Nazwa dokumentu: projekt uchwały Rady Ministrów zmieniającej uchwałę w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa” (ID409)					
Lp.	**Organ wnoszący uwagi**	**Jednostka redakcyjna, do której wnoszone są uwagi**	**Treść uwagi**	**Propozycja zmian zapisu**	**Odniesienie do uwagi**
1	**RCL**	Uwaga ogólna	Wyrażona w uzasadnieniu do projektu uchwały intencja Projektodawcy zakłada, że „*Celem* [uchwały] *jest także poprawa efektywności i bezpieczeństwa świadczenia usług przez administrację publiczną i inne podmioty, które zostały objęte zakresem uchwały*”. Zważywszy, że uchwała jest aktem prawa wewnętrznie obowiązującego powstaje wątpliwość, czy tak określony cel przez Projektodawcę zostanie osiągnięty. Akty o charakterze prawa wewnętrznego zgodnie z art. 93 Konstytucji RP nie mogą stanowić podstawy decyzji wobec obywateli i podmiotów niepozostających w stosunku podległości do organu wydającego akt. Tym samym regulacje uchwały nie mogą znaleźć zastosowania do podmiotów, które nie należą do kręgu jednostek podległych Radzie Ministrów lub nadzorowanych przez Radę Ministrów. Jeżeli intencją Projektodawcy w ramach niniejszej uchwały jest uregulowanie relacji pomiędzy organami władzy publicznej, administracją publiczną lub innymi podmiotami, wówczas ze względu na zasadę legalizmu konieczne będą zmiany odpowiednich przepisów ustawowych.		**Wyjaśnienie uwagi** Nie można zgodzić się z twierdzeniem, że intencja projektodawcy wychodzi poza zakres podmiotowy uchwały z racji tego, że uchwała nie może wiązać podmiotów administracji publicznej a jedynie administrację rządową. Przedmiotowy projekt nie nakłada obowiązków na administrację publiczną, ani na obywateli. Nakłada jedynie obowiązek spełnienia przez dostawców usług chmurowych określonych kryteriów bezpieczeństwa (m.in. SCCO lub NSC), który aktualizuje się w sytuacji przystąpienia podmiotu administracji do WIIP (dobrowolnie). Tym samym podmioty administracji publicznej, które nie należą do administracji rządowej a mimo to chciałyby skorzystać z usług

					chmurowych. o których stanowi przedmiotowy projekt, mają prawo wyboru i związania się właściwymi przepisami czy też określonymi wymaganiami z zakresu bezpieczeństwa. Nie należy także pomijać funkcjonalnej podległości administracji publicznej. Niezwykle istotny jest również fakt, że określony w uchwale cel należy rozpatrywać szeroko, w tym właśnie funkcjonalnie. Optymalizując koszty działania administracji rządowej (bezpośrednio podległej RM) zwiększamy bezpieczeństwo jej funkcjonowania. Z uwagi na sieć powiązań pomiędzy podmiotami bezpośrednio podległymi RM, a pozostałymi podmiotami administracji publicznej sumarycznie ten efekt będzie przeniesiony na te podmioty. Projekt zatem przewiduje także efekty pośrednie, które będą dotyczyły m.in. jednostek samorządu terytorialnego czy obywateli. W żaden sposób ich jednak nie wiąże. Projekt nie nakłada na żaden podmiot obowiązku

					korzystania z chmury obliczeniowej. Przystąpienie jest zatem dobrowolne. Jedyny nakaz jaki przewidziano to zakaz korzystania w zakresie poszczególnych rejestrów, natomiast dotyczy on wyłącznie podmiotów, które uchwała może wiązać bezpośrednio. Potwierdzeniem powyższych wyjaśnień jest również fakt, iż projektowana uchwała nie nowelizuje § 6 ust. 1 zmienianej uchwały, który określa katalog podmiotów, które mogą korzystać z usług przetwarzania danych w RChO, a zatem nie zmienia jego początkowo ustalonego zakresu podmiotowego.
2	**RCL**	§ 2 uchwały zmienianej	Zmiany w zakresie pojęć definiowanych uchwałą zmienianą (pojęcie *chmury obliczeniowej* i powiązane z nim pojęcie *podzielonej odpowiedzialności*) odwołują się do *modelu przetwarzania danych.* Podnieść w tym miejscu należy, że informacje o obywatelach i ich sprawach, pozyskane w związku z wykonywaniem zadań publicznych, które mogą być przewarzane w toku korzystania z chmur obliczeniowych, będą podlegać szczególnej ochronie. Zgodnie z art. 51 ust. 5 Konstytucji RP „Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.”. Jeżeli w ramach usług chmurowych miałyby być przetwarzane dane o obywatelach i ich sprawach, które podmioty publiczne gromadzą w ramach realizowania zadań publicznych, to wówczas w przypadku każdego rejestru, ewidencji czy zbioru danych musi istnieć ustawowa		**Wyjaśnienie uwagi** Przytoczone w uchwale definicje nie pozostają w sprzeczności z obowiązującymi przepisami. Przede wszystkim należy zwrócić uwagę na fakt, że nie ma mowy o przenoszeniu jakiejkolwiek odpowiedzialności za przetwarzanie danych na dostawcę usług chmurowych. Za przetwarzanie danych w

			podstawa w przepisach je tworzących do udostępnienia wskazanego zakresu danych podmiotom odpowiedzialnym za realizację usług chmurowych, niezależnie czy podmiotami tymi są podmioty administracji publicznej czy podmioty niepubliczne. Reasumując, dopuszczalność *modelu przetwarzania danych z zastosowaniem podzielonej odpowiedzialności* objętego projektowanymi definicjami wymaga ponownej analizy we wskazanym powyżej kontekście. Dodatkowo model *podzielonej odpowiedzialności* wymaga także analizy z punktu widzenia art. 77 ust. 1 Konstytucji RP. Przyjęta w projekcie zmiany uchwały konstrukcja, w której część tej odpowiedzialności (w związku z przetwarzaniem danych w chmurze) jest przenoszona na podmiot trzeci, nie będący organem władzy publicznej ani podmiotem nadzorowanym lub podległym takiemu organowi, może nie być skuteczna. Zwłaszcza w sytuacji, w której z przepisów powszechnie obowiązujących nie wynikają podstawy do ustalenia zakresu odpowiedzialności każdego z podmiotów uczestniczących w przetwarzaniu informacji o obywatelach i ich sprawach. Jak zauważono powyżej uchwała jest bowiem aktem wewnętrznie obowiązującym i nie może stanowić podstawy do egzekwowania odpowiedzialności w stosunku do podmiotów nie będących w stosunku podległości do organu wydającego ten akt. Określenie w akcie wewnętrznym odpowiedzialności podmiotu nie będącego w stosunku podległości, bez unormowania tej odpowiedzialności w ustawie, spowoduje nieskuteczność takiej odpowiedzialności.		usługach chmurowych odpowiada administrator. Dostawca usług chmurowych dostarcza jedynie odpowiednich usług w odpowiednim modelu dostarczania usług chmurowych (SaaS, PaaS, IaaS) z określonym poziomem SLA i zaimplementowanymi środkami bezpieczeństwa. Każdy z tych modeli dostarczania charakteryzuje się określonym zakresem działań i możliwości konfiguracji usługi i kontroli zastosowanych środków bezpieczeństwa. Ogólnie podział odpowiedzialności określa czym zarządza i do czego ma dostęp dostawca usługi a co leży w tym zakresie po stronie odbiorcy usługi/właściciela danych. Podzielona odpowiedzialność musi być wyraźnie opisana dla każdej usługi. Dopiero na tej podstawie odbiorca usług decyduje o możliwości budowy systemu teleinformatycznego w oparciu o dostarczane usługi i przetwarzanie w nim swoich danych. Odbiorca usług w celu zapewnienia poufności,

					integralności i dostępności danych, implementuje również odpowiednie środki bezpieczeństwa w oparciu o usługi dostawcy, a jeżeli jest to niewystarczające wdraża własne. W przytoczonej nowelizacji uchwały zwracamy uwagę na podział odpowiedzialności właśnie z tego powodu, że jest on w większości mylnie interpretowany jako przenoszenie odpowiedzialności za przetwarzanie danych na dostawcę usług. Zagadnienie to jest opisywane dokładnie w przytaczanych w uchwale standardach SCCO i NSC. Wskazać należy, iż tak długo, jak długo to dana organizacja będzie określać środki i cele przetwarzania, tak długo to ona będzie Administratorem z punktu widzenia RODO – a dostawca usług chmurowych będzie działał jako Podmiot Przetwarzający (tzn. będzie przetwarzał dane osobowe w imieniu organizacji).
3	**RCL**	§ 2 uchwały zmienianej	W zakresie definicji *Rządowego Klastra Bezpieczeństwa*: definicja wprowadza odesłania do usług i środków bezpieczeństwa *„powiązanych z wymaganiami określonymi w Narodowych*	Usunięto wyraz „powiązanie” i przeredagowano	**Uwaga częściowo uwzględniona – wyjaśniona w pozostałym zakresie**

			Standardach Cyberbezpieczeństwa” lub „*ich odpowiedników w europejskim układzie normalizacji*”. (….) Ponadto, skoro niniejszym projektem uchwały wprowadza się określone wymagania o charakterze standardu świadczenia usługi cyfrowej, to może powstać potrzeba dokonania notyfikacji technicznej. Zgodnie bowiem z § 2 pkt 5 lit. e rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 w sprawie krajowego systemu notyfikacji norm i aktów prawnych, pojęcie przepisu technicznego dotyczy także „*postanowienia porozumień dobrowolnych, których stroną są organy administracji rządowej i które zawierają zobowiązania do stosowania, w interesie publicznym, specyfikacji technicznych lub innych wymagań, z wyłączeniem umów podlegających przepisom o zamówieniach publicznych, zwanych dalej "porozumieniami dobrowolnymi”*”. Kwestia ta wymaga ponownej analizy i przedstawienia stosownego uzasadnienia w tym zakresie.	brzmienie przepisu (*„… lub wymagań określonych w Narodowych Standardach Cyberbezpieczeństwa”*).	Usunięto wyraz „powiązanie” i przeredagowano brzmienie przepisu (*„… lub wymagań określonych w Narodowych Standardach Cyberbezpieczeństwa”*). Uwaga w zakresie notyfikacji nie zasługuje na uwzględnienie z racji tego, że projekt ma w znacznej mierze charakter porządkowy, podyktowany koniecznością aktualizacji przepisów ze względu na postęp technologiczny jaki dokonał się od momentu przyjęcia uchwały i pojawiające się nowe wyzwania w obszarze cyberbezpieczeństwa. Należy przy tym zauważyć, że zmieniana uchwała nie była notyfikowana technicznie, a dokonywanie notyfikacji technicznej w znaczny sposób wydłużyłoby procedowanie projektu, co nie jest wskazane ze względu na pilny charakter projektu mający znaczenie m.in. dla podniesienia poziomu bezpieczeństwa przetwarzania danych i świadczenia usług elektronicznych w administracji rządowej.
4	**RCL**	§ 2 uchwały zmienianej	Dodatkowo wymaga ponownej analizy kwestia wewnętrznej spójności niniejszej regulacji. Zgodnie bowiem z § 3 uchwały		**Wyjaśnienie uwagi** Strategia

			dotychczas obowiązującej (w tym zakresie niezmienianej) „*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*.”. Natomiast Narodowe Standardy Cyberbezpieczeństwa, o których mowa w zmienianym przepisie, stanowią zbiór rekomendacji, które zostały opublikowane przez ministra właściwego do spraw informatyzacji jako jedna z form realizacji Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024 w zakresie opracowania i wdrożenia Narodowych Standardów Cyberbezpieczeństwa. Budzi zatem wątpliwość możliwość powołania ich w niniejszej uchwale, zwłaszcza, że odrębnie zostały określone „Standardy Cyberbezpieczeństwa dla Chmur Obliczeniowych” na podstawie niniejszej uchwały. Opublikowane w domenie gov.pl Narodowe Standardy Cyberbezpieczeństwa nie wskazują podstawy prawnej ich przyjęcia, stąd nie jest pewne do jakiego katalogu podmiotów mają mieć zastosowanie i kto jest zobowiązany do ich stosowania oraz jaka jest ich relacja do Standardów Cyberbezpieczeństwa dla Chmur Obliczeniowych wynikających z przedmiotowej uchwały. Relacja tych dwóch rodzajów standardów wymaga również wyjaśnienia. Należy także zwrócić uwagę na to, że § 9 dotychczasowej uchwały, niezmienianej niniejszym projektem, wskazuje, że Rządowy Klaster Bezpieczeństwa „obejmuje” wskazane w tym przepisie usługi. Przepis ten wymaga analizy wobec nowej definicji Rządowego Klastra Bezpieczeństwa, który ma obejmować także *„środki techniczne stosowane do zabezpieczenia Rządowej Chmury Obliczeniowej”.*		Cyberbezpieczeństwa Chmur Obliczeniowych oraz Narodowe Standardy Cyberbezpieczeństwa są dwoma różnymi dokumentami, choć te pierwsze składają się m.in. z tych drugich. Narodowe Standardy Cyberbezpieczeństwa (NSC) bazują na amerykańskim standardzie NIST i zapewniają wysoki poziom bezpieczeństwa. Ponadto wprowadzenie NSC do uchwały WIIP powoduje, że nadana została tym dokumentom moc wiążąca oraz określony został katalog podmiotów, które obowiązane będą korzystać z NSC w sytuacji, gdy na to się zdecydują.
5	**RCL**	§ 2 uchwały zmienianej	W § 2 pkt 1 uchwały projektodawca posługuje się sformułowaniem „*Centrum Przetwarzania Danych*”. Wobec przyjęcia ustawy z dnia 7 lipca 2023 r. w sprawie przygotowania i realizacji inwestycji w sprawie Krajowego Centrum Przetwarzania Danych (Dz. U. poz. 1501) wymaga wyjaśnienia relacja pomiędzy „Krajowym Centrum Przetwarzania Danych” a „Centrum Przetwarzania Danych”, o		**Wyjaśnienie uwagi** Krajowe Centrum Przetwarzania Danych – sieć ośrodków obliczeniowych (Centrów Przetwarzania Danych) połączonych łączami

			którym mowa w niniejszym projekcie uchwały. Definicja *Krajowego Centrum Przetwarzania Danych* z art. 2 pkt 5 ustawy odwołuje się do „obiektów budowlanych” wraz z infrastrukturą teleinformatyczną, do czego odwołuje się także definicja *Centrum Przetwarzania Danych* z niniejszej uchwały zmieniającej.		światłowodowymi wraz z infrastrukturą techniczną niezbędną do ich funkcjonowania, umożliwiających przetwarzanie danych w systemach teleinformatycznych, w szczególności ich zbieranie, przeglądanie, utrwalanie, przechowywanie, organizowanie, opracowywanie, zmienianie, przesyłanie, udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie, w sposób zabezpieczający ciągłość przepływu danych na potrzeby systemów teleinformatycznych wykorzystywanych dla potrzeb w administracji publicznej, dostawców kluczowych usług publicznych oraz przedsiębiorstw; W skrócie KCPD to wiele CPD. Definicja przytoczona w uwadze nie generuje potrzeby zmiany definicji w przedmiotowym projekcie.
6	**RCL**	§ 3a uchwały zmienianej	W zakresie dodawanego § 3a dotyczącego kompetencji Pełnomocnika Rządu do spraw Cyberbezpieczeństwa i udziału Kolegium do spraw Cyberbezpieczeństwa w działaniach wynikających z niniejszej uchwały należy zauważyć, że organy władzy publicznej działają na podstawie i w granicach prawa.		**Wyjaśnienie uwagi** Zmiany w uchwale dotyczące wydawania, zmiany lub odwoływania rekomendacji i gradacji ważności systemów

			Kompetencje Pełnomocnika Rządu do spraw Cyberbezpieczeństwa określa art. 62 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cybebezpieczeństwa. Ustawa stanowi, że do zadań Pełnomocnika należy „*wydawanie rekomendacji dotyczących stosowania urządzeń informatycznych lub oprogramowania na wniosek CSIRT*". W tym pojęciu nie mieszczą się jednak „*rekomendacje dotyczące gradacji ważności systemów*," o których mowa w projektowanej uchwale. Z tego też względu wątpliwe staje się zobowiązanie projektowaną uchwałą Kolegium do spraw Cyberbezpieczeństwa do udziału w wydawania takich rekomendacji. Ponadto projektowany przepis wskazuje, że Pełnomocnik Rządu do spraw Cyberbezpieczeństwa będzie miał możliwość żądania od podmiotów, o których mowa w § 6 ust. 1 uchwały (w zakresie niezmienianym) tj. jednostek sektora finansów publicznych, innych państwowych osób prawnych oraz państwowych jednostek organizacyjnych nieposiadających osobowości prawnej, informacji o spełnieniu wymagań oraz przekazywania informacji zwrotnej do organu nadzorującego te podmioty. Ponieważ relacje pomiędzy poszczególnymi organami władzy publicznej oraz jednostkami organizacyjnymi sektora finansów publicznych, określają ustawy nie jest możliwe tworzenie regulacji na poziomie uchwały, których celem jest wprowadzenie nowych kompetencji i podziału zadań pomiędzy tymi podmiotami.		przez Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa w większym stopniu precyzują powyższe procesy decyzyjne, co będzie miało większe przełożenie na bezpieczeństwo systemów IT. Zadanie określone w uchwale wynika także z zadania określonego w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (art. 62 ust. 1 pkt 4), tj. upowszechnianie nowych rozwiązań i inicjowanie działań w zakresie zapewnienia cyberbezpieczeństwa na poziomie krajowym. Wydawanie rekomendacji dotyczących gradacji ważności systemów i przetwarzanych w nich danych ma bowiem bezpośredni wpływ na cyberbezpieczeństwo oraz bezpieczeństwo danych przetwarzanych w ramach usług chmurowych. Tym samym nowa kompetencja ww. Pełnomocnika pozostaje w związku z zadaniami określonymi w przepisach prawa powszechnie obowiązującego. W przedmiocie relacji podmiot

					– Pełnomocnik, należy podkreślić, że podmiot może, a nie musi korzystać z usług o których mowa w uchwale WIIP. Chcąc jednak skorzystać z tych usług musi zastosować odpowiednie przepisy uchwały i dopiero wtedy realizuje się zależność podmiot-Pełnomocnik, która jest jednak pośrednia, ponieważ to dostawca usług chmurowych danego podmiotu musi zadeklarować, że spełnia wymagania określone w Narodowych Standardach Cyberbezpieczeństwa (NSC). Przepis określający wymagania skierowany jest zatem do dostawcy usług chmurowych, którego usług następnie podmiot będzie mógł skorzystać.
7	**RCL**	§ 3b uchwały zmienianej	W zakresie § 3b należy zauważyć, że ograniczenia do korzystania z usług chmurowych w ramach Publicznej Chmury Obliczeniowej przewidziane niniejszą uchwałą dla niektórych systemów teleinformatycznych nie są adekwatnym środkiem do osiągnięcia celu zakładanego przez projektodawcę. Wskazane w tym przepisie systemy pozostają bowiem w dyspozycji organów wskazanych w przepisach ustawowych na podstawie których uruchomiono te systemy. Organy te w zakresie administrowania i zarządzania systemami dysponują własnymi kompetencjami. Przykładowo w odniesieniu do Krajowego Systemu Informacyjnego Policji do zapewnienia utrzymania, rozwoju i modyfikacji tego systemu został upoważniony Komendant Główny Policji (art. 21nb ustawy z dnia 6		**Wyjaśnienie uwagi** W uchwale przewiduje się dobrowolność przystąpienia do rozwiązań chmurowych. Uchwała nie nakłada zatem obowiązku korzystania z RChO lub PChO. Przewiduje natomiast katalog wyłączeń określonych systemów z uwagi na charakter przetwarzanych w nich danych. Należy również podkreślić, że

			kwietnia 1990 r. o Policji). To zatem w ustawach, które tworzą te systemy należałoby uregulować możliwość korzystania z usług chmurowych a także ograniczenia możliwości korzystania z konkretnego rodzaju usług w momencie realizowania przez wskazane w nich organy swoich ustawowych kompetencji. Tym bardziej, że korzystanie z usługi chmurowej wiąże się (zgodnie z intencją wyrażoną w projekcie) z przetwarzaniem danych.		administratorzy wskazanych systemów nie zgłosili analogicznych uwag co do katalogu wyłączeń. Do tej pory systemy te częściowo były wyłączone przez załącznik nr 2, a więc ich wyłączenie również nie opierało się o ustawę.
8	**RCL**	§ 6 uchwały zmienianej	W zakresie zmiany w § 6 (§ 1 pkt 3 projektu uchwały) – wymaga zauważenia, że regulacja ta określa warunki korzystania z Rządowej Chmury Obliczeniowej, przy czym warunki te dotyczą także podmiotów sektora finansów publicznych, które nie należą do podmiotów administracji rządowej tzn. m. in. jednostek samorządu terytorialnego. Regulowanie w uchwale Rady Ministrów wymagań nakładanych na podmioty, które nie należą do jednostek podległych Radzie Ministrów budzi wątpliwości.		**Wyjaśnienie uwagi** Przedmiotowy projekt nie nakłada obowiązków na administrację publiczną. Nakłada jedynie obowiązek spełnienia określonych kryteriów bezpieczeństwa na dostawców usług chmurowych (m.in. SCCO lub NSC), który aktualizuje się w sytuacji przystąpienia podmiotu administracji do inicjatywy WIIP. Tym samym podmioty administracji publicznej, które nie należą do administracji rządowej a mimo to chciałyby skorzystać z usług chmurowych, o których stanowi przedmiotowy projekt, mają prawo wyboru i związania się właściwymi przepisami czy też określonymi wymaganiami z zakresu bezpieczeństwa. Nie należy także pomijać funkcjonalnej podległości

					administracji publicznej. Projekt dostarcza rozwiązanie ponadsektorowe, dostępne dla odbiorców z obszaru administracji rządowej oraz w przypadku usług chmury publicznej, dla wszystkich jednostek administracji. Jednostki administracji samorządowej uzyskają m.in. dostęp do dedykowanych narzędzi wspierających proces zamawiania usług IT. **Co istotne, projekt nie wprowadza w tym przepisie zmian podmiotowych** a jedynie dookreśla jakie wymagania należy spełnić, aby skorzystać z usług przetwarzania w RChO lub PChO dodając możliwość spełnienia wymagań wskazanych w NSC lub w ich odpowiednikach określonych w europejskim układzie normalizacji. Podkreślić należy, że przepisy dotyczące deklaracji lub certyfikacji skierowane są w stronę dostawcy usług chmurowych, a nie podmiotu administracji.
9	**RCL**	§ 11 uchwały zmienianej	W zakresie § 11 (§ 1 pkt 5 projektu uchwały) – wymaga wyjaśnienia czy finansowanie wydatków wynikających z niniejszej uchwały znalazło swoje odzwierciedlenie w ustawie budżetowej.		**Wyjaśnienie uwagi** Do projektu ustawy budżetowej na rok 2024 zgłoszone zostało

					zapotrzebowanie na środki niezbędne do realizacji inicjatywy w ramach rezerwy celowej, tj. w sposób w jaki obecnie jest finansowana. Podyktowane jest to m.in. faktem, iż nie ma podstawy prawnej do zabezpieczania środków na WIIP w ramach części 27 budżetu państwa, ponieważ nowelizacja jest na etapie projektu. Po jej przyjęciu i wejściu w życie dopiero wtedy zrealizuje się podstawa prawna do zmiany finansowania, a tym samym odpowiedniego przesunięcia środków z rezerwy celowej na części 27 budżetu państwa.
10	**RCL**	Załącznik do uchwały	W zakresie zmian projektowanych w załączniku nr 1 (§ 1 pkt 6 projektu uchwały) – ze względu na wprowadzone niniejszym załącznikiem normy o charakterze technicznym ponownie wymaga rozważenia kwestia notyfikacji technicznej przepisów niniejszej uchwały. Dodatkowo wymaga wyjaśnienia w jakiej procedurze podmiot właściwy będzie podlegał certyfikacji, z uwagi na brak przepisów odnoszących się do procedury certyfikacji w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Kwestia procedury certyfikacji wymaga odpowiedniego wyjaśnienia.		**Wyjaśnienie uwagi** Uwaga w zakresie notyfikacji nie zasługuje na uwzględnienie z racji tego, iż projekt ma w znacznej mierze charakter porządkowy, podyktowany koniecznością aktualizacji przepisów ze względu na postęp technologiczny jaki dokonał się od momentu przyjęcia uchwały i pojawiające się nowe wyzwania w obszarze cyberbezpieczeństwa. Dodatkowo *vide* wyjaśnienie braku potrzeby dokonywania

					notyfikacji technicznej, ujęte w stanowisku projektodawcy do uwagi Rządowego Centrum Legislacji do § 1 pkt 1 lit. g projektu. W zakresie certyfikacji należy wyjaśnić, że celowo nie określono procedury certyfikacji. Wynika to z faktu, iż zdecydowano się na przyjęcie modelu polegającego na tym, że dany dostawca usług chmurowych z którego usług zamierza skorzystać podmiot administracji obowiązany jest przedstawić deklarację spełnienia określonych w uchwale wymagań bądź certyfikację w tym zakresie. Certyfikacja nie będzie zatem prowadzona jako proces, a wyłącznie przedkładany przez dostawcę będzie już posiadany certyfikat, który potwierdza spełnianie przez usługę wymagań określonych w projekcie uchwały.
11	**RCL**	§ 2 i § 5 uchwały zmienianej	W § 2 uchwały zmienianej projekt zmienia definicję *sieci rządowej*, określając, że będzie to sieć GOV.net. Wskazano, że minister właściwy do spraw wewnętrznych będzie operatorem takiej sieci. Pojęcie to nie jest znane ani ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne ani ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Wymaga zatem wyjaśnienia jaki w świetle obowiązujących przepisów będzie status takiego operatora, a biorąc pod uwagę, że działalność telekomunikacyjna stanowi		**Wyjaśnienie uwagi** Zmiana została wprowadzona zgodnie z uwagą MSWiA na etapie uzgodnień (uwaga wraz ze stanowiskiem projektodawcy została udostępniona w Biuletynie Informacji Publicznej

			działalność regulowaną jaka będzie jego relacja i pozycja wobec regulacji przedsiębiorców telekomunikacyjnych czy świadczenia usług na tym rynku. Co więcej w § 5 (w nowym brzmieniu) wskazuje się, że zasady wykorzystania sieci rządowej na potrzeby Rządowej Chmury Obliczeniowej będzie określało porozumienie zawarte pomiędzy ministrem właściwym do spraw wewnętrznych a ministrem właściwym do spraw informatyzacji. Jednocześnie usługa Rządowej Chmury Obliczeniowej ma być przypisana podmiotom administracji publicznej (nie zostało wskazane – czy krąg obejmie wyłącznie administrację rządową czy również jednostki samorządu terytorialnego, a uchwała RM nie jest właściwym aktem prawnym do regulowania sytuacji administracji samorządowej). Ponieważ obowiązkiem działania władzy publicznej, które będą związane z korzystaniem z usług chmurowych będą dotyczyć danych obywateli niniejsza uchwała, ani porozumienie zawarte pomiędzy ministrami nie są adekwatnym środkiem prawnym do regulowania tych kwestii.		Ministerstwa Cyfryzacji). Sieć GovNet jest siecią podkładową dla sieci TESTA-NG, która korzysta z infrastruktury sieciowej sieci GovNet. Tym samym sieć GovNet jest siecią nadrzędną i nie ma potrzeby wyodrębniania sieci TESTA-NG w zaproponowanej przez projektodawcę definicji sieci. Mając na uwadze odrębność sieci GovNet od sieci, o których mowa w ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, czy też ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, to minister właściwy do spraw wewnętrznych będący operatorem sieci rządowej nie wpływa na działalność przedsiębiorców telekomunikacyjnych czy świadczenie usług na tym rynku. Poza tym organy kierujące jednostkami organizacyjnymi podległymi ministrowi właściwemu do spraw wewnętrznych lub przez niego nadzorowanymi, uwzględnione w definicji sieci rządowej, nie są podmiotami

					zarządzającymi wskazanymi sieciami. Podmiotem zarządzającym w odniesieniu do tych sieci jest wyłącznie minister właściwy do spraw wewnętrznych.
12	**RCL**	§ 8 uchwały zmienianej	Kompetencje Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego reguluje rozdział 6 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Wprowadzanie kompetencji tych Zespołów i uprawnienia do występowania o opinię do tych zespołów dla podmiotów korzystających z usług chmurowych wymaga zatem odpowiedniej zmiany w ustawie.		**Wyjaśnienie uwagi** Niniejsza zmiana nie jest podyktowana wprowadzeniem kompetencji właściwych Zespołów do uchwały, a ma jedynie na celu wyeliminowanie problemów interpretacyjnych związanych ze stosowaniem przedmiotowej uchwały. Celem zmiany jest wyraźne doprecyzowanie, iż wniosek o wydanie opinii ma charakter fakultatywny, a opinia ma spełniać rolę pomocniczą dla uprawnionego podmiotu w procesie podejmowania decyzji o skorzystaniu z PChO. Szczegółowe wyjaśnienie wprowadzonej zmiany zawarte zostało w uzasadnieniu projektowanej uchwały.
13	**RCL**	§ 2 projektu	Biorąc pod uwagę zmiany dokonywane niniejszą uchwałą wymaga ponownej analizy przepis dostosowujący. Przepis ten wskazuje, że wszelkie podmioty korzystające dotychczas z usług Rządowej Chmury Obliczeniowej lub Publicznej Chmury Obliczeniowej uważa się za spełniające wymagania określone w niniejszej uchwale. Przepisy uchwały nie ustanawiają przy tym żadnej procedury weryfikacji spełniania przez te podmioty nowo wprowadzanych		**Wyjaśnienie uwagi** Dostawcy usług, którzy świadczą usługi w ramach Inicjatywy WIIP na podstawie SCCO, nadal będą mogli świadczyć swoje usługi na podstawie tych standardów.

			standardów (wymogów).		Projektowana zmiana nie zakłada odstąpienia od SCCO, a jedynie dopuszcza możliwość świadczenia usług w oparciu o inne standardy. Powyższy zabieg umożliwia płynne przejście przez proces zmiany wykorzystywanego rozwiązania bez konieczności weryfikacji. NSC i SCCO są standardami tak zbliżonymi i tak kompatybilnymi ze sobą, że procedura weryfikacji nie jest konieczna. Celem nowelizacji jest umożliwienie poszczególnym dostawcom płynnego przejścia na standardy NSC jeżeli dotychczas korzystali z SCCO ale jednocześnie zagwarantowanie możliwości korzystania z SCCO nadal po wejściu w życie przedmiotowej uchwały. Mając to na uwadze nie zachodzi potrzeba zmiany lub dookreślenia przepisu przejściowego.