**Raport**

**z konsultacji dotyczący *projektu uchwały Rady Ministrów zmieniającej uchwałę w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa”***

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

Projekt ***uchwały Rady Ministrów zmieniającej uchwałę w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa”*** został poddany opiniowaniu.

Projekt w ramach opiniowania został przekazany łącznie do 12 podmiotów: **Otrzymały go:**

1. Agencja Bezpieczeństwa Wewnętrznego;
2. Agencja Wywiadu;
3. Centralne Biuro Antykorupcyjne;
4. Rządowe Centrum Bezpieczeństwa;
5. Służba Kontrwywiadu Wojskowego;
6. Urząd Komisji Nadzoru Finansowego;
7. Służba Wywiadu Wojskowego;
8. Komenda Główna Policji;
9. Centrum e-Zdrowie;
10. Straż Graniczna;
11. Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni;
12. Urząd Ochrony Danych Osobowych.

W ramach opiniowania wpłynęły uwagi Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni, Centrum e-Zdrowie i Urzędu Ochrony Danych Osobowych.

Pozostałe podmioty nie wniosły uwag do projektu.

Z uwagi na konieczność pilnego wejścia w życie i szczególny charakter regulacji nie przeprowadzono konsultacji publicznych projektu.

Omówienie zgłoszonych uwag zostało przedstawione w **załączniku do niniejszego Raportu**.

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 zasięgnięto 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.** | **Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni** | ***Uwaga ogólna (§1 poz. 1 tabeli)*** | W § 1 projektu, który zmienia tabelę zawartą w ust. 1 załącznika nr 2, proponuje się poz. 1 nadać brzmienie:   |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | „1 | Systemy teleinformatyczne, w których są przetwarzane informacje niejawne | X | **X** | **X** | **X** | Dotyczy to systemów teleinformatycznych, które wprost w przepisach powszechnie obowiązujących są określone jako systemy niejawne lub w stosunku do których uprawnione organy wskazały, że są w nich przetwarzane informacje niejawne.  **W zależności od dokonanej analizy przez podmiot odpowiedzialny za system teleinformatyczny i uzyskania akredytacji systemu teleinformatycznego.”** |   Zapis w pozycji nr 1 w tabeli zawartej w projekcie uchwały Rady Ministrów w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa”, w dalszym ciągu, będzie uniemożliwiał Siłom Zbrojnym RP korzystanie z chmury obliczeniowej w zakresie systemów teleinformatycznych niejawnych.  Uwzględniając wnioski z agresji Rosji na Ukrainę i skutki jakie odniosła ta agresja na funkcjonowanie wszystkich systemów teleinformatycznych Ukrainy, zapis ten powinien być skorygowany do takiej samej formy jak wiersz pozycje 2 (art. 11 ustawy o ABW cyt.: „(…) oraz służb rozpoznania SZ RP”), 3, 4, aby SZP RP były w stanie w pełni realizować swoje zadania w zakresie obronności państwa. Doświadczenia z wojny w Ukrainie wskazują na konieczność posiadania możliwości skorzystania z publicznej chmury obliczeniowej, zarówno pod względem interoperacyjności, jak i ciągłości dostarczania usług.  Zwrócić również należy uwagę na fakt, iż aktualnie w NATO zatwierdzana jest polityka wykorzystania usług chmurowych do poziomu NATO Restricted (AC322-WP(2024)0018-REV1-U), czego następstwem powinna być zdolność państw NATO do kooperacji na tej płaszczyźnie cyberprzestrzeni. | **Uwaga uwzględniona**  Dokonano zmian – z odpowiednią modyfikacją zaproponowanego brzmienia (wyjaśnienie tej kwestii zamieszczono w uzasadnieniu do projektu). |
| **2.** | **Centrum e-Zdrowie** | ***Uwaga ogólna*** | Centrum e-Zdrowia pragnie wskazać, że proponowany kierunek zmian wpisuje się w identyfikowane przez Centrum e-Zdrowia potrzeby w zakresie korzystania z zasobów publicznej chmury obliczeniowej w ramach realizacji projektów e-zdrowia. W ocenie Centrum e-Zdrowia, na obecnym etapie rozwoju systemów teleinformatycznych w obszarze e-zdrowia, w tym wchodzących w skład systemu informacji w ochronie zdrowia, należy bardzo poważnie rozważyć korzystanie z publicznej chmury obliczeniowej, tak aby możliwe było wykorzystanie pełnych jej funkcjonalności, przy jednoczesnym oczywiście zapewnieniu odpowiedniego poziomu bezpieczeństwa wszystkich publicznych usług w obszarze e-zdrowia. W przeciwnym razie może dojść do sytuacji, w której skalowalność systemów informatycznych, ze względu na zwiększony ruch użytkowników, zostanie zagrożona lub wręcz całkowicie uniemożliwione zostanie ich poprawne działanie. Należy dodatkowo podkreślić, że chmura publiczna dostarcza gotowe rozwiązania technologiczne umożliwiające analizę dużych zbiorów danych z wykorzystaniem algorytmów uczenia maszynowego, co jest bardzo istotne z punktu widzenia projektów w obszarze e-zdrowia, które wiążą się z przetwarzaniem dużych ilości danych.  Postępująca informatyzacja służby zdrowia pociąga za sobą zwiększające się potrzeby zasobów informatycznych. W obecnych warunkach rynkowych coraz więcej innowacyjnych rozwiązań technologicznych e-zdrowia jest dostępnych jedynie jako usługi chmurowe. Taka bariera technologiczna już występuje w obszarach badań genetycznych, przetwarzania dużej ilości danych (Big Data), sztucznej inteligencji (AI), platformach analitycznych, platformach „low-code”, pozwalających na szybkie dostarczanie rozwiązań biznesowych dla ograniczonej grupy użytkowników, narzędzi cyberbezpieczeństwa, czy specjalistyczny rozwiązań e-Health.  Mając powyższe na względzie, Centrum e-Zdrowia przeprowadziło analizę regulacji prawnych dotyczących korzystania z publicznej chmury obliczeniowej, która uwidoczniła istniejące ograniczenia regulacyjne o charakterze wewnątrzadministracyjnym, uniemożliwiające skorzystanie z jej zasobów, wprowadzając istotne ograniczenia co do możliwości przetwarzania danych. Co istotne przy tym przepisy prawa powszechnie obowiązującego, zdaniem Centrum e-Zdrowia, nie stoją na przeszkodzie wykorzystywania publicznych chmur obliczeniowych w jurysdykcji EOG oraz usług jakie dostarczają w modelu XaaS (wszystko jako usługa) przez systemy rozwijane w CeZ. Aktualne ograniczenia w zakresie korzystania z publicznych chmur obliczeniowych wynikają jednak szczególnie ze Standardów Cyberbezpieczeństwa Chmur Obliczeniowych wer. 1.0.; dalej jako „SCCO”). Przewidują one, że w stosunku do danych w sektorze e-zdrowia (dane osobowe, tajemnica zawodowa, podlegające ochronie ustawowej, będące w myśl SCCO kontrolowanymi informacjami urzędowymi) ich przetwarzanie może następować wyłącznie w centrach danych w jurysdykcji polskiej. Zwracamy jednak uwagę, że specyfika publicznej chmury obliczeniowej powoduje, że zastrzeżenie ograniczenia przetwarzania jedynie do Polski, może okazać się niewykonalne w realizacji. Część operatorów bowiem może nie dysponować polskimi (a unijnymi) centrami danych (co jest zgodne z powszechnie obowiązującymi przepisami prawa). Sytuacje wyjścia do innej jurysdykcji mogą pojawić się także, np. w przypadku serwisu technicznego, korzystania (nawet czasowego) z awaryjnej infrastruktury umiejscowionej w innym kraju UE/EOG, czy współdzielenia pewnych zasobów. W ocenie Centrum e-Zdrowia możliwość realizacji działań w zakresie wykorzystania publicznej chmury obliczeniowej w projektach e-zdrowia powinna być zatem niezależna od przetwarzania danych osobowych wyłącznie w Centrum Przetwarzania Danych na obszarze Polski, a z dopuszczeniem jurysdykcji unijnej /EOG. Przyjęcie bowiem a priori określonych wyłączeń i wymagań nie odzwierciedla rzeczywistych potrzeb oraz specyfiki różnych procesów przetwarzania danych. Nie znajduje ponadto poparcia w praktycznych doświadczeniach ostatnich lat, wynikających m.in. z rozwiązań przyjmowanych w okresie pandemii COVID19. W związku z powyższym, kluczowym aspektem zmian, poza procedowaną nowelizacją Uchwały WIIP, jest także weryfikacja i aktualizacja dokumentu SCCO w powyższym zakresie. Aktualizacja ta powinna w ocenie Centrum e-Zdrowia zmierzać w stronę elastycznego podejścia bazującego na analizie ryzyka dokonanej przez podmiot odpowiedzialny za system teleinformatyczny (tzw. właściciela biznesowego danego systemu). Pozwoli to na indywidualną ocenę projektów z uwzględnieniem indywidualnych okoliczności faktycznych. Mając na względzie przygotowywaną nowelizację, zapewni to jednocześnie spójność z Uchwałą WIIP w docelowym zakresie. | **Uwaga wyjaśniona**  Projektodawca podziela stanowisko wyrażone przez CeZ. Standardy Cyberbezpieczeństwa Chmur Obliczeniowych będą musiały zostać zaktualizowane jednak dopiero wtedy gdy wejdzie w życie nowelizacja uchwały WIIP. Projektodawca zwraca uwagę, że szeroko opisał w uzasadnieniu do projektu potrzebę aktualizacji SCCO i zobowiązał się do jej dokonania po przyjęciu projektu ucwały. W innej sytuacji nawet po wejściu w życie nowelizacji uchwały WIIP przeniesienie systemów teleinformatycznych do PChO byłoby niemożliwe albo znacznie utrudnione. |
| **3.** | **Urząd Ochrony Danych Osobowych** | **Uwaga ogólna** | Zgodnie z projektowaną uchwałą zmianie ulegnie załącznik nr 2 do 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) określający kryteria klasyfikacji systemów teleinformatycznych, które mogą korzystać z usług przetwarzania w Rządowej Chmurze Obliczeniowej (RChO) lub w Publicznych Chmurach Obliczeniowych (PChO). W wyniku przedmiotowej zmiany w ww. chmurach obliczeniowych będą mogły funkcjonować wszystkie systemy teleinformatyczne administracji rządowej, z wyłączeniem systemów, w których są przetwarzane informacje niejawne. Oznacza to włączenie do chmur obliczeniowych, po przeprowadzeniu analizy przez podmiot odpowiedzialny za dany system teleinformatyczny, m. in. systemów wykorzystywanych przez służby specjalne (**pkt 2** tabeli), służby mundurowe i wymiar sprawiedliwości (**pkt 4** tabeli) oraz tych systemów, w których są przetwarzane szczególne kategorie danych osobowych w rozumieniu art. 9 i 10 rozporządzenia 2016/679 (**pkt 8** tabeli). Biorąc pod uwagę wysoce newralgiczny charakter danych przetwarzanych w tych systemach, organ nadzorczy wskazuje na konieczność przeprowadzenia przez projektodawcę **testu** **prywatności w procesie tworzenia prawa**, w tym oceny skutków dla ochrony danych art. 25 ust. 13 rozporządzenia 2016/679, jak i art. 35 (w szczególności ust. 14 i ust. 105), w związku z przyjmowaniem podstawy prawnej przetwarzania. Przeprowadzenie ww. testu prywatności powinno wykazać czy faktycznie zmiany projektowanej uchwały zwiększą poziom cyberbezpieczeństwa i ochrony danych przetwarzanych w państwowych chmurach obliczeniowych, bez wpływu na ryzyko naruszenia danych zwykłych i szczególnych kategorii przetwarzanych przez administrację publiczną. | **Uwaga uwzględniona**  Projektodawca zgodnie z uwagą Prezesa UODO przeprowadził test prywatności w procesie stanowienia prawa. Projektodawca podziela stanowisko, że zastosowanie testu daje możliwość dokonania oceny ryzyk i tym samym uwzględnienie odpowiednich środków prawnych umożliwiających wyeliminowanie ryzyka naruszenia danych poszczególnych kategorii, które docelowo mają być przetwarzane w ramach RChO i PChO.  W związku z powyższym projektodawca przeprowadził test prywatności z uwzględnieniem stanu wiedzy technicznej, charakteru przetwarzanych informacji oraz celu ich przetwarzania, a także wziął pod uwagę cel, którym kieruje się w niniejszym projekcie. Zdaniem projektodawcy interes administratora przemawiający za przetwarzaniem danych jest prawnie i faktycznie uzasadniony, a przetwarzanie danych jest niezbędne do realizacji celu wynikającego z tego 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.  OSR i uzasadnienie zostało doprecyzowane o informację w przedmiocie przeprowadzonego testu. |