Warszawa, dnia 24 września 2019 r.

Poz. 862

UCHWAŁA NR 97
RADY MINISTRÓW

z dnia 11 września 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 oraz zarządzanie zasobami Rządowej Chmury Obliczeniowej, z wykorzystaniem w szczególności sieci teletransmisji pozostających w dyspozycji podmiotów publicznych;

2) budowę, rozwój i utrzymanie Rządowego Klastra Bezpieczeństwa;

3) zapewnienie podmiotom administracji publicznej możliwości nabywania usług przetwarzania w publicznych chmurach obliczeniowych;

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

5) określenie Standardów Cyberbezpieczeństwa Chmur Obliczeniowych.

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

§ 2. Użyte w uchwale określenia oznaczają:

1) Centrum Przetwarzania Danych (CPD) – serwerownię w zasobach administracji rządowej lub obiekt budowlany, w którym zlokalizowana jest infrastruktura teleinformatyczna i związane z nią elementy (np.: systemy telekomunikacyjne, zasoby przetwarzania) wraz z nadmiarowymi źródłami zasilania, dodatkowymi sieciami teletransmisyjnymi, środkami kontroli środowiska (np. klimatyzacją, systemami gaśniczymi), urządzeniami i systemami bezpieczeństwa oraz ochroną fizyczną obiektu;

2) chmura hybrydowa – sposób wdrażania chmury obliczeniowej, w którym infrastruktura składa się z dwóch lub więcej odrębnych infrastruktur teleinformatycznych dostarczanych z chmury obliczeniowej (prywatnej, wspólnotowej lub publicznej), które pozostają odrębnymi jednostkami powiązanymi ze sobą znormalizowaną lub zastrzeżoną technologią, umożliwiającą przenoszenie danych i aplikacji między chmurami obliczeniowymi (np. w celu równoważenia obciążenia);

3) chmura obliczeniowa – model przetwarzania umożliwiający powszechny i wygodny dostęp za pośrednictwem sieci do wspólnej puli konfigurowalnych zasobów przetwarzania (np. sieci, serwerów, pamięci masowych, aplikacji i usług),

które są szybko udostępniane z katalogu usług przy minimalnym wysiłku ze strony zespołów zarządzania lub dostawcy usług, składający się z trzech modeli usług (SaaS, PaaS, IaaS), czterech sposobów wdrażania chmur (chmura prywatna, chmura wspólnotowa, chmura publiczna, chmura hybrydowa) oraz charakteryzujący się pięcioma zasadniczymi cechami (samoobsługą na żądanie, szerokim dostępem do sieci, dynamicznym gromadzeniem zasobów, szybkim i elastycznym przydzielaniem i zwalnianiem zasobów, pomiarami i optymalizacją usług), w którym stosowana jest zasada współdzielonej odpowiedzialności między dostawcą i odbiorcą usług chmurowych, a kluczowe technologie wykorzystywane do budowy tego modelu obejmują: szybkie i wydajne sieci rozległe, wydajne oraz relatywnie niedrogie serwery (uwzględniając ich liczbę) oraz wysokowydajną wirtualizację sprzętu;

4) chmura prywatna – sposób wdrażania chmury obliczeniowej, w którym infrastruktura jest udostępniana do wyłącznego użytku przez jedną organizację obejmującą wielu odbiorców usług, może być własnością tej organizacji, strony trzeciej lub ich kombinacji bądź może być przez nie zarządzana i obsługiwana oraz zainstalowana w siedzibie tej organizacji lub poza nią;

5) chmura publiczna – sposób wdrażania chmury obliczeniowej, w którym infrastruktura jest udostępniana do użytku publicznego, może być własnością organizacji biznesowej, akademickiej lub rządowej lub ich kombinacji bądź może być przez nie zarządzana i obsługiwana oraz jest zainstalowana w siedzibie dostawcy chmury;

6) chmura wspólnotowa – sposób wdrażania chmury obliczeniowej, w którym infrastruktura jest przeznaczona do wyłącznego użytku przez określoną grupę organizacji mających wspólne założenia (m.in. misję, wymagania bezpieczeństwa, politykę, zgodność z regulacjami), może być własnością jednej lub więcej organizacji wchodzącej w skład grupy, strony trzeciej lub ich kombinacji bądź może być przez nie zarządzana i obsługiwana i jest zainstalowana w siedzibie organizacji lub poza nią;

7) infrastruktura chmury – zasoby przetwarzania stanowiące zbiór sprzętu i oprogramowania zgrupowanego w puli zasobów, umożliwiający spełnienie pięciu zasadniczych cech przetwarzania w chmurze obliczeniowej zawierające warstwę zarówno fizyczną (składającą się z zasobów sprzętowych, które są niezbędne do obsługi dostarczanych usług w chmurze obliczeniowej i zazwyczaj obejmują składniki serwera, pamięci masowej i sieci), jak i warstwę abstrakcji znajdującą się powyżej warstwy fizycznej (składającą się z oprogramowania rozmieszczonego w warstwie fizycznej, która posiada zasadnicze cechy chmury obliczeniowej);

8) infrastruktura jako usługa (IaaS) – model usługi chmurowej zapewniający infrastrukturę chmury, na której odbiorca usług jest w stanie wdrożyć i uruchomić dowolne oprogramowanie (systemy operacyjne i aplikacje), jednak nie zarządza ani nie kontroluje infrastruktury chmury, z wyjątkiem kontroli nad systemami operacyjnymi, pamięcią masową i wdrożonymi aplikacjami oraz, ewentualnie, ograniczonej kontroli nad wybranymi komponentami sieciowymi (np. zapór sieciowych);

9) platforma jako usługa (PaaS) – model usługi chmurowej umożliwiający odbiorcy usług wdrożenie na infrastrukturze chmury aplikacji stworzonych przez siebie lub nabytych, które zostały przygotowane przy użyciu języków programowania, bibliotek, usług i narzędzi obsługiwanych przez dostawcę, w przypadku której 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, nad ustawieniami konfiguracji dla środowiska udostępnienia aplikacji;

10) oprogramowanie jako usługa (SaaS) – model usługi chmurowej umożliwiający odbiorcy usług wykorzystanie aplikacji uruchomionych na infrastrukturze chmury dostarczanej przez dostawcę usług dostępnej na różnych urządzeniach klienckich za pośrednictwem np. przeglądarki internetowej lub klienta aplikacji oraz w przypadku której 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;

11) publiczne chmury obliczeniowe – usługi chmury publicznej świadczone przez dostawców komercyjnych spełniające w szczególności wymagania w zakresie poufności, integralności i dostępności zdefiniowanych pod kątem zapewnienia bezpieczeństwa informacji administracji publicznej;

12) Rządowa Chmura Obliczeniowa – chmurę wspólnotową administracji publicznej;

13) Rządowy Klaster Bezpieczeństwa (RKB) – usługi bezpieczeństwa oraz środki techniczne stosowane do zabezpieczenia Rządowej Chmury Obliczeniowej będące implementacją wymagań Standardów Cyberbezpieczeństwa Chmur Obliczeniowych;

14) sieci rządowe – sieci teletransmisyjne zarządzane przez ministra właściwego do spraw wewnętrznych;

15) Standardy Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO) – zbiór wymagań prawnych, organizacyjnych i technicznych zapewniających cyberbezpieczeństwo w modelach wdrażania chmur obliczeniowych.

§ 3. Minister właściwy do spraw informatyzacji, w porozumieniu z ministrem właściwym do spraw wewnętrznych, Ministrem Obrony Narodowej oraz Ministrem – Członkiem Rady Ministrów, Koordynatorem Służb Specjalnych, określa Standardy Cyberbezpieczeństwa Chmur Obliczeniowych.

§ 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 przetwarzania w Rządowej Chmurze Obliczeniowej.

4. Usługi przetwarzania w Rządowej Chmurze Obliczeniowej będą świadczone, w szczególności w modelach „infrastruktura jako usługa" (IaaS), „platforma jako usługa" (PaaS) oraz „oprogramowanie jako usługa" (SaaS).

5. Usługi przetwarzania w Rządowej Chmurze Obliczeniowej będą świadczone w CPD, których posiadaczami są 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 posiadane przez nie zasoby teleinformatyczne.

§ 5. 1. CPD, o których mowa w § 4 ust. 5, będą przyłączone do Rządowej Chmury Obliczeniowej z inicjatywy operatora Rządowej Chmury Obliczeniowej. Warunkiem przyłączenia jest złożenie operatorowi Rządowej Chmury Obliczeniowej przez posiadacza CPD pisemnego oświadczenia potwierdzającego spełnienie minimalnych wymagań organizacyjnych i technicznych dla posiadaczy CPD oraz ich CPD przyłączonych do Rządowej Chmury Obliczeniowej, określonych w załączniku nr 1 do uchwały.

2. Do oświadczenia, o którym mowa w ust. 1, posiadacz CPD dołącza uwierzytelnioną kopię obowiązującego porozumienia zawartego między posiadaczem CPD a ministrem właściwym do spraw wewnętrznych, regulującego kwestie związane z korzystaniem z sieci rządowej.

3. Sposób i zakres przyłączenia oraz zasady korzystania z CPD przyłączonego do Rządowej Chmury Obliczeniowej określa porozumienie zawarte między posiadaczem CPD a ministrem właściwym do spraw informatyzacji.

4. Zasady i sposób wykorzystania sieci rządowej na potrzeby Rządowej Chmury Obliczeniowej określa porozumienie zawarte między właściwym operatorem sieci rządowej a ministrem właściwym do spraw informatyzacji. Ocena spełniania przez posiadacza CPD minimalnych wymagań organizacyjnych i technicznych w zakresie możliwości przyłączenia CPD do sieci rządowej będzie każdorazowo dokonywana przez strony porozumienia.

5. Przepisu ust. 4 nie stosuje się, w przypadku gdy przed datą zawarcia porozumienia, o którym mowa w ust. 4, posiadacz CPD zawarł z ministrem właściwym do spraw wewnętrznych porozumienie regulujące kwestie związane z korzystaniem z sieci rządowej.

§ 6. 1. Z usług przetwarzania w Rządowej Chmurze Obliczeniowej lub publicznych chmurach obliczeniowych mogą korzystać:

1) podmioty sektora finansów publicznych, o których mowa w art. 9 pkt 1–13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2019 r. poz. 869, 1622 i 1649);

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 w publicznych chmurach obliczeniowych, określonych w załączniku nr 2 do uchwały.

§ 7. 1. Podmioty, o których mowa w § 6 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 korzystania z usług przetwarzania w Rządowej Chmurze Obliczeniowej oraz prawa i obowiązki stron, w szczególności:

1) zastosowane standardy techniczne świadczenia usług;

2) podział odpowiedzialności i jej ograniczenia;

3) zasady przeprowadzania lub zlecania przez strony audytu dotyczącego sposobu realizacji porozumienia;

4) procedury rozpoczęcia korzystania z usług;

5) podział obowiązków i odpowiedzialności związany z korzystaniem z usług, w tym obowiązki dostawcy usług oraz zapewnienie ustalonego w porozumieniu poziomu jakości świadczenia usług (SLA);

6) zasady obsługi technicznej świadczonej w ramach utrzymania usług;

7) obowiązki w zakresie praw własności intelektualnej;

8) procedury bezpieczeństwa oraz zasady reagowania na incydenty;

9) obowiązki w zakresie ochrony danych osobowych;

10) procedury rezygnacji podmiotu z korzystania z usług oraz warunki wypowiedzenia porozumienia;

11) zasady prowadzenia rozliczeń za korzystanie z usług;

12) obowiązki informacyjne w zakresie świadczenia usług.

2. Podmioty, o których mowa w § 6 ust. 1, nie mogą korzystać z usług przetwarzania w Rządowej Chmurze Obliczeniowej w celu prowadzenia działalności gospodarczej.

§ 8. Podmioty, o których mowa w § 6 ust. 1, w celu skorzystania z usług przetwarzania w publicznych chmurach obliczeniowych wnioskują do właściwego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie krajowym prowadzonego przez Ministra Obrony Narodowej, Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy lub Szefa Agencji Bezpieczeństwa Wewnętrznego o wydanie opinii w zakresie możliwości wykorzystania publicznych chmur obliczeniowych. Niewydanie opinii w terminie 30 dni od dnia otrzymania wniosku jest równoznaczne z wydaniem opinii pozytywnej.

§ 9. 1. RKB obejmuje usługi:

1) bezpieczeństwa teleinformatycznego, świadczone w oparciu o przeznaczone do tego celu systemy bezpieczeństwa realizujące zadania wyłącznie na potrzeby Inicjatywy WIIP;

2) monitorowania poziomu bezpieczeństwa opartego o przeznaczone do tego celu zespoły:

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

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

2. RKB zapewnia bezpieczeństwo:

1) połączenia między poszczególnymi CPD, w których umieszczona zostanie infrastruktura Rządowej Chmury Obliczeniowej;

2) komunikacji między Rządową Chmurą Obliczeniową a odbiorcami jej usług w oparciu o udostępnioną dla CPD i odbiorców usług infrastrukturę sieci rządowej;

3) połączenia infrastruktury teleinformatycznej Rządowej Chmury Obliczeniowej z publiczną siecią Internet przez przeznaczone do tego celu zabezpieczone punkty styku.

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 w porozumieniu, o którym mowa w § 7 ust. 1.

4. Operatorem RKB jest minister właściwy do spraw informatyzacji.

5. Operator RKB w szczególności:

1) świadczy usługi bezpieczeństwa z wykorzystaniem środków technicznych i zespołów, o których mowa w ust. 1 pkt 2;

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

3) informuje o zagrożeniach bezpieczeństwa i incydentach, jak operator usługi kluczowej, o którym mowa w art. 11 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560);

4) planuje rozwój usług RKB;

5) uzgadnia z operatorem sieci rządowej potrzeby w zakresie wykorzystania łączy teletransmisyjnych do wymiany danych w ramach Rządowej Chmury Obliczeniowej;

6) planuje rozwój i wykorzystanie zabezpieczonych punktów styku z publiczną siecią Internet dla usług świadczonych w Rządowej Chmurze Obliczeniowej.

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.

§ 10. 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 o udzielenie zamówienia publicznego 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. 53, 730 i 1655).

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

4. Prowadzenie postępowań o udzielenie zamówienia publicznego oraz zawieranie umów w sprawie zamówień publicznych, o których mowa w ust. 3, realizowane będzie w zamówieniu wspólnym lub przez centralnego zamawiającego wskazanego przez Prezesa Rady Ministrów, zgodnie z przepisami ustawy 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 wysoce skalowalnych i niezawodnych usług przetwarzania w publicznych chmurach obliczeniowych, będzie ogłaszał postępowania o udzielenie zamówienia publicznego na świadczenie usług przetwarzania w publicznych chmurach obliczeniowych.

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

2. Podział rezerwy dokonywany jest zgodnie z przepisami ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, przy czym minister właściwy do spraw informatyzacji dokonuje weryfikacji i akceptacji przedłożonych wniosków o podział rezerwy.

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.

§ 12. Podmioty, o których mowa w § 6 ust. 1, zamierzające korzystać z usług przetwarzania w Rządowej Chmurze Obliczeniowej, projektując systemy teleinformatyczne po wejściu w życie uchwały, przeprowadzają klasyfikację, o której mowa w § 6 ust. 2.

§ 13. 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.

§ 14. Minister właściwy do spraw informatyzacji przekaże Kolegium do Spraw Cyberbezpieczeństwa Standardy Cyberbezpieczeństwa Chmur Obliczeniowych, o których mowa w § 3, w terminie dwóch miesięcy od dnia wejścia w życie uchwały.

§ 15. Uchwała wchodzi w życie z dniem następującym po dniu ogłoszenia, z wyjątkiem § 11, który wchodzi w życie z dniem 1 stycznia 2021 r.

Prezes Rady Ministrów: *M. Morawiecki*

Załączniki do uchwały nr 97 Rady Ministrów
z dnia 11 września 2019 r. (poz. 862)

Załącznik nr 1

MINIMALNE WYMAGANIA ORGANIZACYJNE I TECHNICZNE DLA POSIADACZY CPD ORAZ CPD PRZYŁĄCZONYCH DO RZĄDOWEJ CHMURY OBLICZENIOWEJ

1. Posiadacz CPD w zakresie świadczenia usług przetwarzania w Rządowej Chmurze Obliczeniowej spełnia wymagania zapewnienia zgodności swojego działania określone w Krajowych Ramach Interoperacyjności i ustawie z dnia 10 maja 2018 r. 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) CPD jest własnością Skarbu Państwa albo państwowych osób prawnych lub udział w prawie własności tych podmiotów wynosi co najmniej 51%;
2) klasa 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 komory lub klatki w komorze przeznaczonej wyłącznie na potrzeby infrastruktury Rządowej Chmury Obliczeniowej oraz zabezpieczenie rezerwy mocy nie mniej niż 2,5 kW/m^2 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 przeznaczonej do tego celu sieci rządowej;
   2) posiada dostęp do sieci publicznej przez co najmniej 2 niezależne łącza różnych operatorów;
   3) posiada możliwość zarządzania przez usługi RKB potwierdzoną przez operatora RKB.
4. Infrastruktura Rządowej Chmury Obliczeniowej umieszczona w CPD spełnia wymagania:
   1) w zakresie wsparcia dla infrastruktury:
      a) używana infrastruktura (w szczególności: serwery, macierze, urządzenia sieciowe) posiada aktywną gwarancję wsparcia producenta; w przypadku gdy gwarancja wsparcia nie jest odnawiana, posiadacz CPD musi o tym poinformować odbiorców usług,
      b) używana infrastruktura korzysta z oprogramowania instalowanego z autoryzowanych źródeł przez przeszkolony i autoryzowany personel,
      c) 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;
   2) w zakresie wsparcia dla oprogramowania:
      a) używane oprogramowanie pochodzi z autoryzowanych źródeł i jest przygotowywane do instalacji oraz instalowane przez przeszkolony i autoryzowany personel,
      b) 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,
      c) 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,

d) posiadacz CPD zapewnia, że usługę realizuje wyłącznie wyszkolony i autoryzowany personel,

e) w przypadku używania oprogramowania open source wymagania, o których mowa w lit. 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 po spełnieniu jednego z następujących warunków:

1) przejściu pozytywnej weryfikacji zgodności z SCCO prowadzonej przez instytucję wskazaną przez operatora RKB;
2) sprawdzeniu przez operatora RKB systemu bezpieczeństwa w zakresie dotyczącym aktywów Rządowej Chmury Obliczeniowej;
3) uzyskaniu certyfikacji.

7. Posiadacz CPD, który nie spełnia wymagań, o których mowa w ust. 1–3, może rozpocząć korzystanie z Rządowej Chmury Obliczeniowej po spełnieniu następujących warunków:

1) złożeniu deklaracji zgodności z wymaganiami norm, o których mowa w ust. 1;
2) przejściu pozytywnej weryfikacji zgodności z SCCO 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. Koszty czynności związanych z deklaracją zgodności 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 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. 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 możliwości skorzystania z usług chmurowych określonych w uchwale" 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 możliwości skorzystania z usług chmurowych określonych w uchwale" 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)] (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

[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. Dedykowana Infrastruktura Teleinformatyczna to środowisko informatyczne pozostające pod kontrolą jednostki administracji publicznej, realizowane poza Rządową Chmurą Obliczeniową.

1	Systemy teleinformatyczne, w których są przetwarzane informacje niejawne	X				Dotyczy to systemów, które wprost w przepisach ustaw są określone jako systemy niejawne lub w stosunku do których uprawnione organy wskazały, iż są w nich przetwarzane informacje niejawne.
2	Systemy teleinformatyczne służb specjalnych w rozumieniu art. 11 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu	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.
3	Systemy teleinformatyczne wykorzystywane do prowadzenia rejestrów[2)], ewidencji[3)] oraz innych baz danych[4)] 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.

[2)] W przypadku gdy przepisy materialne posługują się pojęciem rejestru.
[3)] W przypadku gdy przepisy materialne posługują się pojęciem ewidencja.
[4)] W przypadku gdy przepisy materialne posługują się dla oznaczenia systemu teleinformatycznego innymi pojęciami niż rejestr lub ewidencja.

4	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.
5	Systemy 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.
6	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 z dnia 24 maja 2002 r.	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

	o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu[5)]					wchodzą w zakres podmiotowy uchwały oraz systemów podmiotów prywatnych, np. systemów teleinformatycznych, przy użyciu których wydawane są środki identyfikacji elektronicznej.
7	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.
8	Systemy teleinformatyczne wykorzystywane do prowadzenia rejestrów, ewidencji oraz innych baz danych, w których są przetwarzane szczególne kategorie danych osobowych w rozumieniu art. 9 i art. 10 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie		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.

[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.

	swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)					
9	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 zarówno jako skutek konstytutywny, jak i deklaratoryjny.
10	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.

11	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 niebędące częścią systemów należących do kategorii 4–9. Pod warunkiem zakwalifikowania podmiotu odpowiedzialnego za system do zakresu podmiotowego uchwały.
12	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 doręczanie przez te organy dokumentów stanowiących elementy postępowań administracyjnych oraz innych, przewidzianych w przepisach prawa, czynności realizowanych przez te organy.

13	Systemy teleinformatyczne służące do prowadzenia wewnętrznego elektronicznego obiegu dokumentacji/ elektronicznego zarządzania dokumentacją		X	X	X	O możliwości przetwarzania w danej możliwej chmurze decyduje wynik analizy.
14	Systemy teleinformatyczne klasy ERP i CRM itp.		X	X	X	O możliwości przetwarzania w danej możliwej chmurze decyduje wynik analizy.
15	Pozostałe systemy teleinformatyczne		X	X	X	Kategoria obejmuje inne systemy świadczące usługi obsługowe na wewnętrzny użytek, zapewniające komunikację, np. systemy ekstranetowe, intranetowe lub poczty elektronicznej.

2. 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 chmurach obliczeniowych". 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 chmurach obliczeniowych, analiza powinna uwzględniać w szczególności, czy:

a) 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,
b) system teleinformatyczny zasila danymi systemy referencyjne państwa,
c) system korzysta z systemów referencyjnych państwa,
d) 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 w oparciu o analizę ryzyka.

Kryteria do przeprowadzenia szacowania ryzyka obejmują co najmniej następujące atrybuty:

1. poufność informacji, w zakresie której należy przeanalizować co najmniej:
   1.1. 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:
   2.1. czy naruszenie integralności (np. nieautoryzowane zmodyfikowanie) danych będzie uniemożliwiało lub będzie powodowało istotne zagrożenie dla realizacji szczególnych zadań państwa;
   2.2. 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;
   2.3. czy wpis lub zmiana wpisów w systemie powoduje bezpośrednie skutki prawne;
3. dostępność informacji, w zakresie której należy przeanalizować co najmniej:
   3.1. czy naruszenie dostępności danych (np. brak dostępu do danych) będzie uniemożliwiało lub będzie powodowało istotne zagrożenie dla realizacji szczególnych zadań państwa;
   3.2. 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);
   3.3. 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.