w jego imieniu, niektórych zadań, o których mowa w ust. 1, jednostkom podległym lub nadzorowanym przez ten organ. Powierzenie następuje na podstawie porozumienia.

3. W porozumieniu, o którym mowa w ust. 2, określa się zasady sprawowania przez organ do spraw podmiotów krytycznych kontroli nad prawidłowym wykonywaniem powierzonych zadań.

4. Prezes Rady Ministrów powierza Szefowi Centrum realizację zadań organu do spraw podmiotów krytycznych w odniesieniu do sektora administracji publicznej, z wyłączeniem nakładania kar pieniężnych, o których mowa w rozdziale 11. Przepisy ust. 2 zdanie drugie oraz ust. 3 stosuje się odpowiednio.

Art. 6x. Organy do spraw podmiotów krytycznych za pośrednictwem Pojedynczego Punktu Kontaktowego prowadzą konsultacje i bieżącą wymianę informacji z właściwymi organami państw członkowskich w przypadku gdy podmioty krytyczne:

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

Art. 6y. 1. Szef 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 Komisji Europejskiej oraz Grupie do spraw Podmiotów Krytycznych sprawozdań dotyczących incydentów istotnych zgłaszanych przez podmioty krytyczne mających wpływ na ciągłość świadczonych przez nich usług kluczowych na terytorium Rzeczypospolitej Polskiej oraz ciągłość świadczonych usług kluczowych w państwach członkowskich Unii Europejskiej;

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

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

1) informacje na temat infrastruktury krytycznej zlokalizowanej na terytorium Rzeczypospolitej Polskiej służącej realizacji usług kluczowych w innych państwach członkowskich;
2) dobre praktyki związane ze zgłaszaniem i obsługą incydentów istotnych;
3) propozycje do programu prac Grupie do spraw 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 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 informacje pochodzące z Grupy do spraw Podmiotów Krytycznych dotyczące:

1) analiz i ocen krajowych strategii państw członkowskich Unii Europejskiej w zakresie odporności podmiotów krytycznych, a także dobrych praktyk w obszarze zapewnienia świadczenia usług kluczowych;

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

5. Pojedynczy Punkt Kontaktowy przekazuje Komisji Europejskiej:

1) niezwłocznie informacje o:
   a) wyznaczonych organach do spraw podmiotów krytycznych, Pojedynczym Punkcie Kontaktowym, ich zadaniach oraz późniejszych zmianach w tym zakresie,
   b) przepisach dotyczących kar pieniężnych;
2) informacje umożliwiające ocenę wdrażania dyrektywy 2022/2557, obejmujące w szczególności:
   a) środki umożliwiające identyfikację podmiotów krytycznych,
   b) wykaz usług kluczowych,
   c) liczbę zidentyfikowanych podmiotów krytycznych w każdym sektorze, o którym mowa w załączniku do ustawy, oraz wskazanie ich znaczenia w odniesieniu do tego sektora,
   d) progi istotności skutku zakłócającego dla świadczonej usługi kluczowej brane pod uwagę przy kwalifikowaniu podmiotów jako podmiotów krytycznych;
3) informacje o zadaniach organów właściwych w sprawach podmiotów krytycznych;
4) informacje o środkach mających na celu zwiększenie odporności podmiotów krytycznych.

Rozdział 8

Obowiązki podmiotów krytycznych

Art. 6z. 1. Podmiot krytyczny wdraża zintegrowany system zarządzania bezpieczeństwem świadczenia usługi kluczowej zapewniający:

1) prowadzenie systematycznej oceny ryzyka z uwzględnieniem:

a) zagrożeń i związanych z tym ryzyk wymienionych w Krajowej Ocenie Ryzyka oraz innych zagrożeń naturalnych i spowodowanych przez człowieka, charakterystycznych dla świadczonej usługi kluczowej,

b) stopnia zależności innych sektorów lub podsektorów określonych w załączniku do ustawy od usługi kluczowej świadczonej przez podmiot krytyczny oraz stopnia zależności tego podmiotu krytycznego od usług kluczowych świadczonych przez inne podmioty w innych sektorach, w tym w stosownych przypadkach w sąsiadujących państwach członkowskich Unii Europejskiej i w państwach trzecich,

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

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

a) polityk zarządzania ryzykiem,

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

c) ochrony infrastruktury krytycznej niezbędnej do świadczenia usługi kluczowej, zgodnie z art. 6l,

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 świadczenie usługi kluczowej do czasu jej pełnego odtworzenia, w infrastruktury krytycznej niezbędnej do świadczenia tej usługi,

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

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

j) realizacji okresowych audytów i certyfikacji;

3) bieżącą współpracę z właściwymi podmiotami administracji publicznej 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. Podmiot krytyczny wdraża rozwiązania organizacyjno-techniczne, o których mowa w ust. 1 pkt 2, z uwzględnieniem wymagań określonych w:

1) Polskich Normach:

a) PN-EN ISO/IEC 27001,

b) PN-EN ISO 22301,

c) PN-EN 50131 lub

d) PN-EN 60839 lub

e) PN-EN 62676;

2) minimalnych standardach ochrony infrastruktury krytycznej, o których mowa w przepisach wykonawczych wydanych na podstawie art. 6l ust. 4.

3. Podmiot krytyczny, w celu zapewnienia wdrożenia rozwiązań, o których mowa w ust. 1 pkt 2, żąda od usługodawców w postępowaniach przetargowych lub zamówieniach:

1) zdolności do ochrony informacji niejawnych oraz stosowania tych przepisów przy projektowaniu i wykonywaniu obiektów, urządzeń instalacji i innych systemów będących elementami infrastruktury krytycznej;

2) certyfikatów potwierdzających posiadanie właściwych kompetencji i uprawnień wskazanych w akcie wykonawczym wydanym na podstawie art. 6zf ust. 9.

4. Podmiot krytyczny przeprowadza po raz pierwszy ocenę ryzyka, o której mowa w ust. 1 pkt 1, w terminie 9 miesięcy od otrzymania informacji o ujęciu w wykazie podmiotów krytycznych, a następnie nie rzadziej niż raz na 4 lata.

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

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

1) dokumentacja dotycząca systemu zarządzania bezpieczeństwem informacji wytworzona zgodnie z wymaganiami Polskiej Normy PN-EN ISO/IEC 27001;
2) dokumentacja systemu zarządzania ciągłością działania usługi kluczowej wytworzona zgodnie z wymaganiami Polskiej Normy PN-EN ISO 22301;
3) dokumentacja ochrony fizycznej oraz zabezpieczeń technicznych, o których mowa w art. 6z ust. 1 pkt 2 lit. b;
4) dokumentacja ochrony infrastruktury krytycznej, o której mowa w art. 6m;
5) inne elementy niż wskazane w pkt 1-4, biorąc pod uwagę rodzaj świadczonej usługi kluczowej.

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

4. 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;
3) oznaczanie kolejnych wersji dokumentów umożliwiające określenie zmian dokonanych w tych dokumentach.

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

Art. 6zb. 1. Podmiot krytyczny:

1) zapewnia obsługę incydentów;
2) zapewnia dostęp do informacji o zarejestrowanych incydentach organom do spraw podmiotów krytycznych oraz Szefowi Centrum;

3) klasyfikuje incydent jako istotny, na podstawie progów uznawania incydentu za istotny, określonych w przepisach wykonawczych wydanych na podstawie ust. 3;
4) zgłasza incydent istotny niezwłocznie, nie później niż w terminie 24 godzin od momentu jego wystąpienia lub wykrycia do organu właściwego w sprawach podmiotów krytycznych oraz Szefa Centrum;
5) współdziała podczas obsługi incydentu istotnego z organem właściwym w sprawach podmiotów krytycznych lub Szefem Centrum;
6) informuje organ właściwy w sprawach podmiotów krytycznych oraz Szefa Centrum o usunięciu incydentu istotnego.

2. Zgłoszenie, o którym mowa w ust. 1 pkt 4, sporządza się i składa za pomocą systemu, o którym mowa w art. 46 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, albo na piśmie utrwalonym w postaci elektronicznej, opatrzonym kwalifikowanym podpisem elektronicznym, podpisem osobistym albo podpisem zaufanym, w przypadku braku możliwości dokonania zgłoszenia w systemie.

3. Rada Ministrów określi, w drodze rozporządzenia, progi uznania incydentu za istotny według zdarzenia w poszczególnych sektorach i podsektorach określonych w załączniku do ustawy, uwzględniając:
1) liczbę użytkowników dotkniętych zakłóceniem,
2) czas trwania zakłócenia usługi kluczowej,
3) obszar geograficzny, którego dotyczy zakłócenie,
4) inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują

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

Art. 6zc. 1. Zgłoszenie, o którym mowa w art. 6zb ust. 1 pkt 4, zawiera:
1) dane podmiotu zgłaszającego, w tym firmę przedsiębiorcy, numer we właściwym rejestrze, siedzibę i adres;
2) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby dokonującej zgłoszenia;
3) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji;
4) opis wpływu incydentu istotnego na świadczenie usługi kluczowej, w tym:
   a) usługi kluczowej zgłaszającego, na którą incydent miał wpływ,

b) liczbę użytkowników usługi kluczowej, na których incydent miał wpływ,

c) moment wystąpienia i wykrycia incydentu istotnego oraz czas jego trwania,

d) obszar geograficzny, którego dotyczy incydent istotny,

e) wpływ incydentu istotnego na świadczenie usług kluczowych przez inne podmioty krytyczne,

f) przyczynę zaistnienia incydentu istotnego i sposób jego przebiegu oraz skutki jego oddziaływania na świadczoną usługę kluczową;

5) informacje umożliwiające właściwemu organowi do spraw podmiotów krytycznych oraz Szefowi Centrum określenie, czy incydent istotny dotyczy innych państw członkowskich Unii Europejskiej;

6) informacje o podjętych działaniach zapobiegawczych;

7) informacje o podjętych działaniach naprawczych;

8) inne istotne informacje.

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

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

Art. 6zd. Podmiot krytyczny:

1) 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;

2) informuje właściwe organy zarządzania kryzysowego o incydencie, w przypadku gdy może on doprowadzić do sytuacji kryzysowej.

Art. 6ze.1. Podmiot krytyczny może przekazywać właściwym organom do spraw podmiotów krytycznych oraz Szefowi 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 w postaci elektronicznej, a w przypadku braku możliwości przekazania w postaci elektronicznej, przy użyciu innych dostępnych środków komunikacji.

Art. 6zf. 1. Podmiot krytyczny ma obowiązek przeprowadzania, na własny koszt, co najmniej raz na 3 lata, audytu zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej, w zakresie obejmującym rozwiązania organizacyjno-techniczne wdrożone z uwzględnieniem Polskich Norm, o których mowa w art. 6z ust. 2 pkt 1.

2. Organ do spraw podmiotów krytycznych może nakazać przeprowadzenie audytu, o którym mowa w ust. 1, wraz z określeniem terminu przekazania sprawozdania z przeprowadzonego audytu.

3. Audyt może być prowadzony przez:

1) jednostkę certyfikującą akredytowaną lub upoważnioną do certyfikacji na zgodność z Polskimi Normami wskazanymi w przepisach wykonawczych wydanych na podstawie ust. 9;
2) co najmniej dwóch audytorów, w tym jednego z ukończonym szkoleniem audytora wiodącego.

4. Jednostka certyfikująca lub audytorzy są obowiązani do zachowania w tajemnicy informacji uzyskanych w związku z przeprowadzanym audytem, z zachowaniem przepisów o ochronie informacji niejawnych i innych informacji prawnie chronionych. Audyt nie może być przeprowadzony przez osobę realizującą w podmiocie audytowanym zadania, o których mowa w art. 6z ust. 1, art. 6za ust. 1 oraz art. 6zb ust. 1, lub która realizowała te zadania w podmiocie audytowanym nie później niż w terminie 1 roku przed rozpoczęciem audytu.

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

6. Przepisu ust. 1 nie stosuje się do podmiotów krytycznych, które posiadają aktualne certyfikaty zgodności z odpowiednimi Polskimi Normami wskazanymi w przepisach wykonawczych wydanych na podstawie ust. 9.

7. Podmiot krytyczny przedstawia kopię sprawozdania z przeprowadzonego audytu właściwemu organowi do spraw podmiotów krytycznych w terminie 7 dni roboczych od dnia jego otrzymania lub Szefowi Centrum na jego uzasadniony wniosek. Kopię sprawozdania z przeprowadzonego audytu lub kopię certyfikatu przekazuje się za pomocą systemu, o którym mowa w art. 46 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa albo na piśmie utrwalonym w postaci elektronicznej, opatrzonym

kwalifikowanym podpisem elektronicznym, podpisem osobistym albo podpisem zaufanym, w przypadku braku możliwości dokonania zgłoszenia w systemie.

8. Jednostka certyfikująca lub audytorzy prowadzący audyt lub certyfikację systemu zarządzania ciągłością działania powinni spełniać wymagania bezpieczeństwa osobowego i przemysłowego w zakresie dostępu do informacji niejawnych o klauzuli „poufne”.

9. Rada Ministrów określi, w drodze rozporządzenia, wykaz:

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

Art. 6zg. 1. Podmiot krytyczny zapewnia udział struktur organizacyjnych lub pracowników niezbędnych do zapewnienia niezakłóconego świadczenia usługi kluczowej w szkoleniach i ćwiczeniach, w tym w ćwiczeniach z zakresu obrony cywilnej, ochrony ludności, zarządzania kryzysowego oraz obronnych.

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

3. Ćwiczenia, o których mowa w ust. 1, polegają na praktycznej realizacji zadań z zakresu, o którym mowa w ust. 1.

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

Art. 6zh. 1. Podmiot krytyczny wyznacza osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami do spraw podmiotów krytycznych oraz Szefem Centrum, w szczególności zapewniającą koordynację obiegu informacji, zwaną dalej „osobą do kontaktów”.

2. Podmiot krytyczny wyznacza osobę do kontaktów w terminie 30 dni od dnia otrzymania informacji o ujęciu w wykazie podmiotów krytycznych.

3. Osoba do kontaktów:

1) jest pracownikiem podmiotu krytycznego;

2) korzysta z pełni praw publicznych;
3) posiada wiedzę, umiejętności i doświadczenie w zakresie zarządzania bezpieczeństwem, z uwzględnieniem przedmiotu działalności podmiotu świadczące usługę kluczową;
4) nie była skazana prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe;
5) spełnia wymagania bezpieczeństwa osobowego w zakresie dostępu do informacji niejawnych o klauzuli „poufne”.

4. Osoba do kontaktów podlega bezpośrednio organowi zarządzającemu podmiotu krytycznego.

5. O wyznaczeniu osoby do kontaktów podmiot krytyczny informuje niezwłocznie właściwy organ do spraw podmiotów krytycznych oraz Szefa Centrum, przekazując dane tej osoby obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej.

6. Podmiot krytyczny zapewnia osobie do kontaktów organizacyjne i techniczne warunki realizacji zadań.

Art. 6zi. 1. Podmiot krytyczny może prowadzić sprawdzenie przeszłości w przypadku swoich pracowników lub kandydatów na pracowników, którzy:
1) pełnią lub mogą pełnić newralgiczne role w strukturach organizacyjnych podmiotu krytycznego lub wykonywać zadania na jego rzecz;
2) są lub mogą być upoważnieni do posiadania bezpośredniego lub zdalnego dostępu do budynków i terenów podmiotu krytycznego, obiegu informacji lub systemów kontroli, w tym w związku z bezpieczeństwem podmiotu krytycznego.

2. Newralgiczną rolę w strukturach organizacyjnych podmiotu krytycznego lub przy wykonywaniu zadań na jego rzecz pełnią osoby:
1) reprezentujące podmiot krytyczny samodzielnie lub łącznie z innymi osobami na podstawie statutu, umowy lub innego aktu założycielskiego;
2) pełniące funkcje kierownicze lub koordynacyjne;
3) wykonujące zadania związane z:
   a) procesami zapewniającymi niezakłócone świadczenie usługi kluczowej,
   b) funkcjonowaniem infrastruktury krytycznej niezbędnej do świadczenia usługi kluczowej.

3. Sprawdzenie przeszłości obejmuje:
1) potwierdzenie tożsamości osoby, która podlega sprawdzeniu przeszłości;

2) sprawdzenie rejestrów karnych pod kątem przestępstw, które miałyby znaczenie dla zajmowanego stanowiska lub w przypadku ubiegania się o to stanowisko we wszystkich państwach pobytu z ostatnich 5 lat;
3) potwierdzenie informacji o zatrudnieniu, wykształceniu, zdobywaniu umiejętności, podnoszeniu kwalifikacji oraz wszystkich przerwach w zatrudnieniu z ostatnich 5 lat.

4. Wniosek podmiotu krytycznego w zakresie, o którym mowa w ust. 3 pkt 2, jest kierowany do właściwych organów państw członkowskich z uwzględnieniem:

1) decyzji ramowej Rady 2009/315/WSiSW z dnia 26 lutego 2009 r. w sprawie organizacji wymiany informacji pochodzących z rejestru karnego pomiędzy państwami członkowskimi oraz treści tych informacji (Dz.U. L 93 z 7.4.2009, s. 23);
2) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/816 z dnia 17 kwietnia 2019 r. ustanawiające scentralizowany system służący do ustalania państw członkowskich posiadających informacje o wyrokach skazujących wydanych wobec obywateli państw trzecich i bezpaństwowców (ECRIS-TCN) na potrzeby uzupełnienia europejskiego systemu przekazywania informacji z rejestrów karnych oraz zmieniające rozporządzenie (UE) 2018/1726 (Dz.U. L 135 z 22.5.2019, s. 1)

2. Podmiot krytyczny powtarza sprawdzenia nie rzadziej niż raz na pięć lat.

Rozdział 9

Podmiot krytyczny o szczególnym znaczeniu europejskim

Art. 6zj. 1. Podmiot krytyczny informuje właściwy organ do spraw podmiotów krytycznych oraz Pojedynczy Punkt Kontaktowy o fakcie świadczenia usługi kluczowej na rzecz co najmniej sześciu państw członkowskich Unii Europejskiej lub w co najmniej sześciu państwach członkowskich Unii Europejskiej.

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. 6s ust. 1 pkt 1-7.

Art. 6zk.1. Właściwy organ do spraw podmiotów krytycznych, za pośrednictwem Pojedynczego Punktu Kontaktowego, inicjuje i prowadzi konsultacje z Komisją Europejską oraz właściwymi organami państw członkowskich Unii Europejskiej w celu

ustalenia, czy podmiot krytyczny świadczący usługę kluczową na terytorium Rzeczypospolitej Polskiej, świadczy ją na rzecz co najmniej sześciu państw członkowskich Unii Europejskiej lub w co najmniej sześciu państwach członkowskich Unii Europejskiej.

2. Na podstawie ustaleń będących wynikiem konsultacji właściwy organ do spraw podmiotów krytycznych informuje podmiot krytyczny, o którym mowa w art. 6zj ust. 1, o uznaniu za podmiot krytyczny o szczególnym znaczeniu europejskim oraz obowiązkach z tym związanych, w szczególności obowiązkach, o których mowa w rozdziale 8 .

Art. 6zl. 1. Właściwy organ do spraw podmiotów krytycznych, we współpracy z Pojedynczym Punktem Kontaktowym, zapewnia współpracę z Komisją Europejską oraz właściwymi organami państwa członkowskiego, na rzecz którego lub w którym jest świadczona usługa kluczowa, w tym prowadzi wymianę informacji w zakresie:

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

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

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

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

1) po dokonaniu analizy sprawozdania z ustaleń misji doradczej, przedkłada Komisji Europejskiej informację o stopniu wdrożenia rozwiązań organizacyjno-technicznych służących zapewnieniu odporności podmiotu krytycznego o szczególnym znaczeniu europejskim lub przedkłada rekomendacje w zakresie zwiększenia odporności tego podmiotu, w celu wydania przez Komisję Europejską opinii dotyczącej wywiązywania się z nałożonych obowiązków przez ten podmiot

lub wskazującej środki, które można wprowadzić, aby zwiększyć odporność tego podmiotu;

2) przekazuje opinię, o której mowa w pkt 1, podmiotowi krytycznemu o szczególnym znaczeniu europejskim oraz zapewnia wsparcie w przypadku konieczności wdrożenia dodatkowych środków zwiększających odporność;

3) informuje Komisję Europejską oraz właściwe organy państwa członkowskiego, na rzecz którego lub w którym jest świadczona usługa kluczowa, o środkach zwiększających odporność, wprowadzonych z uwzględnieniem opinii, o której mowa w pkt 1, albo informację o braku konieczności wprowadzania tych środków.

Rozdział 10

Nadzór i kontrola podmiotów krytycznych

Art. 6zm. 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 oraz infrastruktury krytycznej należącej do tych podmiotów;

2) przeprowadza lub zleca audyt zintegrowanego systemu zarządzania bezpieczeństwem świadczenia usługi kluczowej, w zakresie obejmującym wdrożenie rozwiązań uwzględniających Polski Normy, o których mowa w art. 6z ust. 2;

3) nakłada kary pieniężne na podmioty krytyczne.

Art. 6zn. Do kontroli realizowanej wobec podmiotów:

1) będących przedsiębiorcami stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. - Prawo przedsiębiorców (Dz. U. z 2024 r. poz. 236);

2) niebędących przedsiębiorcami stosuje się przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. z 2020 r. poz. 224) określające zasady i tryb przeprowadzania kontroli.

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

1) swobodnego wstępu i poruszania się po terenie podmiotu kontrolowanego bez obowiązku uzyskiwania przepustki;
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. 6zp. 1. Kontrolowane podmioty zapewniają osobie prowadzącej czynności kontrolne warunki niezbędne do sprawnego przeprowadzenia kontroli, w szczególności przez zapewnienie niezwłocznego przedstawienia żądanych dokumentów, terminowego udzielania ustnych i pisemnych wyjaśnień w sprawach objętych kontrolą, udostępniania niezbędnych urządzeń technicznych, a także sporządzania we własnym zakresie kopii lub wydruków dokumentów oraz informacji zgromadzonych na nośnikach, w urządzeniach lub w systemach informacyjnych.

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

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

2. Osoba prowadząca czynności kontrolne wobec podmiotów 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 osoby prowadzącej czynności kontrolne;
4) datę rozpoczęcia i zakończenia czynności kontrolnych;
5) określenie przedmiotu i zakresu kontroli;
6) opis stanu faktycznego ustalonego w toku kontroli oraz inne informacje mające istotne znaczenie dla przeprowadzonej kontroli, w tym zakres, przyczyny i skutki stwierdzonych nieprawidłowości;
7) zalecenia pokontrolne;
8) wyszczególnienie załączników.

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

5. Przed podpisaniem protokołu podmiot kontrolowany może, w terminie 7 dni od dnia przedstawienia mu go do podpisu, złożyć pisemne zastrzeżenia do tego protokołu.

6. W razie zgłoszenia zastrzeżeń osoba prowadząca czynności kontrolne dokonuje ich analizy i w razie potrzeby podejmuje dodatkowe czynności kontrolne, a w przypadku stwierdzenia zasadności zastrzeżeń zmienia lub uzupełnia odpowiednią część protokołu w formie aneksu do protokołu.

7. W razie nieuwzględnienia zastrzeżeń w całości lub w części osoba prowadząca czynności kontrolne informuje podmiot kontrolowany na piśmie.

8. O odmowie podpisania protokołu osoba prowadząca czynności kontrolne czyni w protokole wzmiankę zawierającą datę jej dokonania.

9. Protokół w postaci papierowej sporządza się w dwóch egzemplarzach, z których jeden pozostawia się podmiotowi kontrolowanemu, a w przypadku protokołu sporządzonego w postaci elektronicznej doręcza się go podmiotowi kontrolowanemu.

Art. 6zr. 1. Jeżeli na podstawie informacji zgromadzonych w protokole kontroli organ do spraw podmiotów krytycznych uzna, że mogło dojść do naruszenia przepisów ustawy przez podmiot kontrolowany, przekazuje zalecenia pokontrolne dotyczące usunięcia nieprawidłowości.

2. Od zaleceń pokontrolnych nie przysługują środki odwoławcze.

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

Rozdział 11

Przepisy o karach pieniężnych dla podmiotów krytycznych

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

1) nie przeprowadza systematycznej oceny ryzyka, o której mowa w art. 6z ust. 1 pkt 1;
2) nie wdraża rozwiązań organizacyjno-technicznych, o których mowa w art. 6z ust. 1 pkt 2;
3) nie prowadzi dokumentacji, o której mowa w art. 6za ust. 1;
4) nie wykonuje obowiązku, o których mowa w art. 6zb ust. 1 pkt 1;
5) nie wykonuje obowiązku, o których mowa w art. 6zb ust. 1 pkt 4;
6) nie przeprowadza audytu;
7) nie wyznacza osoby do kontaktów;
8) uniemożliwia lub utrudnia wykonywanie kontroli;
9) nie wykonał w wyznaczonym terminie zaleceń pokontrolnych
10) nie wdrożył środków ochrony infrastruktury krytycznej, o których mowa w art. 6l ust. 1 pkt 2;
11) nie opracował dokumentacji ochrony infrastruktury krytycznej , o której mowa w art. 6m ust. 1.

2. Wysokość kary pieniężnej, o której mowa w:

1) ust. 1 pkt 1, wynosi do 100 000 zł;
2) ust. 1 pkt 2, wynosi do 150 000 zł;
3) ust. 1 pkt 3, wynosi do 50 000 zł;
4) ust. 1 pkt 4, wynosi do 15 000 zł za każdy stwierdzony przypadek zaniechania obsługi incydentu;
5) ust. 1 pkt 5, wynosi do 20 000 zł za każdy stwierdzony przypadek niezgłoszenia incydentu istotnego;
6) ust. 1 pkt 6, wynosi do 200 000 zł;
7) ust. 1 pkt 7, wynosi do 15 000 zł:
8) ust. 1 pkt 8, wynosi do 50 000 zł;
9) ust. 1 pkt 9, wynosi do 200 000 zł;

10) ust. 1 pkt 10, wynosi do 150 000 zł;

11) ust. 1 pkt 11, wynosi do 50 000 zł.

3. Jeżeli w wyniku kontroli organ właściwy do spraw podmiotów krytycznych stwierdzi, że podmiot krytyczny uporczywie narusza przepisy ustawy, powodując:

1) bezpośrednie i poważne zagrożenie dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi,

2) zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług kluczowych

- podmiot krytyczny podlega karze w wysokości do 1 000 000 zł.

Art. 6zt. 1. Kary pieniężne, o których mowa w art. 6zs, nakładają, w drodze decyzji, właściwe organy do spraw podmiotów krytycznych.

2. Wpływy z tytułu kar pieniężnych, o których mowa w art. 6zs, stanowią przychód Funduszu Cyberbezpieczeństwa, o którym mowa w art. 2 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 677 oraz z 2024 r. poz. 834), w zakresie maksymalnej kwoty prognozowanych kosztów związanych z przyznaniem świadczenia teleinformatycznego, o którym mowa w art. 5 tej ustawy.

9) po art. 6zt dodaje się oznaczenie „Rozdział 12 Organy właściwe w sprawach zarządzania kryzysowego i ich zadania";

10) w art. 7a w ust. 2 pkt 1 otrzymuje brzmienie:

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

11) w art. 7ba w ust. 2 pkt 1 otrzymuje brzmienie:

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

12) w art. 10 ust. 2-3 otrzymują brzmienie:

"2. Centrum kieruje Szef powoływany i odwoływany przez Prezesa Rady Ministrów.

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

3. Zastępców Szefa Centrum powołuje i odwołuje Prezes Rady Ministrów, na wniosek Szefa Centrum.";

13) po art. 11a dodaje się art. 11b–11 e w brzmieniu:

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

1) koordynuje:
   a) udział przedstawicieli Rzeczypospolitej Polskiej w pracach Komitetu Odporności NATO oraz zapewnia wsparcie merytoryczne prowadzonych prac,
   b) opracowywanie stanowisk Rzeczypospolitej Polskiej na potrzeby procesów planowania obronnego Organizacji Traktatu Północnoatlantyckiego;
2) prowadzi Narodowy Punkt Kontaktowy zapewniający przekazywanie zadań oraz uruchamianie procedur Organizacji Traktatu Północnoatlantyckiego, w tym uruchamianie przedsięwzięć i procedur systemu zarządzania kryzysowego.

Art. 11c. 1. Szef Centrum zapewnia funkcjonowanie systemu teleinformatycznego wykorzystywanego jako narzędzie wspierające realizację zadań zarządzania kryzysowego, zwanego dalej „systemem".

2. System zapewnia możliwość:

1) zgłaszania informacji o potencjalnych zagrożeniach oraz zaistniałych zagrożeniach;
2) gromadzenie informacji o zagrożeniach oraz analizę tych informacji;
3) gromadzenie informacji o siłach i środkach niezbędnych do realizacji zadań zarządzania kryzysowego;
4) agregowanie i korelowanie pozyskiwanych informacji.

3. Użytkownikami systemu są:

1) ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych podległych ministrom kierującym działami administracji rządowej lub przez nich nadzorowanych;
2) wojewodowie;
3) starostowie.

4. Użytkownikami systemu mogą być wójtowie, burmistrzowie, prezydenci miast.

5. Podmioty, o których mowa w ust. 3 i 4, przekazują do systemu informacje o potencjalnych zagrożenia oraz zaistniałych zagrożeniach niezwłocznie po uzyskaniu takich informacji.

6. Administratorem danych osobowych przetwarzanych w systemie jest Szef Centrum

7. Przetwarzanie danych osobowych zgromadzonych w systemie nie wymaga realizacji obowiązków, o których mowa w art. 12-22 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

8. Dane osobowe zgromadzone w systemie podlegają zabezpieczeniom zapobiegającym nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu i są przechowywane wyłącznie przez okres niezbędny do realizacji zadań.

Art. 11d. 1. Informacje z systemu są udostępniane użytkownikom systemu, o których mowa w art. 11c ust. 3 i 4.

2. Informacje z systemu udostępnia się na wniosek, o ile są one niezbędne do realizacji ich ustawowych zadań, innym podmiotom niż wskazane w art. 11c ust. 3 i 4.

Art. 11e. Rada Ministrów określi, w drodze rozporządzenia:

1) zakres informacji przekazywanych do systemu przez jego użytkowników, oraz sposób i tryb ich wprowadzania;
2) zakres informacji, do których zapewnia się dostęp użytkownikom systemu;
3) sposób i tryb zakładania i obsługi konta użytkowników systemu,
4) wymogi bezpieczeństwa teleinformatycznego, które muszą spełnić podmioty systemu, aby uzyskać dostęp do systemu

- uwzględniając konieczność zapewnienia sprawnego wykonywania zadań zarządzania kryzysowego oraz zapewnienia odpowiedniego poziomu bezpieczeństwa danych zgromadzonych w systemie.";

14) w art. 12:

a) ust. 1 otrzymuje brzmienie:

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

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

3) współpracują z operatorami infrastruktury krytycznej lub podmiotami krytycznymi w zakresie realizacji zadań ochrony infrastruktury krytycznej oraz zapewnienia niezakłóconego świadczenia usług kluczowych;
4) zapewniają funkcjonowania stałego dyżuru w ramach podwyższania gotowości obronnej państwa",

b) uchyla się ust. 2 i 2a,

c) ust. 2c otrzymuje brzmienie:

„2c. Do zadań zespołów, o których mowa w ust. 2b, należy:
1) dokonywanie okresowej oceny ryzyka na potrzeby Krajowej Oceny Ryzyka;
2) dokonywanie okresowej oceny gotowości do reagowania w przypadku wystąpienia sytuacji kryzysowej w zakresie organizacyjnym, technicznym i finansowym;
3) opiniowanie projektów planów zarządzania kryzysowego;
4) opiniowanie wykazu infrastruktury krytycznej w ramach swojej właściwości;
5) wypracowywanie wniosków i propozycji dotyczących zapobiegania i przeciwdziałania zagrożeniom.”;

15) w art. 13 uchyla się ust. 2a;

16) w art. 14 ust. 4 otrzymuje brzmienie:

"4. Minister właściwy do spraw administracji publicznej, w uzgodnieniu z ministrem właściwym do spraw wewnętrznych oraz po zasięgnięciu opinii Szefa Centrum, wydaje, w drodze zarządzenia, wojewodom wytyczne do wojewódzkich planów zarządzania kryzysowego.";

17) art. 20b otrzymuje brzmienie:

"Art. 20b. Ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych, wojewodowie, starostowie, wójtowie (burmistrzowie, prezydenci miast), operatorzy infrastruktury są obowiązani do udzielania Szefowi Centrum, w wyznaczonym terminie, żądanych przez niego informacji i wyjaśnień niezbędnych do realizacji zadań Centrum określonych w ustawie.”;

18) art. 21a otrzymuje brzmienie:

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

2. Operatorzy infrastruktury krytycznej niezwłocznie informują Szefa Centrum oraz właściwe 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 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2024 r. poz. 34, 731 i 834), zwany dalej „operatorem”, jest obowiązany, na żądanie Szefa Centrum, do niezwłocznego, nieodpłatnego wysłania lub wysyłania, komunikatów do wszystkich lub określonych przez Szefa Centrum grup użytkowników końcowych, w szczególności przebywających na określonym przez niego obszarze, jednorazowo lub przez wskazany przez Szefa Centrum okres.

4. Obowiązek, o którym mowa w ust. 3, nie obejmuje wysłania lub wysyłania komunikatu użytkownikom końcowym, których karty SIM są zainstalowane i wykorzystywane w urządzeniach telemetrycznych.

5. Operator po wysłaniu komunikatu niezwłocznie przekazuje Szefowi Centrum informację o liczbie kart SIM użytkowników końcowych, do których komunikat został wysłany i którym komunikat został dostarczony.

6. Rada Ministrów określi, w drodze rozporządzenia, sposób i tryb współpracy Szefa 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.";

19) po art. 25d dodaje się oznaczenie „Rozdział 13 Finansowanie zadań zarządzania kryzysowego";

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

„4a. Środki finansowe z rezerwy celowej, o której mowa w ust. 4, mogą być przeznaczone na realizację przedsięwzięć związanych z zarządzaniem ryzykiem oraz reagowaniem w przypadku wystąpienia sytuacji kryzysowej oraz usuwaniem jej skutków i odtwarzaniem zasobów.”;

21) po art. 31 dodaje się oznaczenie „Rozdział 14 Przepisy dostosowujące, przejściowe i końcowe".

Art. 2. W ustawie z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2021 r. poz. 1995) w art. 5 w ust. 2 pkt 5 otrzymuje brzmienie:

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

Art. 3. W ustawie z dnia 29 listopada 2000 r. - Prawo atomowe (Dz. U. z 2023 r. poz. 1173 i 1890 oraz z 2024 r. poz. 834) w art. 41o pkt 4 otrzymuje brzmienie:

"4) Szef Rządowego Centrum Bezpieczeństwa - w zakresie zarządzania kryzysowego, ochrony infrastruktury krytycznej oraz monitorowania potencjalnych zagrożeń w rozumieniu przepisów ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122 …);".

Art. 4. W ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2024 r. poz. 812) wprowadza się następujące zmiany:

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

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

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

„1. W celu zapobiegania i przeciwdziałania oraz zwalczania zdarzeń o charakterze terrorystycznym dotyczących istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub sieci teleinformatycznych objętych wykazem, o którym mowa w art. 6i ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, a także systemów teleinformatycznych operatorów infrastruktury krytycznej, o których mowa w art. 3 pkt 3a tej ustawy, lub danych przetwarzanych w tych systemach oraz zapobiegania i wykrywania przestępstw o

charakterze terrorystycznym w tym obszarze oraz ścigania ich sprawców ABW może przeprowadzać ocenę bezpieczeństwa tych systemów teleinformatycznych, zwaną dalej „oceną bezpieczeństwa”.”;

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

„1. W celu zapobiegania i przeciwdziałania oraz zwalczania zdarzeń o charakterze terrorystycznym dotyczących istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub sieci teleinformatycznych objętych wykazami, o których mowa w art. art. 6i ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, a także systemów teleinformatycznych operatorów infrastruktury krytycznej, o których mowa w art. 3 pkt 3a tej ustawy, lub danych przetwarzanych w tych systemach oraz zapobiegania i wykrywania przestępstw o charakterze terrorystycznym w tym obszarze oraz ścigania ich sprawców ABW wdraża w tych podmiotach system wczesnego ostrzegania o zagrożeniach występujących w sieci Internet, zwany dalej „systemem ostrzegania”, prowadzi go i koordynuje jego funkcjonowanie.”.

Art. 5. W ustawie z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2024 r. poz. 597) w art. 24 ust. 5 otrzymuje brzmienie:

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

Art. 6. W ustawie z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw aktywów państwowych oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych (Dz. U. z 2020 r. poz. 2173 oraz z 2024 r. poz. 834) wprowadza się następujące zmiany:

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

„1. Ustawa określa szczególne uprawnienia przysługujące ministrowi właściwemu do spraw aktywów państwowych w spółkach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych, których mienie zostało ujawnione w wykazie, o którym mowa w art. 6i ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122 oraz z 2024 r. poz. 834), zwanych dalej „spółkami”.”;

2) w art. 5 ust. 4 otrzymuje brzmienie:

„4. Pełnomocnik do spraw ochrony infrastruktury krytycznej może być koordynatorem do spraw ochrony infrastruktury krytycznej, o którym mowa w art. 6o ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.”;

3) w art. 4 ust.1, art. 5 ust. 1 i ust. 2 pkt 5 i 6, art. 6 ust. 4-6 wyraz "dyrektor" zastępuje się wyrazem "Szef".".

Art. 7. W ustawie z dnia 14 grudnia 2012 r. o odpadach (Dz. U. z 2023 r. poz. 1587, 1597, 1688, 1852 i 2029) w art. 25 w ust. 6i pkt 2 otrzymuje brzmienie:

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

Art. 8. W ustawie z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2024 r. poz. 383) w art. 4 w pkt 8 lit. b otrzymuje brzmienie:

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

Art. 9. W ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913, 1703 oraz z 2024 r. poz. 834) wprowadza się następujące zmiany:

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

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

3) w art. 26:

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

zastępuje się wyrazami ,,operatorów infrastruktury krytycznej, o których mowa w art. 3 pkt 3a”,

b) w ust. 5 pkt 1 otrzymuje brzmienie:

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

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

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

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

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

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

e) w art. 7 w ust. 8 w pkt 11, w art. 15 w ust. 7 w pkt 2, w art. 36 w ust. 3, 6 i 7 pkt 4, w art. 39 w ust. 4, w art. 66 w ust. 4 w pkt 1, w art. 67 w ust. 1 w pkt 4, wyraz "Dyrektor " zastępuje się wyrazem "Szef".

Art. 10. W ustawie z dnia 17 grudnia 2020 r. o rezerwach strategicznych (Dz. U. z 2023 r. poz. 294 oraz z 2024 r. poz. 834) wprowadza się następujące zmiany:

1) w art. 2:

a) pkt 1 otrzymuje brzmienie:

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

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

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

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

2) w art. 8:

a) w ust. 2 pkt 21 otrzymuje brzmienie:

"21) Szefem Rządowego Centrum Bezpieczeństwa;",

b) w ust. 4 pkt 1 i 2 otrzymują brzmienie:

"1) ocenę ryzyka zidentyfikowanych zagrożeń oraz sposobów i środków reagowania na zagrożenia, z uwzględnieniem rozwiązań zawartych w planie zarządzania kryzysowego, o którym mowa w art. 5g ust. 1 ustawy o zarządzaniu kryzysowym;

2) wnioski wynikające z wykonania postanowień Strategii Oporności Podmiotów Krytycznych, o której mowa w art. 5f ustawy o zarządzaniu kryzysowym, w zakresie sprawowania nadzoru nad infrastrukturą krytyczną oraz podmiotami krytycznymi zapewniającymi świadczenie usług kluczowych;";

3) w art. 9 w ust. 1 pkt 1 otrzymuje brzmienie:

„1) wnioski dotyczące tworzenia, utrzymywania i likwidacji rezerw wynikające z oceny ryzyka zidentyfikowanych zagrożeń zawartej w Krajowej Ocenie Ryzyka, o której mowa w art. 5c ustawy o zarządzaniu kryzysowym, oraz wnioski, o których mowa w art. 8 ust. 4 pkt 2;".

Art. 11. W ustawie z dnia 27 stycznia 2023 r. o kontroli niektórych inwestycji (Dz. U. z 2023 r. poz. 415 oraz z 2024 r. poz. 834) w art. 13 w ust. 3 pkt 22 otrzymuje brzmienie:

"22) Szefa Rządowego Centrum Bezpieczeństwa.".

Art. 12. W ustawie z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. poz. 1703) art. 15 otrzymuje brzmienie:

„Art. 15. W zakresie dotyczącym współpracy Szefa Rządowego Centrum Bezpieczeństwa z operatorem ruchomej publicznej sieci telekomunikacyjnej w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne przy realizacji obowiązków określonych w art. 21a ust. 3 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2023 r. poz. 122 oraz …), przepisów art. 10-14 nie stosuje się.”.

Art. 13. 1. Krajową Ocenę Ryzyka, o której mowa w art. 5c ust. 1 ustawy zmienianej w art. 1, Rada Ministrów przyjmuje po raz pierwszy w terminie do dnia 17 stycznia 2026 r.

2. Strategia odporności podmiotów krytycznych, o której mowa w art. 5f ust. 1 ustawy zmienianej w art. 1, Rada Ministrów przyjmuje po raz pierwszy w terminie do dnia 17 stycznia 2026 r.

Art. 14. 1. Krajowy Plan Zarządzania Kryzysowego, o którym mowa w art. 5e ust. 1 ustawy zmienianej w art. 1, Rada Ministrów przyjmuje po raz pierwszy w terminie do dnia 1 września 2026 r. Plany zarządzania kryzysowego, o których mowa w rozdziale 3 ustawy zmienianej w art. 1, sporządza się po raz pierwszy w terminie w terminie 6 miesięcy od dnia przyjęcia Krajowego Planu Zarządzania Kryzysowego, o którym mowa w art. 5e ust. 1 ustawy zmienianej w art. 1. Plany sporządzone po raz pierwszy nie zawierają oceny osiągniętych efektów oraz wniosków z wdrożonych działań, o których mowa w art. 5e ust. 3 pkt 3 lit. e ustawy zmienianej w art. 1.

2. Plany zarządzania kryzysowego sporządzone i zatwierdzone na podstawie ustawy zmienianej w art. 1 w brzmieniu dotychczasowym pozostają w mocy do czasu sporządzenia planów, o których mowa w ust. 1.

Art. 15. Szczegółowe kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi, o których mowa w art. 5b ust. 2 pkt 3 ustawy zmienianej w art. 1 w brzmieniu dotychczasowym, pozostają w mocy do czasu sporządzenia kryteriów, o których mowa w art. 6f ust. 1 ustawy zmienianej w art. 1 ustawy zmienianej w art. 1.

Art. 16. Jednolity wykaz obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy zmienianej w art. 1 w brzmieniu dotychczasowym, pozostaje w mocy do czasu sporządzenia wykazu, o którym mowa w art. 6i ust. 1 ustawy zmienianej w art. 1, i może być w tym czasie aktualizowany.

Art. 17. Właściciele, posiadacze samoistni i zależni obiektów instalacji, urządzeń i usług ujętych w jednolitym wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy zmienianej w art. 1 w brzmieniu dotychczasowym, realizują zadania w zakresie ochrony infrastruktury krytycznej na podstawie art. 6 ustawy zmienianej w art. 1 w brzmieniu dotychczasowym do czasu ujęcia w wykazie infrastruktury krytycznej, o którym mowa w art. 6i ustawy zmienianej w art. 1.

Art. 18. 1. Kryteria, o których mowa w art. 6f ust. 1 ustawy zmienianej w art. 1 zostaną sporządzone po raz pierwszy w terminie do dnia 17 stycznia 2026 r.

2. Wykaz infrastruktury krytycznej, o którym mowa w art. 6i ustawy zmienianej w art. 1, zostanie sporządzony w terminie do dnia 17 stycznia 2026 r.

Art. 19. Przepis art. 26 ust. 4a ustawy zmienianej w art. 1 ma zastosowanie po raz pierwszy do opracowania budżetów jednostek samorządu terytorialnego na 2025 r.

Art. 20. Przepisy wykonawcze wydane na podstawie art. 21a ustawy zmienianej w art. 1 w brzmieniu dotychczasowym zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 21a ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą, jednak nie dłużej niż przez 12 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 21. System teleinformatyczny wykorzystywany jako narzędzie wspierające realizację zadań zarządzania kryzysowego, o którym mowa w art. 11c ustawy zmienianej w art. 1, zostanie wdrożony w terminie 24 miesięcy od dnia wejścia w życie ustawy.

Art. 22. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 20 – gospodarka, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2025 r. – 1 023 301,01 zł;
2) w 2026 r. – 1 098 847,80 zł;
3) w 2027 r. – 1 175 877,03 zł;
4) w 2028 r. – 1 258 306,01 zł;
5) w 2029 r. – 1 346 513,26 zł;
6) w 2030 r. – 1 512 903,84 zł;
7) w 2031 r. – 1 541 911,20 zł;
8) w 2032 r. – 1 649 999,17 zł;
9) w 2033 r. – 1 765 664,11 zł;
10) w 2034 r. – 1 889 437,17 zł.

2. Minister właściwy do spraw gospodarki monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw gospodarki wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności organu do spraw podmiotów krytycznych dla sektora przestrzeni kosmicznej.

Art. 23. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 21 – gospodarka morska, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2025 r. – 511 650,50 zł;
2) w 2026 r. – 549 423,90 zł;
3) w 2027 r. – 587 938,51 zł;
4) w 2028 r. – 629 153,00 zł;
5) w 2029 r. – 673 256,63 zł;
6) w 2030 r. – 756 451,92 zł;
7) w 2031 r. – 770 955,60 zł;
8) w 2032 r. – 824 999,59 zł;
9) w 2033 r. – 882 832,06 zł;
10) w 2034 r. – 944 718,58 zł.

2. Minister właściwy do spraw gospodarki morskiej monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw gospodarki morskiej wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności organu do spraw podmiotów krytycznych podsektora transportu wodnego.

Art. 24. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 22 – gospodarka wodna, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2025 r. – 511 650,50 zł;
2) w 2026 r. – 549 423,90 zł;
3) w 2027 r. – 587 938,51 zł;
4) w 2028 r. – 629 153,00 zł;
5) w 2029 r. – 673 256,63 zł;
6) w 2030 r. – 756 451,92 zł;
7) w 2031 r. – 770 955,60 zł;
8) w 2032 r. – 824 999,59 zł;
9) w 2033 r. – 882 832,06 zł;
10) w 2034 r. – 944 718,58 zł.

2. Minister właściwy do spraw gospodarki wodnej monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu

na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw gospodarki wodnej wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności organu do spraw podmiotów krytycznych dla sektora wody pitnej oraz sektora ścieków.

Art. 25. 1.Maksymalny limit wydatków z budżetu państwa dla części budżetowej 26 – łączność, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2025 r. – 511 650,50 zł;
2) w 2026 r. – 549 423,90 zł;
3) w 2027 r. – 587 938,51 zł;
4) w 2028 r. – 629 153,00 zł;
5) w 2029 r. – 673 256,63 zł;
6) w 2030 r. – 756 451,92 zł;
7) w 2031 r. – 770 955,60 zł;
8) w 2032 r. – 824 999,59 zł;
9) w 2033 r. – 882 832,06 zł;
10) w 2034 r. – 944 718,58 zł.

2. Minister właściwy do spraw łączności monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw łączności wdraża mechanizm korygujący polegający na ograniczeniu finansowania organu do spraw podmiotów krytycznych dla sektora usług pocztowych i kurierskich.

Art. 26. 1.Maksymalny limit wydatków z budżetu państwa dla części budżetowej 27 – informatyzacja, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2025 r. – 511 650,50 zł;
2) w 2026 r. – 549 423,90 zł;
3) w 2027 r. – 587 938,51 zł;
4) w 2028 r. – 629 153,00 zł;
5) w 2029 r. – 673 256,63 zł;
6) w 2030 r. – 756 451,92 zł;

7) w 2031 r. – 770 955,60 zł;
8) w 2032 r. – 824 999,59 zł;
9) w 2033 r. – 882 832,06 zł;
10) w 2034 r. – 944 718,58 zł.

2. Minister właściwy do spraw informatyzacji monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw informatyzacji wdraża mechanizm korygujący polegający na ograniczeniu finansowania organu do spraw podmiotów krytycznych dla sektora infrastruktura cyfrowa oraz sektora zarządzanie usługami ICT.

Art. 27. 1.Maksymalny limit wydatków z budżetu państwa dla części budżetowej 32 – rolnictwo, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2025 r. – 511 650,50 zł;
2) w 2026 r. – 549 423,90 zł;
3) w 2027 r. – 587 938,51 zł;
4) w 2028 r. – 629 153,00 zł;
5) w 2029 r. – 673 256,63 zł;
6) w 2030 r. – 756 451,92 zł;
7) w 2031 r. – 770 955,60 zł;
8) w 2032 r. – 824 999,59 zł;
9) w 2033 r. – 882 832,06 zł;
10) w 2034 r. – 944 718,58 zł.

2. Minister właściwy do spraw rolnictwa monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw rolnictwa wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności organu do spraw podmiotów krytycznych dla sektora produkcji, przetwarzania i dystrybucji żywności.

Art. 28. 1.Maksymalny limit wydatków z budżetu państwa dla części budżetowej 39 – transport, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2025 r. – 511 650,50 zł;
2) w 2026 r. – 549 423,90 zł;
3) w 2027 r. – 587 938,51 zł;
4) w 2028 r. – 629 153,00 zł;
5) w 2029 r. – 673 256,63 zł;
6) w 2030 r. – 756 451,92 zł;
7) w 2031 r. – 770 955,60 zł;
8) w 2032 r. – 824 999,59 zł;
9) w 2033 r. – 882 832,06 zł;
10) w 2034 r. – 944 718,58 zł.

2. Minister właściwy do spraw transportu monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw transportu wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności organu do spraw podmiotów krytycznych dla sektora transportu z wyłączeniem podsektora transportu wodnego.

Art. 29. 1.Maksymalny limit wydatków z budżetu państwa dla części budżetowej 42 – sprawy wewnętrzne, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:
1) w 2025 r. – 37 129 378,64 zł;
2) w 2026 r. – 8 598 301,35 zł;
3) w 2027 r. – 9 048 848,11 zł;
4) w 2028 r. – 9 709 822,52 zł;
5) w 2029 r. – 10 043 328,64 zł;
6) w 2030 r. – 11 781 617,35 zł;
7) w 2031 r. – 11 357 096,55 zł;
8) w 2032 r. – 11 802 342,18 zł;
9) w 2033 r. – 12 470 109,98 zł;
10) w 2034 r. – 13 363 348,05 zł;

2. Minister właściwy do spraw wewnętrznych monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego

na dany rok budżetowy limitu wydatków minister właściwy do spraw wewnętrznych wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności Centrum w zakresie realizacji powierzonych zadań organu do spraw podmiotów krytycznych dla sektora administracja publicznej, prowadzenia Pojedynczego Punktu Kontaktowego oraz prowadzenia systemu teleinformatycznego, o którym mowa w art. 11c. Wdrożenie mechanizmu korygującego następuje w uzgodnieniu z Prezesem Rady Ministrów.

Art. 30. 1.Maksymalny limit wydatków z budżetu państwa dla części budżetowej 46 – zdrowie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2025 r. – 511 650,50 zł;
2) w 2026 r. – 549 423,90 zł;
3) w 2027 r. – 587 938,51 zł;
4) w 2028 r. – 629 153,00 zł;
5) w 2029 r. – 673 256,63 zł;
6) w 2030 r. – 756 451,92 zł;
7) w 2031 r. – 770 955,60 zł;
8) w 2032 r. – 824 999,59 zł;
9) w 2033 r. – 882 832,06 zł;
10) w 2034 r. – 944 718,58 zł.

2. Minister właściwy do spraw zdrowia monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw zdrowia wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności organu do spraw podmiotów krytycznych dla sektora zdrowia oraz sektora produkcji, wytwarzania i dystrybucji chemikaliów i innych produktów przemysłowych.

Art. 31. 1.Maksymalny limit wydatków z budżetu państwa dla części budżetowej 47 – energia, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2025 r. – 511 650,50 zł;
2) w 2026 r. – 549 423,90 zł;
3) w 2027 r. – 587 938,51 zł;
4) w 2028 r. – 629 153,00 zł;
5) w 2029 r. – 673 256,63 zł;

6) w 2030 r. – 756 451,92 zł;
7) w 2031 r. – 770 955,60 zł;
8) w 2032 r. – 824 999,59 zł;
9) w 2033 r. – 882 832,06 zł;
10) w 2034 r. – 944 718,58 zł.

2. Minister właściwy do spraw energii monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw energii wdraża mechanizm korygujący polegający na ograniczeniu finansowania organu do spraw podmiotów krytycznych dla sektora energii.

Art. 32. 1.Maksymalny limit wydatków z budżetu państwa dla części budżetowej 51 – klimat, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:
1) w 2025 r. – 511 650,50 zł;
2) w 2026 r. – 549 423,90 zł;
3) w 2027 r. – 587 938,51 zł;
4) w 2028 r. – 629 153,00 zł;
5) w 2029 r. – 673 256,63 zł;
6) w 2030 r. – 756 451,92 zł;
7) w 2031 r. – 770 955,60 zł;
8) w 2032 r. – 824 999,59 zł;
9) w 2033 r. – 882 832,06 zł;
10) w 2034 r. – 944 718,58 zł.

2. Minister właściwy do spraw klimatu monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw klimatu wdraża mechanizm korygujący polegający na ograniczeniu finansowania organu do spraw podmiotów krytycznych dla sektora gospodarowania odpadami.

Art. 33. 1.Maksymalny limit wydatków z budżetu państwa dla części budżetowej 69 – żegluga śródlądowa, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2025 r. – 511 650,50 zł;
2) w 2026 r. – 549 423,90 zł;
3) w 2027 r. – 587 938,51 zł;
4) w 2028 r. – 629 153,00 zł;
5) w 2029 r. – 673 256,63 zł;
6) w 2030 r. – 756 451,92 zł;
7) w 2031 r. – 770 955,60 zł;
8) w 2032 r. – 824 999,59 zł;
9) w 2033 r. – 882 832,06 zł;
10) w 2034 r. – 944 718,58 zł.

2. Minister właściwy do spraw żeglugi śródlądowej monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw klimatu wdraża mechanizm korygujący polegający na ograniczeniu finansowania organu do spraw podmiotów krytycznych dla podsektora transportu wodnego.

Art. 34. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej:

1) 85/02 – województwo dolnośląskie,
2) 85/04 – województwo kujawsko-pomorskie,
3) 85/06 – województwo lubelskie,
4) 85/08 – województwo lubuskie,
5) 85/10 – województwo łódzkie,
6) 85/12 – województwo małopolskie,
7) 85/14 – województwo mazowieckie,
8) 85/16 – województwo łódzkie,
9) 85/18 – województwo podkarpackie,
10) 85/20 – województwo podlaskie,
11) 85/22 – województwo pomorskie,
12) 85/24 – województwo śląskie,
13) 85/26 – województwo świętokrzyskie,
14) 85/28 – województwo warmińsko-mazurskie,
15) 85/30 – województwo wielkopolskie,

16) 85/32 – województwo zachodniopomorskie

- będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2025 r. – 170 550,17 zł;
2) w 2026 r. – 183 141,30 zł;
3) w 2027 r. – 195 979,50 zł;
4) w 2028 r. – 209 717,67 zł;
5) w 2029 r. – 224 418,88 zł;
6) w 2030 r. – 252 150,64 zł;
7) w 2031 r. – 256 985,20 zł;
8) w 2032 r. – 274 999,86 zł;
9) w 2033 r. – 294 277,35 zł;
10) w 2034 r. – 314 906,19 zł.

2. Właściwy wojewoda monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków właściwy wojewoda wdraża mechanizm korygujący polegający na ograniczeniu finansowania realizacji zadań w zakresie identyfikacji infrastruktury krytycznej na terenie województwa.

Art. 35. Ustawa wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Załączniki do ustawy z dnia … (Dz. U. poz. …)

Załącznik nr 1

Podmioty kluczowe

I	II	III
Sektor	Podsektor	Rodzaj 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 (Dz. U. z 2023 r. poz. 633, 1688 i 2029).
		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 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.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne świadczący usługę o której mowa w art. 3 pkt. 6f tej ustawy.
		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, prowadzące działalność gospodarczą w zakresie przetwarzania albo magazynowania energii elektrycznej.
		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.
	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.
		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.
	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 (Dz. U. z 2023 r. poz. 294)
	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	Operatorzy instalacji służących do produkcji wodoru.
		Operatorzy instalacji służących do magazynowania wodoru.
		Operatorzy instalacji służących do przesyłu wodoru.
		Operatorzy instalacji służących do dystrybucji wodoru.
	Energetyka jądrowa	Państwowe przedsiębiorstwo użyteczności publicznej, o którym mowa w art. 114 ust. 1 ustawy z dnia 29 listopada 2000 r. Prawo atomowe.
		Operator składowiska odpadów promieniotwórczych, posiadający zezwolenie na eksploatację, o którym mowa w art. 4 ust. 1 pkt 3 ustawy z dnia 29 listopada 2000 r. Prawo atomowe
		Operator elektrowni jądrowej, posiadający zezwolenie na eksploatację, o którym mowa art. 4 ust. 1 pkt 2 ustawy z dnia 29 listopada 2000 r. -Prawo atomowe lub koncesję na wytwarzanie energii elektrycznej lub ciepła, o których mowa art. 32 ust. 1 pkt 1 ustawy z dnia 10 kwietnia 1997 r. - Prawo energetyczne
		Podmiot będący operatorem zakładu wydobywania rud uranu i toru ze złóż i do ich

		wstępnego przetwarzania, posiadający zezwolenie, o którym mowa art. 4 ust. 1 pkt 2 ustawy z dnia 29 listopada 2000 r. Prawo atomowe lub koncesję na wydobywanie kopalin, o której stanowi art. 22 ust. 1 pkt 2 ustawy z dnia 9 czerwca 2011 r. Prawo geologiczne i górnicze
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 (Dz. Urz. UE L 97 z 09.04.2008, str. 72).
		Zarządzający lotniskiem, o którym mowa w art. 2 pkt 7 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze (Dz. U. z 2023 r. poz. 2110).
		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 dla przewoźników lotniczych 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 (Dz. U. z 2023 r. poz. 1786, 1720 i 2029), 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, 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 (Dz. Urz. UE L 129 z 29.04.2004, str. 6), 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 (Dz. U. z 2024 r. poz. 395).

		Podmiot zarządzający portem, o którym mowa w art. 2 pkt 6 ustawy z dnia 20 grudnia 1996 r. o portach i przystaniach morskich (Dz. U. z 2023 r. poz. 1796).
		Podmiot zarządzający obiektem portowym, o którym mowa w art. 2 pkt 11 rozporządzenia (WE) 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 (Dz. U. z 2023 r. poz. 1666 i 2005).
	Transport drogowy	Organy, o których mowa w art. 19 ust. 2, 5 i 5a ustawy z dnia 21 marca 1985 r. o drogach publicznych (Dz. U. z 2024 r. poz. 320).
		Podmioty, o których mowa w art. 43a ust. 1 ustawy z dnia 21 marca 1985 r. o drogach publicznych.
Bankowość i infrastruktura rynków finansowych		Instytucja kredytowa, o której mowa w art. 4 ust. 1 pkt 17 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2023 r. poz. 2488).
		Bank krajowy, o którym mowa w art. 4 ust. 1

		pkt 1 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe.
		Oddział banku zagranicznego, o którym mowa w art. 4 ust. 1 pkt 20 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe.
		Oddział instytucji kredytowej, o którym mowa w art. 4 ust. 1 pkt 18 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 (Dz. U. z 2023 r. poz. 646, 825, 1723 i 1941).
		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.
Zdrowie		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.
		Podmioty prowadzące działalność badawczo-

		rozwojową w zakresie produktów leczniczych zdefiniowanych w art. 1 pkt 2 dyrektywy Parlamentu Europejskiego i Rady 2001/83/WE.
		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.
		Jednostka podległa ministrowi właściwemu do spraw zdrowia albo przez niego nadzorowana, właściwa w zakresie systemów informacyjnych ochrony zdrowia.
		Narodowy Fundusz Zdrowia.
		Przedsiębiorca prowadzący działalność polegającą na prowadzeniu hurtowni farmaceutycznej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne (Dz. U. z 2022 r. poz. 2301, 605, 650, 1859 i 1938).
		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.
		Importer produktu leczniczego/substancji czynnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.
		Wytwórca produktu leczniczego/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.
		Dystrybutor substancji czynnej 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.
Woda pitna		Podmiot dostarczający wodę przeznaczoną do spożycia przez ludzi, w tym przedsiębiorstwo wodociągowo-kanalizacyjne oraz podmiot prowadzący hurtową sprzedaż wody, z wyłączeniem podmiotów, dla których dostarczanie wody przeznaczonej do spożycia przez ludzi jest inną niż istotną częścią ich ogólnej działalności.
Ścieki		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.
Infrastruktura	Infrastruktura cyfrowa	Dostawca punktu wymiany ruchu

cyfrowa	z wyłączeniem komunikacji elektronicznej	internetowego.
		Dostawca usług DNS, z wyłączeniem operatorów głównych serwerów nazw.
		Rejestr nazw domen najwyższego poziomu (TLD).
		Dostawca usług chmurowej.
		Dostawca usług ośrodka przetwarzania danych.
		Dostawca sieci dostarczania treści.
		Dostawca usług zaufania.
		Krajowa Izba Rozliczeniowa S.A.
		Podmiot świadczący usługę rejestracji nazw domen.
	Komunikacja elektroniczna	Przedsiębiorca telekomunikacyjny.
		Podmiot świadczący usługę komunikacji interpersonalnej niewykorzystującej numerów.
Administracja publiczna		Kancelaria Prezesa Rady Ministrów
		Ministerstwa obsługujące ministrów kierujących działami administracji rządowej
		Urzędy podległe Prezesowi Rady Ministrów lub przez niego nadzorowane
		Urzędy podległe ministrowi kierującemu działem administracji rządowej lub przez niego nadzorowane
		Urzędy wojewódzkie
Przestrzeń kosmiczna		Operator infrastruktury naziemnej, który wspiera świadczenie usług kosmicznych, z wyjątkiem przedsiębiorców komunikacji elektronicznej.
Produkcja, przetwarzanie i dystrybucja		Przedsiębiorstwa spożywcze w rozumieniu art. 3 pkt 2 rozporządzenia (WE) nr 178/2002 Parlamentu Europejskiego i Rady, zajmujące

żywności		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.
		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.
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 (Dz. U. z 2023 r. poz.1587, 1597, 1688, 1852 i 2029), polegające na zbieraniu odpadów, zobowiązane do uzyskania wpisu w rejestrze, o którym mowa w art. 49 ust. 1 ustawy o odpadach, z wyłączeniem przedsiębiorstw, dla których usługi te nie stanowią podstawowej działalności gospodarczej określonej zgodnie z przepisami wydanymi na podstawie art. 40 ust. 2 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 o odpadach, z wyłączeniem przedsiębiorstw, dla których usługi te nie stanowią podstawowej działalności gospodarczej określonej zgodnie z przepisami wydanymi na podstawie art. 40 ust. 2 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej.
	Przetwarzanie odpadów, w tym sortowanie, 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 w tym sortowaniu, 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. 2 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej.
	Działania wykonywane w charakterze sprzedawcy odpadów lub pośrednika w	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,

	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. 2 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej.