Uwagi Polskiej Izby Informatyki i Telekomunikacji [PIIT] do projektu uchwały RM ws inicjatywy „Wspólna Infrastruktura Informatyczna Państwa”

Nazwa projektu dokumentu: **Projekt uchwały Rady Ministrów w sprawie Inicjatywy "Wspólna Infrastruktura Informatyczna Państwa"**				
L.p.	Podmiot wnoszący uwagi	Jednostka redakcyjna, do której wnoszone są uwagi	Treść uwagi	
1.	PIIT	Uchwała § 1 ust. 2 i dalsze	Polska Izba Informatyki i Telekomunikacji widząc w projekcie Uchwały pozytywny ruch w stronę wymienionych w Ocenie Skutków Regulacji oszczędności, podniesienia cyberbezpieństwa, praktycznego wdrożenia modelu chmury obliczeniowej itd. zwraca uwagę na konieczność przygotowania dokumentu strategicznego związanego z tworzeniem i eksploatacją Wspólnej Infrastruktury Informacyjnej Państwa. Uważamy, że taki dokument powinien m.in. • Przedstawić doświadczenia innych krajów, zwłaszcza krajów członkowskich UE w procesie tworzenia i rozwijania chmur rządowych • Przedstawić listę aktów prawnych wymagających nowelizacji oraz kierunków tej nowelizacji, m.in. ustawa o informatyzacji, Rozporządzenie KRI, rozporządzenia sektorowe itd. oraz planu zmian tych aktów prawnych • Przedstawić relację WIIP związaną z tworzeniem wspólnego rynku cyfrowego w Europie (m.in. RODO, Rozporządzenie Free Flow of non-personal Data, dyrektywa NIS i np. wymagania wobec Dostawców Usług Cyfrowych) oraz usług pan-europejskich • Stworzenie zasad klasyfikacji danych w administracji, ich zabezpieczeń, zasad przetwarzania, archiwizacji itd. itp. • Wykorzystać dokumenty takie jak ENISA Security Framework for Governmental Clouds i wnioski z niego płynące dla wdrożenia RCO Przedstawione przez PIIT uwagi mogą być bezpośrednio zastosowane przy tworzeniu takiego dokumentu. **Uważamy stworzenie takiego dokumentu strategicznego za pilne, a prace nad nim powinny przebiegać równolegle do prac nad uchwałą. Mamy także świadomość, że pełne wdrożenie RCO i dołączenie do niego CPD należących do innych jednostek administracji będzie procesem, który będzie wymagał czasu (patrz uwaga nr 5 dotycząca zasad certyfikacji), stąd możliwość wykorzystania go do przygotowania odpowiedniego dokumentu strategicznego.** **Polska Izba Informatyki i Telekomunikacji deklaruje swoją pomoc merytoryczną przy stworzeniu takiego dokumentu.**	

2.	PIIT	Uchwała - całość	Prosimy o wyjaśnienie sposobu wykorzystania dokumentu dostępnego on line https://www.gov.pl/documents/31305/436699/Projekt_Rekomendacji_Ministra_Cyfryzacji_dotycz%C4%85cych_warunk%C3%B3w_technicznych_i_organizacyjnych_powierzenia_danych_administracji_publicznej_do_przetwarzania_w_publicznej_chmurze_obliczeniowej.odt/17bef34f-b621-1aac-e497-9686f362f0e1 zatytułowanego „Projekt Rekomendacji Ministra Cyfryzacji dotyczących warunków technicznych i organizacyjnych powierzenia danych administracji publicznej do przetwarzania w publicznej chmurze obliczeniowej" Projekt 2018.07.09. Dokument ten, był wielokrotnie omawiany z przedstawicielami przemysłu i do którego zgłoszono w ubiegłym roku wiele uwag, zawiera wiele rekomendacji odmiennych od zapisów zaproponowanych w treści uchwały wraz załącznikami.	
3.	PIIT	§ 1	Propozycja: Umieszczenie definicji chmury obliczeniowej w projekcie Uchwały. Uzasadnienie: w tekście Uchwały korzysta się z pojęć takich jak chmura obliczeniowa, prywatna chmura obliczeniowa, publiczna chmura obliczeniowa itd. itp. Również pojęć takich jak PaaS, IaaS, SaaS. W polskim prawie obecna jest tylko „Usługa przetwarzania w chmurze" zdefiniowana jako „Usługa umożliwiającą dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania przez wielu użytkowników", ustawa o krajowym systemie cyberbezpieczeństwa, Załącznik nr 2. Natomiast nie ma aktu, w którym zdefiniowana jest chmura obliczeniowa – wprowadzenie takiej definicji pozwoli także na uniknięcie używania pojęcia chmury dla innych usług teleinformatycznych, które są nazywane „chmurą" dla celów marketingowych. Poniżej proponujemy wprowadzenie tylko definicji chmury obliczeniowej, którą opcjonalnie można uzupełnić o definicje chmury prywatnej i chmury publicznej. Propozycja zapisu definicji bazuje na zmodyfikowanej przez Komisję Europejską definicji NIST (źródło: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_PL.pdf) **Chmura obliczeniowa** **Model umożliwiający powszechny, wygodny, udzielany na żądanie dostęp za pośrednictwem sieci do wspólnej puli możliwych do konfiguracji zasobów przetwarzania (np. sieci, serwerów, przestrzeni przechowywania, aplikacji i usług), które można szybko dostarczyć i uwolnić przy minimalnym wysiłku zarządzania lub działań dostawcy usługi.**	
4.	PIIT	§ 1 i § 11	Propozycja: wpisanie zasady pierwszeństwa korzystania ze Wspólnej Infrastruktury Informatycznej Państwa oraz w związku z tym usunięcia § 11. Propozycja brzmienia: § 1 (nowy) ust. 2	

			2. Przyjmuje się zasadę pierwszeństwa Wspólnej Infrastruktury Informatycznej Państwa dla budowania, rozwijania i wykorzystania wszystkich nowych i modyfikowanych systemów teleinformatycznych administracji publicznej. Uzasadnienie: taka zasada została wpisana w „Objaśnienia ogólne" w Załączniku nr 2, ale jest ona na tyle ważna, że powinna znaleźć się w samej treści Uchwały. Oczywiste korzyści wymienione w OSR są wystarczającym uzasadnieniem. Jednocześnie można usunąć § 11, który w sposób mniej zobowiązujący wskazywał tylko możliwość uzgodnień i to ograniczoną do Rządowej Chmury Obliczeniowej.	
5.	PIIT	Załącznik nr 1 pkt. 1	Podano niewłaściwe nazwy norm. Powinno być: 1. PN-ISO/IEC 20000-1 Technika informatyczna -- Zarządzanie usługami -- Część 1: Wymagania dla systemu zarządzania usługami 2. PN-EN-ISO/IEC 27001 Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji – Wymagania 3. PN-EN ISO 22031 Bezpieczeństwo powszechne -- Systemy zarządzania ciągłością działania – Wymagania Norma PN-ISO 31000 Zarządzanie ryzykiem – Wytyczne nie określa wymagań, gdyż jest zbiorem dobrych praktyk. Z tego powodu nie można uzyskać na tę normę potwierdzenia zgodności (nie ma określonych wymagań). Norma ta powinna być usunięta z listy. W wymaganiach zabrakło konieczności uwzględnienia norm specyficznych dla usług chmurowych w systemie zarządzania bezpieczeństwem informacji zgodnego z normą PN-EN ISO/IEC 27001: 1. PN-ISO/IEC 27017 Technika informatyczna -- Techniki bezpieczeństwa -- Praktyczne zasady zabezpieczenia informacji na podstawie ISO/IEC 27002 dla usług w chmurze 2. PN-ISO/IEC 27018 Technika informatyczna -- Techniki bezpieczeństwa -- Praktyczne zasady ochrony danych identyfikujących osobę (PII) w chmurach publicznych działających jako przetwarzający PII Należałoby również rozważyć uzyskanie certyfikatu CSA STAR (Cloud Security Alliance). Należy, jednakże zauważyć, że jedynie normy PN-EN-ISO/IEC 27001 oraz PN-EN ISO 22301 są normami zharmonizowanymi i jako takie mogą być przywoływane bezpośrednio w prawie wspólnotowym (normy zharmonizowane opracowuje jedna z europejskich organizacji normalizacyjnych w odpowiedzi na zlecenie normalizacji pochodzące od Komisji Europejskiej; normy zharmonizowane pozwalają wykazać, że dane produkty lub usługi są zgodne z wymogami technicznymi określonymi w odpowiednich przepisach prawa UE).	

			Odstąpienie od konieczności posiadania akredytowanych certyfikatów w zakresie wyżej wymienionych norm jest **niedopuszczalne (podobnie jak 18 miesięczne vacatio legis)**. Certyfikaty te posiadają takie platformy jak Microsoft Azure (https://azure.microsoft.com/pl-pl/overview/trusted-cloud/compliance/), czy Amazon Web Services (https://aws.amazon.com/compliance/programs/). Certyfikacje takie posiadają też znacznie mniejsi gracze na rynku, tacy jak: OVH (np. ISO/IEC 27001, PCI DSS poziom 1 dla usług płatniczych); ATMAN Cloud (ATM S.A.) (certyfikat ISO/IEC 27001), OCTAWAVE (Certyfikat ISO/IEC 27001 oraz CSA STAR) i inne. **Certyfikaty muszą być akredytowane, aktualne, wydane przed rozpoczęciem świadczenia usług, a ich zakres musi być adekwatny do świadczonych usług**.	
6.	PIIT	Załącznik nr 2 Tabela	Propozycja: Połączenie kategorii „Publiczna Chmura Obliczeniowa w jurysdykcji krajowej" oraz „Publiczna Chmura Obliczeniowa w jurysdykcji państwa UE" do kategorii „publiczna chmura obliczeniowa" Propozycja (alternatywa): w liniach 7 i 9 oznaczyć „x" dla kolumny „Publiczna Chmura Obliczeniowa w jurysdykcji państwa UE" Uzasadnienie: a) Nie ma definicji czym jest chmura obliczeniowa w jurysdykcji krajowej a czym chmura w jurysdykcji państwa UE – czy chodzi o pochodzenie podmiotu (dostawcy) usługi chmurowej? Lokalizację CPD takiego dostawcy? Czy chodzi o pochodzenie podmiotu, z którym zostanie podpisana umowa na usługi publicznej chmury obliczeniowej? Co, jeśli taki dostawca ma centrum zapasowe poza granicami Polski? Itd. itp. b) Dyrektywa NIS oraz ustawa o krajowym systemie cyberbezpieczeństwa zakłada ponadgraniczne świadczenie usług przez Dostawców Usług Cyfrowych, a zatem należałoby oczekiwać, że dla rozróżnienie na „jurysdykcję krajową" i „jurysdykcję państwa UE" będzie dotyczyło usług, które mają jeszcze wyższe wymagania bezpieczeństwa niż usługi kluczowe w rozumieniu ustawy o KSC; c) W projekcie rozróżnienie tych dwóch chmur publicznych występuje tylko w punktach 7 i 9, przy czym brak widocznego rzeczywistego uzasadnienia, dlaczego wprowadzono takie rozróżnienie; d) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej wprost zakazuje tworzenia przeszkód w swobodnym przepływie danych, a co więcej wszelkie istniejące przeszkody powinny być usunięte do 30 maja 2021 roku. ;	
7.	PIIT	Załącznik nr 2 Tabela pozycja 1.	Propozycja: Proponujemy rozważyć wykorzystanie Rządowej Chmury Obliczeniowej dla przetwarzania informacji o klauzuli „zastrzeżone" (po uprzedniej nowelizacji Rozporządzenia Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego).	

			Propozycja zapisu: Oznaczenie „X” także w kolumnie „Rządowa Chmura Obliczeniowa”, zaś w kolumnie „Objaśnienia dla poszczególnych kategorii” wpisać „Przetwarzanie w RCO tylko informacji o klauzuli „zastrzeżone” – po nowelizacji Rozporządzenia Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego Uzasadnienie: Informacje niejawne o klauzuli „zastrzeżone” są potencjalnie najczęściej stosowanymi informacjami, przy czym akredytacji bezpieczeństwa dokonuje kierownik jednostki organizacyjnej przekazując odpowiednio ABW lub SKW przygotowaną dokumentację (art. 48 p. 9 i nast.). Jest także możliwe, że system teleinformatyczny będzie działał w więcej niż jednej jednostce. W przypadku RCO oszacowanie ryzyk oraz przygotowanie bezpiecznego przetwarzania informacji opatrzonych klauzulą „zastrzeżone” będzie niemal bez wątpienia wyższe niż w wielu jednostkach organizacyjnych wymienionych w par. 6 Uchwały, w szczególności zaś jeśli z narzędzi RCO miałyby korzystać nie tylko jednostki administracji rządowej, ale także samorządy (patrz Ocena Skutków Regulacji załączona do projektu uchwały), gdzie poziom cyberbezpieczeństwa przy dzisiejszych zagrożeniach nie jest dostateczny. Sądzimy, że Rozporządzenie Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego z 20 lipca 2011 powstawało w czasie, kiedy model chmury obliczeniowej nie był rozpoznany i wymaga nowelizacji niezależnie od omawianej tutaj Uchwały. Warto przy tej okazji dokonać dodatkowej pracy i wprowadzić zapisy dotyczące chmury dla informacji o klauzuli „zastrzeżone”, w tym także dotyczące wymagań CPD serwującego usługi chmurowe, w którym takie informacje mogą być przetwarzane.	
8.	PIIT	Załącznik nr 2 Tabela pozycja 4.	Propozycja: doprecyzowanie zapisu tego punktu Propozycja zapisu: Systemy teleinformatyczne wykorzystywane do prowadzenia rejestrów, ewidencji oraz innych baz danych, **w których dane stanowią tajemnicę prawnie chronioną wynikającą z innych przepisów powszechnych**, i prowadzonych przez organy wymiaru sprawiedliwości, służby lub formacje umundurowane oraz służby odpowiedzialne za zapewnienie porządku i bezpieczeństwa publicznego, z wyłączeniem służb wskazanych w pkt 5. Uzasadnienie: Wymienione w pozycji 4 organy wymiaru sprawiedliwości, służby i formacje – podobnie jak wszystkie pozostałe organy administracji – mają dane, które mogą być sklasyfikowane w różny sposób. Obecny sposób zapisu wyłącza je w sposób sektorowy z praktycznie jakiegokolwiek wykorzystania chmury publicznej, a bez trudu można wskazać różne zastosowania, gdzie takie usługi mogłyby mieć ogromne zastosowanie. Oczywiście optymalnym rozwiązaniem byłoby wprowadzenie odpowiedniej klasyfikacji danych w administracji publicznej, podobnie jak to zostało już wprowadzone w wielu krajach. W dniu dzisiejszym praktycznie oprócz	

			informacji publicznych, informacji niejawnych, rozróżnienia na dane osobowe i nieosobowe oraz danych specyficznie opisanych przez oddzielne przepisy (tajemnica skarbowa, szczególne kategorie danych osobowych) mamy ogromną ilość informacji, która nie jest sklasyfikowana.	
9.	PIIT	Załącznik nr 2 Tabela pozycja 7.	Propozycja: oznaczenie „x" kolumny „Publiczna Chmura Obliczeniowa w jurysdykcji państwa UE" Uzasadnienie: patrz uwaga 6 dot. połączenia w jedną kolumn dla publicznej chmury obliczeniowej	
10.	PIIT	Załącznik nr 2 Tabela pozycja 9.	Propozycja: oznaczenie „x" kolumny „Publiczna Chmura Obliczeniowa w jurysdykcji państwa UE" Uzasadnienie: patrz uwaga 6 dot. połączenia w jedną kolumn dla publicznej chmury obliczeniowej	
11.	PIIT	Załącznik nr 2 Tabela pozycja 15	Propozycja: dopisanie do kolumny „Objaśnienia do poszczególnych kategorii" dodatkowej kategorii „Środowiska testowe z danymi testowymi, bez danych produkcyjnych" Propozycja alternatywna: stworzenie dodatkowego rzędu w tabeli z oznaczeniem „Środowiska prototypowe nie zawierające danych produkcyjnych (dane testowe)" i zaznaczeniem „x" w trzech kolumnach RCO, oraz dla chmur publicznych Uzasadnienie: Projekty (np. finansowane z funduszy UE) w pierwszych fazach polegają na zakupie i uruchomieniu dużej ilości infrastruktury i licencji na podstawie wstępnych założeń. Prototyp jest dostępny po wielu miesiącach i wtedy często okazuje się, że jest nie do przyjęcia. Alternatywą jest bądź albo oddać pieniądze do UE, bądź brnąć dalej w rozwiązanie, o którym wiadomo, że nie jest optymalne. Jednocześnie niezależnie od wyboru infrastruktura już jest „moralnie" zestarzała. Rozwiązaniem jest wykorzystanie chmury obliczeniowej do momentu powstania prototypu (na tym etapie w tworzonym systemie są tylko dane testowe). Dopiero po odebraniu pierwszych etapów projektu aplikacja jest przenoszona na produkcję i zasilana danymi. Oczywiście finalne rozwiązanie może być rozwiązaniem chmurowym, ale również może trafić do infrastruktury on-premise. Taki scenariusz: -obniża ryzyko projektowe -skraca czas projektu o pierwsze fazy dostawy i instalacji/konfiguracji -oszczędza opłaty maintanance itp. w pierwszych fazach projektu -pozwala zrobić poprawny sizing/skalowanie -chroni przed starzeniem się technologii, kiedy nie jest używana	

12.	PIIT	Załącznik nr 2 Tabela pozycja 15a	Propozycja: Dodanie jeszcze jednej linii w tabeli dla systemów superkomputerowych (HPC). Propozycja brzmienia: Kategoria systemów: Środowiska superkomputerowe Oraz zaznaczenie „x" w dwóch kolumnach dla chmur publicznych Uzasadnienie: Środowiska superkomputerowe są w chwili obecnej normalną częścią oferty chmury publicznej, a co więcej dostępne narzędzia wymagają coraz mniejszego przygotowania osób jest stosujących. Polskie centra superkomputerowe przede wszystkim mają służyć badaniom naukowym, natomiast dostępność dla zastosowań w administracji jest ograniczona i droga. Dlatego też ich wykorzystanie jest incydentalne. Widzimy natomiast możliwość prowadzenia niektórych obliczeń z wykorzystaniem HPC w takich zagadnieniach jak symulacje dla finansów publicznych, ubezpieczeń społecznych, ochrona zdrowia, statystyka czy nawet bezpieczeństwo narodowe (to ostatnie oczywiście z ograniczeniami).	
13.	PIIT	Załącznik nr 2 punkt 2	Propozycja: dopisanie nowego punktu przed podpunktem 1) Propozycja zapisu: **Dla systemów teleinformatycznych opisanych w kategoriach 11 oraz 15 i znajdujących się w katalogach udostępnionych w Systemie Zapewnienia Usług Chmurowych dokonywanie analizy nie jest wymagane.** Uzasadnienie: Uproszczenie procesu wykorzystania RCO lub usług chmury publicznej. § 8 ust. 1 wskazuje na to, że minister właściwy prowadzi procesy związane z zarządzaniem Systemu Zapewnienia Usług Chmurowych, czyli można to uznać za wstępną analizę usług chmurowych. Jednocześnie, niezależnie od tego czy system jest w infrastrukturze własnej czy w chmurze, każdy organ administracji publicznej obowiązują przepisy wynikające z ustawy o informatyzacji, Rozporządzenia Krajowe Ramy Interoperacyjności lub innych przepisów. A zatem dla tych najprostszych przypadków – kategorie 11 i 15 – można przyjąć, że nie jest potrzebna dodatkowa prac analityczna. Uwaga: jeśli zostanie przyjęta uwaga 11 (środowiska testowe) to również one nie wymagają robienia analizy z zastrzeżeniem jakie dane testowe będą wykorzystywane (jak te dane zostały przygotowane, czy przypadkiem nie jest to kopia danych rzeczywistych). Warto także rozważyć relację pomiędzy zapisami dotyczącymi wymagań analizy, a wymaganiami wobec Dostawców Usług Cyfrowych wynikających z ustawy o krajowym systemie cyberbezpieczeństwa oraz Rozporządzenia 2018/151.	

14.	PIIT	Załącznik nr 2 punkt 2 ustęp 1.	Propozycja: usunąć wszystkie zapisy tego ustępu od słów „lub w publicznych chmurach obliczeniowych”. Uzasadnienie: pozostała część ustępu jest bądź oczywista, bądź jest powtórzeniem informacji z tego samego ustępu	
15.	PIIT	Załącznik nr 2 punkt 2	Propozycja: w przypadku, kiedy jednostki sektora finansów publicznych wymienione w § 6 ust. 1 punkty 1) i 2) nie zamierzają wykorzystać Wspólnej Infrastruktury Informatycznej Państwa dodać wymaganie przygotowania przez te jednostki analizy obejmującej przyczyny techniczne, organizacyjne, prawne i finansowe takiej decyzji Propozycja brzmienia: **2) Jednostki sektora finansów publicznych wymienione w § 6 ust. 1 punkty 1) i 2), które dla swoich systemów teleinformatycznych nie zamierzają wykorzystać Wspólnej Infrastruktury Informatycznej Państwa winny przygotować analizę obejmującą przyczyny techniczne, organizacyjne, prawne i finansowe takiej decyzji przed rozpoczęciem procesu projektowania, budowania lub modyfikacji systemu teleinformatycznego.** **Analiza taka nie jest wymagana dla systemów teleinformatycznych, dla których niezbędna jest wyłącznie Dedykowana Infrastruktura Teleinformatyczna (DIT) zgodnie z listą kategorii systemów teleinformatycznych wymienionych w niniejszym załączniku.** **Analiza powinna zostać przekazana ministrowi właściwemu ds. informatyzacji przed podjęciem decyzji o pierwszych wydatkach z funduszy publicznych na cel związany z analizowanym systemem teleinformatycznym.** Uzasadnienie: Przyczyny stworzenia WIIP zostały przedstawione w OSR, a wprowadzenie WIIP powinno podnieść bezpieczeństwo, skrócić czas uruchamiania, uprościć zarządzanie zasobami, obniżyć koszty itd. itp. Jednocześnie jest jasne, że dla wielu systemów teleinformatycznych czy to obecnie eksploatowanych czy będących w trakcie procesu planowania, czy procesu zamówień publicznych przenoszenie ich do WIIP może nie być racjonalne. Również WIIP może nie dysponować w danym momencie odpowiednimi zasobami informatycznymi dla realizacji takich systemów. Dlatego też wymagane będzie od jednostek finansów publicznych wymienionych w § 6 ust. 1 p. 1) i 2) przygotowanie analizy wskazującej przyczyny odstąpienia od wykorzystania WIIP. **Uwaga: ostateczna decyzja o tym czy wykorzystany zostanie WIIP czy też nie pozostaje przy tej jednostce, do ministra właściwego ds. informatyzacji trafia wyłącznie przygotowana przez jednostkę analiza**. Dzięki takim analizom minister właściwy ds. informatyzacji, który jest za nią odpowiedzialny będzie miał dla celów planistycznych dwie dopełniające informacje – o zakresie wykorzystania WIIP oraz o potencjalnym zakresie wykorzystania WIIP, który nie doszedł do skutku. Pozwoli to na racjonalny	

			rozwój WIIP tak by w kolejnych latach w coraz większym stopniu taka infrastruktura mogła być wykorzystywana.	
			Uwagi o charakterze porządkowym	
16.	PIIT	§ 3 ust. 1	Propozycja: Przeniesienie zapisu § 3. ust. 1. jako pierwszego ustępu w § 5 Uzasadnienie: treść tego punktu dotyczy CPD, który szczegółowo jest opisany w § 5	
17.	PIIT	§ 3 ust. 2	Propozycja: Przeniesienie tego punktu jako drugiego ustępu w § 4 Uzasadnienie: lepsze umiejscowienie treści tego zapisu – poprawa czytelności.	
18.	PIIT	§ 3 ust. 2	Propozycja: usunięcie „oraz innymi organami administracji rządowej” Uzasadnienie: potrzeba współpracy ministra właściwego do spraw informatyzacji z ministrem właściwym do spraw finansów publicznych oraz ministrem właściwym do spraw wewnętrznych jest zapisana w dalszej części Uchwały natomiast nie ma w niej odniesienie do żadnych innych organów administracji rządowej. Współpraca na zasadach ogólnych jest oczywista i nie wymaga zapisu w uchwale. Współpraca związana z porozumieniami zawartymi z innymi organami wynika z zapisów tych porozumień.	
19.	PIIT	§ 3 ust. 3	Propozycja: usunięcie Uzasadnienie: ten ustęp nie wnosi niczego do treści uchwały. Wymienione są typowe usługi chmurowe, a zapis, że będą „w szczególności” świadczone mówi, że w zasadzie każde usługi chmurowe mogą być w RCO…	
20.	PIIT	§ 3 ust. 4	Propozycja: prosimy o precyzyjne zdefiniowanie czego dotyczy ten ustęp lub jego usunięcie Uzasadnienie: W § 3. Ust.2. zapisane jest kto będzie świadczył usługi RCO (minister właściwy do spraw informatyzacji), zaś w § 4 ust.2 zapisane jest komu powierza realizację zadania (Centralnemu Ośrodkowi Informatyki). Jaką inną sytuację zatem opisuje § 3 ust.4.?	
21.	PIIT	§ 5 ust. 2	Propozycja: usunięcie tego ustępu Uzasadnienie: zapis § 2 ust. 2. zawiera to co zostało zapisane w § 5 ust. 2. – nie ma potrzeby powtarzania tej samej informacji	
22.	PIIT	§ 7 ust. 7	Propozycja: usunięcie tego ustępu Uzasadnienie: zapis jest niezrozumiały…	
23.	PIIT	§ 8 ust. 3 pkt. 2) oraz § 8 ust. 4	Propozycja: proponujemy połączyć te dwa punkty Propozycja nowego brzmienia § 8 ust. 3 pkt. 2) katalog usług przetwarzania w publicznych chmurach obliczeniowych, aktualizowany po przeprowadzeniu postępowania na zakup usług przetwarzania w publicznej chmurze obliczeniowej zgodnie z przepisami ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień	

			publicznych (Dz. U. z 2018 r. poz. 1986 i 2215) **oraz zawarciu umów z wykonawcami**.	
24.	PIIT	§ 10 ust. 2	Propozycja: usunąć ten ustęp Uzasadnienie: dotyczy CPD, które nie są przyłączane do RCO, stąd dokonywanie przez posiadaczy tych CPD takich analiz jest zbędne; patrz także uwaga nr 27 (dotycząca Załącznika nr 1 punkt 5)	
25.	PIIT	Załącznik nr 1 oraz § 5 ust. 1	Propozycja: wprowadzenie nowego punktu § 5 ust. 1a w brzmieniu **Pisemne oświadczenie, o którym mowa w § 5 ust. 1. składane jest operatorowi Rządowej Chmury Obliczeniowej nie rzadziej niż co 12 miesięcy.** Uzasadnienie: Zgodnie z zapisami § 5 ust. 1 posiadacz CPD składa oświadczenie o spełnianiu minimalnych wymagań tylko raz. Nie ma żadnych mechanizmów, które by nakazywały regularnego sprawdzania stanu CPD i wypełniania tych wymagań. Brakuje jakichkolwiek mechanizmów kontrolnych dla operatora RCO. Uznajemy, że skoro wystarczającym jest oświadczenie posiadacza CPD o wypełnianiu warunków to wystarczy wskazać częstotliwość takiego oświadczenia.	
26.	PIIT	Załącznik nr 1 punkt 2 podpunkt 1)	Propozycja: ujednolicenie treści tego podpunktu z § 3 ust. 1 Uchwały Propozycja brzmienia: **obiekt CPD jest własnością organów administracji rządowej albo jednostki im podległej lub nadzorowanej** Uwaga: należy wyjaśnić kwestie „własności organów administracji rządowej". Formalnie „własność" zarezerwowana jest dla Skarbu Państwa, natomiast zarząd nad nią powierzany jest organowi administracji rządowej.	
27.	PIIT	Załącznik nr 1 punkt 5	Propozycja: usunąć Uzasadnienie: Posiadacz CPD, którego infrastruktura nie wchodzi do RCO nie musi spełniać wymagań zapisanych tą Uchwałą.	