

<p><b>Nazwa projektu</b></p> <p>Rozporządzenie Rady Ministrów w sprawie minimalnych wymagań w zakresie bezpieczeństwa fizycznego, technicznego, osobowego, cyberbezpieczeństwa, prawnego oraz ciągłości działania infrastruktury krytycznej</p> <p><b>Ministerstwo wiodące i ministerstwa współpracujące</b></p> <p>Dyrektor Rządowego Centrum Bezpieczeństwa</p> <p><b>Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu</b></p> <p>Zbigniew Muszyński, Dyrektor Rządowego Centrum Bezpieczeństwa</p> <p><b>Kontakt do opiekuna merytorycznego projektu</b></p> <p>Jarosław Pudzianowski, Szef Wydziału Ochrony Infrastruktury Krytycznej tel. 727-666-108, e-mail: <a href="mailto:jaroslaw.pudzianowski@rcb.gov.pl">jaroslaw.pudzianowski@rcb.gov.pl</a></p> <p>Dorota Duda, główny specjalista Wydziału Ochrony Infrastruktury Krytycznej, tel. 887 401 517, e-mail: <a href="mailto:dorota.duda@rcb.gov.pl">dorota.duda@rcb.gov.pl</a></p>	<p><b>Data sporządzenia</b></p> <p><b>28.05.2026 r.</b></p> <p><b>Źródło:</b></p> <p><b>Upoważnienie Prezesa Rady Ministrów</b></p> <p>Art. 6ze ust. 4 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (upoważnienie w wersji zawartej w ustawie z dnia 15 maja 2026 r. o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw (Druk Sejmowy nr 2355)).</p> <p><b>Nr w wykazie prac</b></p> <p>RD301</p>
---	---

## OCENA SKUTKÓW REGULACJI

### 1. Jaki problem jest rozwiązywany?

Celem projektowanej regulacji jest wprowadzenie jednolitych, minimalnych, wymagań dla operatorów infrastruktury krytycznej w sześciu obszarach bezpieczeństwa, tj. fizycznym, technicznym, osobowym, cyberbezpieczeństwa, prawnym oraz ciągłości działania.

Dotychczasowe podejście oparte na zaleceniach i dobrych praktykach (vide załącznik 1 do NPOIK *Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje*) nie zapewniało dostatecznego przełożenia na praktykę zamówień, inwestycji i utrzymania środków ochrony, co skutkowało zróżnicowaniem standardów, rozbieżnościami interpretacyjnymi oraz utrzymywaniem się luk bezpieczeństwa w obszarach wymagających zintegrowanego podejścia.

Problem ma wymiar praktyczny – operatorzy infrastruktury krytycznej są zobowiązani do prowadzenia analizy zagrożeń i wdrażania adekwatnych rozwiązań, lecz bez minimalnego standardu wykonawczego trudniej jest zapewnić porównywalność, kontrolowalność i skuteczność wdrażanych środków oraz ograniczać ryzyko zakłóceń o skutkach kaskadowych.

### 2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Rekomendowanym rozwiązaniem jest wydanie rozporządzenia określającego minimalne wymagania w sześciu obszarach bezpieczeństwa infrastruktury krytycznej o charakterze funkcjonalnym, wdrażane adekwatnie do wyników analizy zagrożeń.

Oczekiwany efekt to:

- ✓ ujednoczenie minimalnego poziomu zabezpieczeń infrastruktury krytycznej;
- ✓ ułatwienie określania warunków zamówień na usługi i środki techniczne niezbędne do ochrony infrastruktury krytycznej poprzez wprowadzenie jednolitego, minimalnego i weryfikowalnego punktu odniesienia dla specyfikacji zamówień, kryteriów oceny ofert oraz odbioru i rozliczenia dostaw warunków zamówień;
- ✓ zmniejszenie problemów organizacyjnych, prawnych i finansowych w procesach inwestycyjnych dla operatorów infrastruktury krytycznej w zakresie ww. sześciu obszarów bezpieczeństwa infrastruktury krytycznej;
- ✓ ograniczenie ryzyka przyjmowania rozwiązań niespełniających wymaganego poziomu zabezpieczenia (m.in. przez mechanizmy testowania/odbioru/certyfikacji systemów);
- ✓ poprawa zdolności do reagowania na incydenty i utrzymania ciągłości działania;
- ✓ zwiększenie efektywności nadzoru i kontroli nad operatorami infrastruktury krytycznej.

### 3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

-----



pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
<b>Wydatki ogółem</b>	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
<b>Saldo ogółem</b>	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0

Źródła finansowania	Rozporządzenie nie wpływa na sektor finansów publicznych, w tym na budżet państwa oraz budżetów jednostek samorządu terytorialnego.											
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Nie dotyczy											

**7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe**

		Skutki						
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	Łącznie (0-10)
W ujęciu pieniężnym (w mln zł, ceny stałe z ..... r.)	duże przedsiębiorstwa							
	sektor mikro-, małych i średnich przedsiębiorstw							
	rodzina, obywatele oraz gospodarstwa domowe (dodaj/usuń)							
W ujęciu niepieniężnym	duże przedsiębiorstwa	Regulacja będzie miała korzystny wpływ poprzez zwiększenie przejrzystości wymagań inwestycyjnych i zakupowych, ustanowienie minimalnego, jednoznacznego standardu odniesienia dla planowania i realizacji inwestycji w środki ochrony infrastruktury krytycznej oraz ograniczenie ryzyka nabywania rozwiązań niespełniających wymaganego poziomu zabezpieczenia. Ujednoczenie minimalnych wymagań sprzyja optymalizacji procesów inwestycyjnych, ograniczeniu ryzyka niewłaściwego gospodarowania środkami finansowymi oraz zwiększeniu przewidywalności i efektywności zarządzania bezpieczeństwem.						
	sektor mikro-, małych i średnich przedsiębiorstw	Regulacja będzie miała korzystny wpływ poprzez zwiększenie przejrzystości wymagań inwestycyjnych i zakupowych, ustanowienie minimalnego, jednoznacznego standardu odniesienia dla planowania i realizacji inwestycji w środki ochrony infrastruktury krytycznej oraz ograniczenie ryzyka nabywania rozwiązań niespełniających wymaganego poziomu zabezpieczenia. Ujednoczenie minimalnych wymagań sprzyja optymalizacji procesów inwestycyjnych, ograniczeniu ryzyka niewłaściwego gospodarowania środkami finansowymi oraz zwiększeniu przewidywalności i efektywności zarządzania bezpieczeństwem.						
	rodzina, obywatele oraz gospodarstwa domowe	Wpływ ma charakter pośredni i przejawia się w ograniczeniu ryzyka zakłóceń w świadczeniu usług kluczowych, w tym usług energetycznych, transportowych, telekomunikacyjnych czy wodno-kanalizacyjnych, co przekłada się na zwiększenie komfortu życia obywateli.						
	Osoby starsze i niepełnosprawne	Wpływ ma charakter pośredni i przejawia się w ograniczeniu ryzyka zakłóceń w świadczeniu usług kluczowych, w tym usług energetycznych, transportowych, telekomunikacyjnych czy wodno-kanalizacyjnych, co przekłada się na zwiększenie komfortu życia obywateli.						

Niemierzalne	(dodaj/usuń)	
	(dodaj/usuń)	
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	<p>Oszacowanie kosztów przedsiębiorców w zakresie dostosowania się do nowych regulacji nie jest możliwe. Środki techniczne i organizacyjne wdrażane przez przedsiębiorców będą uzależnione od analizy zagrożeń oraz obecnego stanu zabezpieczeń ochrony infrastruktury krytycznej.</p> <p>Obecnie wielu przedsiębiorców, będących właścicielami lub posiadaczami infrastruktury krytycznej wdraża systemy zarządzania bezpieczeństwem lub ciągłością działania zgodnie z obowiązującymi w tym zakresie normami lub posiada certyfikację zgodności z tymi normami. Wskazanie minimalnych wymagań w zakresie wdrażania rozwiązań zapewniających ochronę infrastruktury krytycznej jest konieczne i niezbędne dla osiągnięcia celów ustawy – należy uznać, iż została tu zachowana zasada proporcjonalności.</p>	

### 8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

X nie dotyczy	
Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	<input type="checkbox"/> tak <input type="checkbox"/> nie <input type="checkbox"/> nie dotyczy
<input type="checkbox"/> zmniejszenie liczby dokumentów <input type="checkbox"/> zmniejszenie liczby procedur <input type="checkbox"/> skrócenie czasu na załatwienie sprawy <input type="checkbox"/> inne:	<input type="checkbox"/> zwiększenie liczby dokumentów <input type="checkbox"/> zwiększenie liczby procedur <input type="checkbox"/> wydłużenie czasu na załatwienie sprawy <input type="checkbox"/> inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	<input type="checkbox"/> tak <input type="checkbox"/> nie <input type="checkbox"/> nie dotyczy

Komentarz:

-----

### 9. Wpływ na rynek pracy

Oczekiwany jest umiarkowany wzrost zapotrzebowania na specjalistów posiadających kompetencje w obszarach bezpieczeństwa fizycznego i systemów zabezpieczeń technicznych, cyberbezpieczeństwa (w tym IT i OT) oraz zarządzania ciągłością działania. Wzrost ten będzie dotyczył w szczególności realizacji działań związanych z projektowaniem, wdrażaniem, audytem, certyfikacją oraz szkoleniem personelu w zakresie minimalnych wymagań. Efekt będzie miał charakter rozłożony w czasie i związany zarówno z etapem dostosowawczym po wejściu w życie regulacji, jak i z późniejszym utrzymaniem oraz doskonaleniem przyjętych rozwiązań.

### 10. Wpływ na pozostałe obszary

<input type="checkbox"/> środowisko naturalne <input type="checkbox"/> sytuacja i rozwój regionalny <input type="checkbox"/> sądy powszechne, administracyjne lub wojskowe	<input type="checkbox"/> demografia <input type="checkbox"/> mienie państwowe <input type="checkbox"/> inne:	<input type="checkbox"/> informatyzacja <input type="checkbox"/> zdrowie
Omówienie wpływu	Brak wpływu.	

### 11. Planowane wykonanie przepisów aktu prawnego

Wykonanie przepisów rozporządzenia nastąpi po dniu jego wejściu w życie.

### 12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

Dyrektor Rządowego Centrum Bezpieczeństwa będzie przedkładał Radzie Ministrów coroczne sprawozdania z realizacji dokumentu strategicznego jakim będzie Krajowa Strategia Odporności Podmiotów Krytycznych. W sprawozdaniu znajdą się m.in. aspekty związane ze „skutecznością” uwzględniania minimalnych wymagań przy wdrażaniu przez operatorów rozwiązań w zakresie bezpieczeństwa infrastruktury krytycznej.

**13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)**

Nie dotyczy.