Projekt z dnia 15 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 warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo**

Na podstawie art. 14 ust. 4 ustawy z dnia …… 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. ……) zarządza się, co następuje:

**§ 1.** Rozporządzenie określa warunki organizacyjne i techniczne dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo.

**§ 2. 1.** Podmiot świadczący usługi z zakresu cyberbezpieczeństwa, w zakresie warunków organizacyjnych odnoszących się do tej działalności:

1) posiada i utrzymuje w aktualności system zarządzania bezpieczeństwem informacji spełniający wymagania Polskiej Normy PN ISO/IEC 27001;
2) zapewnia ciągłość działania usłudze reagowania na incydenty, polegającej na podejmowaniu działań w zakresie rejestrowania i obsługi zdarzeń naruszających bezpieczeństwo systemów teleinformatycznych zgodnie z wymaganiami Polskiej Normy PN-EN ISO 22301;
3) upublicznia w języku polskim i angielskim deklarację swojej polityki działania w zakresie określonym dokumentem RFC 2350 publikowanym przez Internet Engineering Task Force (IETF);
4) zapewnia wsparcie operatorowi usługi kluczowej w trybie całodobowym przez wszystkie dni w roku, z czasem reakcji adekwatnym do charakteru usługi kluczowej;
5) dysponuje personelem posiadającym umiejętności i doświadczenie w zakresie:
   a) identyfikowania zagrożeń w odniesieniu do systemów teleinformatycznych,

---

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).

b) analizowania oprogramowania szkodliwego i określania jego wpływu na system teleinformatyczny operatora usługi kluczowej,

c) zabezpieczania śladów kryminalistycznych na potrzeby postępowań prowadzonych przez organy ścigania.

2. Wewnętrzna struktura organizacyjna odpowiedzialna za cyberbezpieczeństwo spełnia warunki, o których mowa w pkt 1, 2, 4 i 5.

**§ 3. 1.** Podmioty, o których mowa w § 1, dysponują pomieszczeniami, do których posiadają wyłączne prawo użytkowania, wyposażonymi w zabezpieczenia techniczne adekwatne do przeprowadzonego szacowania ryzyka, w tym co najmniej:

1) system sygnalizacji włamania i napadu klasy 2 według Polskiej Normy PN-EN 50131-1;
2) system kontroli dostępu klasy 2 według Polskiej Normy PN-EN 60839-11-1, zapewniający osobie przyznanie dostępu do pomieszczenia poprzez rzecz posiadaną przez tą osobę oraz zapamiętanie zdarzenia przyznania dostępu danej osobie wraz z datą i czasem;
3) system wykrywania i sygnalizacji pożaru z powiadamianiem do centrum odbiorczego alarmów pożarowych;
4) szafy służące do przechowywania dokumentów oraz informatycznych nośników danych, o istotnym znaczeniu dla prowadzonej działalności, klasy S1 spełniającymi wymagania Polskiej Normy PN-EN 14450, chyba że inne przepisy wymagają wyższej klasy odporności szaf;
5) zewnętrzne drzwi wejściowe do pomieszczeń o klasie odporności RC4 według wymagań Polskiej Normy PN-EN 1627, wyposażone w zamki o klasie nie niższej niż klasa odporności drzwi;
6) wewnętrzne drzwi do pomieszczeń o klasie odporności RC2 według wymagań Polskiej Normy PN-EN 1627, wyposażone w zamki o klasie nie niższej niż klasa odporności drzwi;
7) okna o klasie odporności RC4 według wymagań Polskiej Normy PN-EN 1627, o ile na podstawie przeprowadzonego szacowania ryzyka dostęp do nich rodziłby nieakceptowalne ryzyko nieuprawnionego wejścia do pomieszczenia.

**2.** W przypadku, gdy pomieszczenia wskazane w ust. 1 nie są wyposażone w system, o którym mowa w ust. 1 pkt 3, dopuszcza się, po wykonaniu szacowania ryzyka, wyposażenie tych pomieszczeń w czujki wykrywające pożar podłączone do systemu sygnalizacji włamania

i napadu, jeżeli stacja monitorująca alarmy z tego systemu będzie w stanie ustalić przyczynę poszczególnych alarmów.

**§ 4.** Podmioty, o których mowa w § 1, w zakresie spełnienia warunków technicznych dysponują:

1) sprzętem komputerowym oraz specjalizowanymi narzędziami informatycznymi umożliwiającymi:
   a) automatyczne rejestrowanie zgłoszeń incydentów,
   b) analizę kodu oprogramowania uznanego za szkodliwe,
   c) badanie odporności systemów teleinformatycznych na przełamanie zabezpieczeń;
2) środkami łączności umożliwiającymi wymianę informacji z podmiotem, dla którego świadczy usługi oraz właściwym Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego działającym na poziomie krajowym.

**§ 5.** Podmioty, o których mowa w § 1, które rozpoczęły świadczenie usług przed dniem wejścia w życie przepisów niniejszego rozporządzenia dostosują się do jego wymagań w terminie 6 miesięcy od dnia wejścia w życie rozporządzenia.

**§ 6.** 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/

## UZASADNIENIE

Projekt rozporządzenia Ministra Cyfryzacji w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo stanowi wykonanie upoważnienia ustawowego zawartego w art. 14 ust. 4 ustawy z dnia …….. 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. …), zwanej dalej „ustawą”.

Celem projektowanych przepisów jest określenie wymagań dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa dla operatorów usług kluczowych oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo, mających wykonywać zadania nałożone na nich przez art. 8, art. 9, art. 10 ust. 1 - 3, art. 11 ust. 1 - 3 oraz art. 13 ustawy. Chodzi tu o obowiązkowe elementy schematu organizacyjnego mającego zapewnić cyberbezpieczeństwo systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych.

Adresatami projektu 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 oraz podmioty świadczące usługi z zakresu cyberbezpieczeństwa.

Projektowany przepis § 2 ust. 1 pkt 1 określa, że podmiot świadczący usługi w zakresie cyberbezpieczeństwa dla operatorów usług kluczowych musi posiadać i utrzymywać w aktualności system zarządzania bezpieczeństwem informacji. System zarządzania bezpieczeństwem informacji stanowi narzędzie zarządcze, pozwalające w uporządkowany sposób zapewnić bezpieczeństwo informacji w zakresie dostępności, integralności, poufności i autentyczności, z uwzględnieniem bezpieczeństwa osobowego, eksploatacji i architektury systemów oraz pozwala sprawować skuteczny nadzór nad bezpieczeństwem. Powszechnie uznaje się, że spełnienie przez system zarządzania bezpieczeństwem informacji wymagań międzynarodowej normy ISO/IEC 27001 jest najlepszym sposobem osiągnięcia celu w tym zakresie. Wspomniana międzynarodowa norma została wprowadzona do polskiego systemu prawa jako Polska Norma PN ISO/IEC 27001. Mając na względzie przepis art. 5 ust. 4 ustawy z dnia 12 września 2002 r. o normalizacji (Dz. U. 2015 r. poz. 1483) uprawnione jest

bezpośrednie przywołanie tej normy w projektowanym rozporządzeniu. Każdorazowo zastosowanie będzie miała aktualna wersja normy.

Biorąc pod uwagę, że Polska Norma PN ISO/IEC 27001 jedynie w sposób ogólny formułuje wymagania dotyczące zarządzania ciągłością działania, a także z uwagi na to, że zapewnienie przez podmiot świadczący usługi cyberbezpieczeństwa ciągłości wsparcia świadczonego dla operatora usługi kluczowej jest istotnym elementem zapewnienia bezpieczeństwa samej usługi kluczowej, w § 2 ust. 1 pkt 2 projektu przywołano wymagania zawarte w Polskiej Normie PN-EN ISO 22301, która uściśla wymagania dotyczące zapewnienia ciągłości działania.

Dobrą praktyką podmiotów świadczących usługi z zakresu cyberbezpieczeństwa jest upublicznianie deklaracji polityki swojego działania. Powszechnie przyjęto, że deklaracja taka opracowywana jest zgodnie z wymaganiami określonymi przez dokument RFC 2350 opracowany przez organizację Internet Engineering Task Force, który to dokument jest dostępny w sieci Internet, na witrynie pod adresem https://www.ietf.org/rfc/rfc2350.txt. Również dobrą praktyką jest to, aby tekst deklaracji dostępny był nie tylko w języku narodowym, ale również w języku angielskim, wobec czego wymóg takiej deklaracji zawarty został w § 2 ust. 1 pkt 3. Wymóg ten nie dotyczy wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo, ponieważ nie są one podmiotami niezależnymi, lecz działają w ramach organizacji operatorów usług kluczowych i nie świadczą usług na zewnątrz organizacji.

Z uwagi na to, że zwykle usługi kluczowe świadczone są w systemie całodobowym, przez wszystkie dni w roku, operator takiej usługi musi mieć wsparcie w taki samym układzie czasowym, co zostało wskazane w § 2 ust. 1 pkt 4 projektu.

Niezbędnym elementem sprawnego funkcjonowania usług wsparcia dla operatorów usług kluczowych w zakresie cyberbezpieczeństwa jest dysponowanie przez podmiot zapewniający te usługi personelem o odpowiednich kwalifikacjach. Wymagane kalifikacje, niezbędne do właściwego wykonywania przez personel podmiotu zadań z zakresu usług wsparcia, wskazane zostały w § 2 ust. 1 pkt 5.

Podmioty świadczące usługi z zakresu cyberbezpieczeństwa i wewnętrzne struktury organizacyjne odpowiedzialne za cyberbezpieczeństwo muszą zapewnić bezpieczeństwo fizyczne i środowiskowe dla lokalizacji, w której świadczone są usługi. Służą temu wymagania sformułowane w § 3. Na wymagania te składają się zarówno wymagania dotyczące bezpieczeństwa prawnego jak i wymagania dotyczące zabezpieczeń technicznych. Mając na

względzie to, że wymagania dotyczące systemów zabezpieczenia technicznego znajdują odzwierciedlenie w polskim systemie normatywnym uzasadnione jest przywoływanie odpowiednich Polskich Norm w treści § 3. Jednocześnie, aby uniknąć nadmiernych obciążeń zgodnie z § 3 ust. 2 w uzasadnionych przypadkach możliwe jest odstępstwo od konieczności posiadania systemu sygnalizacji pożaru.

Przepisy § 4 określają minimalne wymagania, jakie podmioty muszą spełnić w zakresie posiadanego potencjału technicznego.

W przypadku podmiotów, które rozpoczęły swoją działalność przed wejściem w życie projektowanego rozporządzenia wprowadza się sześciomiesięczny okres przejściowy na dostosowanie się do jego przepisów.

Mając na względzie przepis art. 19 ust. 1 dyrektywy Parlamentu Europejskiego i Rady UE 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa NIS) (Dz. Urz. UE L 194 z 19.7.2016, s. 1) dopuszczalne jest odwoływanie się do stosowania europejskich lub uznanych międzynarodowo norm i specyfikacji mających znaczenie dla bezpieczeństwa sieci i systemów informatycznych.

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.

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**<br>Projekt rozporządzenia Ministra Cyfryzacji w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo<br><br>**Ministerstwo wiodące i ministerstwa współpracujące**<br>Ministerstwo Cyfryzacji<br>**Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu**<br>Karol Okoński, Podsekretarz Stanu w Ministerstwie Cyfryzacji<br><br>**Kontakt do opiekuna merytorycznego projektu**<br>Jakub Dysarz, Departament Cyberbezpieczeństwa,<br>tel. (22) 245 58 38, e-mail:jakub.dysarz@mc.gov.pl | **Data sporządzenia**<br>15 czerwca 2018 r.<br><br>**Źródło:**<br>Upoważnienie ustawowe - art. 14 ust. 4 ustawy……..... o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. …)<br><br>**Nr w wykazie prac MC:**<br>Nr 111 |

# OCENA SKUTKÓW REGULACJI

## 1. Jaki problem jest rozwiązywany?

Ustawa o krajowym systemie cyberbezpieczeństwa nałożyła na operatorów usług kluczowych obowiązki związane z wdrożeniem i zapewnieniem właściwego funkcjonowania systemu zarządzania bezpieczeństwem w systemach informacyjnych, wykorzystywanych do świadczenia usług kluczowych. Dla wykonania tych zadań każdy operator winien powołać wewnętrzną strukturę odpowiedzialną za cyberbezpieczeństwo lub zawrzeć umowę z podmiotem świadczącym usługi z tego zakresu.
Konieczne było unormowanie minimalnych wymagań, które powinny spełnić te struktury bądź podmioty, w celu właściwej i skutecznej realizacji zadań z zakresu cyberbezpieczeństwa.

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

Wydanie rozporządzenia określającego warunki organizacyjne i techniczne dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo. Rozporządzenie precyzuje wymogi organizacyjne (posiadanie SZBI, zapewnianie ciągłości działania, dysponowanie właściwym personelem) i techniczne (dotyczące pomieszczeń i posiadanego sprzętu komputerowego). Rozporządzenie ustala okres sześciu miesięcy na dostosowanie się do wymogów wprowadzonych niniejszym rozporządzeniem.

## 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, | Dostosowanie posiadanych struktur do wymogów rozporządzenia lub skorzystanie z usług podmiotów, które |

| | | | |
|---|---|---|---|
| | | dwadzieścia podmiotów prowadzących kopalnie węgla kamiennego, jeden podmiot prowadzący kopalnię miedzi) | spełniają wymogi 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 transportu morskiego) | 21 | Szacunki oparte na 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).<br>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 | 253 | Szacunki oparte na danych z rejestrów | |

| | | | |
|---|---|---|---|
| sektorze ochrony zdrowia | | Głównego Inspektora Farmaceutycznego, CSIOZ i MZ.<br><br>Wyjaśnienie: Na potrzeby szacunków poczyniono następujące założenia.<br>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:<br>Dolnośląskie – 12<br>Kujawsko-Pomorskie – 8<br>Lubelskie – 8<br>Lubuskie – 3<br>Łódzkie – 8<br>Małopolskie – 10<br>Mazowieckie – 18<br>Opolskie – 3<br>Podkarpackie – 8<br>Podlaskie – 8<br>Pomorskie – 5<br>Śląskie – 15<br>Świętokrzyskie – 5<br>Warmińsko-mazurskie – 3<br>Wielkopolskie – 12<br>Zachodniopomorskie – 5.<br><br>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.<br><br>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). | Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności). |
|---|---|
| ☐ zmniejszenie liczby dokumentów<br>☐ zmniejszenie liczby procedur<br>☐ skrócenie czasu na załatwienie sprawy<br>☐ inne: | ☐ zmniejszenie liczby dokumentów<br>☐ zmniejszenie liczby procedur<br>☐ skrócenie czasu na załatwienie sprawy<br>☐ inne: |

| | |
|---|---|
| Wprowadzane obciążenia są przystosowane do ich elektronizacji. | Wprowadzane obciążenia są przystosowane do ich elektronizacji. |
| | |

**9. Wpływ na rynek pracy**

Projekt rozporządzenia nie ma wpływu na rynek pracy.

**10. Wpływ na pozostałe obszary**

| | | |
|---|---|---|
| ☐ środowisko naturalne<br>☐ sytuacja i rozwój regionalny<br>☐ inne: | ☐ demografia<br>☐ mienie państwowe | ☐ informatyzacja<br>☐ 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.