Projekt z dnia 13 czerwca 2018 r.

R O Z P O R Z Ą D Z E N I E

M I N I S T R A C Y F R Y Z A C J I [1)]

z dnia ……..... 2018 r.

w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu

Na podstawie art. 15 ust. 8 ustawy z dnia …….. 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. ……) zarządza się, co następuje:

§ 1. Rozporządzenie określa wykaz certyfikatów uprawniających do przeprowadzania audytu w rozumieniu art. 15 ustawy z dnia …… 2018 r. o krajowym systemie cyberbezpieczeństwa, stanowiący załącznik do rozporządzenia.

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

MINISTER CYFRYZACJI

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

[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 …..
2018 r. (poz. ….)

WYKAZ CERTYFIKATÓW UPRAWNIAJĄCYCH DO PRZEPROWADZANIA 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 stanowi wykonanie upoważnienia ustawowego, zawartego w art. 15 ust. 8 ustawy o krajowym systemie cyberbezpieczeństwa, zwanej dalej „ustawą”.

Celem projektowanych przepisów jest określenie wymagań uprawniających do przeprowadzania audytu bezpieczeństwa u operatora usługi kluczowej. Wymienione certyfikaty uwzględniają zakres wiedzy specjalistycznej wymagany od osób, które się nimi legitymują. Obowiązek przeprowadzania audytu określony jest w art. 15 ust. 1 ustawy. Audyt powinien odbywać się co najmniej raz na dwa lata.

W rozporządzeniu wzięto pod uwagę następujące uznane certyfikaty:

1. Certified Internal Auditor (CIA), który jest międzynarodowym certyfikat 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 kwalifikację 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), przeznaczony 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 ustalająca 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 procesu certyfikacji 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.

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.

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, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

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

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 Rozporządzenie Ministra Cyfryzacji w sprawie wykazu certyfikatów uprawniających do przeprowadzania audytu **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** 13 czerwca 2018 **Źródło:** **Upoważnienie ustawowe -** art. 15 ust. 8 ustawy z dnia ….. 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. …) **Nr w wykazie prac** 112

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Ustawa o krajowym systemie cyberbezpieczeństwa nakłada na operatora usługi kluczowej obowiązek zapewnienia przeprowadzania, co najmniej raz na dwa lata, audytu bezpieczeństwa systemu informacyjnego, wykorzystywanego do świadczenia usługi kluczowej.

Audyt może być przeprowadzony przez:

1) jednostkę oceniającą zgodność, akredytowaną zgodnie z ustawą z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650) w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych;

2) co najmniej dwóch audytorów posiadających:

a) certyfikaty określone w przepisach wydanych na podstawie ust. 8 lub

b) co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, lub

c) co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymujących się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych;

3) sektorowy zespół cyberbezpieczeństwa, ustanowiony w ramach sektora lub podsektora wymienionego w załączniku nr 1 do ustawy, jeżeli audytorzy spełniają warunki, o których mowa w pkt 2.

Konieczne jest ustalenie katalogu certyfikatów uprawniających do przeprowadzania audytów.

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

Wydanie rozporządzenia określającego katalog certyfikatów uprawniających do przeprowadzania audytów. Rozwiązanie to powinno w sposób skuteczny i kompleksowy zapewnić właściwe przeprowadzanie audytu.

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 wydobywania kopalin	24	Szacunki oparte na załączniku do projektu ustawy oraz danych URE (trzy podmioty prowadzące kopalnie węgla brunatnego, dwadzieścia podmiotów prowadzących kopalnie węgla kamiennego, jeden podmiot prowadzący kopalnię miedzi)	Audytorzy przeprowadzający dla operatorów usług kluczowych audyty będą musieli posiadać certyfikaty wymienione w rozporządzeniu (chyba że spełnią inne warunki, wskazane w ustawie – doświadczenie lub praca dla jednostki akredytowanej).
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	21	Szacunki oparte na	

usługi kluczowe w sektorze transportu w podsektorze transportu wodnego (dotyczącym transportu morskiego)		załączniku do projektu ustawy oraz danych MGMiŻŚ (założono objęcie dziesięciu 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	31	Przedsiębiorstwa	

usługi kluczowe w sektorze zaopatrzenia w wodę pitną i jej dystrybucję		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.)		0	0	0	0	0	0	0
	sektor przedsiębiorstw – przedsiębiorcy, będący operatorami usług kluczowych – szacunkowy koszt dla przedsiębiorcy	0	0	0	0	0	0	0
	sektor przedsiębiorstw – przedsiębiorcy, którzy chcą świadczyć usługi z zakresu reagowania na incydenty – szacunkowy koszt dla przedsiębiorcy	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 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 prowadzeniem działalności gospodarczej lub zawodowej. 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.