**Raport z konsultacji**

***projektu uchwały Rady Ministrów zmieniającej uchwałę w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa”*** *(ID409)*

1. **Omówienie wyników konsultacji publicznych i opiniowania**

Projekt ***uchwały Rady Ministrów zmieniający uchwałę w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa”*** został poddany opiniowaniu w sierpniu br., z terminem 14 dni na zgłoszenie ewentualnych uwag. Ze względu na konieczność pilnego wejścia w życie i szczególny charakter regulacji nie przeprowadzono konsultacji publicznych projektu.

Projekt w ramach opiniowania został przekazany łącznie do 9, następujących podmiotów:

1) Centralnego Ośrodka Informatyki;

2) Prezesa Urzędu Ochrony Danych Osobowych;

3) Agencji Bezpieczeństwa Wewnętrznego;

4) Centrum e-Zdrowie;

5) Urzędu Komisji Nadzoru Finansowego;

6) Agencji Wywiadu;

7) Komendy Głównej Policji;

8) Rady do Spraw Cyfryzacji;

9) Komisji Wspólnej Rządu i Samorządu Terytorialnego.

W ramach opiniowania wpłynęły uwagi Urzędu Ochrony Danych Osobowych, Komisji Nadzoru Finansowego oraz Rady do Spraw Cyfryzacji.

Pozostałe podmioty nie wniosły uwag do projektu.

Omówienie zgłoszonych uwag zostało przedstawione w załączniku do niniejszego raportu.

Projekt był przedmiotem opiniowania Komisji Wspólnej Rządu i Samorządu, która wyraziła pozytywną opinię dotyczącą projektu, po przyjęciu stanowiska w trybie obiegowym w dniu 26 września br.

Konferencja uzgodnieniowa dotycząca omówienia zgłoszonych uwag i propozycji nie jest przewidywana.

1. **Omówienie wyników zasięgnięcia opinii, dokonania konsultacji albo uzgodnienia projektu z właściwymi organami i instytucjami Unii Europejskiej, w tym Europejskim Bankiem Centralnym**

Z uwagi na zakres projektu nie zasięgano opinii oraz nie dokonywano konsultacji i uzgodnień z organami i instytucjami Unii Europejskiej, w tym z Europejskim Bankiem Centralnym.

*Załącznik do Raportu*

**ZESTAWIENIE UWAG I PROPOZYCJI ZGŁOSZONYCH W RAMACH OPINIOWANIA PROJEKTU UCHWAŁY RADY MINISTRÓW ZMIENIAJĄCEJ UCHWAŁĘ W SPRAWIE INICJATYWY „WSPÓLNA INFRASTRUKTURA INFORMATYCZNA PAŃSTWA”**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Organ wnoszący uwagi** | **Jednostka redakcyjna, do której wnoszone są uwagi** | **Treść uwagi** | **Stanowisko Projektodawcy** |
| **1.** | **Urząd Ochrony Danych Osobowych** | **§ 1 pkt 1 lit. e** (§ 2 pkt 13 zmienianej uchwały) *–*§ 1 pkt 1 lit. d w poprzedniej wersji projektu | Z projektowaną zmianą wiąże się  wprowadzenie sytemu rekomendacji Pełnomocnika Rządu do Spraw  Cyberbezpieczeństwa dotyczących gradacji ważności systemów w oparciu o ocenę  krytyczności gromadzonych i przetwarzanych w nich danych (nowy § 3a), gdyż  Narodowe Standardy Cyberbezpieczeństwa oraz ich odpowiedniki określone w  europejskim układzie normalizacji nie zawierają takiej gradacji. W ocenie organu  nadzorczego rozwiązanie występujące w dotychczasowym stanie prawnym, gdzie  obowiązuje jeden standard cyberbezpieczeństwa dla chmur obliczeniowych Standardy  Cyberbezpieczeństwa Chmur Obliczeniowych, jest rozwiązaniem bardziej sprzyjającym  zasadzie integralności i poufności (art. 5 ust. 1 lit. f rozporządzenia 2016/6791),  chociażby przez jego kompletność w odniesieniu do ww. sytemu gradacji oraz  umocowanie bezpośrednio w § 3 uchwały nr 97 Rady Ministrów z dnia 11 września 2019  r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa”. W ocenie  organu nadzorczego deklarowane w uzasadnieniu do projektowanej uchwały  zwiększanie poziomu bezpieczeństwa przetwarzania danych w chmurach obliczeniowych  powinno odbyć się poprzez ewentualną modyfikację Standardów Cyberbezpieczeństwa  Chmur Obliczeniowych i utrzymanie ich jako jednolitego standardu dotyczącego  cyberbezpieczeństwa w chmurach obliczeniowych. | **Wyjaśnienie uwagi**  Zgłoszona uwaga nie odpowiada celowi nowelizacji pomijając przy tym fakt, że Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa obowiązkowo będzie wydawał, zmieniał, uchylał rekomendacje dotyczące gradacji ważności systemów w oparciu o ocenę krytyczności gromadzonych i przetwarzanych w nich danych.  Należy mieć także na uwadze fakt, iż dostawcy będą mieli możliwość wyboru pomiędzy stosowaniem SCCO (i określoną w ramach tego dokumentu gradacją), a NSC i gradacją określoną w ramach rekomendacji Pełnomocnika. Niezależnie od dokonanego wyboru zagwarantowano wysoki poziom bezpieczeństwa gromadzonych i przetwarzanych danych. Wynika to z faktu, iż NSC oparte są o amerykański standard NIST, który jest jednym z najbardziej kompleksowych rozwiązań w tym zakresie. NIST są regularnie aktualizowane m.in. ze względu na fakt, iż są stosowane przez różnego rodzaju podmioty amerykańskie. Jednocześnie zastosowany w drodze nowelizacji mechanizm pozwala na elastyczne stosowanie coraz wyższych standardów bez konieczności każdorazowego aktualizowania uchwały. Dotychczasowe rozwiązanie, rekomendowane w zgłaszanej uwadze, ogranicza się do SCCO, czyli dokumentu, który był bardzo rzadko aktualizowany, a poszczególne rozwiązania w nim zawarte i tak były wzorowane wprost na NIST (NSC), w związku z czym było to zarówno rozwiązanie wtórne jak i mało elastyczne, nieadekwatne do dynamiki procesów jakie funkcjonują w zakresie WIIP. Stąd też wprowadzenie przez projektodawcę możliwości stosowania odpowiedników standardów w europejskim układzie normalizacji, celem stosowania jak najbardziej aktualnych i precyzyjnych standardów, które są regularnie aktualizowane i spełniają kryteria w najbardziej zaawansowanych środowiskach usług chmurowych. |
| **2.** | **Urząd Ochrony Danych Osobowych** | **§ 1 pkt 6 lit. c** (§ 6 ust. 3 zmienianej uchwały) – § 1 pkt 3 lit. bw poprzedniej wersji projektu | Dopuszczenie możliwości poprzestania na deklaracji podmiotu równoważnie z wymogiem certyfikacji może z dużą dozą prawdopodobieństwa spowodować, że deklaracje, o których mowa w projektowanym przepisie staną się środkiem zasadniczym dotyczącym zapewnienia  bezpieczeństwa danych, gdyż certyfikacja jest procesem kosztownym i czasochłonnym.  Biorąc pod uwagę fakt, że deklaracja podmiotu o spełnieniu wymagań Rządowego  Klastra Bezpieczeństwa może nie odpowiadać rzeczywistości, projektowane rozwiązanie  stwarza wysokie ryzyko negatywnego wpływu na standardy bezpieczeństwa  przetwarzania danych w chmurach obliczeniowych, co narusza zasadę integralności i poufności (art. 5 ust. 1 lit. f rozporządzenia 2016/679). | **Wyjaśnienie uwagi**  Dopuszczenie możliwości złożenia deklaracji lub posiadania odpowiedniej certyfikacji (alternatywa łączna) przez dostawcę usług chmurowych stanowi gwarancję odpowiedniego poziomu bezpieczeństwa przetwarzanych danych (poza obowiązkiem spełnienia warunków wynikających z SCCO lub wskazanych w projekcie NSC).  Nie można pominąć kwestii dobrowolności skorzystania z rozwiązań jakie oferuje uchwała WIIP. Dostawca, który nie może spełnić wymagań, a tym samym złożyć deklaracji nie może skorzystać z tychże rozwiązań i oferować swoich usług podmiotom administracji (lub też administracja nie może na podstawie WIIP korzystać z usług oferowanych przez takiego dostawcę). Ponadto należy mieć na uwadze, że podmioty chcące skorzystać z proponowanych rozwiązań z reguły (jeśli nie zawsze), dysponują określoną infrastrukturą w związku z czym spełnienie określonych wymagań nie powinno implikować szczególnego nakładu środków i zaangażowania pracowników. Jednocześnie nie można nie zauważyć, iż nawet czysto hipotetyczne i abstrakcyjne złożenie deklaracji niezgodnej z warunkami technicznymi, nie powinno pociągnąć za sobą negatywnych konsekwencji dla danego podmiotu w aspekcie bezpieczeństwa, w tym szczególności integralności i poufności przetwarzanych danych z uwagi, na wyżej opisane standardy bezpieczeństwa towarzyszące rozwiązaniom chmurowym. Słabość rozwiązań on-premise tak częstych w wielu podmiotach publicznych została już zdiagnozowana w 2018 r. przez Ministerstwo Cyfryzacji, kiedy to w drodze przeprowadzonej inwentaryzacji stwierdzono, że 87% zasobów IT w podmiotach administracji nie spełnia podstawowych standardów technicznych.  Mając to na uwadze, projektowane rozwiązanie nie stwarza ryzyka negatywnego wpływu na standardy bezpieczeństwa przetwarzania danych w chmurach obliczeniowych, naruszających zasadę integralności i poufności. |
| **3.** | **Komisja Nadzoru Finansowego** | **§ 1 pkt 7** (§ 7 ust. 1 pkt 11 zmienianej uchwały) | W konsekwencji zaproponowanej przez projektodawcę zmiany sposobu finansowania Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa” (projektowane zmiany w § 11 uchwały nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa” (M.P. z 2021 r. poz. 1006)), które należy ocenić pozytywnie, konieczne wydaje się uchylenie pkt 11 w § 7 w ust. 1 tej uchwały. Wskazany przepis określa bowiem, że elementem obligatoryjnym porozumienia zawieranego między Ministrem Cyfryzacji a podmiotem zamierzającym skorzystać z usług przetwarzania w Rządowej Chmurze Obliczeniowej są „zasady prowadzenia rozliczeń za korzystanie z usług”. Skoro jednak projektodawca zamierza zmienić sposób finansowania tej inicjatywy, wskazując jako jedyne źródło finansowania część 27 budżetu Państwa – Informatyzacja, to przepis wymagający dokonywania rozliczeń za korzystanie z tych usług wydaje się bezprzedmiotowy. | **Uwaga uwzględniona**  Przepis został uchylony. |
| **4.** | **Rada do Spraw Cyfryzacji** | § 1 pkt 1 lit. a (§ 2 pkt 1 zmienianej uchwały) | W definicji CPD zamiast środkami kontroli środowiska powinno być: „systemu kontroli i monitorowania warunków środowiskowych”  W serwerowniach, w celu utrzymania optymalnych dla urządzeń warunków środowiska (temperatura, wilgotność, itp.) stosuje się systemy monitorowania i kontroli warunków środowiskowych, które mają za zadanie utrzymanie zalecanych przez producentów sprzętu warunków oraz ostrzeganie lub zadziałanie urządzeń pomocniczych w przypadku przekroczenia wartości krytycznych. | **Uwaga uwzględniona** |
| **5.** | **Rada do Spraw Cyfryzacji** | **Uwaga ogólna** | Każdy podmiot, który zamierzałby wykorzystać model chmury obliczeniowej musi wykazać się zgodnością ze standardami wskazanymi przez Wspólną Infrastrukturę Informacyjną Państwa (WIIP). Jednak procedury ich zastosowania są w świetle projektu zmian w uchwale RM niejasne a zasady oceny zgodności nie są znane. Do tego dochodzi niekiedy niezwykła wprost obszerność standardów - Narodowe Standardy Cyberbezpieczeństwa liczą ponad 1200 stron. Nie jest także jasna relacja (mapowanie) do innych wymagań określonych przepisami prawa . Jaka jest relacja NSC do ustawy o Krajowym Systemie Cyberbezpieczeństwa (UKSC) - standardów SCCO czy RODO ?. Mówimy o podstawowych wymaganiach a przecież powstaną kolejne przepisy w ciągu najbliższych miesięcy związanych z  wdrożeniem dyrektyw NIS2 czy CER. Stawia to podmioty publiczne, zainteresowane przetwarzaniem danych w chmurze , przed trudnym zadaniem przygotowania złożonego procesu przy niepewnych warunkach. | **Wyjaśnienie uwagi**  Zgodność ze standardami wskazanymi przez WIIP musi wykazać dostawca usług chmurowych, nie podmiot.  Obszerność standardów, zarówno SCCO z załącznikami jak i wskazanych NSC wynika przede wszystkim z dążenia do zapewnienia jak najwyższego poziomu bezpieczeństwa przetwarzanych danych w chmurze obliczeniowej. Priorytetem w przenoszeniu danych do chmury jest bowiem ich bezpieczeństwo, w szczególności tych danych, których ewentualny wyciek może mieć wpływ na bezpieczeństwo państwa i porządek publiczny.  Należy również mieć na uwadze, że SCCO i NSC powinno być stosowane odpowiednio do wymagań określonych w przepisach prawa powszechnie obowiązującego, które mają prymat w hierarchii źródeł prawa.  Wymagania o których mowa w uwadze będą musieli spełnić dostawcy usług chmurowych, nie podmioty. W interesie podmiotów jest natomiast to, aby wymagania zawarte w uchwale zostały określone w sposób, który zapewnia maksymalne bezpieczeństwo z punktu widzenia infrastruktury i danych, które są przetwarzane. |
| **6.** | **Rada do Spraw Cyfryzacji** | **Uwaga ogólna** | Standardy NSC są przeniesieniem norm amerykańskich, co samo w sobie nie jest złym rozwiązaniem a nawet zasługującym na pozytywna ocenę tylko, że nie odpowiadają one – nawet na poziomie terminologii – obowiązującym w Polsce aktom prawa powszechnie zarówno krajowego jak i UE .  Przykłady :  a) casus dot. SCCO: jak w rozumieniu obowiązującego prawa, zwłaszcza ustawy o krajowym systemie cyberbezpieczeństwa (UKSC) , należy ocenić zapisane w SCCO określenie wpływu na bezpieczeństwo (ograniczony, poważny, silny lub katastrofalny)?  b) casus NSC 800-144 - jest normą dotyczącą bezpieczeństwa i prywatności w chmurze publicznej. Jest to norma z 9 grudnia 2011 roku czyli na parę lat przed rozporządzeniem 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 swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, znane jako RODO/GDPR. Jak stosować zatem przepisy dot. ochrony prywatności gdy nie odnoszą się one do danych osobowych który ochrona jest esencją prawa do prywatności? | **Wyjaśnienie uwagi**  SCCO w przyszłości zostanie zaktualizowane, aby pozostać w pełni zgodne z projektowaną obecnie nowelizacją uchwały.  NSC bazują natomiast na amerykańskich standardach NIST, które są regularnie przeglądane i aktualizowane pod kątem ich zgodności i aktualności w zakresie potrzeb. Wprowadzane są zatem kolejne wersje danego standardu. Zastosowany w drodze nowelizacji mechanizm pozwala na elastyczne stosowanie coraz wyższych standardów bez konieczności każdorazowego aktualizowania uchwały. Dotychczasowe rozwiązanie ogranicza się tylko do SCCO, czyli dokumentu, który był bardzo rzadko aktualizowany, a poszczególne rozwiązania w nim zawarte i tak były wzorowane wprost na NIST (NSC), w związku z czym było to zarówno rozwiązanie wtórne jak i mało elastyczne, nieadekwatne do dynamiki procesów jakie funkcjonują w zakresie WIIP. Stąd też wprowadzenie przez projektodawcę możliwości stosowania odpowiedników standardów w europejskim układzie normalizacji, celem stosowania jak najbardziej aktualnych i precyzyjnych standardów, które są regularnie aktualizowane i spełniają kryteria w najbardziej zaawansowanych środowiskach usług chmurowych. Identyczną funkcję spełniają rekomendacje Pełnomocnika. Pozwala to na szybkie reagowanie na zmieniającą się rzeczywistość w związku z rozwojem nowych technologii. Stosując standardy należy –ponownie – wziąć pod uwagę także przepisy prawa powszechnie obowiązującego. |
| **7.** | **Rada do Spraw Cyfryzacji** | **Uwaga ogólna** | Uzyskanie zgodności z SCCO lub z wymienionymi Narodowymi Standardami Cyberbezpieczeństwa lub ich europejskimi odpowiednikami.  Niestety, wymienione dokumenty nie są tożsame w swoich wymaganiach, co może prowadzić do poważnych konsekwencji. Przykładem może być przetwarzanie danych osobowych, które SCCO dopuszczają w zasadzie wyłącznie na poziomie SCCO2 a projekt NSC dopuszcza także przetwarzanie danych osobowych w publicznej chmurze obliczeniowej.  NSC 800-53A liczy ponad tysiąc stron - wprowadza pojęcia takie jak SAISO (Senior Agency Information Security Officer) czy SAOP (Senior Agency Offical for Privacy, który jest terminem zupełnie inaczej zdefiniowanym niż europejski Inspektor Ochrony Danych). Czy zatrudniając Inspektora Ochrony Danych tzw. IOD podmiot spełnia kryterium posiadania SAOP? | **Wyjaśnienie uwagi**  Należy pamiętać o tym, że podmiot może WYBRAĆ stosowanie SCCO, a może wybrać stosowanie NSC i określonych przez Pełnomocnika rekomendacji. Są to zatem dwie niezależne od siebie ścieżki. Należy również wziąć pod uwagę przepisy prawa powszechnie obowiązującego, które mają pierwszeństwo przed aktami rodzaju SCCO czy NSC, a więc konieczne jest zapewnienie zgodności np. w zakresie przetwarzania danych również z RODO. Dostawca usług chmurowych powinien więc dostosować wymagania określone w SCCO i NSC do określonych warunków. Analogicznie w przypadku NSC, które odwołują się do standardów amerykańskich – w przypadkach w których nie jest możliwe zastosowanie standardu w pełni, ponieważ nie istnieją w prawie polskim odpowiedniki np. wskazanych podmiotów, które pełnią dokładnie te same funkcje, należy standard stosować w sposób ODPOWIEDNI, a więc adekwatny, konieczny i proporcjonalny. |
| **8.** | **Rada do Spraw Cyfryzacji** | **§ 1 pkt 2** (§ 3a zmienianej uchwały) | Gradacja ważności systemów - zapewne ważne i potrzebne wymaganie zgodności z rekomendacjami dotyczącymi „gradacji ważności systemów” , które mają być publikowane przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa ( par. 3a, ust. 1. i ust. 2) – nie ma nawet projektu rekomendacji, ani opartej w źródłach prawa „gradacji ważności systemów”. Trudno więc ocenić znaczenie tego kryterium i jego wpływ na działania podmiotów. Jednocześnie istnieje obowiązek poinformowania Pełnomocnika o stosowaniu rekomendacji przez podmioty ( par. 3a ust. 4) i ocena tego wniosku przez Pełnomocnika ( par. 3a ust. 5) . Nie wiadomo jednak jak powinna wyglądać procedura, ani jakie informacje powinny być zawarte we wniosku/deklaracji zgodności; wiadomo natomiast, że Pełnomocnik może przekazać informację o nieuwzględnianiu rekomendacji do organu sprawującego nadzór. Z uzasadnienia do projektu wynika jednak że „potencjalnie stanowić może podstawę do wszczęcia kontroli w danym podmiocie”. Wydaje się ze ta materia powinna być przedmiotem regulacji ustawowej zwłaszcza w zakresie jakim dotyczyć ma JST.  Zakładano w uzasadnieniu do projektu że :  „Konieczne jest ponadto uproszczenie kryteriów klasyfikacji systemów teleinformatycznych, które mogą korzystać z usług przetwarzania w Rządowej Chmurze Obliczeniowej (RChO) lub w PChO – obecnie kryteria te są zawarte w załączniku nr 2 do uchwały, który ma skomplikowany układ.”  Wydaje się więc że projekt zmian w Uchwale nie spełnia założonego celu a -uproszczenia a wręcz przeciwnie jeden skomplikowany system zastępuje drugim nie mniej skomplikowanym i niejasnym. | **Wyjaśnienie uwagi**  Zmiany w uchwale dotyczące wydawania, zmiany lub odwoływania rekomendacji i gradacji ważności systemów 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 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 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 NSC. |
| **9.** | **Rada do Spraw Cyfryzacji** | **§ 1 pkt 2** (§ 3b zmienianej uchwały) | Wykluczenie niektórych systemów z możliwości przetwarzania w chmurze publicznej .  Ponadto § 3b projektu uchwały wyłącza możliwość wykorzystania chmury publicznej do przetwarzania niektórych systemów rejestrów publicznych lub Platformy Ochrony Zdrowia . Przepis w obecnej wersji budzi wątpliwości co do tego czy będą mogły być przetwarzane dane np. z rejestru PESEL lub tworzone kopie części tego rejestru skoro sam rejestr źródłowy nie może być przetwarzany w chmurze publicznej?  Przepis ten nie powinien być także przeszkodą w przypadku podejmowania decyzji o ewakuacji kluczowych systemów państwowych do chmury publicznej w bezpiecznej lokalizacji lub w ramach projektu e Ambasada. | **Wyjaśnienie uwagi**  Wprowadzony katalog wyłączeń dotyczy tylko systemów czy rejestrów jako całości. Nie dotyczy natomiast przetwarzania danych, które stanowią tylko pewien element systemu i w związku z tym mogą pojawić się także w innych – nie wyłączonych rejestrach czy danych. |