

**UWAGI W RAMACH UZGODNIEN Z KOMISJĄ WSPÓLNA RZĄDU I SAMORZĄDU TERYTORIALNEGO**

**Informacja o projekcie:**

<b>Tytuł</b>	Uchwała Rady Ministrów zmieniająca uchwałę nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa”
<b>Autor</b>	Ministerstwo Cyfryzacji
<b>Projekt z dnia</b>	18 września 2023 r.

**Informacje o zgłaszającym uwagi:**

<b>Urząd</b>	
<b>Organizacja samorządowa</b>	Związek Powiatów Polskich
<b>Osoba do kontaktu</b>	Grzegorz Kubalski
<b>e-mail</b>	
<b>tel.</b>	

**Uwagi:**

<b>Lp.</b>	<b>Część dokumentu, do którego odnosi się uwaga (np. art., nr str., rozdział)</b>	<b>Treść uwagi (propozycja zmian)</b>	<b>Uzasadnienie uwagi</b>	<b>Stanowisko resortu</b>	<b>Odniesienie do stanowiska resortu</b>
1.	§1 pkt 2 w zakresie dodawanego §3a ust. 1	Zmienić adresata normy albo określić w treści uchwały dopuszczalny zakres rekomendacji (np. poprzez zdefiniowanie pojęcia gradacji ważności systemów) jednoznacznie wskazujący, że obowiązki wynikające z rekomendacji leżą po stronie podmiotów korzystających z usług, nie zaś dostawców usług.	Pomimo dokonanych zmian redakcyjnych nadal adresatem normy §3a ust. 1 są nie dostawcy usług chmurowych, ale podmioty korzystające z usług dostawców (np. jednostki samorządu terytorialnego). Zgodnie z treścią uzasadnienia „Przepis ten znajdzie zastosowanie w sytuacji, gdy podmiot zdecyduje się skorzystać z usług chmurowych świadczonych przez dostawcę, który stosuje NSC wskazane w projekcie, a nie SCCO.” Wydaje się zatem, że rola podmiotu publicznego ogranicza się do wybrania usług chmurowych świadczonych przez dostawcę stosującego NSC. Jeśli tak to nie jest jasne co w ramach wdrażania rekomendacji jest w stanie wykonać		

			podmiot korzystający z usługi. W efekcie należy albo doprecyzować zakres rekomendacji albo wskazać, że obowiązki w zakresie wdrażania rekomendacji spoczywają na dostawcy usług chmurowych.		
2.	§1 pkt 2 w zakresie dodawanego §3a ust. 5	Zmienić konsekwencje nieuwzględnienia rekomendacji w przypadku podmiotów administracji samorządowej.	Przywołany przepis jest dostosowany do specyfiki administracji rządowej – zbudowanej w oparciu o strukturę hierarchiczną. Jest on chybiony w przypadku administracji samorządowej. Ogólnym organem nadzoru nad jednostkami samorządu terytorialnego jest wojewoda, ale jego nadzór ogranicza się wyłącznie do kwestii legalności działań. Rekomendacje nie są źródłem prawa powszechnie obowiązującego, a zatem ich nieuwzględnienie nie może stanowić podstawy działania dla wojewody jako organu nadzoru. Oznacza to występowanie Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa do organu sprawującego nadzór nad jednostkami samorządu terytorialnego. Być może pomysłodawcy przepisu chodziło o sytuację, w której np. informacje o nieuwzględnieniu rekomendacji przez szkołę przekazuje się wójtowi - ale – niekoniecznie to jednoznacznie wynika z przepisu.		
3.	§1 pkt 4 lit. a	Zmiana adresata normy na dostawcę usług chmurowych, np. „Dostawcy usług chmurowych opartych na przetwarzaniu danych w RChO lub PChO są zobowiązani do spełniania	Pomimo dokonanej zmiany w redakcji przepisu pozostają wątpliwości interpretacyjne. Obowiązek spełnienia wymogów cyberbezpieczeństwa powinien		

		wymagań, o których mowa w §2 pkt 13 lit. a-c lub pkt 15, lub w ich odpowiednikach określonych w europejskim systemie normalizacyjnym.”	dotyczyć <u>oferowanych</u> usług chmurowych wykorzystujących przetwarzanie danych w RChO lub PChO. Obecne brzmienie przepisu przenosi ten obowiązek dopiero na etap <u>korzystania</u> z usług. Co więcej – ponieważ uzależnia korzystanie z usług przetwarzania danych przez podmioty uprawnione do spełnienia warunków przez dostawców nie jest jasne, czy przewidziane w dodawanym ust. 3 deklaracje mają być składane operatorowi RChO/PChO, czy każdemu z podmiotów, które chcą z usług korzystać i jako takie są obowiązane do weryfikacji – co jest po prostu niewykonalne w przypadku mniejszych jednostek.		
--	--	--	--	--	--