Projekt

ROZPORZĄDZENIE

MINISTRA CYFRYZACJI[1)]

z dnia

w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu

Na podstawie art. 15 ust. 8 ustawy z dnia ... o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. ...) zarządza się, co następuje:

§ 1. Rozporządzenie określa wykaz certyfikatów uprawniających do przeprowadzenia audytu w rozumieniu art. 15 ustawy z dnia …… o krajowym systemie cyberbezpieczeństwa, stanowiący załącznik do rozporządzenia.

§ 2. Rozporządzenie wchodzi w życie z dniem …

MINISTER CYFRYZACJI

[1)] Minister Cyfryzacji kieruje działem administracji rządowej – informatyzacja, na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 20 kwietnia 2018 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (Dz. U. poz. 761)

Załącznik
do rozporządzenia
Ministra Cyfryzacji
z dnia ….. (poz. ….)

WYKAZ CERTYFIKATÓW UPRAWNIAJĄCYCH DO PRZEPROWADZENIA AUDYTU

1) Certified Internal Auditor (CIA);
2) Certified Information System Auditor (CISA);
3) Certified Information Security Manager (CISM);
4) Certified in Risk and Information Systems Control (CRISC);
5) Certified in the Governance of Enterprise IT (CGEIT);
6) Certified Information Systems Security Professional (CISSP);
7) Systems Security Certified Practitioner (SSCP);
8) Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN ISO/IEC 27001;
9) Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN ISO 22301.

UZASADNIENIE

Projekt rozporządzenia Ministra Cyfryzacji w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu został przygotowany na podstawie delegacji ustawowej, zamieszczonej w art. 15 ust. 8 projektu ustawy o krajowym systemie cyberbezpieczeństwa, określanej dalej jako „ustawa".

Celem projektowanych przepisów jest określenie wymagań uprawniających do przeprowadzania audytu bezpieczeństwa u Operatora usługi kluczowej. Wymienione certyfikaty swoimi wymaganiami uwzględniają zakres wiedzy specjalistycznej od osób się nimi legitymującymi. Obowiązek przeprowadzania audytu określony jest w art. 15 ust. 1 ustawy i powinien odbywać się co najmniej raz na dwa lata.

Projektując rozporządzenie wzięto pod uwagę następujące uznane certyfikaty:

1. Certified Internal Auditor (CIA), który jest międzynarodowym certyfikatem wydawanym przez Instytut Audytorów Wewnętrznych (Institute of Internal Auditors, IIA). Certyfikat CIA potwierdza standardy i kompetencje zawodowe audytorów wewnętrznych, a egzamin sprawdza wiedzę, umiejętności i kwalifikacje niezbędne do wykonywania zawodu audytora wewnętrznego.

2. Certified Information System Auditor (CISA), który jest certyfikatem wydawanym przez Stowarzyszenie ds. Audytu i Kontroli Systemów Informatycznych (Information Systems Audit and Control Association, ISACA), przeznaczonym dla osób odpowiedzialnych za zapewnienie bezpieczeństwa IT organizacji oraz monitorowanie, zarządzanie i ochronę systemów biznesowych. Certyfikat CISA jest uznawanym na całym świecie standardem gwarantującym odpowiednią wiedzę i umiejętności audytorów IT w zakresie oceny luk w zabezpieczeniach i wdrażania mechanizmów kontrolnych w przedsiębiorstwach.

3. Certified Information Security Manager (CISM), który jest certyfikatem w zakresie zarządzania bezpieczeństwem informacji, wydawanym przez Stowarzyszenie ds. Audytu i Kontroli Systemów Informatycznych (Information Systems Audit and Control Association, ISACA). Celem certyfikacji jest upowszechnienie wspólnego zasobu wiedzy dla osób zarządzających bezpieczeństwem informacji. CISM koncentruje się na zarządzaniu ryzykiem jako podstawą bezpieczeństwa informacji. Dotyczy również szerszych zagadnień, takich jak zarządzanie bezpieczeństwem informacji, a także kwestii

praktycznych, takich jak zarządzanie programami w zakresie bezpieczeństwa informacji i zarządzanie incydentami bezpieczeństwa.

4. Certified in Risk and Information Systems Control (CRISC), który jest certyfikatem przeznaczonym dla osób zajmujących się problematyką IT i zarządzaniem ryzkiem w przedsiębiorstwach. Wydawanie certyfikatów jest akredytowane przez instytucję ustalającą normy techniczne obowiązujące w USA - American National Standards Institute (ANSI) pod oznaczeniem ISO/IEC 17024:2012. Norma ta dotyczy ogólnych wymagań dla jednostek certyfikujących osoby oraz zawiera zasady i wymagania dotyczące jednostki certyfikującej osoby w odniesieniu do specyficznych wymagań, łącznie z opracowywaniem i utrzymywaniem programu certyfikacji osób.

5. Certified in the Governance of Enterprise IT (CGEIT), który jest certyfikatem przeznaczonym dla osób zajmujących się kwestiami IT w przedsiębiorstwie, a także osób odpowiedzialnych za doradztwo związane z IT. Gwarantuje on wiedzę, umiejętności i praktyczne doświadczanie osób go posiadających w zakresie testowania, sprawdzania poprawności i poświadczania w obszarze zarządzania IT.

   Za rozwój, utrzymanie, testowanie i monitorowanie odpowiada Stowarzyszenie ds. Audytu i Kontroli Systemów Informatycznych (Information Systems Audit and Control Association, ISACA).

6. Certified Information Systems Security Professional (CISSP), który jest certyfikatem gwarantującym niezależne i obiektywne świadectwo eksperckie w dziedzinie bezpieczeństwa teleinformatycznego. Certyfikat spełnia standard ISO 17024:2003 oraz akredytowany jest przez ANSI (American National Standards Institute).

7. Systems Security Certified Practitioner (SSCP), który jest certyfikatem dla osób zajmujących się bezpieczeństwem IT. Jego uzyskanie potwierdza zdolność wdrażania, monitorowania i administrowania infrastrukturą IT w zgodności polityką bezpieczeństwa informatycznego i procedurami, które zapewniają poufność, integralność i dostępność danych.

8. Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN ISO/IEC 27001. Niniejsza międzynarodowa norma określa wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji w odniesieniu do organizacji. Norma obejmuje

również wymagania dotyczące szacowania i postępowania z ryzykiem dotyczącym bezpieczeństwa informacji, dostosowanych do potrzeb organizacji. Wymogi określone w niniejszej normie są ogólne i mają zastosowanie do wszystkich organizacji, niezależnie od typu, wielkości i charakteru.

9. Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN ISO 22301. Niniejsza norma określa wymagania dotyczące planowania, ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i ciągłego doskonalenia udokumentowanego systemu zarządzania, aby zmniejszyć prawdopodobieństwo wystąpienia uciążliwych incydentów, przygotować się na ich wystąpienia, odpowiedzieć na ich działanie i wyjść z kryzysu gdy się pojawiają.

Projektowane rozporządzenie wejdzie w życie w dniu wejścia w życie ustawy o krajowym systemie cyberbezpieczeństwa.

Przedmiot projektowanej regulacji jest zgodny 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.

Projektowana regulacja nie będzie wymagała notyfikacji Komisji Europejskiej w trybie ustawy z dnia 30 kwietnia 2004 r. o postępowaniu w sprawach dotyczących pomocy publicznej (Dz. U. z 2018 r. poz. 362).

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

Projekt zostanie udostępniony na stronie Rządowego Centrum Legislacji w serwisie „Rządowy Proces Legislacyjny" oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministerstwa 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 Rozporządzenie Ministra Cyfryzacji w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Podsekretarz Stanu – Karol Okoński **Kontakt do opiekuna merytorycznego projektu** Andrzej Szyszko, Departament Cyberbezpieczeństwa, Zastepca Dyrektora, tel. (22) 245 57 05, e-mail: andrzej.szyszko@mc.gov.pl	**Data sporządzenia** 19 kwietnia 2018 r. **Źródło:** art. 15 ust. 8 ustawy z dnia ……. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. …) **Nr w wykazie prac legislacyjnych Rady Ministrów** XXX

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

W związku z regulacją zawartą w art. 15 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa, która normuje obowiązek operatora usługi kluczowej do przeprowadzania, co najmniej raz na dwa lata, audytu bezpieczeństwa systemów informacyjnych, wykorzystywanych do świadczenia usługi kluczowej, zwany dalej „audytem", powstała konieczność przeprowadzania audytu przez osoby posiadające certyfikaty, które zakresem swojego programu certyfikacyjnego dają rękojmię właściwego przeprowadzenia audytu.

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

Określenie właściwych certyfikatów:

1) Certified Internal Auditor (CIA).
2) Certified Information System Auditor (CISA).
3) Certified Information Security Manager (CISM).
4) Certified in Risk and Information Systems Control (CRISC).
5) Certified in the Governance of Enterprise IT (CGEIT).
6) Certified Information Systems Security Professional (CISSP).
7) Systems Security Certified Practitioner (SSCP).
8) Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN ISO/IEC 27001.
9) Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN ISO 22301.

Wymienione wyżej rozwiązania powinny w sposób skuteczny i kompleksowy zapewnić właściwe przeprowadzenie audytu.

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

Ze względu na szczegółowość projektowanej regulacji, odstąpiono od przeprowadzenia analiz prawnoporównawczych.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Podmioty świadczące usługi kluczowe w sektorze energetycznym w podsektorze elektroenergetycznym	20	Szacunki oparte na załączniku nr 1 do projektu ustawy oraz danych URE (OSP, pięciu największych OSD dla gospodarstw domowych, dziewięciu największych OSD dla przedsiębiorców, pięciu największych sprzedawców prądu).	Podmioty świadczące usługi kluczowe w sektorze energetycznym w podsektorze elektroenergetycznym
Podmioty świadczące usługi kluczowe w sektorze energetycznym w podsektorze ropy naftowej	4	Szacunki oparte na załączniku nr 1 do projektu ustawy oraz danych URE (OSP oraz czterej najwięksi przedsiębiorcy posiadający koncesję na dystrybucję, wytwarzanie,	Podmioty świadczące usługi kluczowe w sektorze energetycznym w podsektorze ropy naftowej

		magazynowanie lub przeładunek paliw ciekłych oraz na obrót paliwami ciekłymi).	
Podmioty świadczące usługi kluczowe w sektorze energetycznym w podsektorze gazu	22	Szacunki oparte na załączniku nr 1 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 energetycznym w podsektorze gazu
Podmioty świadczące usługi kluczowe w sektorze transportu w podsektorze transportu lotniczego	28	Szacunki oparte na załączniku nr 1 do projektu ustawy oraz danych ULC (jeden przewoźnik lotniczy, zarządzający ośmioma największymi portami lotniczymi, pięć podmiotów obsługujących urządzenia pomocnicze znajdujące się w portach lotniczych oraz służba kontroli ruchu lotniczego).	Podmioty świadczące usługi kluczowe w sektorze transportu w podsektorze transportu lotniczego
Podmioty świadczące usługi kluczowe w sektorze transportu w podsektorze transportu kolejowego	10	Szacunki oparte na załączniku nr 1 do projektu ustawy oraz danych UTK (trzech największych zarządców infrastruktury kolejowej, czterech największych przewoźników kolejowych osobowych oraz trzech największych przewoźników kolejowych towarowych). Nie wzięto pod uwagę liczby operatorów infrastruktury usługowej ze względu na fakt, że rejestr obiektów infrastruktury usługowej zostanie utworzony przez Prezesa UTK do 30 czerwca 2018 r.	Podmioty świadczące usługi kluczowe w sektorze transportu w podsektorze transportu kolejowego

Projekt rozporządzenia oddziałuje na przedsiębiorców, jak również na osoby fizyczne, które będą chciały świadczyć usługi w zakresie wykonywania audytów. Koszty uzyskania uprawnień wynikających z rozporządzenia należy traktować jako zwykłe koszty związane z prowadzenia działalności gospodarczej lub zawodowej.

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

W ramach konsultacji i opiniowania projekt zostanie przesłany do:
1) Prezes Urzędu Komunikacji Elektronicznej,
2) Prezes Urzędu Ochrony Konkurencji i Konsumentów,
3) Generalnego Inspektora Ochrony Danych Osobowych,
4) Prezesa Głównego Urzędu Statystycznego,
5) Polskiej Izby Informatyki i Telekomunikacji,
6) Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji,
7) Polskiej Izby Komunikacji Elektronicznej,
8) Krajowej Izby Gospodarczej,
9) Krajowej Izby Komunikacji Ethernetowej,
10) Polskiej Izby Radiodyfuzji Cyfrowej,

11) Polskiej Izby Handlu,
12) Fundacji Bezpieczna Cyberprzestrzeń,
13) Polskiego Towarzystwa Informatycznego,
14) Fundacji Nowoczesna Polska,
15) Fundacji Projekt Polska,
16) Internet Society Poland,
17) Stowarzyszenia Inżynierów Telekomunikacji,
18) Fundacji Panoptykon,
19) Rady Dialogu Społecznego,
20) Business Centre Club – Związku Pracodawców,
21) Niezależnego Samorządowego Związku Zawodowego „Solidarność",
22) Ogólnopolskiego Porozumienia Związków Zawodowych,
23) Forum Związków Zawodowych,
24) Pracodawców Rzeczypospolitej Polskiej,
25) Konfederacji Lewiatan,
26) Związku Przedsiębiorców i Pracodawców,
27) Związku Rzemiosła Polskiego,
28) Związku Pracodawców Mediów Publicznych,
29) Związku Pracodawców Branży Internetowej IAB Polska,
30) Federacji Związków Zawodowych Pracowników Telekomunikacji,
31) Federacji Konsumentów.

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 zostanie udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny oraz na stronach internetowych Ministerstwa Cyfryzacji.

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)												

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	

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.)								
	sektor przedsiębiorstw – przedsiębiorcy, będący operatorami usług kluczowych – szacunkowy koszt dla przedsiębiorcy							
	sektor przedsiębiorstw – przedsiębiorcy, którzy chcą świadczyć usługi z zakresu reagowania na incydenty – szacunkowy koszt dla przedsiębiorcy							
W ujęciu niepieniężnym	duże przedsiębiorstwa	Operatorzy usług kluczowych będą zobowiązani do spełnienia wymogów określonych w rozporządzeniu.						
	sektor mikro-, małych i średnich przedsiębiorstw	Operatorzy usług kluczowych będą zobowiązani do spełnienia wymogów określonych w rozporządzeniu.						
	rodzina, obywatele oraz gospodarstwa domowe	Rodziny, obywatele, gospodarstwa domowe – regulacje zamieszczone w rozporządzeniu przyczynią się do zwiększenia bezpieczeństwa usług, z których korzystają wszyscy obywatele.						
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń								

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

Pozytywny – przepisy przyczynią się do wzrostu zatrudnienia w obszarze cyberbezpieczeństwa.

10. Wpływ na pozostałe obszary		
☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ inne:	☐ demografia ☐ mienie państwowe	☒ informatyzacja ☐ zdrowie
Omówienie wpływu	Przepisy rozporządzenia przyczynią się do zwiększenia poziomu cyberbezpieczeństwa, co będzie miało pozytywny wpływ na przedsiębiorców i obywateli.	
11. Planowane wykonanie przepisów aktu prawnego		
Po upływie okresów przewidzianych na wprowadzenie odpowiednich rozwiązań (vacatio legis) bądź dostosowanie istniejących przez adresatów aktu.		
12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?		
Nie jest planowana ewaluacja.		
13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)		