Projekt z dnia 15 czerwca 2018 r.

R O Z P O R Z Ą D Z E N I E

R A D Y M I N I S T R Ó W

z dnia ……..... 2018 r.

w sprawie dokumentacji cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych

Na podstawie art. 10 ust. 5 ustawy z dnia …… 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. …….) zarządza się, co następuje:

§ 1. Rozporządzenie określa rodzaje dokumentacji dotyczącej cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych.

§ 2. W skład dokumentacji dotyczącej cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usługi kluczowej wchodzą:

1) dokumentacja normatywna;
2) dokumentacja operacyjna.

§ 3. W skład dokumentacji, o której mowa w § 2 pkt 1 wchodzi w szczególności:

1) dokumentacja systemu zarządzania bezpieczeństwem informacji wytworzona zgodnie z wymaganiami normy PN ISO/IEC 27001;
2) plan ochrony infrastruktury, z wykorzystaniem której świadczona jest usługa kluczowa;
3) plan zapewnienia ciągłości działania usługi kluczowej wytworzony zgodnie z wymaganiami normy PN-EN ISO 22301;
4) dokumentacja techniczna systemu teleinformatycznego wykorzystywanego do świadczenia usługi kluczowej;
5) inna dokumentacja, której potrzeba istnienia wynika ze specyfiki świadczonej usługi kluczowej.

§ 4. 1. Plan ochrony, o którym mowa w § 3 pkt 2 zawiera w szczególności:

1) charakterystykę wykorzystywanych obiektów infrastruktury;
2) analizę stopnia zagrożenia dla wykorzystywanych obiektów infrastruktury;
3) ocenę aktualnego stanu ochrony;
4) opis zabezpieczeń technicznych obiektu;
5) zasady organizacji i wykonywania ochrony fizycznej;

6) dane dotyczące specjalistycznej uzbrojonej formacji ochronnej, jeśli występuje.

2. W przypadku gdy obiekt podlega obowiązkowej ochronie zastosowanie mają przepisy ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2017 r. poz. 2213 oraz z 2018 r. poz. 138).

§ 5. 1. W skład dokumentacji, o której mowa w § 2 pkt 2 wchodzą w szczególności:

1) procedury oraz instrukcje wynikające z dokumentacji normatywnej;
2) wzory zapisów dokumentujących wykonanie procedury;
3) zapisy dokumentujące każdorazowe wykonanie procedury.

2. Zapisy, o których mowa w ust. 1 pkt. 3, mogą być tworzone zarówno w postaci papierowej, jak i w postaci elektronicznej.

§ 6. Rozporządzenie wchodzi w życie z dniem wchodzi w życie z dniem …… 2018 r.

PREZES RADY MINISTRÓW

ZA ZGODNOŚĆ POD WZGLĘDEM PRAWNYM,
REDAKCYJNYM I LEGISLACYJNYM
Katarzyna Prusak-Górniak
Dyrektor Departamentu Prawnego
w Ministerstwie Cyfryzacji
/- podpisano elektronicznie/

UZASADNIENIE

Projekt rozporządzenia Rady Ministrów w sprawie dokumentacji cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych stanowi wykonanie upoważnienia ustawowego, zawartego w art. 10 ust. 5 ustawy o krajowym systemie cyberbezpieczeństwa, zwanej dalej „ustawą”.

Celem projektowanych przepisów jest określenie wymagań dla dokumentacji technicznej, opisującej zasady oraz metody zapewniania cyberbezpieczeństwa systemów informacyjnych wykorzystywanych dla realizacji usług kluczowych, zaś ich adresatami są przedsiębiorcy oraz podmioty publiczne w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570), będący operatorami usług kluczowych w rozumieniu ustawy.

W ślad za praktyką stosowaną w zarządzaniu dokumentacja określona w projekcie dzieli się na dwie podstawowe klasy: dokumentację normatywną i dokumentację operacyjną. Dokumentację normatywną stanowią przepisy prawa powszechnego oraz wewnętrzne akty normatywne wydawane na przykład w postaci zarządzeń i decyzji przez kierownictwo danego podmiotu. Drugą z klas dokumentacji jest dokumentacja operacyjna, sporządzana w ramach prowadzenia bieżącej działalności danego podmiotu, a w szczególności dokumentacja w postaci zapisów z wykonanych czynności, stanowiąca ślad audytowy, na podstawie którego można stwierdzić prawidłowość wykonywania nałożonych obowiązków. Podział taki został uwzględniony w treści projektowanego § 2.

W § 3 wskazany został minimalny zakres dokumentacji normatywnej, która musi być prowadzona przez operatora usługi kluczowej. Zakres tej dokumentacji mieści się w ramach dokumentacji, którą musi prowadzić operator infrastruktury krytycznej w rozumieniu przepisów ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2017 r. poz. 209 oraz z 2018 r. poz. 1566). Oznacza to, że operator usługi kluczowej, który jest jednocześnie operatorem infrastruktury krytycznej, nie musi tworzyć odrębnej dokumentacji na podstawie projektowanego rozporządzenia. Mając na uwadze cel prowadzenia dokumentacji normatywnej na podkreślenie zasługuje konieczność prowadzenia dokumentacji związanej z systemem zarządzania bezpieczeństwem informacji oraz zarządzaniem ciągłością działania zgodnie z powszechnie stosowanymi w tym zakresie Polskimi Normami.

W § 4 wskazany został minimalny zakres informacji, które powinien zawierać plan ochrony infrastruktury operatora usługi kluczowej. Zakres ten jest tożsamy z zakresem informacji dotyczącym planów ochrony obiektów podlegających obowiązkowej ochronie, o którym mowa w art. 7 ust. 2 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2017 r. poz. 2213 oraz z 2018 r. poz. 138).

W § 5 wyszczególniony został minimalny zakres dokumentacji operacyjnej. Szczególne znaczenie mają zapisy stanowiące ślad audytowy, które pozwalają audytorom i kontrolerom na stwierdzenie poprawności funkcjonowania podmiotu w zakresie zapewniania cyberbezpieczeństwa co do realizacji usługi kluczowej.

Przewiduje się, że dokumenty poświadczające każdorazowe wykonanie procedury mogą być prowadzone w postaci papierowej lub elektronicznej, zależnie od okoliczności. Ustanawia się obowiązek sprawowania nadzoru nad dokumentacją przez operatora i definiuje minimalny zakres czynności nadzorczych.

Mając na uwadze treść przepisu art. 19 ust. 1 dyrektywy Parlamentu Europejskiego i Rady (UE) nr 2016/1148 z dnia 6 lipca 2016 r. (Dz. Urz. UE L 194 z 19.7.2016 s. 1), zgodnie z którym, w celu zapewnienia spójnego wdrażania poszczególnych przepisów dyrektywy dopuszczalnym jest odwoływanie się do stosowania europejskich lub uznanych międzynarodowo norm i specyfikacji mających znaczenie dla bezpieczeństwa sieci i systemów informatycznych, wobec czego zamieszczono w przepisach projektu wskazania odpowiednich norm, co powinno przyczynić się do bardziej precyzyjnego określenia wymogów dokumentacji, jakie mają spełnić operatorzy usług kluczowych.

Rozporządzenie wejdzie w życie z dniem …….. 2018 r.

Projekt rozporządzenia nie jest sprzeczny z prawem Unii Europejskiej.

Projektowana regulacja nie zawiera przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597) i nie podlega notyfikacji Komisji Europejskiej.

Wejście w życie rozporządzenia nie będzie miało wpływu na działalność mikroprzedsiębiorców, małych i średnich przedsiębiorców.

Projekt nie wymaga przedłożenia instytucjom i organom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Projekt został udostępniony na stronie Rządowego Centrum Legislacji w serwisie „Rządowy Proces Legislacyjny” oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Cyfryzacji, zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248).

Nazwa projektu Projekt rozporządzenia Ministra Cyfryzacji w sprawie dokumentacji cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Karol Okoński, Podsekretarz Stanu w Ministerstwie Cyfryzacji **Kontakt do opiekuna merytorycznego projektu** Jakub Dysarz, Departament Cyberbezpieczeństwa, tel. (22) 245 58 38, e-mail:jakub.dysarz@mc.gov.pl	**Data sporządzenia** 15 czerwca 2018 r. **Źródło:** Upoważnienie ustawowe - art. 10 ust. 5 ustawy z dnia .... o krajowym systemie cyberbezpieczeństwa (Dz. U. ….) **Nr w wykazie prac RM:** **RD387**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Zgodnie z art. 10 ustawy o krajowym systemie cyberbezpieczeństwa na operatorach usług kluczowych spoczywają obowiązki opracowania, stosowania i aktualizacji dokumentacji dotyczącej cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych oraz ustanowienia nadzoru nad tą dokumentacją.
Przepis zawiera wyłączenie w zakresie realizacji tego obowiązku przez właścicieli, posiadaczy samoistnych lub zależnych obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej ujętych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy o zarządzaniu kryzysowym, którzy realizują obowiązki tego typu na podstawie tej ustawy. Rozwiązanie powyższe ogranicza tym samym obowiązki tworzenia podwójnej dokumentacji tj. związanej z zarządzaniem kryzysowym i dotyczącej cyberbezpieczeństwa, o ile dany operator usług kluczowych, o którym mowa w przepisach o zarządzaniu kryzysowym posiada zatwierdzony plan ochrony infrastruktury krytycznej, uwzględniający dokumentację dotyczącą cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych.

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

Wydanie rozporządzenia określającego rodzaje i minimalną zawartość dokumentacji, potrzebnej dla zapewnienia odpowiedniego poziomu bezpieczeństwa systemów.
Wybrano podział na dokumentację normatywną (zawierającą między innymi dokumentację SZBI, plan ochrony, dokumentację techniczną) i dokumentację operacyjną (zawierającą procedury oraz instrukcje wynikające z dokumentacji normatywnej, wzory zapisów dokumentujących wykonanie procedury jak i same zapisy dokumentujące wykonanie procedury).
Projekt dopuszcza tworzenie zapisów w formie elektronicznej jak i papierowej, oraz uwzględnia istniejące regulacje z ustawy o ochronie osób i mienia.

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

Nie dotyczy.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Podmioty świadczące usługi kluczowe w sektorze energii w podsektorze	24	Szacunki oparte na załączniku do projektu ustawy oraz danych URE (trzy podmioty	Przygotowanie dokumentacji zgodnie z wymogami ustanowionymi

wydobywania kopalin		prowadzące kopalnie węgla brunatnego, dwadzieścia podmiotów prowadzących kopalnie węgla kamiennego, jeden podmiot prowadzący kopalnię miedzi)	przepisami rozporządzenia
Podmioty świadczące usługi kluczowe w sektorze energii w podsektorze energii elektrycznej	30	Szacunki oparte na załączniku do projektu ustawy oraz danych URE (pięć największych podmiotów wytwarzających prąd, OSP, pięciu największych OSD dla gospodarstw domowych, dziewięciu największych OSD dla przedsiębiorców, pięciu największych sprzedawców prądu)	
Podmioty świadczące usługi kluczowe w sektorze energii w podsektorze ciepła	3	Szacunki oparte na załączniku do projektu ustawy oraz danych URE (trzy podmioty prowadzące elektrociepłownie, nieobjęte podsektorem energia elektryczna)	
Podmioty świadczące usługi kluczowe w sektorze energii w podsektorze ropy naftowej	4	Szacunki oparte na załączniku do projektu ustawy oraz danych URE (OSP oraz czterej najwięksi przedsiębiorcy posiadający koncesję na dystrybucję, wytwarzanie, magazynowanie lub przeładunek paliw ciekłych oraz na obrót paliwami ciekłymi)	
Podmioty świadczące usługi kluczowe w sektorze energii w podsektorze gazu	22	Szacunki oparte na załączniku do projektu ustawy oraz danych URE (OSP, OSD, przedsiębiorcy dostarczający lub magazynujący gaz lub gaz ziemny oraz dziesięć największych	

		przedsiębiorstw gazowych w rozumieniu art. 2 pkt 1 dyrektywy 2009/73/WE)	
Podmioty świadczące usługi kluczowe w sektorze energii w zakresie dostaw i usług dla sektora energii oraz jednostki nadzorowane i podległe ministrowi właściwemu do spraw energii oraz ministrowi właściwemu do spraw gospodarki złożami kopalin	15	Dane za BIP Ministra Energii: dwanaście instytutów badawczych, Zakład Unieszkodliwiania Odpadów Promieniotwórczych, Agencja Rezerw Materiałowych i Prezes Wyższego Urzędu Górniczego	
Podmioty świadczące usługi kluczowe w sektorze transportu w podsektorze transportu lotniczego	28	Szacunki oparte na załączniku do projektu ustawy oraz danych ULC (czterech przewoźników lotniczych, zarządzający ośmioma największymi portami lotniczymi, piętnaście podmiotów obsługujących urządzenia pomocnicze znajdujące się w portach lotniczych oraz służba kontroli ruchu lotniczego)	
Podmioty świadczące usługi kluczowe w sektorze transportu w podsektorze transportu kolejowego	10	Szacunki oparte na załączniku do projektu ustawy oraz danych UTK (trzech największych zarządców infrastruktury kolejowej, czterech największych przewoźników kolejowych osobowych oraz trzech największych przewoźników kolejowych towarowych).	
Podmioty świadczące usługi kluczowe w sektorze transportu w podsektorze transportu wodnego (dotyczącym	21	Szacunki oparte na załączniku do projektu ustawy oraz danych MGMiŻŚ (założono objęcie dziesięciu	

transportu morskiego)		największych armatorów, ośmiu portów morskich oraz trzech operatorów VTS)	
Podmioty świadczące usługi kluczowe w sektorze transportu w podsektorze transportu wodnego (dotyczącym transportu śródlądowego)	0	Informacje z MGMiŻŚ.	
Podmioty świadczące usługi kluczowe w sektorze transportu w podsektorze transportu drogowego	24	Szacunki oparte na załączniku do projektu ustawy oraz danych MI (jeden zarządca dróg krajowych, szesnastu zarządców dróg wojewódzkich, dwóch operatorów systemów ITS na poziomie krajowym i pięciu w miastach). Jest możliwe poszerzenie tej grupy o zarządców dróg powiatowych i gminnych, jednak nie były brane pod uwagę w szacunkach.	
Podmioty świadczące usługi kluczowe w sektorze bankowości i infrastruktury rynków finansowych	67	Szacunki oparte na załączniku do projektu ustawy oraz danych KNF (dwadzieścia największych banków, dziesięć największych banków spółdzielczych, dziesięć największych SKOK, dziesięć największych krajowych zakładów ubezpieczeń, dziesięć największych instytucji płatniczych, dwa banki państwowe, jedna giełda, PWPW, dwaj operatorzy systemu obrotu i jeden kontrahent centralny).	
Podmioty świadczące usługi kluczowe w sektorze zaopatrzenia w wodę pitną i jej dystrybucję	31	Przedsiębiorstwa wodno-kanalizacyjne, z danych RCB dot. infrastruktury krytycznej.	

Podmioty świadczące usługi kluczowe w sektorze ochrony zdrowia	253	Szacunki oparte na danych z rejestrów Głównego Inspektora Farmaceutycznego, CSIOZ i MZ. Wyjaśnienie: Na potrzeby szacunków poczyniono następujące założenia. Uznano, że operatorami usług kluczowych będą podmioty lecznicze (podmioty realizujące świadczenia szpitalne), które miały więcej niż 18 000 hospitalizacji rocznie. Odpowiednio dla województw jest to: Dolnośląskie – 12 Kujawsko-Pomorskie – 8 Lubelskie – 8 Lubuskie – 3 Łódzkie – 8 Małopolskie – 10 Mazowieckie – 18 Opolskie – 3 Podkarpackie – 8 Podlaskie – 8 Pomorskie – 5 Śląskie – 15 Świętokrzyskie – 5 Warmińsko-mazurskie – 3 Wielkopolskie – 12 Zachodniopomorskie – 5. Pozostałe podmioty, które spełniały wymogi z załącznika, to NFZ, CSIOZ, pięćdziesięciu największych podmiotów prowadzących hurtownie farmaceutyczne, pięćdziesiąt największych podmiotów prowadzących największe apteki oraz dwudziestu	

		największych wytwórców, importerów lub dystrybutorów substancji czynnych. Uszczegółowienie powyższych danych, w tym doprecyzowanie informacji w zakresie faktycznej liczby podmiotów objętych niniejszą regulacją zostanie dokonane w treści uzasadnień do projektów rozporządzeń wykonawczych do ustawy definiujących progi istotności incydentu oraz wykazu usług kluczowych.	
Podmioty świadczące usługi kluczowe w sektorze infrastruktury cyfrowej	8	Szacunki oparte na analizie informacji rynkowych	

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Projekt rozporządzenia będzie przedmiotem konsultacji publicznych, opiniowania i uzgodnień międzyresortowych.
Zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248), projekt rozporządzenia zostanie udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Ministerstwa Cyfryzacji oraz na stronie Rządowego Centrum Legislacji w serwisie „Rządowy Proces Legislacyjny".

6. Wpływ na sektor finansów publicznych

(ceny stałe z …… r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	*Łącznie (0-10)*
Dochody ogółem	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
Wydatki ogółem	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
Saldo ogółem	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	Przyjęte rozwiązania nie spowodują dodatkowych skutków finansowych dla sektora finansów publicznych, w tym budżetu państwa i 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	0	0	0	0	0	0	0
	sektor mikro-, małych i średnich przedsiębiorstw	0	0	0	0	0	0	0
	rodzina, obywatele oraz gospodarstwa domowe	0	0	0	0	0	0	0
W ujęciu niepieniężnym	duże przedsiębiorstwa	0	0	0	0	0	0	0
	sektor mikro-, małych i średnich przedsiębiorstw	0	0	0	0	0	0	0
	rodzina, obywatele oraz gospodarstwa domowe	0	0	0	0	0	0	0
Niemierzalne	(dodaj/usuń)	0	0	0	0	0	0	0

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Projekt rozporządzenia nie ma wpływu na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na sytuację ekonomiczną i społeczną rodziny, osób niepełnosprawnych oraz osób starszych, a także na obywateli i gospodarstwa domowe.

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

☒ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☐ nie ☐ nie dotyczy

☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☐ zwiększenie liczby dokumentów ☐ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☐ tak ☐ nie ☐ nie dotyczy

9. Wpływ na rynek pracy

Projekt rozporządzenia nie ma wpływu na rynek pracy.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ inne:	☐ demografia ☐ mienie państwowe	☐ informatyzacja ☐ zdrowie

Omówienie wpływu	Nie dotyczy.

11. Planowane wykonanie przepisów aktu prawnego

Projektowane rozporządzenie wejdzie w życie z dniem …… 2018 r.

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

Nie dotyczy.

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

Brak załączników.