Projekt z dnia 11 lipca 2019 r.

**UCHWAŁA NR…**

**RADY MINISTRÓW**

z dnia ……..……………. 2019 r.

**w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa”**

Kierując się potrzebą zapewnienia bezpieczeństwa danych przetwarzanych w systemach teleinformatycznych podmiotów administracji publicznej oraz optymalizacji kosztów utrzymania tych systemów, uznając, że wprowadzenie jednolitych wysokich standardów ochrony systemów informatycznych i wspieranie podmiotów administracji publicznej   
w utrzymaniu tych systemów oraz uzyskiwaniu usług niezbędnych do ich budowy, rozwoju   
i utrzymania przyczyni się do zapewnienia wysokiego poziomu usług świadczonych społeczeństwu przez administrację publiczną, uchwala się, co następuje:

**§ 1.** 1. Przyjmuje się Inicjatywę „Wspólna Infrastruktura Informatyczna Państwa”, zwaną dalej „Inicjatywą WIIP”.

2. Inicjatywa WIIP obejmuje:

1) budowę, rozwój i utrzymanie prywatnej chmury obliczeniowej administracji publicznej, zwanej dalej „Rządową Chmurą Obliczeniową”, z wykorzystaniem w szczególności sieci teletransmisji pozostających w dyspozycji podmiotów publicznych;

2) budowę, rozwój i utrzymanie Rządowego Klastra Bezpieczeństwa, zwanego dalej „RKB”;

3) zapewnienie podmiotom administracji publicznej możliwości nabywania usług przetwarzania w publicznych chmurach obliczeniowych od wykonawców wybranych w zamówieniu wspólnym lub przez centralnego zamawiającego;

4) zapewnienie funkcjonowania systemu teleinformatycznego wspomagającego zarządzanie usługami przetwarzania w Rządowej Chmurze Obliczeniowej i w publicznych chmurach obliczeniowych, zwanego dalej „Systemem Zapewnienia Usług Chmurowych”;

5) określenie przez ministra właściwego do spraw informatyzacji Katalogu Wymagań Bezpieczeństwa Systemów Teleinformatycznych, zwanego dalej „KWBST”.

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

1) Centrum Przetwarzania Danych (CPD) – serwerownię w zasobach administracji publicznej; obiekt budowlany wykorzystywany jako lokalizacja dla infrastruktury teleinformatycznej i związanych z nią elementów (np.: systemów telekomunikacyjnych, zasobów przetwarzania) wraz z nadmiarowymi źródłami zasilania, dodatkowymi sieci teletransmisji, środkami kontroli środowiska (np. klimatyzacja, systemy gaśnicze), urządzeniami i systemami bezpieczeństwa oraz ochroną fizyczną obiektu;

2) chmura hybrydowa – chmurę, której infrastruktura składa się z dwóch lub więcej odrębnych infrastruktur teleinformatycznych dostarczanych z chmury obliczeniowej (prywatnej, społecznościowej lub publicznej), które pozostają odrębnymi jednostkami, ale są powiązane ze sobą znormalizowaną lub zastrzeżoną technologią, umożliwiającą przenoszenie danych i aplikacji pomiędzy chmurami obliczeniowymi (np. w celu równoważenia obciążenia);

3) chmura obliczeniowa – chmurę, której model przetwarzania umożliwia powszechny   
i wygodny dostęp za pośrednictwem sieci do wspólnej puli konfigurowalnych zasobów przetwarzania (np. sieci, serwery, pamięci masowe, aplikacje i usługi), które mogą być szybko udostępniane przy minimalnym wysiłku ze strony zespołów zarządzania lub dostawcy usług. Chmura obliczeniowa dostarcza usług w modelu chmurowym, który promuje dostępność i składa się z pięciu podstawowych cech przetwarzania (model samoobsługowy, dostęp do sieci, pule zasobów, elastyczność, rozliczanie usług); trzy modele usług (SaaS, PaaS, IaaS); oraz cztery modele wdrażania (chmura prywatna, chmura społecznościowa, chmura publiczna, chmura hybrydowa); kluczowe technologie wspomagające obejmują: szybkie i wydajne sieci rozległe, wydajne oraz relatywnie niedrogie serwery (uwzględniając ich liczbę) oraz wysokowydajną wirtualizację sprzętu;

4) chmura prywatna – chmurę, której infrastruktura jest udostępniana do wyłącznego użytku przez jedną organizację obejmującą wielu odbiorców usług i może być własnością, być zarządzana i obsługiwana przez organizację lub stronę trzecią lub ich kombinację oraz może być zainstalowana w siedzibie organizacji lub poza nią;

5) chmura publiczna – chmurę, której infrastruktura jest udostępniana do użytku publicznego i może być własnością, być zarządzana i obsługiwana przez organizację biznesową, akademicką lub rządową lub ich kombinację oraz jest zainstalowana w siedzibie dostawcy chmury;

6) infrastruktura chmury – zasoby przetwarzania, stanowiące zbiór sprzętu   
i oprogramowania zgrupowanego w pule zasobów, który umożliwia spełnienie pięciu podstawowych cech przetwarzania w chmurze (patrz chmura obliczeniowa); infrastrukturę chmury można postrzegać jako zawierającą zarówno warstwę fizyczną, jak i warstwę abstrakcji; warstwa fizyczna składa się z zasobów sprzętowych, które są niezbędne do obsługi dostarczanych usług w chmurze i zazwyczaj obejmują składniki serwera, pamięci masowej i sieci; warstwa abstrakcji składa się z oprogramowania rozmieszczonego w warstwie fizycznej, która przejawia istotne cechy chmury; koncepcyjnie warstwa abstrakcji znajduje się powyżej warstwy fizycznej;

7) infrastruktura jako usługa (IaaS) – usługę świadczoną w modelu chmurowym zapewniającą infrastrukturę chmury, na których odbiorca usług jest w stanie wdrożyć   
i uruchomić dowolne oprogramowanie (systemy operacyjne i aplikacje); odbiorca usług nie zarządza ani nie kontroluje podstawowej infrastruktury chmury, ale ma kontrolę nad systemami operacyjnymi, pamięcią masową i wdrożonymi aplikacjami oraz ewentualnie ograniczoną kontrolę wybranych komponentów sieciowych (np. firewall);

8) platforma jako usługa (PaaS) – usługę umożliwiającą odbiorcy usług wdrożenie na infrastrukturze chmury aplikacji utworzonych przez siebie lub nabytych, które zostały przygotowane przy użyciu języków programowania, bibliotek, usług i narzędzi obsługiwanych przez dostawcę; odbiorca usług nie zarządza ani nie kontroluje infrastruktury chmury, w tym sieci, serwerów, systemów operacyjnych oraz pamięci masowych, ale ma kontrolę nad wdrożonymi aplikacjami i ewentualnie ustawieniami konfiguracji dla środowiska hostingu aplikacji;

9) oprogramowanie jako usługa (SaaS) – usługę umożliwiającą odbiorcy usług wykorzystanie aplikacji uruchomionej na infrastrukturze chmury dostarczanej przez dostawcę usług; aplikacje są dostępne na różnych urządzeniach klienckich za pośrednictwem cienkiego klienta, takiego jak przeglądarka internetowa (np. poczta elektroniczna) lub klienta aplikacji; odbiorca usług nie zarządza ani nie kontroluje infrastruktury chmury, w tym sieci, serwerów, systemów operacyjnych, pamięci masowej, a nawet parametrów konfiguracyjnych aplikacji, z wyjątkiem ograniczonych ustawień konfiguracji aplikacji specyficznych dla użytkownika;

10) standard RKB – funkcjonalno-techniczną implementację KWBST, stanowiącą rozwiązania, środki techniczne oraz usługi bezpieczeństwa stosowane na poziomie: połączenia infrastruktury telekomunikacyjnej Rządowej Chmury Obliczeniowej   
z publiczną siecią telekomunikacyjną Internet poprzez bezpieczny punkt styku; komunikacji pomiędzy Rządową Chmurą Obliczeniową a odbiorcami jej usług w oparciu o udostępnione dla RKB warstwy sieci rządowej; połączenia pomiędzy poszczególnymi CPD; sieci „MGMT” – wewnętrza sieć zarządzania dostępna tylko dla zespołów administratorów środowiska przetwarzania Rządowej Chmury Obliczeniowej; dostępu użytkownika do Rządowej Chmury Obliczeniowej z sieci rządowych; dostępu użytkownika do Rządowej Chmury Obliczeniowej z sieci Internet; dostępu uprzywilejowanego – administratorzy użytkownika; dostępu uprzywilejowanego – administratorzy operatora Rządowej Chmury Obliczeniowej i zespół bezpieczeństwa operatora RKB; wymiany danych pomiędzy użytkownikami w ramach środowiska Rządowej Chmury Obliczeniowej;

11) sieci rządowe – sieci teletransmisyjne umożliwiające wymianę komunikacji pomiędzy publicznymi podmiotami krajowymi (GovNet, OST112), Unii Europejskiej oraz NATO (TESTA-NG), pozostające w gestii ministra właściwego do spraw wewnętrznych.

**§ 3.** 1. Realizację Inicjatywy WIIP powierza się ministrowi właściwemu do spraw informatyzacji.

2. Minister właściwy do spraw informatyzacji, w porozumieniu z ministrem właściwym do spraw wewnętrznych, Ministrem Obrony Narodowej oraz Ministrem – Koordynatorem Służb Specjalnych, przygotuje KWBST w terminie dwóch miesięcy od dnia wejścia w życie uchwały oraz przekaże go Radzie Ministrów.

**§ 4.** 1. Minister właściwy do spraw informatyzacji zapewnia budowę, rozwój i utrzymanie oraz zarządzanie zasobami Rządowej Chmury Obliczeniowej, jako operator Rządowej Chmury Obliczeniowej.

2. Minister właściwy do spraw informatyzacji może powierzyć realizację we własnym imieniu zadania, o którym mowa w ust. 1, jednostce przez niego nadzorowanej.

3. Operator Rządowej Chmury Obliczeniowej tworzy katalog usług przetwarzania w Rządowej Chmurze Obliczeniowej i udostępnia go podmiotom, o których mowa w § 6 ust. 1, których systemy teleinformatyczne spełniają kryteria klasyfikacji do korzystania z usług przetwarzanych w Rządowej Chmurze Obliczeniowej.

4. Usługi przetwarzania w Rządowej Chmurze Obliczeniowej będą świadczone, w szczególności w modelu „Infrastruktura jako usługa” (IaaS) i „Platforma jako usługa” (PaaS) oraz „Oprogramowanie jako usługa” (SaaS).

5. Usługi przetwarzania w Rządowej Chmurze Obliczeniowej będą świadczone w CPD, których posiadaczami są właściwe organy administracji rządowej.

6. Organy administracji rządowej współpracują z ministrem właściwym do spraw informatyzacji, w celu świadczenia usług przetwarzania w Rządowej Chmurze Obliczeniowej w oparciu o istniejące zasoby teleinformatyczne.

**§ 5.** 1. CPD, o których mowa w § 4 ust. 5, będą przyłączone do Rządowej Chmury Obliczeniowej po złożeniu pisemnego oświadczenia operatorowi Rządowej Chmury Obliczeniowej, przez posiadacza CPD, potwierdzającego spełnienie minimalnych wymagań organizacyjnych i technicznych dla posiadaczy CPD oraz ich obiektów CPD przyłączonych do Rządowej Chmury Obliczeniowej, określonych w załączniku nr 1 do uchwały.

2. Sposób i zakres przyłączenia oraz zasady korzystania z CPD przyłączonego do Rządowej Chmury Obliczeniowej będą określone w porozumieniu zawartym między właściwym organem administracji rządowej będącym posiadaczem CPD, a ministrem właściwym do spraw informatyzacji.

3. Zasady i sposób wykorzystania sieci teletransmisji na potrzeby Rządowej Chmury Obliczeniowej będą określane w porozumieniu zawartym między właściwym operatorem sieci, a ministrem właściwym do spraw informatyzacji, a ocena spełnienia minimalnych wymagań organizacyjnych i technicznych w zakresie możliwości przyłączania do sieci teletransmisji będzie każdorazowo uzgadniana między stronami porozumienia.

**§ 6.** 1. Z usług przetwarzania w Rządowej Chmurze Obliczeniowej mogą korzystać:

1) podmioty sektora finansów publicznych, o których mowa w art. 9 ust. 1-13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2019 r. poz. 869);

2) inne państwowe osoby prawne utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyłączeniem przedsiębiorstw, banków i spółek prawa handlowego;

3) inne, niż określone w ustawie z dnia 27 sierpnia 2009 r. o finansach publicznych, państwowe jednostki organizacyjne nieposiadające osobowości prawnej.

2. Korzystanie przez podmioty, o których mowa w ust. 1, z usług przetwarzania   
w Rządowej Chmurze Obliczeniowej lub publicznych chmurach obliczeniowych uzależnione jest od spełnienia kryteriów klasyfikacji systemów teleinformatycznych, które mogą korzystać z usług przetwarzania w Rządowej Chmurze Obliczeniowej lub publicznych chmurach obliczeniowych, określonych w załączniku nr 2 do uchwały.

3. Podmioty, o których mowa w ust. 1, w celu skorzystania z usług przetwarzania w Rządowej Chmurze Obliczeniowej, wnioskują do ministra właściwego do spraw informatyzacji o zawarcie porozumienia, określającego szczegółowe warunki techniczne oraz prawa i obowiązki stron, w szczególności:

1) zastosowane standardy, podział odpowiedzialności, ograniczenia odpowiedzialności oraz zasady audytu;

2) procedury wejścia do Rządowej Chmury Obliczeniowej;

3) podział obowiązków i odpowiedzialności związany z użytkowaniem usług, w tym obowiązki dostawcy usług oraz zapewnienie ustalonego poziomu SLA;

4) zasady obsługi technicznej;

5) obowiązki w zakresie praw własności intelektualnej;

6) procedury bezpieczeństw oraz zasady reagowania na incydenty;

7) obowiązki w zakresie ochrony danych osobowych;

8) procedury wyjścia z Rządowej Chmury Obliczeniowej oraz warunki wypowiedzenia umowy;

9) zasady prowadzenia rozliczeń za wykorzystanie usług;

10) obowiązki informacyjne w zakresie świadczenia usług.

**§ 7.** 1. RKB obejmuje usługi:

1) bezpieczeństwa teleinformatycznego, świadczone w oparciu o dedykowane systemy bezpieczeństwa, które realizują zadania wyłącznie na potrzeby Inicjatywy WIIP;

2) monitorowania poziomu bezpieczeństwa opartego o dedykowane zespoły:]

a) Centrum Zarzadzania Siecią (Network Operations Center „NOC”),

b) Operacyjnego Centrum Bezpieczeństwa (Security Operations Center „SOC”).

2. RKB zapewnia bezpieczeństwo:

1) połączenia infrastruktury telekomunikacyjnej Rządowej Chmury Obliczeniowej   
z publiczną siecią telekomunikacyjną Internet poprzez bezpieczny punkt styku;

2) komunikacji pomiędzy Rządową Chmurą Obliczeniową a odbiorcami jej usług w oparciu o udostępnione dla RKB warstwy sieci rządowej;

3) bezpieczeństwo połączenia między poszczególnymi CPD.

3. Zasoby teletransmisyjne wykorzystane do podłączenia odbiorców usług przetwarzania w Rządowej Chmurze Obliczeniowej oraz sposób ich finansowania będą każdorazowo uzgadniane między ministrem właściwym do spraw informatyzacji, a odbiorcą usług.

4. Operatorem RKB jest minister właściwy do spraw informatyzacji.

5. Operator RKB w szczególności:

1) świadczy usługi utrzymania systemów bezpieczeństwa;

2) zapewnia utrzymanie i rozwój zespołów, o których mowa w ust. 1 pkt 2;

3) informuje właściwe podmioty o zagrożeniach bezpieczeństwa i incydentach;

4) planuje rozwój usług RKB;

5) razem z operatorem sieci rządowej, planuje rozwój i wykorzystanie łącz transmisji dla świadczenia usług przetwarzania w Rządowej Chmurze Obliczeniowej;

6) planuje rozwój i wykorzystanie punktów dostępowych i łącz transmisji dla świadczenia dostępu do Internetu.

6.  Minister właściwy do spraw informatyzacji może powierzyć realizację we własnym imieniu zadań, o których mowa w ust. 5, jednostce przez niego nadzorowanej lub innemu wybranemu podmiotowi, z zachowaniem procedur przewidzianych przepisami prawa.

**§ 8.** 1.Minister właściwy do spraw informatyzacji zapewnia funkcjonowanie Systemu Zapewnienia Usług Chmurowych, będącego systemem teleinformatycznym wspomagającym zamawianie oraz zarządzanie usługami przetwarzania w Rządowej Chmurze Obliczeniowej   
i w publicznych chmurach obliczeniowych świadczonymi dla podmiotów, o których mowa   
w § 6 ust. 1.

2. W Systemie Zapewnienia Usług Chmurowych udostępnia się:

1) katalog usług przetwarzania w Rządowej Chmurze Obliczeniowej, regularnie aktualizowany;

2) katalog usług przetwarzania w publicznych chmurach obliczeniowych, aktualizowany po przeprowadzeniu postępowania na zakup usług przetwarzania w publicznych chmurach obliczeniowych zgodnie z przepisami ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2018 r. poz. 1986 i 2215 oraz z 2019 r. poz. 730).

3. Usługi przetwarzania w publicznych chmurach obliczeniowych będą umieszczane   
w katalogu, o którym mowa w ust. 2 pkt 2, po zawarciu umów.

4. Prowadzenie postępowań o zamówienia publiczne oraz zawieranie umów, o których mowa w ust. 3, realizowane będzie w zamówieniu wspólnym lub przez centralnego zamawiającego wskazanego przez Prezesa Rady Ministrów, zgodnie z ustawą z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych.

5. Zamawiający wyznaczony do przeprowadzenia wspólnego zamówienia lub centralny zamawiający, w celu zapewnienia podmiotom, o których mowa w § 6 ust. 1, nabywania najbardziej zaawansowanych technologicznie usług przetwarzania w publicznych chmurach obliczeniowych, będzie ogłaszał postępowania o udzielenie zamówienia publicznego na świadczenie usług przetwarzania w publicznych chmurach obliczeniowych.

**§ 9.** 1. Źródłem Finansowania Inicjatywy WIIP będą środki budżetu państwa w ramach rezerwy celowej pod nazwą „Finansowanie Inicjatywy Wspólna Infrastruktura Informatyczna Państwa”.

2. O uruchomienie rezerwy celowej będzie wnioskował minister właściwy do spraw informatyzacji.

3. Środki na rezerwę celową, o której mowa w ust. 1, będą pochodziły ze środków finansowych, które dotychczas były przeznaczone, a także były lub będą planowane na zapewnienie usług przetwarzania, pozwalających na rozwój i utrzymanie systemów teleinformatycznych przenoszonych na Rządową Chmurę Obliczeniową.

**§ 10.** 1. Podmioty, o których mowa w § 6 ust. 1, projektując systemy teleinformatyczne, po wejściu w życie uchwały, przeprowadzają klasyfikację, o której mowa w § 6 ust. 2.

2. Systemy teleinformatyczne spełniające kryteria klasyfikacji do korzystania z usług przetwarzania w Rządowej Chmury Obliczeniowej uzyskują opinię ministra właściwego do spraw informatyzacji w zakresie możliwości wykorzystania Rządowej Chmury Obliczeniowej.

**§ 11.** 1. Minister właściwy do spraw informatyzacji w terminie do końca lutego danego roku występuje do podmiotów, o których mowa w § 6 ust. 1, o wskazanie wstępnego zapotrzebowania na usługi przetwarzania w Rządowej Chmurze Obliczeniowej, w roku następnym.

2. Podmioty, o których mowa w § 6 ust. 1, w terminie do końca marca danego roku przekazują ministrowi właściwemu do spraw informatyzacji wstępne zapotrzebowanie,   
o którym mowa w ust. 1.

3. Minister właściwy do spraw informatyzacji w terminie do końca kwietnia danego roku ustala na podstawie zapotrzebowania, o którym mowa w ust. 2, wykaz usług przetwarzania   
w Rządowej Chmurze Obliczeniowej na rok następny oraz prognozowany wykaz kosztów poszczególnych usług przetwarzania w Rządowej Chmurze Obliczeniowej i przekazuje je podmiotom, o których mowa w § 6 ust. 1.

**§ 12.** Uchwała wchodzi w życie z dniem następującym po dniu ogłoszenia.

**PREZES RADY MINISTRÓW**

Załączniki do uchwały Nr ….

Rady Ministrów

z dnia ………… 2019 r. (poz. …)

Załącznik nr 1

**Minimalne wymagania organizacyjne i techniczne dla posiadaczy CPD oraz ich obiektów CPD przyłączonych do Rządowej Chmury Obliczeniowej**

1. Posiadacz CPD w zakresie świadczenia usług przetwarzania danych w Rządowej Chmurze Obliczeniowej spełnia wymagania zapewnienia zgodności swojego działania określone w Krajowych Ramach Interoperacyjności i ustawie o ochronie danych osobowych, w tym minimum poniższych standardów lub ich odpowiedników w polskim lub europejskim układzie normalizacji:

1. PN-EN ISO/IEC 27001 dotyczące zarządzania bezpieczeństwem informacji;
2. PN-EN ISO 22301 dotyczące zarządzania ciągłością działania;
3. PN-ISO/IEC 27005 dotyczące zarządzania ryzykiem w bezpieczeństwie informacji.

2. CPD spełnia wymagania:

1. obiekt CPD jest własnością skarbu państwa albo jednostek samorządu terytorialnego albo państwowych lub samorządowych osób prawnych lub udział w prawie własności tych podmiotów wynosi co najmniej 51%;
2. klasa obiektu CPD wynosi minimum 3 według PN-EN 50600 w kategoriach: dostępność, zabezpieczenie przed nieuprawnionym dostępem, zabezpieczenie przed zagrożeniami środowiskowymi, potwierdzona oświadczeniem posiadacza obiektu albo odpowiednim certyfikatem zgodności;
3. w CPD istnieje węzeł sieci rządowej lub występuje możliwość jego zbudowania w ciągu 1 roku od dnia podjęcia decyzji o przyłączeniu CPD do Rządowej Chmury Obliczeniowej, potwierdzona przez ministra właściwego do spraw wewnętrznych;
4. istnieje techniczna możliwość wydzielenia w CPD dedykowanej komory lub klatki   
   w komorze na potrzeby infrastruktury Rządowej Chmury Obliczeniowej oraz zabezpieczenie rezerwy mocy nie mniej niż 2,5 kW/m2 wydzielonej powierzchni;
5. w CPD jest zapewniona ochrona fizyczna obiektu;
6. CPD posiada system monitorowania pomieszczeń oraz nadzorowania ruchu osób umożliwiający generowanie raportów pozwalających na weryfikację dostępu fizycznego osób do urządzeń infrastruktury Rządowej Chmury Obliczeniowej.

3. Infrastruktura sieci łączności CPD spełnia wymagania:

1. posiada dostęp do dedykowanej sieci rządowej;
2. posiada dostęp do sieci publicznej przez co najmniej 2 niezależne łącza różnych operatorów;
3. posiada możliwość świadczenia usług RKB potwierdzoną przez operatora RKB.

4. Infrastruktura przetwarzania Rządowej Chmury Obliczeniowej umieszczona w CPD spełnia wymagania:

1. w zakresie wsparcia dla infrastruktury:
2. używana infrastruktura (w szczególności: serwery, macierze, urządzenia sieciowe) posiadają aktywną gwarancję wsparcia producenta. W przypadku, gdy gwarancja wsparcia nie jest odnawiana, posiadacz CPD musi o tym poinformować odbiorców usług,
3. używana infrastruktura korzysta z firmware instalowanego z autoryzowanych źródeł przez przeszkolony i autoryzowany personel,
4. uszkodzone elementy wyposażenia, które zawierają lub mogą zawierać dane odbiorców usług lub dane konfiguracji środowiska infrastruktury przetwarzania lub infrastruktury sieciowej nie opuszczają pomieszczenia lub wydzielonej strefy CPD: w przypadku uszkodzonych nośników danych muszą one zostać trwale zniszczone pod nadzorem autoryzowanego personelu;
5. w zakresie wsparcia dla oprogramowania:
6. używane oprogramowanie pochodzi z autoryzowanych źródeł i jest przygotowywane do instalacji oraz instalowane przez przeszkolony i autoryzowany personel,
7. używane oprogramowanie zawiera wymagane poprawki bezpieczeństwa, a w szczególności te, które producent opisał, jako krytyczne; posiadacz CPD zapewnia weryfikowalny i powtarzalny proces aktualizacji źródeł oprogramowania używanego do świadczenia usług,
8. używane oprogramowanie posiada wsparcie producenta w zakresie aktualizacji i poprawek bezpieczeństwa, a w przypadku oprogramowania używanego do świadczenia usług (np. oprogramowanie systemów operacyjnych, oprogramowanie do wirtualizacji) także hot-line w trybie 24/7/365,
9. posiadacz CPD zapewnia, że wyłącznie wyszkolony i autoryzowany personel realizuje usługę,
10. w przypadku używania oprogramowania open source wymagania a – d stosuje się odpowiednio, przy czym rolę producenta oprogramowania przejmuje posiadacz CPD.

5. Posiadacz CPD, który nie udostępnia infrastruktury przetwarzania, spełnia wyłącznie wymagania, o których mowa w ust. 1-3.

6. Potwierdzenie wymagań określonych w ust. 1-3 odbywa się na podstawie dokumentacji przedstawionej przez posiadacza CPD.

7. Posiadacz CPD, który nie spełnia wymagań, o których mowa w ust. 1-3, może zostać podłączony do Rządowej Chmury Obliczeniowej po spełnieniu następujących warunków:

1. złożeniu oświadczenia zgodności z wymaganymi certyfikatami;
2. przejścia pozytywnej weryfikacji zgodności z KWBST prowadzonej przez instytucję wskazaną przez operatora RKB;
3. podpisaniu stosownego porozumienia dającego operatorowi RKB możliwość sprawdzania systemu bezpieczeństwa w zakresie dotyczącym aktywów Rządowej Chmury Obliczeniowej.

8. W przypadku konieczności przeprowadzenia audytu i certyfikacji, koszty realizacji takich zadań ponosi posiadacz CPD.

Załącznik nr 2

**Kryteria klasyfikacji systemów teleinformatycznych,**

**które mogą korzystać z usług przetwarzania w Rządowej Chmurze Obliczeniowej lub w publicznych chmurach obliczeniowych**

**Kryteria obejmują:**

1. Kategorie systemów teleinformatycznych, które mogą korzystać z usług przetwarzania w Rządowej Chmurze Obliczeniowej lub w publicznych chmurachobliczeniowych wraz z oznaczeniem możliwości utrzymania w Rządowej Chmurze Obliczeniowej lub w publicznych chmurachobliczeniowych.

| **Kategorie systemów teleinformatycznych, które mogą korzystać z usług w Rządowej Chmurze Obliczeniowej lub w publicznych chmurach obliczeniowych wraz z oznaczeniem możliwości utrzymania w Rządowej Chmurze Obliczeniowej lub w publicznych chmurach obliczeniowych**  **Objaśnienie ogólne:**  Kategorie systemów teleinformatycznych przedstawione w tabeli mają charakter co do zasady rozłączny. Kryterium rozróżnienia kategorii uwzględnia główne rodzaje systemów teleinformatycznych działających w organach publicznych oraz ich główne, z punktu widzenia bezpieczeństwa przetwarzania w chmurze, cechy i przeznaczenie. Jeżeli w praktyce może się okazać, że system można zakwalifikować do dwóch lub więcej kategorii. Jeżeli z objaśnień dla poszczególnych kategorii nie wynika pierwszeństwo dla danej kategorii o możliwości przetwarzania w określonym typie chmury obliczeniowej decyduje analiza poszczególnego systemu.  Brak oznaczenia w postaci X w kolumnie „brak wykorzystania chmury” oznacza, że system powinien być utrzymywany przy wykorzystaniu usług chmurowych (zasada pierwszeństwa chmury), a rodzaj dopuszczalnych usług chmurowych zależy od oznaczenia w tabeli.  Oznaczenie X w kolumnie „brak wykorzystania Rządowej Chmury Obliczeniowej” i kolumnie „Rządowa Chmura Obliczeniowa” oznacza możliwość utrzymywania systemu w ramach Dedykowanej Infrastruktury Teleinformatycznej (DIT) lub w Rządowej Chmurze Obliczeniowej w zależności od wyniku przeprowadzonej analizy.  Analogicznie zasady mają zastosowanie w przypadku pozostałych klasyfikacji. | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Lp.** | **Kategoria systemów** | **Brak możliwości skorzystania z usług chmurowych określonych w uchwale[[1]](#footnote-2)**  **(konieczność korzystania z Dedykowanej Infrastruktury Teleinformatycznej - DIT)** | **Rządowa Chmura Obliczeniowa** | **Publiczna Chmura Obliczeniowa w jurysdykcji krajowej** | **Publiczna Chmura Obliczeniowa w jurysdykcji państwa UE** | **Objaśnienia dla poszczególnych kategorii** |
|  | Systemy teleinformatyczne, w których są przetwarzane informację niejawne | x |  |  |  | Dotyczy to systemów, które wprost z przepisów ustaw są określone, jako systemy niejawne lub w stosunku do których uprawnione organy wskazały, iż są w nich przetwarzane informacje niejawne. |
|  | Systemy teleinformatyczne służb specjalnych w rozumieniu art. 11 ustawy o ABW i AW | x |  |  |  | Dotyczy wszystkich systemów służb specjalnych (niezależnie od tego, czy są w nich przetwarzane informacje niejawne), nawet jeżeli te systemy spełniają kryteria kwalifikujące do innej kategorii systemów. Kategoria ta nie obejmuje systemów, o których mowa w pkt 6. |
|  | Systemy teleinformatyczne wykorzystywane do prowadzenia rejestrów[[2]](#footnote-3), ewidencji[[3]](#footnote-4) oraz innych baz danych[[4]](#footnote-5) przez organy publiczne na podstawie przepisów prawa Unii Europejskiej lub na podstawie zawartych umów międzynarodowych. | X | X | X | X | W zależności od dokonanej analizy przez podmiot odpowiedzialny za system teleinformatyczny. |
|  | Systemy teleinformatyczne wykorzystywane do prowadzenia rejestrów, ewidencji oraz innych baz danych, przez organy wymiaru sprawiedliwości, służby lub formacje umundurowane oraz służby odpowiedzialne za zapewnienie porządku i bezpieczeństwa publicznego, z wyłączeniem służb wskazanych w pkt 5. | X | X |  |  | W zależności od dokonanej analizy przez podmiot odpowiedzialny za system teleinformatyczny. |
|  | System teleinformatyczne wykorzystywane do prowadzenia rejestrów, ewidencji oraz innych baz danych, prowadzone przez straże gminne, straże leśne. |  | X | X | X | O możliwości przetwarzania w danej możliwej chmurze obliczeniowej decyduje wynik analizy. |
|  | Systemy teleinformatyczne wykorzystywane do prowadzenia rejestrów, ewidencji oraz innych baz danych, przez organy publiczne, w których **przetwarzane są dane referencyjne**, wykorzystywane w funkcjonalnościach przewidzianych w art. 35 ustawy o ABW i AW[[5]](#footnote-6) | X | X |  |  | W zależności od dokonanej analizy przez podmiot odpowiedzialny za system teleinformatyczny. Analiza powinna uwzględniać możliwość rozdzielenia komponentów systemów teleinformatycznych, w których realizowane są funkcjonalności ABW i AW.  Nie obejmuje systemów teleinformatycznych, które nie wchodzą w zakres podmiotowy uchwały oraz systemów podmiotów prywatnych np. systemów teleinformatycznych przy użyciu których wydawane są środki identyfikacji elektronicznej |
|  | Systemy teleinformatyczne wykorzystywane do prowadzenia rejestrów, ewidencji oraz innych baz danych, zawierające dane referencyjne inne niż wskazane w pkt. 6 |  | X | X |  | O możliwości przetwarzania w danej możliwej chmurze obliczeniowej decyduje wynik analizy. |
|  | Systemy teleinformatyczne wykorzystywane do prowadzenia rejestrów, ewidencji oraz innych baz danych, w których są przetwarzane szczególne kategorie danych osobowych w rozumieniu art. 9 i 10 RODO. |  | X | X | X | O możliwości przetwarzania w danej możliwej chmurze obliczeniowej decyduje wynik analizy.  O ile systemy mieszczą się w kategoriach 3-6, klasyfikacja powinna być dokonana w oparciu o kryteria z pkt 3-6. |
|  | Systemy teleinformatyczne wykorzystywane do prowadzenia rejestrów, ewidencji oraz innych baz danych innych niż w pkt 3-7 jeżeli prowadzone są one na podstawie przepisów powszechnie obowiązujących a w szczególności wpisy do tych rejestrów ewidencji i baz danych mają skutek prawny. |  | X | X |  | O możliwości przetwarzania w danej możliwej chmurze obliczeniowej decyduje wynik analizy. Skutek prawny systemu rozumiany jest jako skutek konstytutywny jak i deklaratoryjny. |
|  | Systemy teleinformatyczne wykorzystywane do prowadzenia rejestrów, ewidencji oraz innych baz danych innych niż w pkt 1-7 jeżeli prowadzone są one przez podmioty na własny użytek i mają charakter wspomagający. |  | X | X | X | O możliwości przetwarzania w danej możliwej chmurze obliczeniowej decyduje wynik analizy.  Kategoria obejmuje systemy do prowadzenia rejestrów, ewidencji oraz innych baz danych, których nie reguluje prawo powszechnie obowiązujące a organ stworzył je w celu ulepszenia realizacji zadań publicznych np. spisy, wewnętrzne ewidencje lub bazy danych, na podstawie których na bieżąco realizuje określone prawem zadania publiczne. |
|  | Systemy teleinformatyczne wykorzystywane do udostępniania informacji publicznej lub udostępniania informacji sektora publicznego do ponownego wykorzystania (otwarte dane) |  | X | X | X | Kategoria obejmuje samodzielne systemy teleinformatyczne nie będące częścią systemów należących do kategorii 4-9.  Pod warunkiem zakwalifikowania podmiotu odpowiedzialnego za system do zakresu podmiotowego uchwały. |
|  | Systemy teleinformatyczne, w ramach których świadczone są usługi elektroniczne organów administracji publicznej. |  | X | X | X | O możliwości przetwarzania w danej możliwej chmurze obliczeniowej decyduje wynik analizy.  Kategoria obejmuje systemy teleinformatyczne:  - przeznaczone do udostępniania danych z rejestrów, ewidencji lub innych baz danych w drodze zapytań jednostkowych,  - transakcyjne, wykorzystujące dane pochodzące z rejestrów, ewidencji lub innych baz danych,  - pozwalające na wnoszenie do organów administracji publicznej, oraz doręczenia przez te organy, dokumentów stanowiących elementy postępowań administracyjnych, oraz innych, przewidzianych w przepisach prawa, czynności realizowanych przez te organy. |
|  | Systemy teleinformatyczne klasy służące do prowadzenia wewnętrznego elektronicznego obiegu dokumentacji/ elektronicznego zarządzania dokumentacją. |  | X | X | X | O możliwości przetwarzania w danej możliwej chmurze decyduje wynik analizy. |
|  | Systemy teleinformatyczne klasy ERP i CRM itp. |  | X | X | x | O możliwości przetwarzania w danej możliwej chmurze decyduje wynik analizy. |
|  | Pozostałe systemy teleinformatyczne. |  | X | X | x | Kategoria obejmuje inne systemy świadczące usługi obsługowe na wewnętrzny użytek, zapewniające komunikacje np. systemy ekstranetowe, intranetowe lub poczty elektronicznej. |

1. Kryteria analizy możliwości korzystania przez dany system z usług przetwarzania w Rządowej Chmurze Obliczeniowej lub w określonej publicznej chmurze obliczeniowej.

Analiza podmiotu odpowiedzialnego za system teleinformatyczny wykorzystywany do prowadzenia rejestrów, ewidencji oraz innych baz danych oraz pozostałych systemów służy dokonaniu oceny optymalnego i bezpiecznego wykorzystania usług chmurowych ww. kategorii. Analizy należy dokonywać w ramach dostępnych chmur obliczeniowych określonych w tabeli: „Kategorie systemów teleinformatycznych, które mogą korzystać z usług przetwarzania w Rządowej Chmurze Obliczeniowej lub w publicznych chmurach obliczeniowych wraz z oznaczeniem możliwości utrzymania w Rządowej Chmurze Obliczeniowej lub w publicznych chmurachobliczeniowych”**.** W przypadku gdy w wyniku analizy stwierdzona zostanie dopuszczalność utrzymania danego systemu w Rządowej Chmurze Obliczeniowej lub w określonej publicznej chmurze obliczeniowej, system powinien zostać ulokowany w odpowiedniej chmurze. Niekorzystanie w powyższym przypadku z usług chmurowych wymaga uzasadnienia.Do przeprowadzenia analizy zobowiązany jest podmiot odpowiedzialny za system teleinformatyczny.

W przypadku systemów teleinformatycznych, które mogą korzystać z usług przetwarzania w Rządowej Chmurze Obliczeniowej lub w publicznych chmurachobliczeniowych analiza powinna uwzględniać, w szczególności czy:

1. system jest wykorzystywany w obszarach o szczególnym znaczeniu dla realizacji zadań państwa związanych z ewidencją ludności, sprawami karnymi lub karno-skarbowymi, prawami majątkowymi obywateli, ewidencją nieruchomości, praw do nieruchomości oraz pojazdów i kierowców,
2. system teleinformatyczny zasila danymi systemy referencyjne Państwa,
3. czy korzysta z systemów referencyjnych państwa,
4. skutki prawne wpisów i danych zawartych w systemach teleinformatycznych mają wpływ na sytuację prawną (w tym prawno-majątkową) osób lub podmiotów.

Analiza powinna zostać przeprowadzona o oparciu o analizę ryzyka.

Kryteria do przeprowadzenia szacowania ryzyka, obejmują co najmniej następujące atrybuty:

1. poufność informacji, w zakresie której należy przeanalizować co najmniej:
   1. czy naruszenie poufności (np. nieautoryzowane ujawnienie) danych będzie uniemożliwiało lub będzie powodowało istotne zagrożenie dla realizacji szczególnych zadań państwa;
2. integralność informacji, w zakresie której należy przeanalizować co najmniej:
   1. czy naruszenie integralności (np. nieautoryzowane zmodyfikowanie) danych będzie uniemożliwiało lub będzie powodowało istotne zagrożenie dla realizacji szczególnych zadań państwa;
   2. czy system jest systemem referencyjnym dla innych systemów, w tym czy modyfikacja danych w systemie może spowodować / ma wpływ na dane przetwarzane w innym systemie o szczególnym znaczeniu dla realizacji zadań państwa;
   3. czy wpis lub zmiana wpisów w systemie powoduje bezpośrednie skutki prawne;
3. dostępność informacji, w zakresie której należy przeanalizować co najmniej:
   1. czy naruszenie dostępności danych (np. brak dostępu do danych) będzie uniemożliwiało lub będzie powodowało istotne zagrożenie dla realizacji szczególnych zadań państwa;
   2. czy w celu realizacji szczególnych zadań państwa system powinien funkcjonować również w przypadku braku świadczenia usług przez dostawców komercyjnych (np. w przypadku upadłości lub zaprzestania świadczenia usług);
   3. czy system powinien funkcjonować prawidłowo niezależnie od funkcjonowania na rynku dostawców komercyjnych;

Decyzja o wykorzystaniu usług chmury obliczeniowej wskazanej w wyniku klasyfikacji należy do właściciela klasyfikowanego systemu teleinformatycznego.

**UZASADNIENIE**

Celem projektowanej uchwały jest wdrożenie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa”, która obejmuje:

1. budowę, rozwój i utrzymanie prywatnej chmury obliczeniowej administracji publicznej (Rządowej Chmury Obliczeniowej);
2. budowę, rozwój i utrzymanie Rządowego Klastra Bezpieczeństwa;
3. zapewnienie podmiotom administracji publicznej możliwości nabywania usług przetwarzania w publicznych chmurach obliczeniowych od wykonawców wybranych przez centralnego zamawiającego lub w zamówieniu wspólnym;
4. zapewnienie funkcjonowania systemu teleinformatycznego wspomagającego zarządzanie usługami przetwarzania w Rządowej Chmurze Obliczeniowej i w publicznych chmurach obliczeniowych, zwanego dalej „Systemem Zapewnienia Usług Chmurowych”;
5. określenie przez ministra właściwego do spraw informatyzacji Katalogu Wymagań Bezpieczeństwa Systemów Teleinformatycznych.

Inicjatywa WIIP jest odpowiedzią na decyzję Prezesa Rady Ministrów o pilnej realizacji Rządowego Klastra Bezpieczeństwa. W toku prac analitycznych zdecydowano o zmianie pierwotnej koncepcji i przyjęciu podejścia bardziej efektywnego kosztowo, tj. ponosząc koszty inicjalne, które pozwolą na szybsze udostępnienie środowisk i usług dla odbiorców niż gdyby poszczególne jednostki zaspokajały zapotrzebowanie na infrastrukturę i usługi indywidualnie.

Podjęcie niniejszej uchwały jest również konsekwencją ustaleń Komitetu Ekonomicznego Rady Ministrów z dnia 25 września 2018 roku, kiedy to Komitet udzielił pozytywnej rekomendacji dla założeń inicjatywy.

W oparciu o dane gromadzone w ramach inwentaryzacji w Systemie Inwentaryzacji Systemów Teleinformatycznych rozpoznano zakres obejmujący wspólne dla większości podmiotów administracji rządowej problemy. Typowa infrastruktura IT urzędu:

* składa się z niewielkiej liczby serwerów i urządzeń pamięci masowych, zwykle o  niedostatecznym poziomie zabezpieczeń,
* nie posiada serwerowni zapasowej,
* generuje koszty utrzymania związane z zapewnieniem własnego łącza do Internetu, ochrony ruchu sieciowego, systemów zarządzania, zabezpieczenia danych, podtrzymania zasilania, chłodzenia.

Analogiczną diagnozę przeprowadzono w oparciu o dane dotyczące typowych projektów IT finansowanych z funduszy europejskich, również w oparciu o dane dotyczące projektów realizowanych w minionej perspektywie finansowej. Wynikiem pracy były następujące wnioski:

* duże zakupy infrastruktury realizowane były głównie przy okazji realizacji projektu: serwery, macierze, wyposażenie serwerowni, łącza, elementy bezpieczeństwa,
* moc i pojemność infrastruktury zaplanowano pod obciążenie prognozowane na końcu okresu trwałości, co podnosiło inicjalny koszt inwestycji,
* zakup infrastruktury realizowany był jako pierwszy, rozpoczynając bieg okresu amortyzacji sprzętu przed jego faktycznym wykorzystaniem.

Mając na uwadze powyższe zagadnienia realizacja Inicjatywy WIIP stanowi odpowiedź na potrzeby administracji rządowej, poprzez eliminację lub znaczne zmniejszenie obciążeń związanych z aspektami technicznymi na rzecz uwolnienia zasobów kadrowych do realizacji celów merytorycznych.

Główne korzyści dla państwa to:

* poprawa bezpieczeństwa przetwarzania danych i świadczenia usług elektronicznych w administracji rządowej,
* trwałe obniżenie kosztów stałych przetwarzania danych – w długiej perspektywie o ponad 1 mld zł rocznie,
* podniesienie efektywności wydatkowania środków w projektach zawierających elementy infrastruktury IT – poprawa sięgająca 50%,
* skrócenie czasu realizacji nowych przedsięwzięć informatycznych przez szybsze udostępnianie wymaganej infrastruktury IT – realizacja pilnych potrzeb w terminach 1-2 tygodni, zamiast wielu miesięcy,
* zniesienie części barier technicznych dla interoperacyjności systemów działających w oparciu o usługi chmury obliczeniowej.

Wprowadzone zostają pojęcia Rządowej Chmury Obliczeniowej, publicznej chmury obliczeniowej, operatora Rządowej Chmury Obliczeniowej, Rządowego Klastra Bezpieczeństwa (RKB), operatora RKB, jak również zapewnienie podmiotom administracji publicznej możliwości nabywania usług przetwarzania w publicznych chmurach obliczeniowych od wykonawców wybranych przez centralnego zamawiającego lub w zamówieniu wspólnym.

Rządowa Chmura Obliczeniowa obejmuje usługi typu IaaS, PaaS oraz SaaS ujęte w katalogu, świadczone na rzecz podmiotów administracji publicznej. Systemy teleinformatyczne, które powinny znaleźć się w Rządowej Chmurze Obliczeniowej zostaną zakwalifikowane zgodnie z kryteriami określonymi w załączniku nr 2 do uchwały.

Uchwała przewiduje ponadto, iż minister właściwy do spraw informatyzacji, w porozumieniu z ministrem właściwym do spraw wewnętrznych, Ministrem Obrony Narodowej oraz Ministrem – Koordynatorem Służb Specjalnych przygotuje, w terminie dwóch miesięcy od dnia wejścia w życie uchwały, Katalog Wymagań Bezpieczeństwa Systemów Teleinformatycznych (KWBST), tj. zestaw wymagań bezpieczeństwa funkcjonowania systemów teleinformatycznych administracji publicznej.

Operatorem Rządowej Chmury Obliczeniowej jest minister właściwy do spraw informatyzacji, który odpowiedzialny jest za budowę, rozwój i utrzymanie Rządowej Chmury Obliczeniowej. Zadanie to w imieniu ministra może zostać powierzone jednostce przez niego nadzorowanej. Jednostki sektora finansów publicznych posiadające już systemy teleinformatyczne lub tworzące takie systemy, zainteresowane migracją na Rządową Chmurę Obliczeniową wnioskować będą do ministra właściwego do spraw informatyzacji o zawarcie porozumienia określającego szczegółowe warunki takiej migracji oraz prawa i obowiązki stron w związku ze świadczeniem konkretnego zakresu usług przetwarzania w oparciu o infrastrukturę Rządowej Chmury Obliczeniowej. Wzór porozumienia zostanie udostępniony przez ministra właściwego do spraw informatyzacji. Porozumienia pomiędzy jednostkami a ministrem właściwym do spraw informatyzacji nie będą powodować dodatkowych skutków finansowych. Jednostka, której system zostanie migrowany na Rządową Chmurę Obliczeniową dokona blokady środków, które miała zaplanowane w swoim budżecie na rozwój i utrzymanie systemu. Środki z powyższych blokad zostaną ujęte w planowaniu budżetowym na 2020 i kolejne lata w rezerwie celowej przeznaczonej na utrzymanie i rozwój Rządowej Chmury Obliczeniowej. W przypadku pierwszych migracji, z uwagi na brak możliwości utworzenia rezerwy celowej na 2019 r., środki na utrzymanie Rządowej Chmury Obliczeniowej zostaną przekazane ministrowi właściwemu do spraw informatyzacji zgodnie z art. 155 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych lub zapewnione w części 27 budżetu państwa – Informatyzacja.

W przypadku projektowania systemów teleinformatycznych przez administrację publiczną po wejściu w życie uchwały, powinny być one poddane klasyfikacji odnośnie możliwości korzystać z usług przetwarzania w Rządowej Chmurze Obliczeniowej lub publicznych chmurach obliczeniowych, której kryteria określone są w załączniku nr 2 do uchwały. Następnie systemy teleinformatyczne spełniające kryteria klasyfikacji do korzystania z usług przetwarzania w Rządowej Chmury Obliczeniowej powinny uzyskać opinię ministra właściwego do spraw informatyzacji w zakresie możliwości wykorzystania Rządowej Chmury Obliczeniowej.

Organy administracji rządowej będące posiadaczami Centrów Przetwarzania Danych (CPD) będą nawiązywać współpracę w ramach Inicjatywy WIIP z operatorem Rządowej Chmury Obliczeniowej poprzez zawarcie porozumienia. Warunkiem koniecznym będzie pisemne oświadczenie o spełnieniu minimalnych wymagań organizacyjnych i technicznych dla posiadacza CPD zawartych w załączniku nr 1 do uchwały.

W przypadku, gdy konieczne będzie wykorzystanie sieci teletransmisji na potrzeby Rządowej Chmury Obliczeniowej, zawierane będzie porozumienie między właściwym operatorem sieci, a ministrem właściwym do spraw informatyzacji, określające zasady i sposób wykorzystania sieci teletransmisji na potrzeby Rządowej Chmury Obliczeniowej, a ocena spełnienia minimalnych wymagań organizacyjnych i technicznych w zakresie możliwości przyłączania do sieci teletransmisji będzie każdorazowo uzgadniana między stronami porozumienia.

Właściwa ochrona teleinformatyczna zasobów przetwarzanych w Rządowej Chmurze Obliczeniowej jest krytyczna dla zapewnienia bezpieczeństwa teleinformatycznego, poufności oraz integralności danych. Realizacja tego zadania wiąże się z zapewnieniem zasobów na dwóch poziomach:

1. właściwego sprzętu i oprogramowania dla zapewnienia odpowiedniego technicznie poziomu ochrony teleinformatycznej;
2. specjalizowanej organizacji w formie SOC/NOC dla zapewnienia wiedzy oraz adekwatnego sposobu reagowania związanego z zagrożeniami teleinformatycznymi i ich następstwami.

RKB, jako system bezpieczeństwa zapewniał będzie odpowiedni poziom ochrony w newralgicznych punktach styku Rządowej Chmury Obliczeniowej zarówno z sieciami publicznymi jak i z sieciami odbiorców usług przetwarzania.

Budowę i rozwój RKB minister właściwy do spraw informatyzacji może powierzyć jednostce przez niego nadzorowanej lub innemu wybranemu podmiotowi.

Inicjatywa WIIP obejmuje również budowę i utrzymanie systemu teleinformatycznego pod nazwą System Zapewnienia Usług Chmurowych, wspomagającego zarządzanie usługami przetwarzania w chmurze świadczonymi dla podmiotów administracji publicznej. Zgodnie z przyjętymi założeniami system ten obsługiwał będzie proces zamawiania, dostarczania i rozliczania usług przetwarzania w Rządowej Chmurze Obliczeniowej oraz usług przetwarzania w publicznych chmurach obliczeniowych. Za funkcjonowanie Systemu odpowiedzialny będzie minister właściwy do spraw informatyzacji.

Udostępnione w Systemie Zamawiania Usług Chmurowych katalogi usług będą podlegały cyklicznej aktualizacji w przypadku Rządowej Chmury Obliczeniowej, natomiast dla katalogu usług przetwarzania w publicznych chmurach obliczeniowych aktualizacje zależeć będą od postępowań zakupowych realizowanych przez centralnego zamawiającego lub w formule zamówień wspólnych.

Wdrożenie publicznej chmury obliczeniowej w proponowanym kształcie pozwoli na przywrócenie kontroli państwa nad bezpieczeństwem tego rodzaju usług, które obecnie są kupowane bez określonych standardów bezpieczeństwa.

Celem publicznej chmury obliczeniowej jest wypełnienie luki w zakresie dostaw usług infrastrukturalnych dla administracji publicznej. Projekt Systemu Zapewniania Usług Chmurowych ma na celu obsługę procesu realizacji zamówień publicznych na dostawę wybranego katalogu usług. Dostawcy publicznej chmury obliczeniowej muszą spełniać wymagania określone w ogłoszeniu na zamówienie, w tym w zakresie sposobu przetwarzania danych. Dostawcy będą weryfikowani przy każdym zawartym zamówieniu w ramach umów wykonawczych. Dodatkowo zgodnie z klasyfikacją danych i systemów przedstawionych w projekcie uchwały z usług chmury publicznej będzie można korzystać w ograniczonym zakresie (dane publiczne, systemu o niekrytycznym znaczeniu).

Projektowana uchwała wskazuje model finansowania Inicjatywy WIIP, zgodnie z którym środki na realizację pochodzić będą z rezerwy celowej, o której uruchomienie będzie wnioskował minister właściwy do spraw informatyzacji.

Mechanizm zapotrzebowania na Rządową Chmurę Obliczeniową zakłada coroczne prognozowanie zapotrzebowania na usługi przetwarzania, co stanowić będzie mechanizm pozwalający na dostosowanie popytu do możliwości rozwoju usług chmurowych.

Załącznik nr 1 do uchwały opisuje minimalne wymagania względem CPD, które stanowią podstawę infrastruktury przetwarzania danych i gwarantują jej poprawne i bezpieczne działanie. Wymagania dla CPD – zarówno techniczne jak i organizacyjne – stanowią zbiór, którego spełnienie warunkuje ujednolicenie standardu bezpieczeństwa oraz jego odpowiedni poziom, dla systemów, które będą musiały być przetwarzane w ramach Rządowej Chmury Obliczeniowej.

Załącznik nr 2 opisuje zawiera kryteria klasyfikacji systemów teleinformatycznych, które mogą korzystać z usług przetwarzania w Rządowej Chmurze Obliczeniowej lub publicznych chmurach obliczeniowych.

Projekt uchwały 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.

Projekt uchwały nie będzie miał wpływu na działalność mikroprzedsiębiorców, małych i średnich przedsiębiorców.

Projekt uchwały został umieszczony w Biuletynie Informacji Publicznej na stronie internetowej Ministerstwa Cyfryzacji.

Uchwała wchodzi w życie z dniem następującym po dniu ogłoszenia.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Nazwa projektu**  Projekt uchwały Rady Ministrów w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa” (WIIP)  **Ministerstwo wiodące i ministerstwa współpracujące**  Ministerstwo Cyfryzacji  Ministerstwo Finansów  Ministerstwo Spraw Wewnętrznych i Administracji  **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu**  Karol Okoński, Sekretarz Stanu w Ministerstwie Cyfryzacji  **Kontakt do opiekuna merytorycznego projektu**  Joanna Baranowska - Zastępca Dyrektora Departamentu Systemów Państwowych w Ministerstwie Cyfryzacji,  tel. 22 245-55-21, e-mail: joanna.baranowska@mc.gov.pl | | | | | | | | | | | | | | | | | **Data sporządzenia 11.07.2019**  **Źródło:**  Decyzja PRM/RM  **Nr w wykazie prac**  **ID232** | | | | | | | | | |
| **OCENA SKUTKÓW REGULACJI** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1. **Jaki problem jest rozwiązywany?** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Dynamika procesu transformacji cyfrowej administracji publicznej w Polsce, który przebiega stopniowo od kilkudziesięciu lat, jest nadal stosunkowo niska. Czas potrzebny na wdrożenie i ustabilizowanie rozwiązań informatycznych jest długi, zaś koszty wdrożeń i utrzymania infrastruktury rosną. Tymczasem aktualne trendy technologiczne i rynkowe zmierzają w kierunku świadczenia wysoce dostępnych i wydajnych usług realizowanych w modelu chmury obliczeniowej, które pozwalają na skokowy wzrost wydajności systemów informatycznych, przy jednoczesnej optymalizacji kosztów utrzymania oraz prowadzenia rozliczeń w oparciu o ich faktyczne wykorzystanie.  Jednostki administracji publicznej stoją przed pilną potrzebą podniesienia poziomu bezpieczeństwa przetwarzanych danych, wynikającą z rosnącej ilości i złożoności zagrożeń w obszarze cyberbezpieczeństwa. Jednocześnie wzrost kosztów utrzymania infrastruktury IT jednostek administracji publicznej wymaga ciągłej optymalizacji. Obecnie większość urzędów zapewnia infrastrukturę przetwarzania danych oraz dba o jej bezpieczeństwo we własnym zakresie. Takie podejście wiąże się z szeregiem problemów, m.in.:   * powszechnym brakiem planów awaryjnych i centrów zapasowych, ochrony fizycznej, niedostatkami kompetencji i infrastruktury cyberbezpieczeństwa, * wysokimi kosztami przetwarzania danych mimo stosunkowo niskich parametrów funkcjonalnych i poziomu bezpieczeństwa, * długim czasem dostarczania infrastruktury IT dla projektów, nierzadko przekraczającym rok, * inwestycjami w infrastrukturę charakteryzującymi się brakiem optymalizacji (przeskalowane, niedopasowane do rzeczywistych potrzeb), * rozproszonymi i źle zarządzanymi rezerwami mocy i przestrzeni dyskowych, powodującymi niski stopień wykorzystania sprzętu, * nieuzasadnionym wzrostem kosztów związanych z kolejnymi, nieskoordynowanymi zakupami infrastruktury na potrzeby nowych projektów (brak spójnej polityki zarządzania i planowania), * nieefektywnym zarządzaniem infrastrukturą teleinformatyczną państwa, wynikającym z rozproszonej pomiędzy różne jednostki odpowiedzialności za zarządzanie oraz powielaniem funkcjonalności (brak koordynacji, ram organizacyjnych i prawnych do współdzielenia), * brakiem zdefiniowanych spójnych zasad postępowania, standardów wykorzystania i utylizacji zużytego, przestarzałego technologicznie sprzętu komputerowego, nośników danych, ich przechowywania i ochrony, * brakiem interoperacyjności systemów, która może mieć negatywny wpływ na realizację e-usług, zarówno istniejących, jak i nowo tworzonych w ramach projektów, * brakiem spójnej informacji o infrastrukturze informatycznej funkcjonującej w państwie, * rozmyciem odpowiedzialności oraz obniżeniem poziomu bezpieczeństwa funkcjonowania podmiotów państwowych oraz danych i usług w nich funkcjonujących, * brakiem ustandaryzowania elementu własności autorskiej wykorzystywanego oprogramowania oraz utrzymania systemów teleinformatycznych administracji rządowej.   Powyższe ustalenia powstały na bazie doświadczeń zgromadzonych w toku konsultacji i spotkań organizowanych przez Ministerstwo Cyfryzacji z przedstawicielami jednostek administracji publicznej różnego szczebla oraz informacji przekazywanych w ramach prowadzonych cyklicznie badań ankietowych, realizowanych za pośrednictwem Systemu Inwentaryzacji Systemów Teleinformatycznych (SIST). | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1. **Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji i oczekiwany efekt** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Inicjatywa „Wspólna Infrastruktura Informatyczna Państwa” (WIIP) stanowi zespół działań zarządczych i projektowych prowadzący do zapewnienia bezpiecznej i optymalnej kosztowo infrastruktury przetwarzania systemów IT administracji publicznej w modelu gospodarki współdzielenia. Główne działania realizowane będą w trzech obszarach: zapewnieniu bezpiecznej dedykowanej sieci łączącej rządowe ośrodki przetwarzania danych i siedziby urzędów (Rządowy Klaster Bezpieczeństwa – RKB), udostępnieniu usług infrastrukturalnych IT w modelu chmury obliczeniowej w ramach Chmury Rządowej (prywatnej chmury obliczeniowej administracji publicznej) oraz wdrożenia Systemu Zamawiania Usług Chmurowych, który pozwoli na dostęp do usług Rządowej Chmury Obliczeniowej oraz zamówienie usług chmury publicznej, dostarczanych przez dostawców komercyjnych. Projekt dostarczy rozwiązanie ponadsektorowe, dostępne dla odbiorców z obszaru administracji rządowej oraz w przypadku usług chmury publicznej, dla wszystkich jednostek administracji.  Zgodnie z założeniem WIIP w każdym z powyższych obszarów powstawać będą w iteracyjny sposób kolejne wydania. W kontekście bezpieczeństwa kolejne wydania oznaczają wyższy standard bezpieczeństwa (RKB), a w przypadku usług – coraz bogatszy katalog usług.  Koncepcja WIIP zakłada wielostopniowe zabezpieczenie systemów teleinformatycznych podmiotów uczestniczących w WIIP przed zagrożeniami pochodzącymi z sieci publicznej. Uporządkowany i zorganizowany dostęp do ogólnodostępnej sieci Internet daje możliwość ochrony istotnych danych i serwisów rządowych przed atakami. Rozwiązanie takie nie eliminuje zagrożeń, jednak znacznie ogranicza potencjalne skutki ich materializacji oraz pozwala na koncentrację sił i środków dla zapewnienia bezpieczeństwa.  Wykorzystanie chmury obliczeniowej, jako docelowego środowiska informatycznego dla administracji publicznej umożliwi proaktywne świadczenie nowoczesnych usług informatycznych w odróżnieniu od dotychczasowego, reaktywnego modelu świadczenia usług IT.  Koncepcja realizacji WIIP w obszarze usług infrastrukturalnych zakłada zbudowanie środowiska chmury obliczeniowej w oparciu o istniejące centra danych i zaawansowane metody zapewnienia bezpieczeństwa. Katalog usług będzie poszerzany w ramach kolejnych wydań. W pierwszym etapie realizacji planowane jest udostępnianie usług infrastrukturalnych w modelu IaaS (Infrastructure as a Service). W późniejszych fazach realizacji pojawią się również usługi świadczone w modelu PaaS (Platform as a Service), a docelowo również SaaS (Software as a Service).  Realizacja usług powiązana jest z wykorzystywaniem oprogramowania systemów operacyjnych i aplikacji, co wymusza podpisanie nowych, ramowych umów z dostawcami oprogramowania. Z punktu widzenia dostawców oprogramowania komercyjnego, administracja państwowa powinna być postrzegana, jako pojedyncza organizacja. Dzięki temu uzyska ona najlepsze warunki cenowe (ze względu na bardzo duży wolumen sprzedaży) oraz będzie mogła uzgodnić najdogodniejsze i adekwatne dla administracji warunki licencyjne, pozwalające na reużycie i płacenie za rzeczywiste wykorzystanie.  Wykorzystywanie Internetu, jako efektywnego medium dostępowego do witryn administracji państwowej, poza potrzebą zapewnienia ich dostępności na określonym poziomie, wymusza konieczność stosowania skutecznych technologii zapewniających bezpieczeństwo, w tym integralność publikowanych informacji. W związku z tym administracja publiczna musi zmienić sposób patrzenia na architekturę swoich sieci, aby zmaksymalizować ich efektywność i skalowalność. Ważnym elementem funkcjonalności usługowej WIIP będzie możliwość zapewnienia niezakłóconej komunikacji pomiędzy instytucjami (jednostkami organizacyjnymi) uczestniczącymi w projekcie nawet w sytuacjach wystąpienia ataków na dużą skalę w publicznym Internecie.  Projekt uchwały zobowiązuje Radę Ministrów do tworzenia warunków umożliwiających współpracę instytucjom rządowym:   * optymalne wykorzystanie istniejących zasobów kosztownej infrastruktury przetwarzania (budynki serwerowni, poszycie sieciowe), * racjonalnego w skali państwa umiejscowienia zasobów przy jednoczesnej optymalnej kosztowo odpowiedzi na potrzeby związane z infrastrukturą przetwarzania danych, * lepszego wykorzystania efektów synergii, także związanych z posiadanymi kompetencjami IT w poszczególnych jednostkach.   Realizacja Inicjatywy WIIP przyniesie następujące efekty:   1. Podniesienie bezpieczeństwa przetwarzania danych w państwie w sposób optymalny kosztowo (wielokrotnie taniej niż potencjalny koszt podniesienia bezpieczeństwa w obecnym stanie rozproszenia CPD), 2. Systematyczne obniżanie kosztu stałego przetwarzania danych w państwie – od drugiego roku realizacji WIIP wynikające z migracji i wyłączania nieefektywnych ośrodków przetwarzania, 3. Racjonalizacja nakładów na infrastrukturę w nowych projektach – co najmniej dwukrotne obniżenie nakładów na infrastrukturę przy zachowaniu funkcjonalności, skróceniu czasu i podniesieniu bezpieczeństwa - od pierwszego roku projektu, 4. Optymalne wykorzystanie sprzętu, zasobów materialnych i niematerialnych, ludzkich i finansowych, 5. Standaryzacja usług infrastrukturalnych, oraz optymalizacja procesów utrzymania, 6. Efekt skali, który przyczyni się do obniżenia kosztów wytworzenia i utrzymania rozwiązań informatycznych oraz infrastruktury IT, 7. Niskobudżetowe (kilkakrotnie tańsze wobec realizacji wyspowej) zapewnienie mocy obliczeniowej i przestrzeni na dane w bezpiecznym środowisku, 8. Znaczna redukcja deficytu kadr i kompetencji związanych z cyberbezpieczeństwem i administracją infrastruktury poprzez konsolidację zarządzania i wykorzystanie efektu odmiejscowienia infrastruktury i możliwości tworzenia zespołów rozproszonych. | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1. **Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Rozwiązania chmury obliczeniowej dla administracji publicznej zostały wdrożone w takich państwach jak: Estonia, Niemcy, Francja czy Wielka Brytania. Poniżej przedstawiono najważniejsze z nich.  Estonia  Estonia jest jednym liderów nowoczesnych technologii w administracji publicznej na świecie. Jednym z najważniejszych elementów, stanowiących podstawę estońskiego systemu e-administracji jest uruchomione w 2001 r. rozwiązanie X-Road. Narzędzie to łączy usługi oraz bazy danych w sektorze publicznym i prywatnym, umożliwiając ich integrację na potrzeby świadczenia usług dostępnych w ramach portalu e-Estonia. Szacuje się, że 50% mieszkańców Estonii korzysta obecnie z X-Road poprzez portal eesti.ee.  Odpowiednikiem tego rozwiązania jest brytyjskia Government Secure Intranet (GSI).  Wielka Brytania  Wlk. Brytania podjęła w ostatnich latach intensywne działania na rzecz optymalizacji funkcjonowania administracji publicznej, w tym zarządzania infrastrukturą IT. Przejawem tej transformacji w zakresie podejścia do technologii cyfrowej były przyjęte przez rząd wytyczne oraz rozwiązania:   1. Government as a platform – rozwiązanie mające na celu ułatwienie tworzenia rozwiązań informatycznych przez administrację publiczną , oraz 2. Cloud First – wytyczna przyjęta przez rząd w 2013 roku, mająca na celu zmotywowanie podmiotów administracji publicznej do korzystania z rozwiązań chmurowych, w tym przede wszystkim z chmury publicznej.   Brytyjskie agencje wykonawcze Crown Commercial Service oraz Government Digital Service odpowiadają za wdrożenie modelu G-Cloud, w postaci Digital Marketplace, będącym portalem służącym do realizacji zamówień na usługi, w tym usługi chmurowe, przez jednostki administracji publicznej oraz wybrane jednostki spoza administracji publicznej. Zamówienia te realizowane są w wyniku zawarcia umów ramowych z dostawcami usług. Postępowanie ma transparentny i otwarty charakter, spełniając wymagania przetargu publicznego wg wymagań prawa brytyjskiego.  Republika Francuska  Rząd francuski sukcesywnie wprowadza doktrynę państwa w zakresie implementacji chmury obliczeniowej w procesie transformacji cyfrowej działań publicznych. Przedstawiciele administracji zauważają korzyści jakie niesie ze sobą technologia chmury obliczeniowej, tj. skalowalność, ponoszenie kosztów wg rzeczywistego wykorzystania, czy możliwość reużycia danych na dużą skalę. Doktryna (wytyczne) pt. „Wykorzystanie chmury w ramach administracji”, opracowana przez Narodową Agencję ds. Bezpieczeństwa Systemów Informatycznych (ANSSI), została zarekomendowana do stosowania w obrębie wszystkich jednostek administracji państwowej Framcji.  Doktryna dotycząca chmury obliczeniowej państwa ma na celu masowy rozwój wykorzystania tego modelu w obrębie administracji i ostatecznie uczynienie go normą. W tym celu udostępniona zostanie administracji oferta hybrydowa, złożona z trzech grup rozwiązań, do zastosowania w zależności od poziomu i wrażliwości przetwarzania danych, systemów lub aplikacji:   1. Grupa „chmura wewnętrzna”: czerpie korzyści z prac zrealizowanych w ostatnich latach, zmierzających do budowy trzech międzyresortowych forów chmurowych, które stopniowo stają się spójną ofertą "laaS" i "PaaS" opartą na OpenStack, dostępną dla wszystkich ministerstw za pośrednictwem interfejsów upraszczających ich wykorzystanie na dużą skalę. Wszystkie ministerstwa będą mogły wdrażać usługi w trybie "Saas" w oparciu o tę infrastrukturę. Ta grupa będzie uwzględniała wrażliwe dane, procesy i aplikacje oraz specyficzne potrzeby związane z infrastrukturą cyfrową, spełnia wymagania wewnętrzne w zakresie bezpieczeństwa danych i systemów informatycznych. 2. Grupa „chmura dedykowana”: opiera się na standardowej ofercie przetwarzania w chmurze oferowanej przez dostawców komercyjnych i zostanie udostępniona w celu znacznego ograniczenia migracji wraz z pierwszym wdrożeniem „chmury wewnętrznej”. Zostanie ona dostosowana do potrzeb administracji państwowej oraz oparta na dedykowanej infrastrukturze. Dostosowanie obejmować będzie integrację usługi nadzoru ANSSI, a także niektóre elementy platformy France Connect. Ten krąg będzie uwzględniać dane, procesy i aplikacje o niższej wrażliwości, ale wymagające pewnego poziomu bezpieczeństwa. 3. Trzecia grupa „chmura zewnętrzna”: zakłada udostępnienie katalogu komercyjnych ofert cloud computing dostępnych publicznie w Internecie (zwłaszcza Saas), przy realizacji procesu zakupowego przez UGAP, w celu jego ułatwienia. Ta grupa ukierunkowana jest na jak największej liczby ofert na usługi przetwarzania danych, procesów i aplikacji, dzięki którym będzie można korzystać z najnowocześniejszych i najlepszych rozwiązań innowacyjnych w tej dziedzinie. Oferta ta będzie musiała spełniać minimalne kryteria oraz warunki funkcjonalności, odtwarzania i bezpieczeństwa oraz podlegać certyfikacji zgodnie z ich charakterystyką, szczególnie pod względem bezpieczeństwa. | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1. **Podmioty, na które oddziałuje projekt** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Grupa | | | | Wielkość | | | | Źródło danych | | | | | | | Oddziaływanie | | | | | | | | | | | |
| Jednostki centralnej administracji rządowej | | | | 96 | | | | sejm.gov.pl | | | | | | | Regulacja daje podstawy do łączenia zasobów istniejących środowisk IT w celu świadczenia usług w modelu chmurowym. Jednostki administracji centralnej uzyskają dostęp do dedykowanych narzędzi wspierających proces zamawiania usług IT oraz automatyzacji postępowań przetargowych w tym zakresie. | | | | | | | | | | | |
| Jednostki rządowej administracji zespolonej | | | | 1 936 | | | | administracja.mswia.gov.pl | | | | | | | Regulacja daje podstawy do łączenia zasobów istniejących środowisk IT w celu świadczenia usług w modelu chmurowym. Jednostki administracji zespolonej uzyskają dostęp do dedykowanych narzędzi wspierających proces zamawiania usług IT oraz automatyzacji postępowań przetargowych w tym zakresie. | | | | | | | | | | | |
| Jednostki administracji samorządowej | | | | 2 807 | | | | administracja.mswia.gov.pl | | | | | | | Jednostki administracji samorządowej uzyskają dostęp do dedykowanych narzędzi wspierających proces zamawiania usług IT oraz automatyzacji postępowań przetargowych w tym zakresie. | | | | | | | | | | | |
| Przedsiębiorcy działający w sektorze usług IT | | | | 76 302 | | | | eurostat | | | | | | | Przedsiębiorcy świadczący usługi w modelu chmury obliczeniowej uzyskają dostęp do narzędzi wspierających proces oferowania usług IT w ramach częściowo zautomatyzowanych postępowań przetargowych. | | | | | | | | | | | |
| 1. **Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Założenia WIIP były przedmiotem konsultacji między Ministerstwem Cyfryzacji, Ministerstwem Finansów oraz Ministerstwem Spraw Wewnętrznych i Administracji, a także jednostkami zaangażowanymi w przygotowanie koncepcji technicznej i organizacyjnej przedsięwzięcia, do których należą Centralny Ośrodek Informatyki oraz Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy.  Koncepcja projektu Wspólnej Infrastruktury Państwa (WIP) została zaprezentowana przez Ministra Cyfryzacji na posiedzeniu Komitetu Ekonomicznego Rady Ministrów w dniu 25 września 2018 r., kiedy to Komitet udzielił pozytywnej rekomendacji dla prezentowanych założeń.  Projekt uchwały został poddany uzgodnieniom, konsultacjom publicznym i opiniowaniu.  Wszystkie zgłoszone uwagi zostały rozpatrzone, a w przypadku, gdy były uzasadnione – zostały uwzględnione. Dodatkowo z przedstawicielami Ministerstwa Obrony Narodowej, Ministerstwem Sprawiedliwości i Ministerstwa Finansów przeprowadzono uzgodnieniowe spotkania robocze.  Stanowisko do uwag zgłoszonych w ramach uzgodnień, konsultacji publicznych oraz opiniowania zostanie opublikowane w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Cyfryzacji. | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1. **Wpływ na sektor finansów publicznych** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| (ceny stałe z 2019 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** | | | 8,3 | | 99,4 | -38 | | | | -46,7 | -70,7 | | -71,9 | | | -15,8 | | -74,9 | | | -73,2 | | -79 | | -78,8 | -441,3 |
| budżet państwa – prognozowane oszczędności | | | 0 | | 0 | -102,2 | | | | -88,6 | -101,7 | | -103,1 | | | -104,7 | | -106,5 | | | -108,6 | | -111,1 | | -111,1 | -937,6 |
| budżet państwa-nakłady inwestycyjne, koszty operacyjne | | | 8,3 | | 99,4 | 64,2 | | | | 41,9 | 31,0 | | 31,2 | | | 88,9 | | 31,6 | | | 35,4 | | 32,1 | | 32,3 | 496,3 |
| 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** | | | 8,3 | | 99,4 | -38 | | | | -46,7 | -70,7 | | -71,9 | | | -15,8 | | -74,9 | | | -73,2 | | -79 | | -78,8 | -441,3 |
| budżet państwa | | | 8,3 | | 99,4 | -38 | | | | -46,7 | -70,7 | | -71,9 | | | -15,8 | | -74,9 | | | -73,2 | | -79 | | -78,8 | -441,3 |
| 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 | Budżet państwa (część 27 – Informatyzacja oraz rezerwa celowa) lub Europejski Fundusz Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa. | | | | | | | | | | | | | | | | | | | | | | | | | |
| Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń | Wartości nakładów inwestycyjnych oraz kosztów operacyjnych związanych z wdrożeniem komponentów WIIP została oszacowana na podstawie aktualnych ofert rynkowych. Komponenty techniczne oraz niezbędne zasoby organizacyjne zostały oszacowane osobno dla każdego ze strumieni: Rządowej Chmury Obliczeniowej, Rządowego Klastra Bezpieczeństwa oraz Systemu Zapewniania Usług Chmurowych. W przypadku Rządowej Chmury Obliczeniowej założono utrzymanie 30% rezerw w zakresie mocy obliczeniowej oraz dostępnej przestrzeni dyskowej (rok do roku), co pozwoli na skuteczne skalowanie rozwiązania oraz zarządzanie popytem ze strony administracji rządowej.  Źródła finansowania w przyjętej perspektywie przedstawiono w poniższej tabeli w podziale na kategorie wydatków (dane w mln zł):   |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | Źródła finansowania całkowitych kosztów inicjatywy WIIP | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | Łącznie (0-10) | | **Finansowane ze środków budżetu państwa** | 2,2 | 22,0 | 25,1 | 34,0 | 31,0 | 31,2 | 88,9 | 31,6 | 35,4 | 32,1 | 32,3 | **365,8** | | w tym wkład krajowy (POPC 2.1) | 1,3 | 17,2 | 8,7 | 1,7 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | **28,9** | | w tym cz. 27 - Informatyzacja (dotacja celowa) | 0,9 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | **0,9** | | w tym cz. 27 - Informatyzacja (rezerwa celowa) | 0,0 | 4,8 | 16,4 | 32,3 | 31,0 | 31,2 | 88,9 | 31,6 | 35,4 | 32,1 | 32,3 | **336,0** | | **Finansowane ze środków UE\*** | 7,4 | 94,6 | 47,8 | 9,6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | **159,4** | | w tym EFRR (POPC 2.1) | 7,4 | 94,6 | 47,8 | 9,6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | **159,4** | | **Razem** | 9,6 | 116,6 | 72,9 | 43,6 | 31,0 | 31,2 | 88,9 | 31,6 | 35,4 | 32,1 | 32,3 | **525,2** |   \* nakłady w wysokości 159,4 mln zł nie zostały ujęte w tab. 6.  W tabeli 6. Wpływ na sektor finansów publicznych nie ujęto nakładów inwestycyjnych, które będą finansowane ze środków Europejskiego Funduszu Rozwoju Regionalnego (POPC 2.1).  Poniżej przedstawiono źródła finasowania wydatków w latach 2019-2022 w ramach PO PC (w mln zł):   |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | Wydatki całkowite na realizację projektu WIIP (2019-2022) | |  |  |  |  | | Kategoria wydatków | 0 | 1 | 2 | 3 | Razem | | Sprzęt informatyczny | 0,1 | 71,9 | 48,1 | 4,4 | **124,5** | | Oprogramowanie | 0,0 | 23,4 | 4,7 | 3,0 | **31,1** | | Usługi informatyczne | 5,4 | 13,9 | 12,8 | 7,8 | **39,9** | | Wynagrodzenia osobowe | 2,8 | 3,5 | 3,5 | 1,8 | **11,6** | | Wydatki na pokrycie kosztów pośrednich | 0,3 | 0,6 | 0,7 | 0,6 | **2,2** | | Szkolenia | 0,1 | 0,2 | 0,1 | 0,0 | **0,4** | | Informacja i promocja | 0,1 | 0,3 | 0,4 | 0,6 | **1,4** | | Usługi wspomagające realizację projektu | 0,8 | 2,3 | 1,8 | 0,4 | **5,3** | | **Razem** | **9,6** | **116,1** | **72,1** | **18,6** | **216,4** |   Wydatki na realizację projektu WIIP (2019-2022) w podziale na źródła finansowania:   |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | Wydatki na realizację projektu WIIP finansowane w ramach POPC 2.1 | | | | | | | Kategoria wydatków | 0 | 1 | 2 | 3 | Razem | | | Sprzęt informatyczny | 0,1 | 71,9 | 35,6 | 0 | **107,6** | | | Oprogramowanie | 0 | 23,4 | 3,1 | 1,4 | **27,9** | | | Usługi informatyczne | 4,5 | 9,6 | 11,3 | 6,5 | **31,9** | | | Wynagrodzenia osobowe | 2,8 | 3,5 | 3,5 | 1,8 | **11,6** | | | Wydatki na pokrycie kosztów pośrednich | 0,3 | 0,6 | 0,7 | 0,6 | **2,2** | | | Szkolenia | 0,1 | 0,2 | 0,1 | 0 | **0,4** | | | Informacja i promocja | 0,1 | 0,3 | 0,4 | 0,6 | **1,4** | | | Usługi wspomagające realizację projektu | 0,8 | 2,3 | 1,8 | 0,4 | **5,3** | | | **Razem** | **8,7** | **111,8** | **56,5** | **11,3** | **188,3** | |   Wydatki na realizację projektu WIIP finansowane z cz. 27 - Informatyzacja (dotacja celowa)   |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | Kategoria wydatków | 0 | 1 | 2 | 3 | Razem | | Sprzęt informatyczny | 0 | 0 | 0 | 0 | **0,0** | | Oprogramowanie | 0 | 0 | 0 | 0 | **0,0** | | Usługi informatyczne | 0,9 | 0 | 0 | 0 | **0,9** | | Wynagrodzenia osobowe | 0 | 0 | 0 | 0 | **0,0** | | Wydatki na pokrycie kosztów pośrednich | 0 | 0 | 0 | 0 | **0,0** | | Szkolenia | 0 | 0 | 0 | 0 | **0,0** | | Informacja i promocja | 0 | 0 | 0 | 0 | **0,0** | | Usługi wspomagające realizację projektu | 0 | 0 | 0 | 0 | **0,0** | | **Razem** | **0,9** | **0,0** | **0,0** | **0,0** | **0,9** |   Wydatki na realizację projektu WIIP finansowane z rezerwy celowej WIIP   |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | Kategoria wydatków | 0 | 1 | 2 | 3 | Razem | | Sprzęt informatyczny | 0 | 0 | 12,5 | 4,4 | **16,9** | | Oprogramowanie | 0 | 0 | 1,6 | 1,6 | **3,2** | | Usługi informatyczne | 0 | 4,3 | 1,5 | 1,3 | **7,1** | | Wynagrodzenia osobowe | 0 | 0 | 0 | 0 | **0,0** | | Wydatki na pokrycie kosztów pośrednich | 0 | 0 | 0 | 0 | **0,0** | | Szkolenia | 0 | 0 | 0 | 0 | **0,0** | | Informacja i promocja | 0 | 0 | 0 | 0 | **0,0** | | Usługi wspomagające realizację projektu | 0 | 0 | 0 | 0 | **0,0** | | **Razem** | **0,0** | **4,3** | **15,6** | **7,3** | **27,2** |   Poniżej przedstawiono charakterystykę poszczególnych grup wydatków w fazie wdrażania projektu (lata 2019-2021).  **Sprzęt informatyczny**  Wydatki na infrastrukturę obejmują dostawy wyposażenia technicznego Rządowego Klastra Bezpieczeństwa (urządzenia sieciowe, serwery) oraz wyposażenie centrów obliczeniowych, niezbędne w procesie uruchomienia nowych usług infrastrukturalnych. W latach 2020-2021 przewidziano również wydatki na rozwój wdrażanych rozwiązań oraz utrzymania technicznego, finansowane z nowoutworzonej rezerwy celowej.  **Oprogramowanie**  Wydatki na oprogramowanie wynikają z przyjętych założeń architektonicznych i są ściśle powiązane dostawami infrastruktury. Ceny jednostkowe zostały wyznaczone na podstawie rozpoznania rynku.  **Wynagrodzenia osobowe**  Plan wynagrodzeń osobowych sporządzono w oparciu o niezbędne role projektowe oraz aktualne stawki wynagrodzeń obowiązujące w poszczególnych jednostkach zaangażowanych w realizację zadań związanych z inicjatywą WIIP. Plan zatrudnienia przedstawiają poniższa tabela (dane prezentowane jako FTE – ekwiwalent pełnego czasu pracy).   |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | Jednostka | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 | 2025 | 2026 | 2027 | 2028 | 2029 | | Ministerstwo Cyfryzacji | 13 | 13 | 13 | 13 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | | Naukowe i Akademickie Sieci Komputerowe PIB | 8 | 8 | 8 | 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | **Razem** | **22** | **19** | **19** | **19** | **5** | **5** | **5** | **5** | **5** | **5** | **5** |   Sumaryczną wartość planowanych wydatków związanych z zatrudnieniem personelu w latach 2019-2021 przedstawiono poniżej (dane w mln zł):  **Szkolenia**  Zaplanowano szkolenia personelu projektu w zakresie technologii stosowanych w centrach obliczeniowych oraz infrastrukturze bezpieczeństwa sieci i systemów. Rodzaj i zakres szkoleń wynikają ze specyfikacji przedstawionych przez NASK PIB, COI oraz zakresu ról projektowych i zadań niezbędnych do realizacji przewidzianych zadań. Nakłady są ściśle skorelowane z ilością etatów przedstawionych poprzednim punkcie.  **Usługi zewnętrzne**  W zakres usług wewnętrznych zaplanowanych do zakupu weszły:   * doradztwo prawne, * doradztwo techniczne, * usługi body leasing zgodnie z modelem ich pozyskania stosowanym przez Ministerstwo Cyfryzacji, * usługi w zakresie wytworzenia oprogramowania.   Ceny usług skalkulowano w oparciu o dane historyczne oraz wartości obecnie zawartych umów na świadczenie wybranego ich rodzaju.  **Promocja**  Usługi w zakresie promocji obejmują:   * konferencję podsumowująca projekt * konferencje promujące RKB * wielokanałową kampanię informacyjną (administracja publiczna) * plakat informacyjny * tablicę informacyjno-pamiątkową * dostosowanie serwisu internetowego.   Zadanie Promocja projektu wynika wprost zasad promowania projektów finansowanych ze środków Programu Operacyjnego Polska Cyfrowa.  **Koszty pośrednie**  Koszty pośrednie dotyczą kosztów osobowych personelu wspomagającego realizację projektu planowanego na lata 2019-2021.  **Koszty operacyjne w perspektywie 11 lat**  Koszty operacyjne zaplanowano w oparciu o dane dotyczące nakładów inwestycyjnych, konieczność utrzymania odpowiedniego poziomu zatrudnienia zespołów utrzymaniowych oraz prognozy nakładów odtworzeniowych. Prognozę tych kosztów przedstawiono w poniższej tabeli (dane w mln zł).   |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | Kategoria wydatków |  |  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | Łącznie (0-10) |  | | Nakłady odtworzeniowe |  |  | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 57,5 | 0,0 | 3,5 | 0,0 | 0,0 | 61,0 | | Utrzymanie techniczne i serwis |  |  | 0,0 | 0,0 | 0,0 | 5,8 | 5,8 | 5,8 | 5,8 | 5,8 | 5,8 | 5,8 | 5,8 | 46,4 | | Aktualizacja oprogramowania i odnowienia licencji |  |  | 0,0 | 0,0 | 0,0 | 2,2 | 2,2 | 2,2 | 2,2 | 2,2 | 2,2 | 2,2 | 2,2 | 17,6 | | Koszty usług eksperckich |  |  | 0,0 | 0,0 | 0,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 1,0 | 8,0 | | Wynagrodzenia osobowe |  |  | 0,0 | 0,0 | 0,0 | 0,8 | 0,8 | 0,8 | 0,8 | 0,8 | 0,8 | 0,8 | 0,8 | 6,4 | | Koszty pośrednie |  |  | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | 0,0 | | Energia elektryczna |  |  | 0,0 | 0,5 | 0,8 | 0,9 | 0,9 | 0,9 | 0,9 | 0,9 | 0,9 | 0,9 | 0,9 | 8,5 | | Koszty utrzymania systemów (in-house COI) |  |  | 0,0 | 0,0 | 0,0 | 14,3 | 20,3 | 20,5 | 20,7 | 20,9 | 21,2 | 21,4 | 21,6 | 160,9 | | **Razem** |  |  | **0,0** | **0,5** | **0,8** | **25,0** | **31,0** | **31,2** | **88,9** | **31,6** | **35,4** | **32,1** | **32,3** | **308,8** |   Źródłem finansowania ww. kosztów będzie rezerwa celowa WIIP. Średnio w latach 2022-2029 koszty rocznego utrzymania (z uwzględnieniem nakładów odtworzeniowych) wyniosą 28,1 mln zł.  Zaplanowano jednorazowe otworzenie wyposażenia zakupionego w ramach dostawy inicjalnej w latach 2019-2020 oraz stopniowe odtwarzanie infrastruktury rozbudowywanej w kolejnych latach. Dla wszystkich składników majątku przyjęto 5-letni okres odtworzeniowy.  Koszty utrzymania infrastruktury (maintanace) skalkulowano w wysokości 10% nakładów inwestycyjnych. Koszty aktualizacji oprogramowania skalkulowano na poziomie 8% wydatków na zakup.  **Prognoza generowanych oszczędności**  Prognozowane oszczędności ujęte w pozycji dochody budżetu państwa zostały oszacowane na podstawie zebranych danych inwentaryzacyjnych oraz prognozy możliwości przeniesienia wybranych zasobów do wspólnej chmury rządowej oraz wyłączenia z użytkowania zbędnych zasobów. W zakresie oszczędności ujęto również kwestię redukcji ilości postępowań o udzielenie zamówienia publicznego na dostawę usług chmury obliczeniowej w administracji publicznej oraz redukcji czasu potrzebnego na uruchomienie nowych środowisk IT w oparciu o usługi chmury obliczeniowej. Wyszczególniono następujące strumienie finansowe generujące oszczędności:   1. Budowa i rozbudowa RKB – uniknięcie alternatywnego kosztu budowy centrów bezpieczeństwa SOC/NOC przez poszczególne jednostki administracji rządowej; 2. Usługi centralne WIIP na rzecz nowych projektów – oszczędności wynikające z redukcji nakładów inwestycyjnych oraz kosztów utrzymania infrastruktury dla nowych projektów finansowanych z POPC oraz wydatków odtworzeniowych dla infrastruktury zakupionej w ramach POIG w latach 2013-2015; 3. Konsolidacja i wyłączenie nieefektywnych serwerowni – kalkulacja oszczędności z wyłączenia w latach 2019-2021 sześciu obiektów o pow. poniżej 50 m2 i migracji systemów do WIIP; 4. System ZUCH – obejmuje oszczędności czasu pracowników administracji związanego z uproszczeniem procesu zakupu usług chmurowych oraz redukcję kosztów inwestycji w infrastrukturę i utrzymanie systemów IT wynikająca z zakupu usług chmury publicznej.   Podane założenia mogą ulec zmianie ze względu na trwającą aktualizację danych gromadzonych w ramach systemu SIST oraz analizy ekonomiczne związane z opracowaniem studium wykonalności projektu planowanego do realizacji w ramach POPC. Tym samym niniejszy dokument będzie musiał zostać poddany aktualizacji. | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1. **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 2019 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 | | | | | | | Przedsiębiorcy świadczący usługi w modelu chmury obliczeniowej uzyskają dostęp do narzędzi wspierających proces oferowania usług IT w ramach częściowo zautomatyzowanych postępowań przetargowych. | | | | | | | | | | | | | | | | | |
| sektor mikro-, małych i średnich przedsiębiorstw | | | | | | | Przedsiębiorcy świadczący usługi w modelu chmury obliczeniowej uzyskają dostęp do narzędzi wspierających proces oferowania usług IT w ramach częściowo zautomatyzowanych postępowań przetargowych. | | | | | | | | | | | | | | | | | |
| rodzina, obywatele oraz gospodarstwa domowe | | | | | | | brak | | | | | | | | | | | | | | | | | |
| Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń | Projekt uchwały 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. | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1. **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 | | | | | | | | | | | | | | | |
| Komentarz:  Wprowadzane rozwiązania nie wiążą się ze zmianą obciążeń regulacyjnych. | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1. **Wpływ na rynek pracy** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Realizacja programu będzie się wiązać z koniecznością utworzenia nowych miejsc pracy związanych z przygotowaniem i implementacją projektu chmury rządowej, a także z utworzeniem dedykowanych jednostek cyberbezpieczeństwa (SOC/NOC).  W przypadku sektora przedsiębiorstw skutkiem realizacji programu może być redukcja zatrudnienia w działach sprzedaży, związana z uruchomieniem dedykowanego kanału zamawiania usług chmury obliczeniowej w ramach systemu Zamawiania Usług Chmurowych dedykowanego administracji publicznej. | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1. **Wpływ na pozostałe obszary** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| środowisko naturalne  sytuacja i rozwój regionalny  inne: … | | | | | | | demografia  mienie państwowe | | | | | | | | | | | | | informatyzacja  zdrowie | | | | | | |
| Omówienie wpływu | Projektowane rozwiązania stanowią istotną zmianę z procesie realizacji zamówień na usługi IT dla jednostek sektora finansów publicznych. Stanowią również kolejny krok na drodze do adaptacji rozwiązań chmury obliczeniowej w administracji publicznej. Ze względu na potencjalnie szerokie oddziaływanie programu planowane korzyści w postaci redukcji kosztów pozyskania i utrzymania infrastruktury informatycznej obejmą nie tylko administrację rządową, lecz również administrację samorządową, przyczyniając się tym samym do stymulacji rozwoju regionalnego. | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1. **Planowane wykonanie przepisów aktu prawnego** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Uchwała wejdzie w życie z dniem następującym po dniu ogłoszenia. | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1. **W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Ewaluacja efektów projektu będzie prowadzona cyklicznie w trzyletnich, stałych interwałach, w oparciu o podstawowe mierniki efektywności wdrażanych rozwiązań:   1. Ilość jednostek administracji publicznej korzystających usług Rządowej Chmury Obliczeniowej (szt./rok) 2. Ilość jednostek administracji publicznej korzystających modelu zamawiania usług w ramach Systemu Zapewniania Usług Chmurowych (szt./rok) 3. Ilość usług elektronicznych świadczonych na rzecz jednostek administracji publicznej w oparciu o zasoby Rządowej Chmury Obliczeniowej oraz dostawców komercyjnych (szt./rok).   Pierwszy pomiar zaplanowano w roku 2021, kolejne w latach 2024, 2027. Źródłem danych pomiarowych będą automatyczne raporty generowane w ramach wdrażanych systemów IT, tj. rejestr użytkowników, rejestr zawartych porozumień/umów na świadczenie usług elektronicznych, rejestr uruchomionych usług oraz dane przekazywane przez dostawców usług komercyjnych w ramach Systemu Zamawiania Usług Chmurowych (dane bilingowe). | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1. **Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1. Analiza ryzyka zagrożeń dla ochrony danych osobowych w ramach inicjatywy WIIP | | | | | | | | | | | | | | | | | | | | | | | | | | |

Załącznik do OSR

**Analiza ryzyka zagrożeń dla ochrony danych osobowych w ramach inicjatywy WIIP**

Analizę ryzyka sporządzono w oparciu katalog zagrożeń dla ochrony danych związanych z przetwarzaniem danych w chmurze, który został określony w Opinii 5/2012 w sprawie przetwarzania danych w chmurze obliczeniowej, sporządzonej w ramach Grupy Roboczej Artykułu 29 ds. Ochrony Danych oraz metodykę określoną zarządzeniem nr 5 Ministra Cyfryzacji z dnia 27 lutego 2019 r. w sprawie zatwierdzania do realizacji oraz zarządzania projektami, programami i portfelem projektów w resorcie cyfryzacji (Dz. Urz. Ministra Cyfryzacji z 2019 poz. 6).

Prawdopodobieństwa oraz wpływ wystąpienia ryzyka określono w czterostopniowej skali, przyjmując następujące definicje:

1. Prawdopodobieństwo wystąpienia ryzyka:

4 – Bardzo prawdopodobne,

3 – Prawie na pewno wydarzy się,

2 – Mało prawdopodobne,

1 – Prawie na pewno się nie wydarzy.

1. Wpływ ryzyka:

4 – Ryzyko może wpłynąć na uzasadnienie projektu uchwały, w tym efekty wprowadzenia regulacji,

3 – Ryzyko może wpłynąć na plan realizacji projektów objętych inicjatywą,

2 – Ryzyko może wpłynąć na termin i zakres kamieni milowych inicjatywy,

1 – Ryzyko może wpłynąć na dostawę wybranego produktu projektu.

Na podstawie oceny ryzyka oraz wyliczeniu jego istotności można przedstawić ryzyka na wykresie (Rysunek 1). Ocena ryzyka pozwala na określenie najodpowiedniejszej reakcji na ryzyko.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 4 | 4 | 8 | 12 | 16 |
| 3 | 3 | 6 | 8 | 12 |
| 2 | 2 | 4 | 6 | 8 |
| 1 | 1 | 2 | 3 | 4 |
|  | 1 | 2 | 3 | 4 |

*Rysunek 1. Macierz ryzyka*

Poniżej przedstawiono zakres reakcji na zagrożenia związane z wystąpieniem czynników ryzyka:

1. Unikanie – zmiana sposobu realizacji projektu w celu wyeliminowania ryzyka jego wystąpienia lub wpływu;
2. Mitygacja – działanie mające na celu zmniejszenie prawdopodobieństwa wystąpienia lub wpływu wystąpienia ryzyka;
3. Plan rezerwowy – przygotowanie planu działań na wypadek wystąpienia ryzyka;
4. Przeniesienie – przeniesienie skutków finansowych wystąpienia ryzyka na stronę trzecią (np. ubezpieczenie);
5. Współdzielenie – w przypadku wystąpienia ryzyka jego skutki są współdzielone przez dwie strony (np. dwóch kontrahentów);
6. Akceptacja – akceptacja wystąpienia ryzyka, w przypadku gdy zarządzanie nim jest bardziej kosztowne od skutków jego wystąpienia.

Im ryzyko ma wyższą istotność (czerwony kolor na powyższym rysunku), tym bardziej stanowcze działania w celu jego unikania, czy przeniesienia zostały zaplanowane.

Poniżej zaprezentowano tabelę ryzyka dla ochrony danych osobowych w ramach inicjatywy WIIP.

| Kategoria | Rodzaj ryzyka | Prawdopodobieństwo wystąpienia | Istotność ryzyka | Ocena ryzyka | Reakcja | Ocena wpływu i opis działań zaradczych |
| --- | --- | --- | --- | --- | --- | --- |
| Brak kontroli | Brak dostępności ze względu na brak interoperacyjności (uzależnienie od dostawcy, tzw. „vendor lock-in”): Jeżeli dostawca usługi w chmurze bazuje na zastrzeżonej technologii, dla klienta usługi może się okazać trudne przenoszenie danych i dokumentów między różnymi systemami opartymi na cloud computingu (możliwość przenoszenia danych) lub wymiana informacji z podmiotami korzystającymi z usług w chmurze zarządzanych przez innych dostawców (interoperacyjność). | **1** | **1** | **1** | **Akceptacja** | Wybrane zagadnienie ma zastosowanie w dwóch projektach Inicjatywy WIIP: Rządowej Chmury Obliczeniowej oraz Systemie Zapewniania Usług Chmurowych.  W przypadku Rządowej Chmury Obliczeniowej ryzyko wystąpienia vendor loc-in zależy stricte od wymagań klienta usługi, czyli właściciela systemu i danych, które będą przetwarzane. Domyślnie usługi prywatnej chmury obliczeniowej będą oparte na technologiach open source. Jeżeli ze względów technicznych wymagane będzie zastosowanie rozwiązań dostawców komercyjnych decyzja w tym zakresie będzie należeć do klienta usługi.  W przypadku dostawców usług chmury publicznej w ramach system ZUCH przewidziano wymaganie wprowadzenia usług migracji, które pozwalają na przeniesienie systemów i danych pomiędzy różnymi dostawcami. |
| Brak integralności spowodowany przez dzielenie się zasobami: Chmura składa się z współdzielonych systemów i infrastruktur. Dostawcy usług w chmurze przetwarzają dane osobowe wywodzące się z szeregu licznych źródeł - osób, których dane dotyczą, i organizacji – i istnieje możliwość, że mogą powstać sprzeczne interesy i/lub różne cele. | **1** | **1** | **1** | **Akceptacja** | Istotą przetwarzania danych w chmurze obliczeniowej zarówno przez akredytowanych dostawców komercyjnych, jak i operatora Rządowej Chmury Obliczeniowej jest ścisła separacja danych i środowisk obliczeniowych (tenantów) pomiędzy klientami. Stosowane w tym celu technologie oraz zabezpieczenia kryptograficzne dają pewność integralności przetwarzanych danych, a dostawca usług nie ma technicznej możliwości uzyskania dostępu do wybranego tenantu oraz danych w nim przetwarzanych. Standaryzacja zakresu świadczonych usług nie pozostawia również możliwości wystąpienia konfliktu interesów, gdyż dostawca jest odpowiedzialny jedynie za realizację ustalonych w indywidualnych umowach parametrów technicznych świadczonej usługi. |
| Brak poufności w odniesieniu do wniosków z zakresu egzekwowania prawa składanych bezpośrednio do dostawcy usługi w chmurze: dane osobowe przetwarzane w chmurze mogą być przedmiotem wniosków z zakresu egzekwowania prawa pochodzących od organów egzekwowania prawa z państw członkowskich UE oraz krajów trzecich. Istnieje zagrożenie, że dane osobowe mogłyby być ujawnione (zagranicznym) organom egzekwowania prawa bez ważnej podstawy prawnej UE i tym samym doszłoby do naruszenia prawa UE dotyczącego ochrony danych. | **1** | **1** | **1** | **Akceptacja** | Ze względu na charakter oraz właściwość świadczenia usług chmurowych dostawca ma bardzo ograniczony zakres działań wynikający z realizacji wniosków o udzielenie informacji przez osoby fizyczne lub prawne, w tym organy ścigania lub uprawnione służby.  Istotą świadczenia usług chmury obliczeniowej (IaaS, PaaS) ścisła separacja uprawnień dostawcy i klienta. Dostawca zapewnia utrzymanie warstwy fizycznej oraz platform aplikacyjnych, zaś klient samodzielnie tworzy i konfiguruje środowiska swoich systemów, zarządza danymi i sposobem ich przetwarzania, w tym zabezpieczaniem przed nieuprawnionym dostępem osób trzecich. Z tego względu dostawca może jedynie udzielić na wniosek uprawnionych osób informacji o czasie i sposobie dostępu do usług które świadczy (dane o czasie, identyfikatorze logowania administracyjnego, adresacji IP klientów usług). Zastrzeżenia prawne z tego zakresu będą przedmiotem osobnych porozumień pomiędzy stronami. |
| Brak możliwości interwencji ze względu na złożoność i dynamiczność łańcucha outsourcingu: Usługa w chmurze oferowana przez jednego dostawcę może być realizowana poprzez połączenie usług od szeregu innych dostawców, które mogą być dynamicznie dodawane lub usuwane w czasie trwania umowy klienta. | **1** | **1** | **1** | **Akceptacja** | Ze względu na charakter i zakres usług przewidzianych do realizacji w ramach projektów wchodzących w zakres Inicjatywy WIIP nie przewiduje się złożonych i dynamicznych łańcuchów outsourcingu.  W przypadku systemów (rejestrów publicznych), które przetwarzają dane osobowe, wymóg klasyfikacyjny (załącznik 2 do projektu uchwały) lokuje je w Rządowej Chmurze Obliczeniowej, która jest prywatną chmurą obliczeniową administracji publicznej, w której nie zachodzi zjawisko outsourcingu. |
| Brak możliwości interwencji (prawa osób, których dane dotyczą): Dostawca usługi w chmurze może nie zapewnić niezbędnych środków i narzędzi mających pomóc administratorowi zarządzać danymi np. w zakresie dostępu, usunięcia lub poprawienia danych. | **1** | **1** | **1** | **Akceptacja** | Dostawca usług chmurowych udostępnia wszelkie narzędzia zarządzania administracyjnego klientom świadczonych przez niego usług. Klient usługi chmurowej ma wyłączne uprawnienia do zarządzania danymi, w tym dostępu, usuwania lub poprawiania danych. Uprawnienia te mogą być przekazywane dalej uprawnionym użytkownikom, zaś odpowiedzialność za zarządzanie tym procesem leży po stronie klienta. |
| Brak odizolowania: Dostawca usługi w chmurze może wykorzystywać swoją fizyczną kontrolę nad danymi od różnych klientów w celu łączenia danych. Jeżeli dostawcy usługi administrujący przetwarzaniem mieliby wystarczające prawa uprzywilejowanego dostępu (role wysokiego ryzyka), mogliby łączyć informacje od różnych klientów (administratorów danych). | **1** | **1** | **1** | **Akceptacja** | Obecny standard świadczenia usług przetwarzania w chmurach obliczeniowych, zwłaszcza stosowanie metod kryptograficznych, w których posiadaczem kluczy są klienci, nie pozwala na łączenie przetwarzanych danych. Możliwe jest wyłącznie prowadzenie analiz statystycznych w ograniczonym zakresie.  Sposób konstrukcji systemu uprawnień i zarządzania dostępem nie daje administratorom dostawcy dostępu do przetwarzanych danych. |
| Brak informacji na temat przetwarzania (przejrzystości) | W przetwarzanie zaangażowani są liczni przetwarzający i podprzetwarzający (łańcuch przetwarzania). | **1** | **1** | **1** | **Akceptacja** | Ten aspekt nie ma zastosowania w przedmiotowym projekcie. W przypadku pojedynczej usługi chmurowej nie wystąpi łańcuch przetwarzania. W przypadku gdy klient korzystający z usługi będzie chciał korzystać z usług wielu dostawców do realizacji swojego projektu odpowiedzialność za integralność techniczną, logiczną i informacyjną spoczywa po jego stronie. W takim wypadku klient usługi powinien przeprowadzić stosowną analizę ryzyka we własnym zakresie. |
| Dane osobowe są przetwarzane w różnych lokalizacjach geograficznych w ramach EOG. Ma to bezpośredni wpływ na prawo właściwe dla wszelkich sporów z zakresu ochrony danych, które mogą wyniknąć między użytkownikiem a dostawcą. | **1** | **1** | **1** | **Akceptacja** | Aspekt ten dotyczy wyłącznie dostawców usług komercyjnych, posiadających centra przetwarzania danych na terenie EOG. Ponieważ jednym z wymagań w stosunku do tych dostawców będzie konieczność zapewnienia fizycznej infrastruktury przetwarzania na terenie Unii Europejskiej, gdzie kwestie prawa ochrony danych osobowych są harmonizowane na poziomie Komisji Europejskiej, kwestia ta nie ma dużego znaczenia. Dodatkowo standardowym elementem umów na świadczenie usług chmury obliczeniowej będzie wskazanie prawa miejscowego właściwego do rozstrzygania sporów w tym zakresie. |
| Dane osobowe są przekazywane do krajów trzecich poza EOG. Kraje trzecie mogą nie zapewniać odpowiedniego poziomu ochrony danych, a operacje przekazywania mogą nie być zabezpieczone odpowiednimi środkami (np. standardowe klauzule umowne lub wiążące reguły korporacyjne) i tym samym mogą być niezgodne z prawem. | **-** | **-** | **-** | **-** | Ten aspekt nie ma zastosowania do przedmiotowego projektu. Wszystkie usługi chmurowe realizowane w ramach projektów Inicjatywy WIIP będą realizowane na terenie Polski lub krajów należących do EOG. |

Podsumowując wyniki powyższej analizy ryzyka, przyjęte założenia realizacji projektów wchodzących w skład inicjatywy WIIP określają podział odpowiedzialności za realizację systemów informatycznych w oparciu o usługi przetwarzania w chmurze, w taki sposób, by zapewnić ścisłą separacje dostawy infrastruktury i platform systemowych i aplikacyjnych od procesu zarządzania systemami klienta oraz danymi przez nie przetwarzanymi. Odpowiedzialność za prawidłowe zabezpieczenie własnych systemów oraz przetwarzanych danych, w tym danych osobowych, spoczywać będzie na kliencie usług chmurowych. Dostawca zaś będzie odpowiadał za utrzymanie separacji logicznej środowisk obliczeniowych oraz wysoki poziom bezpieczeństwa kryptograficznego oraz integralności zbiorów.

1. Oznaczenie w rubryce: „Brak możliwości skorzystania z usług chmurowych określonych w uchwale” nie oznacza, iż system ten nie może być przetwarzany w innych zamkniętych środowiskach chmurowych, których działania regulują inne przepisy, pragmatyki lub które utworzone zostały przez uprawnione do tego organy. [↑](#footnote-ref-2)
2. W przypadku, gdy przepisy materialne posługują się pojęciem rejestru. [↑](#footnote-ref-3)
3. W przypadku, gdy przepisy materialne posługują się pojęciem ewidencja. [↑](#footnote-ref-4)
4. W przypadku, gdy przepisy materialne posługują się dla oznaczenie systemu teleinformatycznego innymi pojęciami niż rejestr lub ewidencja. [↑](#footnote-ref-5)
5. Zgodnie z art. 35 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu w związku z wykonywaniem swoich zadań Agencje zapewniają ochronę środków, form i metod realizacji zadań, zgromadzonych informacji oraz własnych obiektów i danych identyfikujących funkcjonariuszy tych Agencji.

   [↑](#footnote-ref-6)