**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 nowelizację tabeli w załączniku nr 2 (w ust. 1), tj. tabeli określającej kryteria klasyfikacji systemów teleinformatycznych, które mogą korzystać z usług przetwarzania w Rządowej Chmurze Obliczeniowej (RChO) lub w Publicznych Chmurach Obliczeniowych (PChO). Zmiana polega w szczególności na możliwości umieszczenia poszczególnych systemów teleinformatycznych w PChO w jurysdykcji krajowej lub pozostałych państw Europejskiego Obszaru Gospodarczego (EOG). Powyższe stanowi odpowiedź na potrzeby administracji rządowej, w szczególności służb i formacji umundurowanych, które odpowiadają za bezpieczeństwo państwa.

Do strategicznych kierunków, jakie realizuje Inicjatywa WIIP należy:

1. podniesienie poziomu bezpieczeństwa przetwarzania danych i świadczenia usług elektronicznych w administracji rządowej;
2. trwałe obniżenie kosztów stałych przetwarzania danych;
3. podniesienie efektywności wydatkowania środków w projektach zawierających elementy infrastruktury IT;
4. skrócenie czasu realizacji nowych przedsięwzięć informatycznych przez szybsze udostępnianie wymaganej infrastruktury IT;
5. ograniczenie zjawiska wielokrotnego gromadzenia tych samych danych w środowiskach informatycznych oraz zniesienie barier technologicznych w przypadku rejestrów publicznych;
6. upowszechnienie modelu chmury obliczeniowej jako sposobu funkcjonowania systemów teleinformatycznych państwa (w tym również zmiana technologii wytwarzania oprogramowania).

Celem projektowanej nowelizacji jest także poprawa efektywności i bezpieczeństwa usług świadczonych przez podmioty podlegające pod zakres przedmiotowy uchwały. Zmiany w załączniku nr 2 do uchwały sprowadzają się także do umożliwienia korzystania przez podmioty administracji rządowej z usług przetwarzania w PChO.

Mając na uwadze dynamiczny rozwój nowych technologii, w tym m.in. w zakresie usług chmurowych, oraz fakt, że Inicjatywa WIIP od 2019 r. podlegała tylko jednej, nieznacznej nowelizacji, powyższe zmiany są konieczne dla zapewnienia bezpieczeństwa państwa oraz prawidłowego realizowania *Cloud First Policy[[1]](#footnote-1)*).

W trakcie spotkań z podmiotami, które objęte są przedmiotową uchwałą został zasygnalizowany problem w postaci coraz mniejszej dostępności usług i oprogramowania z zakresu cyberbezpieczeństwa w formie *on premise*. Zdecydowana większość z nich jest dostępna już tylko w oparciu o chmurę obliczeniową. Przeprowadzona analiza rynku skłania do wniosków, że rozwiązania oparte o chmurę obliczeniową są najkorzystniejsze pod względem finansowym i najskuteczniejsze pod względem oferowanych funkcjonalności. Zwraca się uwagę na fakt, że z powodu braku możliwości skorzystania z usług przetwarzania w PChO zagrożone jest bezpieczeństwo państwa, ponieważ obniżane jest bezpieczeństwo danych z uwagi na to, że podmioty administracji rządowej – w szczególności służby i formacje umundurowane – nie są uprawnione do korzystania z nowych, aktualnych i skutecznych rozwiązań i funkcjonalności. Diametralnie zmieniła się zatem sytuacja w stosunku do tej, która miała miejsce w czasie uchwalania Inicjatywy WIIP, gdzie pierwszoplanową rolę odgrywało bezpieczeństwo danych wrażliwych z punktu widzenia bezpieczeństwa państwa, a dostępność usług z zakresu cyberbezpieczeństwa w formie *on premise* była na wysokim poziomie. Z tego względu systemy teleinformatyczne przetwarzające takie dane zostały umieszczone w załączniku nr 2 do uchwały jako te, które można przenieść do RChO lub mogące korzystać wyłącznie z dedykowanej infrastruktury teleinformatycznej. Jak wskazano powyżej, w dzisiejszych czasach – chcąc nadal zapewnić bezpieczeństwo danych i bezpieczeństwo państwa – takie podejście jest niezasadne i nieefektywne. Należy zatem umożliwić korzystanie z PChO przez podmioty administracji rządowej.

Zdecydowano się także na możliwość umieszczenia systemów teleinformatycznych, w których przetwarzane są informacje niejawne w RChO lub w PChO, jednak z zastrzeżeniem, że zależeć to będzie od dokonanej analizy przez podmiot odpowiedzialny za system teleinformatyczny i uzyskania świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego. Akredytacja systemów teleinformatycznych powinna odbywać się z uwzględnieniem art. 48 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2024 r. poz. 632) oraz rozporządzenia Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie wzoru świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego (Dz. U. poz. 926).

Uwzględniając wnioski z agresji Rosji na Ukrainę i skutki jakie wywarła ona na funkcjonowanie wszystkich systemów teleinformatycznych tego państwa, niezbędne jest zapewnienie możliwości przeniesienia systemów teleinformatycznych, w których przetwarzane są informacje niejawne do RChO lub PChO. Wynika to z potrzeby zagwarantowania Siłom Zbrojnym RP pełnej realizacji swoich zadań w zakresie obronności państwa. Doświadczenia z agresji na Ukrainę wskazują na konieczność posiadania możliwości skorzystania z publicznej chmury obliczeniowej, zarówno pod względem interoperacyjności jak i ciągłości dostarczania usług. Należy również zwrócić uwagę na fakt, że aktualnie w NATO zatwierdzana jest polityka wykorzystania usług chmurowych do poziomu NATO Restricted, czego następstwem powinna być zdolność państw NATO do kooperacji na tej płaszczyźnie w cyberprzestrzeni.

Wskazać przy tym należy, że wybór skorzystania z dedykowanej infrastruktury teleinformatycznej, RChO czy PChO (w jurysdykcji krajowej lub EOG) w dalszym ciągu jest wynikiem analizy gestora systemu (podmiot odpowiedzialny za system teleinformatyczny). Decyzja o skorzystaniu z usług chmurowych dostawcy komercyjnego musi zostać podjęta na podstawie wyników analizy załącznika nr 2 do Inicjatywy WIIP (uchwały), a następnie zostać potwierdzona przez analizę dokonaną na podstawie dokumentu Standardy Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO). SCCO określają poziomy bezpieczeństwa determinujące stosowanie poszczególnych modeli chmur obliczeniowych. Kategoryzacja bezpieczeństwa systemu teleinformatycznego dokonana na podstawie załącznika nr 2 do Inicjatywy WIIP ma bezpośredni wpływ na określenie poziomu wymagań bezpieczeństwa determinującego wybór modelu chmur obliczeniowych. W praktyce oznacza to, że najpierw gestor systemu analizuje sytuację swojego podmiotu na podstawie załącznika nr 2, a następnie na podstawie SCCO.

Kolejną gwarancją bezpieczeństwa jest przepis § 8 obecnie obowiązującej uchwały, który stanowi, że podmioty w celu skorzystania z usług przetwarzania w publicznych chmurach obliczeniowych wnioskują do właściwego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie krajowym prowadzonego przez Ministra Obrony Narodowej, Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy lub Szefa Agencji Bezpieczeństwa Wewnętrznego o wydanie opinii w zakresie możliwości wykorzystania publicznych chmur obliczeniowych. Niewydanie opinii w terminie 30 dni od dnia otrzymania wniosku jest równoznaczne z wydaniem opinii pozytywnej.

Projektodawca przeprowadził ponadto test prywatności w procesie tworzenia prawa z uwzględnieniem stanu wiedzy technicznej, charakteru przetwarzanych informacji oraz celu ich przetwarzania, a także wziął pod uwagę cel, którym kieruje się w niniejszym projekcie. Interes administratora przemawiający za przetwarzaniem danych jest prawnie i faktycznie uzasadniony, a przetwarzanie danych jest niezbędne do realizacji celu wynikającego z jego interesu. Gestorzy systemów, w których przetwarzane są określone dane, odpowiedzialni są za ich bezpieczeństwo, a w szerszej skali przekłada się to na bezpieczeństwo państwa. Wskazać należy, że dane w PChO będą mogły być przetwarzane wyłącznie w jurysdykcji krajowej lub innego państwa EOG, w którym stosowane jest prawo Unii Europejskiej. Chronione będą zatem w pełnym zakresie przez RODO.

W związku ze zmianą załącznika nr 2 w dalszej kolejności niezbędna będzie aktualizacja dokumentu SCCO w zakresie poziomów wymagań bezpieczeństwa. Dokumenty te są ze sobą ściśle powiązane i dotychczas oba uniemożliwiały korzystanie niektórym podmiotom korzystanie z usług przetwarzania w PChO. Wynikało to z klasyfikacji danych i prowadziło do sytuacji, że nawet oprogramowanie bazujące na danych analitycznych nie było dostępne dla tych podmiotów. Po uchwaleniu nowelizacji Inicjatywy WIIP zostanie zatem wydana nowa wersja SCCO obejmująca zmiany w poziomach bezpieczeństwa i analizie ryzyka, tak żeby zapewnić skuteczność Inicjatywy WIIP. Dokument SCCO wydawany jest na podstawie § 3 obecnie obowiązującej uchwały.

Zmiany w SCCO są zasadne także z tego względu, że obowiązujący dokument przygotowany został w lutym 2020 r. i nie był od tego czasu aktualizowany, co sprawia, iż dane w nim zawarte nie są w pełni skorelowane ze specyfiką procesów zachodzących w domenie cyberbezpieczeństwa, w tym w szczególności z obowiązującymi standardami. Nie ulega wątpliwości, że wskazany okres czterech lat w dziedzinie cyberbezpieczeństwa jest czasem znaczących i licznych przeobrażeń, szczególnie w aspekcie zaawansowania form i rodzajów cyberataków, których celem jest bardzo często infrastruktura administracji publicznej. Tym samym aktualizacja dokumentu o takim charakterze wymaga niezwłocznego podjęcia działań celem dostosowania go do dynamiki ww. procesów.

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 oraz z 2004 r. poz.597 ) i nie podlega notyfikacji Komisji Europejskiej. Wprowadzane projektem zmiany mają 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.

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 został udostępniony 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.

Wprowadzenie przepisów przejściowych nie jest konieczne z racji tego, że nie zostaje zawężony katalog systemów teleinformatycznych, które mogą zostać przeniesione do PChO. Zmiany wprowadzane nowelizacją mają charakter rozszerzający, tym samym podmioty, które objęte są zakresem uchwały, gdy wyrażą taką chęć i pozwoli na to przeprowadzona analiza, będą mogły skorzystać z usług przetwarzania w PChO. Podkreślić należy, że uchwała nie nakłada na podmioty obowiązku korzystania z usług RChO lub PChO. Istotne jest natychmiastowe wprowadzenie zmian zwiększających bezpieczeństwo świadczonych usług przez administrację rządową i zasady demokratycznego państwa prawnego nie stoją temu na przeszkodzie.

1. ) *Cloud First Policy* – promowanie usług przetwarzania w chmurze jako technologię „pierwszego wyboru” dla administracji. [↑](#footnote-ref-1)