|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Nazwa dokumentu: 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. |  |  |
| **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 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. |  |  |
| **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 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. |  |  |
| **4** | **RCL** | § 2 uchwały zmienianej | Dodatkowo wymaga ponownej analizy kwestia wewnętrznej spójności niniejszej regulacji. Zgodnie bowiem z § 3 uchwały 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”.* |  |  |
| **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 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. |  |  |
| **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. 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. |  |  |
| **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 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. |  |  |
| **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. |  |  |
| **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. |  |  |
| **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 |  |  |
| **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 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. |  |  |
| **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. |  |  |
| **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 standardów (wymogów). |  |  |