UZASADNIENIE

Projekt uchwały ma na celu aktualizację Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa" – dalej „Inicjatywa WIIP", poprzez nowelizację 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). Projektowany akt zakłada dookreślenie warunków współpracy podmiotów zaangażowanych w realizację Inicjatywy WIIP, która stanowi odpowiedź na potrzeby m.in. administracji rządowej. Celem jest także poprawa efektywności i bezpieczeństwa świadczenia usług przez administrację publiczną i inne podmioty, które zostały objęte zakresem uchwały. Wskazać przy tym należy, że przedmiotowa nowelizacja nie wprowadza bezpośrednich zmian w zakresie podmiotowym tj. nie rozszerza katalogu podmiotów uprawnionych do skorzystania z rozwiązań będących przedmiotem Inicjatywy WIIP oraz nie nakłada bezpośrednich obowiązków na administrację publiczną. Zmiany w uchwale m.in. optymalizują koszty działania administracji rządowej oraz zwiększają bezpieczeństwo jej funkcjonowania. Z uwagi na sieć powiązań pomiędzy podmiotami bezpośrednio podległymi Radzie Ministrów, a pozostałymi podmiotami administracji publicznej, efekt ten będzie przeniesiony na te jednostki. Projekt przewiduje zatem także efekty pośrednie, które będą dotyczyły m.in. jednostek samorządu terytorialnego, a w konsekwencji obywateli korzystających z usług publicznych świadczonych prze te JST. W żaden sposób ich jednak nie wiąże. Do bezpośredniego wpływu na jednostki administracji publicznej zaliczyć można zmiany w systemie ZUCH omówione poniżej.

Do strategicznych kierunków, jakie realizuje Inicjatywa WIIP należy:

- podniesienie poziomu bezpieczeństwa przetwarzania danych i świadczenia usług elektronicznych w administracji rządowej;
- trwałe obniżenie kosztów stałych przetwarzania danych;
- podniesienie efektywności wydatkowania środków w projektach zawierających elementy infrastruktury IT;
- skrócenie czasu realizacji nowych przedsięwzięć informatycznych przez szybsze udostępnianie wymaganej infrastruktury IT;
- ograniczenie zjawiska wielokrotnego gromadzenia tych samych danych w środowiskach informatycznych oraz zniesienie barier technologicznych w przypadku rejestrów publicznych;

- upowszechnienie modelu chmury obliczeniowej, jako głównego sposobu funkcjonowania systemów teleinformatycznych państwa (w tym również zmiana technologii wytwarzania oprogramowania).

Mając na uwadze dynamiczny rozwój nowych technologii, w tym m.in. w zakresie usług chmurowych, wymuszający niejako ciągłe dostosowywanie definicji oraz przepisów, projekt uchwały zakłada szereg zmian w zakresie definiowania. Nowelizacji uchwały przyświecają zatem dwa nadrzędne cele. Po pierwsze – wspomniana potrzeba dostosowania przepisów do aktualnych potrzeb i warunków jakie podyktowane są stale rozwijającym się sektorem nowych technologii, w szczególności usług chmurowych, a po drugie – zapewnienie, aby jak najwięcej podmiotów mogło skorzystać z usług Publicznej Chmury Obliczeniowej (PChO) lub Rządowej Chmury Obliczeniowej (RChO). Osiągnięte to zostanie w szczególności poprzez:

a) likwidację załącznika nr 2,
b) wprowadzenie zamkniętego katalogu systemów wykluczonych z możliwości przeniesienia do PChO,
c) możliwość skorzystania przez podmioty administracji z usług chmurowych, których dostawcy stosują wymagania określone w Standardach Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO) lub Narodowych Standardach Cyberbezpieczeństwa (NSC) -- lub w ich odpowiednikach określonych w europejskim systemie normalizacyjnym.

Zmianie ulegają następujące definicje: CPD, chmury obliczeniowej, chmury publicznej, PChO, RChO, Rządowego Klastra Bezpieczeństwa (RKB) oraz sieci rządowej.

Zmieniając definicję chmury obliczeniowej kierowano się uzyskaniem większej przejrzystości i usunięciem możliwych wątpliwości interpretacyjnych. Wyszczególniono zatem podział na pięć zasadniczych cech chmury obliczeniowej, trzy modele dostarczania usług chmurowych oraz cztery modele wdrażania usług chmurowych. Wskazać jednak należy, iż nie są to wszystkie cechy chmury obliczeniowej w ogóle. Do pozostałych cech należą m.in. rozłożenie kosztów, stabilność i niezawodność, łatwa praca grupowa, niezależność od konkretnych systemów operacyjnych, niezależność od platformy wirtualizacji, a także bezpieczeństwo, ochrona i wsparcie.

Zmiana definicji sieci rządowej podyktowana jest faktem, iż sieć GovNet jest siecią podkładową dla sieci TESTA-NG, która korzysta z infrastruktury sieciowej sieci GovNet i która to sieć dotychczas była wymieniona w definicji. Tym samym sieć GovNet jest siecią

nadrzędną i nie jest konieczne wyodrębnianie sieci TESTA-NG w definicji sieci rządowej. Dodatkowo, podmiotem zarządzającym w odniesieniu do tych sieci jest wyłącznie minister właściwy do spraw wewnętrznych.

Ponadto dodano do uchwały nowe definicje – Systemu Zapewnienia Usług Chmurowych (ZUCH), podzielonej odpowiedzialności oraz brokera usług. Nowe definicje są wynikiem zmian dokonanych w innych definicjach, a ponadto mają na celu wyeliminowanie wątpliwości interpretacyjnych.

Definiując pojęcie podzielonej odpowiedzialności należy wskazać, że nie wiąże się to z koniecznością przenoszenia jakiejkolwiek odpowiedzialności za przetwarzanie danych na dostawcę usług chmurowych. Za przetwarzanie danych w usługach chmurowych odpowiada administrator. Dostawca usług chmurowych dostarcza jedynie odpowiednie usługi we właściwym 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. Podział odpowiedzialności określa, czym zarządza i do czego ma dostęp dostawca usługi chmurowej, a co pozostaje w tym zakresie w kompetencji odbiorcy usługi. Zakres podzielonej odpowiedzialności musi być wyraźnie opisany dla każdej usługi. Dopiero na tej podstawie odbiorca usługi (tj. podmiot administracji) 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 projekcie zwraca się uwagę na podział odpowiedzialności z tego powodu, że jest on w większości mylnie interpretowany jako przenoszenie odpowiedzialności za przetwarzanie danych na dostawcę usług. Zagadnienie to jest także opisywane dokładnie w przytaczanych w uchwale standardach SCCO i NSC. Ponadto, tak długo, jak długo 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).

Istotne znaczenie w aspekcie funkcjonowania RChO ma wprowadzenie w drodze niniejszej nowelizacji definicji ZUCH, stanowiącego portal informacyjno-usługowy mający na celu wspieranie procesu zamawiania oraz zarządzania usługami przetwarzania w RChO oraz w PChO. Model działania ZUCH umożliwia ponadto przeprowadzenie wstępnej kwalifikacji

danego systemu informatycznego poprzez wskazanie, czy może on zostać zaimplementowany do RChO lub PChO, bądź uznanie, iż system ten należy umieścić poza chmurą obliczeniową.

Jedną z kluczowych zmian jest nowelizacja definicji Rządowego Klastra Bezpieczeństwa (RKB), który od wejścia w życie projektu będzie rozumiany jako usługi bezpieczeństwa oraz środki techniczne stosowane do zabezpieczenia RChO będące implementacją wymagań Standardów Cyberbezpieczeństwa Chmur Obliczeniowych lub wymagań określonych i w Narodowych Standardach Cyberbezpieczeństwa[1)]:

a) NSC 800-53A – Ocenianie środków bezpieczeństwa i ochrony prywatności systemów informacyjnych oraz organizacji. Tworzenie skutecznych planów,

b) NSC 800-144 – Wytyczne dotyczące bezpieczeństwa i prywatności w chmurze publicznej,

c) NSC 800-210 – Ogólne wytyczne dotyczące kontroli dostępu do systemów chmury obliczeniowej

– lub w ich odpowiednikach określonych w europejskim systemie normalizacyjnym.

Wskazanie na odpowiedniki standardów w europejskim systemie normalizacyjnym oznacza, że europejski standard musi charakteryzować się takim samym poziomem bezpieczeństwa, mieć taki sam zakres przedmiotowy oraz podmiotowy.

Powyższa zmiana podyktowana jest chęcią umożliwienia większej liczbie podmiotów skorzystania z RChO i PChO. W tym celu podmiot wyrażający chęć skorzystania z usług chmurowych określonych w Inicjatywie WIIP będzie miał od tej pory możliwość wyboru, czy skorzystać z usług chmurowych świadczonych przez dostawców, których usługi spełniają, wymagania określone w SCCO lub NSC wskazanych w uchwale lub ich odpowiedników określonych w europejskim systemie normalizacyjnym. Podkreślić należy, że dostawca może zdecydować się na zaimplementowanie w swoich usługach wymagań określonych w SCCO lub wskazanych w uchwale wszystkich 3 NSC łącznie. Nie ma potrzeby żeby dostawca implementował kumulatywnie wymagania określone w SCCO i NSC. Jest to zatem alternatywa.

Narodowe Standardy Cyberbezpieczeństwa bazują na standardach amerykańskich, które są regularnie przeglądane i aktualizowane pod kątem zapewnienia ich zgodności i aktualności w zakresie potrzeb. Wprowadzane są także kolejne wersje poszczególnych standardów.

[1)] https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber.

Zastosowany w drodze nowelizacji mechanizm pozwala na elastyczne stosowanie coraz wyższych standardów bez konieczności każdorazowego aktualizowania uchwały. Stąd też zdecydowano się, równolegle do SCCO, na wprowadzenie możliwości stosowania NSC lub odpowiedników standardów określonych w europejskim systemie normalizacyjnym, celem stosowania jak najbardziej aktualnych i precyzyjnych standardów, które są regularnie aktualizowane i spełniają kryteria w najbardziej zaawansowanych środowiskach usług chmurowych.

Dla zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzania danych poza obowiązkiem spełniania przez dostawców usług chmurowych warunków wynikających z SCCO lub wskazanych w projekcie NSC, korzystanie przez podmioty, o których mowa w § 6 ust. 1, z usług przetwarzania w RChO lub PChO uzależnione jest od złożenia przez dostawcę usług chmurowych deklaracji o spełnianiu powyższych wymagań albo uzyskaniu certyfikacji odpowiadającej tym standardom (§ 6 ust. 2 i 3). Deklaracja będzie mogła zostać złożona zarówno w formie pisemnej jak i elektronicznej. Wzór deklaracji zostanie opublikowany w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw informatyzacji. W ocenie projektodawcy przede wszystkim w interesie dostawcy usług, a także podmiotu, który z tych usług zamierza korzystać, leży złożenie deklaracji zgodnej z prawdą z uwagi na bezpieczeństwo danych będących w dyspozycji podmiotu, które docelowo mają zostać umieszczone w chmurze obliczeniowej. Ponadto, w prawie powszechnie obowiązującym funkcjonuje szereg instytucji, które aktualizują się w przypadku niezgodności oświadczenia (deklaracji) z prawdą.

Uchwała nie wprowadza ponadto procedury certyfikacji. Założono bowiem, że dostawcy usług chmurowych będą przedstawiać deklarację bądź certyfikację, którą już posiadają. Oznacza to, że nie będzie konieczności przechodzenia dedykowanej i wprowadzonej uchwałą procedury certyfikacji.

Projekt uchwały przewiduje ponadto uchylenie załącznika nr 2, określającego kryteria klasyfikacji systemów teleinformatycznych, które mogą korzystać z usług przetwarzania w RChO lub w PChO. Załącznik ten zostanie zastąpiony znowelizowaną wersją definicji RKB, obowiązkiem złożenia przez dostawcę usług chmurowych deklaracji albo uzyskaniem certyfikacji (§ 6 ust. 2 i 3) oraz nowym § 3a, który stanowi, że Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa – dalej „Pełnomocnik”, po uzyskaniu opinii Kolegium do Spraw Cyberbezpieczeństwa wydaje, zmienia lub odwołuje rekomendacje dotyczące gradacji ważności systemów w oparciu o ocenę krytyczności gromadzonych i przetwarzanych w nich

danych. Poprzez „systemy” należy rozumieć w szczególności systemy informatyczne wykorzystujące usługi chmurowe lub budowane w oparciu o usługi chmurowe. 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. Taki zabieg spowodowany jest tym, że gradacja ważności systemów określona została w SCCO, a zatem niezbędne jest określenie rekomendacji dotyczących gradacji ważności systemów informatycznych wykorzystujących usługi chmurowe w stosunku do tych podmiotów, które nie zdecydowały się na wybór SCCO. Przyjęcie innego rozwiązania sprowadzałoby się do wytworzenia luki w przepisach i znacznie utrudniałoby funkcjonowanie podmiotom, które zdecydowane są korzystać z NSC. Przepis ten zapewni bezpieczeństwo systemów w podmiotach, które korzystają z usług chmurowych świadczonych przez dostawców stosujących NSC wskazane w projekcie lub ich odpowiedniki określone w europejskim systemie normalizacyjnym. Podmiot, o którym mowa w § 3a ust. 1, będzie obowiązany do informowania Pełnomocnika, na jego wniosek, o sposobie i zakresie uwzględniania rekomendacji dotyczących gradacji ważności systemów. Nieuwzględnienie tych rekomendacji przez podmiot będzie stanowiło podstawę do wystąpienia przez Pełnomocnika do organu sprawującego nadzór nad podmiotem z informacją o ich nieuwzględnieniu. Taka informacja potencjalnie stanowić może podstawę do wszczęcia kontroli w danym podmiocie. Celem takiej kontroli miałoby być określenie, czy świadczone usługi zapewniają przede wszystkim bezpieczeństwo przetwarzanych danych, a w przypadku negatywnych wyników kontroli, jej wnioski będą mogły stanowić podstawę do zaprzestania korzystania ze świadczonych usług chmurowych. Zgodnie z zaproponowanym brzmieniem rekomendacje Pełnomocnika po ich przekazaniu ministrowi właściwemu do spraw informatyzacji będą udostępniane na stronie internetowej Biuletynu Informacji Publicznej tego ministra. Każdorazowe wydanie, zmiana lub odwołanie rekomendacji będzie wiązać się z odpowiednią aktualizacją Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji o te dokumenty. Rekomendacje Pełnomocnika pełnią także funkcję pozwalającą na szybkie reagowanie na zmieniającą się rzeczywistość w związku z rozwojem nowych technologii, a tym samym przyczynia się do zagwarantowania bezpieczeństwa przetwarzanych danych.

Uchylany załącznik nr 2 zostanie zastąpiony przez dodany w drodze niniejszej nowelizacji § 3b, który wprowadza zamknięty katalog systemów niedopuszczonych do korzystania za ich pomocą z usług przetwarzania w PChO. Wymienione w katalogu systemy zostały wykluczone z uwagi na szczególny charakter przetwarzanych w nich danych. Podkreślić jednak należy, że

wyłączeniu podlegają konkretnie wskazane systemy i nie dotyczy to poszczególnych danych z których te systemy się składają. Oznacza to, że mogą być one przetwarzane w PChO niezależnie od wyłączenia określonego systemu.

Projekt dokonuje także zmian w brzmieniu §5 ust. 2 i 4, które mają na celu doprecyzowanie, że w odniesieniu do sieci rządowej (w nowym brzmieniu) operatorem sieci jest wyłącznie minister właściwy do spraw wewnętrznych.

Z uwagi na to, że ZUCH jest definiowany w § 2 pkt 16 uchwały, to odpowiedniej zmiany dokonuje się w § 10 uchwały – przepis ten ma jedynie na celu wskazanie podmiotu zapewniającego funkcjonowanie ZUCH. Uchyleniu ulegają ust. 3 i 4 w § 10, na skutek czego w ust. 2 wprowadzono zmianę polegającą na określeniu, iż usługi przetwarzania w PChO będą umieszczane w katalogu usług przetwarzania w PChO niezwłocznie po zawarciu umów ramowych dotyczących zamówień publicznych na dane usługi przetwarzania w chmurze obliczeniowej. Umowy ramowe zawierane zgodnie z PZP na świadczenie usług chmurowych mają na celu uproszczenie procesu nabywania usług chmurowych w ramach PChO przez podmioty administracji publicznej. Do umów ramowych zostaną dopuszczeni zweryfikowani dostawcy, którzy będą spełniali określone wymagania w zakresie bezpieczeństwa, przetwarzania danych, spełnienia wymaganych norm i parametrów stawianych poszczególnym usługom przewidziane dla dostawców zamierzających świadczyć usługi dla administracji publicznej. Korzystając z systemu ZUCH podmiot administracji publicznej zawiera zatem z dostawcą umowę docelową na świadczenie wybranych z katalogu PChO usług bez konieczności opracowywania SIWZ i OPZ.

Istotną zmianą, którą zakłada projekt jest zmiana w zakresie finansowania Inicjatywy WIIP. Do tej pory były to środki budżetu państwa w ramach rezerwy celowej pod nazwą „Finansowanie Inicjatywy Wspólna Infrastruktura Informatyczna Państwa". Rodziło to problemy dla niektórych podmiotów, które zgodnie z brzmieniem przepisów zawartych w uchwale mogły korzystać z RChO lub PChO, ale sposób finansowania był w ich przypadku niemożliwy do zastosowania i w związku z tym miało charakter wykluczający. Zdecydowano się zatem na zmianę sposobu finansowania na środki w ramach części 27 budżetu państwa – Informatyzacja. Przedmiotowa zmiana znacznie uprości zarządzanie środkami finansowymi przeznaczonymi na usługi w modelu chmury obliczeniowej poprzez planowanie i rozliczanie budżetu przez Ministerstwo Cyfryzacji w oparciu o zebrane zapotrzebowania z poszczególnych jednostek administracji publicznej.

Dokonuje się ponadto zmian w załączniku nr 1. Zmiany te mają co do zasady charakter porządkowy i ujednolicający w związku z nowym brzmieniem przepisów zaproponowanych w treści projektu. Zaktualizowano pod tym względem normy, zastępując w ust. 1 w pkt 3 normę PN-ISO/IEC 27005 normą PN – ISO 31000. W ust. 6 pkt 1 oraz ust. 7 pkt 2 dodano obok SCCO również NSC wskazane w projekcie uchwały (lub ich odpowiedników określonych w europejskim systemie normalizacyjnym), a w ust. 6 pkt 3 doprecyzowano, że certyfikacja ma dotyczyć norm wymienionych w ust. 1 załącznika nr 1.Projekt uchwały nie jest sprzeczny z prawem Unii Europejskiej.

Projektowana regulacja nie zawiera przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039, z późn. zm.) i nie podlega notyfikacji Komisji Europejskiej.

Projektowana regulacja nie będzie wymagała notyfikacji Komisji Europejskiej w trybie ustawy z dnia 30 kwietnia 2004 r. o postępowaniu w sprawach dotyczących pomocy publicznej (Dz. U. z 2023 r. poz. 702).

Projekt nie wymaga przedłożenia instytucjom i organom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Wejście w życie projektowanej uchwały nie będzie miało wpływu na działalność mikroprzedsiębiorców, małych i średnich przedsiębiorców.

Projekt uchwały zostanie umieszczony w Biuletynie Informacji Publicznej na stronie podmiotowej urzędu obsługującego ministra właściwego do spraw informatyzacji.

Projektowana uchwała wejdzie w życie z dniem następującym po dniu ogłoszenia. Istotne jest natychmiastowe wprowadzenie zmian zwiększających bezpieczeństwo świadczonych usług przez administrację publiczną i zasady demokratycznego państwa prawnego nie stoją temu na przeszkodzie.