Projekt

# ROZPORZĄDZENIE

# MINISTRA CYFRYZACJI [1)]

z dnia

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

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

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

**§ 2.** Użyte w rozporządzeniu określenia oznaczają:

1) wewnętrzna struktura organizacyjna odpowiedzialna za cyberbezpieczeństwo – wewnętrzną komórkę organizacyjną przedsiębiorcy będącego operatorem usługi kluczowej albo przedsiębiorcę zależnego od operatora usługi kluczowej, świadczącego usługi w zakresie reagowania na incydenty wyłącznie na rzecz tego operatora;
2) podmiot świadczący usługi z zakresu cyberbezpieczeństwa – przedsiębiorcę niezależnego od operatora usługi kluczowej, świadczącego usługi w zakresie reagowania na incydenty dla jednego lub wielu operatorów usług kluczowych;
3) zespół reagowania – wewnętrzną strukturę organizacyjną operatora usługi kluczowej odpowiedzialną za cyberbezpieczeństwo lub podmiot świadczący usługi z zakresu cyberbezpieczeństwa;
4) usługa reagowania na incydenty – działania polegające na rejestrowaniu i obsłudze zdarzeń naruszających bezpieczeństwo 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).

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

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

**§ 4.** Podmiot prowadzący działalność zespołu reagowania jest obowiązany dysponować pomieszczeniami, do których posiada 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.

**§ 5.** W przypadku, gdy obiekt, w którym znajdują się pomieszczenia zespołu reagowania nie jest wyposażony w system, o którym mowa w § 4 pkt 3, dopuszcza się, po wykonaniu szacowania ryzyka i w braku przeciwwskazań wynikających z innych przepisów, wyposażenie tych pomieszczeń w czujki wykrywające pożar podłączone do systemu sygnalizacji włamania i napadu, o ile stacja monitorująca alarmy z tego systemu będzie w stanie ustalić przyczynę poszczególnych alarmów.

**§ 6.** Podmiot prowadzący zespół reagowania w zakresie spełnienia warunków technicznych dysponuje:

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.

**§ 7.** Podmiot świadczący usługi z zakresu cyberbezpieczeństwa, o ile świadczy usługi dla operatora usługi kluczowej będącego jednocześnie operatorem infrastruktury krytycznej w rozumieniu art. 3 pkt 2 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2017 r. poz. 209 i 1566) jest obowiązany posiadać ważne świadectwo bezpieczeństwa przemysłowego, o którym mowa w art. 54 ust. 2 ustawy z dnia z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2018 r. poz. 412 i 650), stosownie do klauzuli informacji niejawnej, z dostępem do której wiązałaby się obsługa incydentu.

**§ 8.** Zespoły reagowania, 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.

**§ 9.** Rozporządzenie wchodzi w życie z dniem ……

**MINISTER CYFRYZACJI**

## UZASADNIENIE

Projekt rozporządzenia Ministra Cyfryzacji w sprawie warunków organizacyjnych i technicznych dla wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo oraz podmiotów świadczących usługi z zakresu cyberbezpieczeństwa dla operatorów usług kluczowych stanowi wykonanie delegacji ustawowej, zamieszczonej w art. 14 ust. 4 ustawy z dnia …… o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. …), określanej dalej jako „ustawa".

Celem projektowanych przepisów jest określenie wymagań dla wewnętrznych struktur organizacyjnych operatorów usług kluczowych oraz podmiotów świadczących usługi z zakresu cyberbezpieczeństwa dla tych operatorów, mających wykonywać zadania nałożone na nich przez art. 8, art. 9, art. 10 ust. 1, art. 11 ust. 1 oraz art. 13 ust. 1 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 w rozumieniu ustawy oraz podmioty świadczące usługi z zakresu cyberbezpieczeństwa.

Definiując zakres podmiotowy projektowanego aktu prawnego przyjęto w § 2 pkt 1, że wewnętrzna struktura organizacyjna operatora usługi kluczowej odpowiedzialna za cyberbezpieczeństwo może być wewnętrzną komórką organizacyjną przedsiębiorcy albo podmiotem zależnym od tego przedsiębiorcy, jednak z tym zastrzeżeniem, że usługi takiego podmiotu zależnego świadczone są wyłącznie na potrzeby przedsiębiorcy, od którego dany podmiot zależy. W przypadku gdyby podmiot zależny od przedsiębiorcy świadczył usługi bezpieczeństwa również dla innych podmiotów, podmiot taki staje się podmiotem świadczącym usługi cyberbezpieczeństwa w rozumieniu definicji zawartej w § 2 pkt 2. Każda ze wskazanych powyżej form organizacyjnych, w przypadku gdy celem jej istnienia jest świadczenie usług w zakresie reagowania na incydenty, staje się zespołem reagowania § 2 pkt 3 projektu.

Projektowany przepis § 3 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.

Mając na względzie to, 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 § 3 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 reagowania na incydenty 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 § 3 pkt 3.

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 § 3 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 § 3 pkt 5.

Podmiot prowadzący działalność zespołu reagowania musi zapewnić bezpieczeństwo fizyczne i środowiskowe dla lokalizacji, w której świadczone są usługi. Służą temu wymagania sformułowane w § 4. 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 § 4. Jednocześnie, aby uniknąć nadmiernych obciążeń nakładanych przepisami prawa na podmiot świadczący usługi bezpieczeństwa, proponowany jest w § 5 zapis dopuszczający, w uzasadnionych przypadkach, odstępstwo od konieczności posiadania systemu sygnalizacji pożaru.

Przepisy § 6 określają minimalne wymagania, jakie podmiot świadczący usługi reagowania na incydenty musi spełnić w zakresie posiadanego potencjału technicznego.

Podmiot świadczący usługi z zakresu cyberbezpieczeństwa na rzecz operatora usługi kluczowej, który jednocześnie jest operatorem infrastruktury krytycznej w rozumieniu art. 3 pkt 2 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2017 r. poz. 209 i 1566), musi posiadać uprawnienie do przetwarzania informacji niejawnych i wymaganie takie określone zostało w § 7. W przypadku wewnętrznej struktury organizacyjnej odpowiedzialnej za cyberbezpieczeństwo zastosowanie mają przepisy ustawy o ochronie informacji niejawnych, które normują przetwarzanie informacji niejawnych w danym podmiocie, wobec czego nie jest konieczne ich dookreślanie w projektowanym rozporządzeniu.

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 Nr 194, str. 1) dopuszczalne jest odwoływanie się do stosowania

europejskich lub uznanych międzynarodowo norm i specyfikacji mających znaczenie dla bezpieczeństwa sieci i systemów informatycznych.

Proponuje się, aby rozporządzenie weszło w życie jednocześnie z wejściem w życie ustawy upoważniającej.

Rozporządzenie podlega uproszczonej notyfikacji w trybie przepisu § 8 ust. 4 rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. z 2002 r. poz. 2039 oraz z 2004 r. poz. 597)

Projekt został 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**<br>Projekt rozporządzenia Ministra Cyfryzacji w sprawie warunków organizacyjnych i technicznych dla wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo oraz podmiotów świadczących usługi z zakresu cyberbezpieczeństwa dla operatorów usług kluczowych<br>**Ministerstwo wiodące i ministerstwa współpracujące**<br>Ministerstwo Cyfryzacji<br>**Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu**<br><br>**Kontakt do opiekuna merytorycznego projektu** | **Data sporządzenia**<br><br>**Źródło:**<br>Art. 14 ust. 4 ustawy z dnia …… o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. ...)<br><br>**Nr w wykazie prac …….** |

## OCENA SKUTKÓW REGULACJI

**1. Jaki problem jest rozwiązywany?**

Na mocy art. 8, art. 9, art. 10 ust. 1, art. 11 ust. 1 oraz art. 13 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa na operatorów usług kluczowych nałożono 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 wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub zawrzeć umowę z podmiotem świadczącym usługi z tego zakresu. Projektowane rozporządzenie ma określać wymagania, 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**

Rozwiązaniem problemu jest opracowanie stosownych przepisów, zgodnie z upoważnieniem zamieszczonym w art. 14 ust. 4 ustawy o krajowym systemie cyberbezpieczeństwa.

**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 energetycznym w podsektorze elektroenergetycznym | 20 | Szacunki oparte na załączniku 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 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 energetycznym w podsektorze ropy naftowej |
| Podmioty świadczące usługi kluczowe w sektorze energetycznym w podsektorze gazu | 22 | Szacunki oparte na załączniku do projektu ustawy oraz danych URE (OSP, OSD, przedsiębiorcy dostarczający | Podmioty świadczące usługi kluczowe w sektorze energetycznym w podsektorze gazu |

| | | | |
|---|---|---|---|
| | | 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 transportu w podsektorze transportu lotniczego | 28 | Szacunki oparte na załączniku 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 do projektu ustawy oraz danych UTK (trzech największych zarządców infrastruktury kolejowej, czterech największych przewoźników kolejowych osobowych oraz trzech największych przewoźników kolejowych towarowych).<br><br>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 |

**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 został udostępniony na stronie podmiotowej Biuletynu Informacji Publicznej MC oraz w Biuletynie Informacji Publicznej na stronie podmiotowej 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 | |

**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 | 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. | | | | | | |
| Niemierzalne | - | Nie dotyczy. | | | | | | |
| 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<br>☒ nie<br>☐ nie dotyczy |
| ☐ zmniejszenie liczby dokumentów<br>☐ zmniejszenie liczby procedur<br>☐ skrócenie czasu na załatwienie sprawy<br>☐ inne: | ☒ zwiększenie liczby dokumentów<br>☒ zwiększenie liczby procedur<br>☐ wydłużenie czasu na załatwienie sprawy<br>☐ inne: |
| Wprowadzane obciążenia są przystosowane do ich elektronizacji. | ☒ tak<br>☐ nie<br>☐ nie dotyczy |

**9. Wpływ na rynek pracy**

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

| **10. Wpływ na pozostałe obszary** | | |
|---|---|---|
| ☐ środowisko naturalne<br>☐ sytuacja i rozwój regionalny<br>☐ inne: | ☐ demografia<br>☐ mienie państwowe | ☒ informatyzacja<br>☐ 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?** | | |
| 100% operatorów ma wdrożone odpowiednie rozwiązania, po roku od wejścia w życie przepisów. | | |
| **13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)** | | |
| – | | |