**Zestawienie uwag zgłoszonych w ramach opiniowania projektu** **uchwały Rady Ministrów w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa”**

| Lp. | Podmiot zgłaszający uwagi | Jednostka redakcyjna do której jest zgłaszana uwaga | Podmiot zgłaszający uwagi | Jednostka redakcyjna |
| --- | --- | --- | --- | --- |
| 1 | Rada ds. Cyfryzacji | Uwaga ogólna | Rada ds. Cyfryzacji ocenia inicjatywę „Wspólna Infrastruktura Informatyczna Państwa” jako słuszny krok w kierunku standaryzacji zarządzania infrastrukturą teleinformatyczną administracji publicznej, zauważając jednak, że projektowane rozwiązanie wymaga dopracowania zarówno pod względem proponowanych rozwiązań organizacyjnych, jak i prawnych. Uchwała w obecnym kształcie może utrudnić proces informatyzacji podmiotów publicznych, ponieważ zobowiązuje je do uzgodnienia z ministrem właściwym do spraw informatyzacji możliwości wykorzystania Rządowej Chmury Obliczeniowej w przypadku projektowania, budowy lub rozwoju istniejących systemów teleinformatycznych. Wskutek tego mogą powstawać opóźnienia wynikające z uzgadniania każdego zadania teleinformatycznego administracji publicznej, z ministrem oraz Centralnym Ośrodkiem Informatyki jako Operatorem Chmury. Uchwała w obecnym kształcie może spowolnić proces inwestycji ITS w kluczowych instytucjach państwowych, co z kolei skłaniać będzie administrację do unikania obowiązkowych uzgodnień, a tym samym doprowadzi do niezrealizowania generalnych założeń projektu WIIP. | Uwaga wyjaśniona. Korzystanie z usług przetwarzania w RChO jest dobrowolne. Opiniowanie przez ministra właściwego ds. informatyzacji nowych projektów teleinformatycznych dotyczy możliwości technicznych wykorzystania RChO. |
| 2 | Rada ds. Cyfryzacji | Uwaga ogólna | Opiniowana uchwała nie określa zależności między ww. uzgadnianiem projektowania nowych rozwiązań informatycznych z obowiązkami i zadaniami Komitetu Rady Ministrów ds. Cyfryzacji. Obecnie, na podejmowanie inicjatyw w obszarze rozwiązań informatycznych administracji publicznej decydujący wpływ ma KRMC, a brak związku uchwały z pracami KRMC rodzi pytanie czy pozytywnie zaopiniowany przez KRMC projekt może zostać zmieniony wskutek obowiązkowych uzgodnień z ministrem właściwym do spraw informatyzacji. | Wyjaśnienie. Obowiązek wynikający z uchwały nie pozostaje w sprzeczności z wymaganiem opiniowania przez KRMC. Konsultacje wskazane w uchwale dotyczą technicznych możliwości skorzystania z RChO i powinny być przeprowadzanie przed skierowaniem projektu na KRMC. Nie ma ryzyka odmiennego zdania ze względu na to, że przewodniczącym KRMC jest minister właściwy ds. informatyzacji. |
| 3 | Rada ds. Cyfryzacji | Uwaga ogólna | Finansowanie WIIP ze środków, które dotychczas były przeznaczone lub będą planowane na rozwój i utrzymanie systemów teleinformatycznych administracji publicznej przenoszonych na Rządową Chmurę Obliczeniową spowoduje wzrost ryzyka związanego z realizacją założonych celów. Rozpatrując ten czynnik, należy uwzględnić jednocześnie brak precyzyjnych regulacji dotyczących wydatkowania środków na rozwój i utrzymanie istniejących już systemów, za które odpowiada organ administracji inny niż minister właściwy ds. informatyzacji, a które znajdą się w Chmurze. Dysponentem środków będzie Centralny Ośrodek Informatyki, ale odpowiedzialność za realizowanie zadań, do których stworzono systemy, będzie nadal po stronie Organu. Uchwała nie precyzuje podziału kompetencji i odpowiedzialności w tym zakresie, jak również nie określa kto będzie decydentem oraz kto będzie odpowiadał za kształt modyfikacji systemów i planowanie zamówień publicznych. Nie jest również jasne, który podmiot będzie obarczony kosztami utrzymania Centrów Przetwarzania Danych. | Uwaga wyjaśniona. RChO dostarcza tylko infrastrukturę informatyczną w modelu usługowym zdejmując odpowiedzialność za jej rozwój i utrzymanie z właściciela systemu. Nie zdejmuje to jednak odpowiedzialności za rozwój i utrzymanie systemu informatycznego jako takiego. RChO będzie dostarczać ustandaryzowanych usług infrastrukturalnych w ilości niezbędnej pokrywającej zidentyfikowany popyt. Jasno nie określono podziału kompetencji i odpowiedzialności w obszarze rozwoju i utrzymania systemu informatycznego, ponieważ wynika to z typu usługi infrastrukturalnej dostarczanej z chmury. I tak, typ IaaS dzieli odpowiedzialność pomiędzy Operatora RChO i właściciela systemu np.: dla maszyny wirtualnej (usługa IaaS) za utrzymanie, zabezpieczenie, rozwój infrastruktury informatycznej składającej się na tę usługę odpowiada operator RChO a za elementy systemu operacyjnego, jego konfiguracji wraz z aplikacjami i danymi odpowiada jego właściciel. Zadaniem MC jest zidentyfikowanie potencjalnego popytu na konkretne usługi i zabezpieczenie zawczasu wymaganego jej wolumenu. |
| 4 | Rada ds. Cyfryzacji | Uwaga ogólna | Zdaniem Rady ds. Cyfryzacji realizacja zakupów przez centralnego zamawiającego, tj. Centrum Obsługi Administracji Rządowej, którego działania dotychczas koncentrowały się na obszarach innych niż zakupy rozwiązań klasy ITS i usługi klasy enterprise, może mieć wpływ na, obecnie już i tak długi, czas realizacji postępowań zakupowych. Zakupy wspólne w administracji są proste, gdy dotyczą produktów jednorodnych i masowych, a nie sektorowych i specjalistycznych. Na przykładzie infrastruktury klasy enterprice należy zaznaczyć, że przeciętny przetarg trwa obecnie co najmniej 8 miesięcy (czas liczony od decyzji o zakupie do dostawy urządzeń). Skoncentrowanie tych wszystkich działań w jednej instytucji zamawiającej, poszerzającej jednocześnie zakres zadań swego zespołu, znacznie utrudni możliwości zaspokojenia nawet dotychczasowych potrzeb zamawiających. Ponadto, należy zwrócić uwagę na aktualne zasady finansowania zakupów za pośrednictwem COAR, który powiększane są o wynagrodzenie dla tego podmiotu. Z uchwały nie wynika, czy budżet COAR będzie powiększony kosztem dotychczasowych zamawiających, niezależnych względem siebie, czy finansowanie będzie niezależne, dodatkowe, co może spowodować wzrost kosztów IT w państwie. | Uwaga wyjaśniona. W przypadku RChO zakupy będą realizowane raz dla wszystkich, którzy korzystają lub będą korzystać z RChO. W modelu tradycyjnym zakupy infrastruktury realizowane są w modelu reaktywnym (zaspokajają już zidentyfikowaną potrzebę biznesową). W modelu chmurowym zakupy infrastruktury niezbędnej do świadczenia usług realizowane są w modelu proaktywnym (przewidujemy zapotrzebowanie na usługi zaspokajające przyszłe potrzeby biznesowe i zawczasu kupujemy adekwatną infrastrukturę). Takie działanie istotnie skróci czas niezbędny do zaspokojenia potrzeby biznesowej. |
| 5 | Rada ds. Cyfryzacji | Uwaga ogólna | Jednocześnie Rada ds. Cyfryzacji zwraca uwagę na konieczność precyzyjnego zakreślenia obszaru technicznego oraz uwzględnienia szczególnego charakteru ITS, jakim jest Infrastruktura Krytyczna. Nie określono wyraźnie czy IK ma korzystać z Rządowej Chmury Obliczeniowej, czy może być jej częścią, choć oba warianty budzą szereg wątpliwości. Ponadto, projektodawca posługuje się pojęciem „sieci łączności rządowej”, co nasuwa wątpliwości o którą sieć de facto chodzi - Sieć Łączności Rządowej (sieć telekomunikacyjna, w zakresie świadczenia usług głosowych) czy GovNet (sieć teletransmisji danych i usług z obszaru bezpieczeństwa Państwa oraz wymiany danych w sektorze publicznym).  W zakresie bezpieczeństwa projekt nie uwzględnia istnienia systemów, które z racji spełnianych funkcji nie mogą się być objęte Rządowym Klastrem Bezpieczeństwa (RKB) (bezpieczeństwo chmury obliczeniowej), a decydentem w sprawach polityk bezpieczeństwa tych systemów powinien pozostać podmiot odpowiedzialny za realizację zadań opartych o te systemy czy sieci. Ocena skutków regulacji nie przedstawia danych dotyczących istniejących Centrów Przetwarzania Danych, sieci i innych rozwiązań, na których ma opierać się Chmura Obliczeniowa. Wiążąc ten fakt z obowiązkiem przeprowadzenia analizy istniejących CPD pod kątem spełniania wymogów uchwały, dopiero po jej uchwaleniu, należy jednoznacznie przeanalizować czy proponowane rozwiązanie ma oparcie w realnie istniejących zasobach teleinformatycznych. | Uwaga uwzględniona. Pojęcie sieci łączności rządowej zostało doprecyzowane w projekcie Uchwały pod pojęciem „sieci rządowe”. Kwestie związane z bezpieczeństwem oraz rolami m.in. MSWiA zostały doprecyzowane. W OSR zawarto dane nt. kosztów wdrożenia RChO w najbliższych latach oraz szacowanej wartości oszczędności (redukcji kosztu utrzymania IT po stronie klientów chmury). W przypadku pierwszych dwóch lokalizacji CPD niezbędnych do uruchomienia pierwszego katalogu usług analizy możliwości technicznych zostały już przeprowadzone. |
| 6 | Rada ds. Cyfryzacji | Uwaga ogólna | Rada zwraca uwagę również na brak wymogu potwierdzenia spełnienia wymagań zapewnienia zgodności ze standardami ISO działania Centrum Przetwarzania Danych danego podmiotu i przejściem przez proces certyfikacji. Dodatkowo, sam obowiązek zapewnienia zgodności ze standardami ISO może być spełniony dopiero po przyłączeniu CPD do Rządowej Chmury Obliczeniowej. Takie rozwiązanie może prowadzić do oparcia Chmury na Centrach nie spełniających wymagań w zakresie zarządzania ciągłością działania czy ryzykiem. | Uwaga uwzględniona. Przeredagowano opis wymagań w zakresie standardów dla CPD podłączanych do RKB. |
| 7 | Zakład Ubezpieczeń Społecznych | § 6 ust. 1 pkt 5 i 7 | Mając na uwadze wrażliwość danych oraz konieczność zachowania wysokiego stopnia bezpieczeństwa przetwarzanych danych, dotyczących podmiotów odpowiedzialnych za bezpieczeństwo państwa (m.in. ABW, AW, SKW), w naszej ocenie Zakład Ubezpieczeń Społecznych powinien mieć możliwość dokonania wyboru typu usług, których przetwarzanie zostanie przeniesione na Rządową Chmurę Obliczeniową. Proponujemy usunięcie zapisów dotyczących Zakładu Ubezpieczeń Społecznych z § 6 ust. 1 pkt 5 projektu wraz z odpowiednim sformułowaniem wyłączenia w pkt 7 omawianego przepisu, co spowoduje przeniesienie Zakładu do podmiotów wymienionych w § 6 ust. 2 pkt 1, czyli jednostek sektora finansów publicznych fakultatywnie korzystających z usług przetwarzania w Rządowej Chmurze Obliczeniowej.  W związku z powyższym proponujemy wykreślenie w § 6 ust. 1 pkt 5 projektu wyrazów „Zakład Ubezpieczeń Społecznych i zarządzane przez niego fundusze oraz" oraz zastąpienie w § 6 ust. 1 pkt 7 projektu wyrazów „z wyłączeniem przedsiębiorstw, banków i spółek prawa handlowego" wyrazami „z wyłączeniem przedsiębiorstw, banków, spółek prawa handlowego i Zakładu Ubezpieczeń Społecznych". | Uwaga uwzględniona. Dokonano zmian § 6 ust. 1 i 2, z których wyraźnie wynika, że korzystanie z Rządowej Chmury Obliczeniowej jest dobrowolne. |
| 8 | Prezes Urzędu Ochrony Danych Osobowych | Uwaga ogólna | (..) w ocenie Prezesa Urzędu Ochrony Danych Osobowych, Projektodawca powinien, w pierwszej kolejności, przeprowadzić kompleksową ocenę skutków planowanej operacji przetwarzania (usługi przetwarzania w Rządowej Chmurze Obliczeniowej) dla ochrony danych osobowych, zgodnie z art. 35 ust. 1 rozporządzenia 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z pozn. zm."), powoływanego dalej z zastosowaniem skrótu „rozporządzenie 2016/679". Wydaje się bowiem, iż ocena taka, o ile w ogóle została przeprowadzona, to jedynie pobieżnie. Wskazuje na to brak odzwierciedlenia w projekcie następujących kwestii: a) zakresu danych przetwarzanych w usłudze przetwarzania w Rządowej Chmurze Obliczeniowej, b) zagadnienia anonimizacji i pseudonimizacji danych, c) problematyki regularnego wykonywania kopii zapasowych oraz okresu ich przechowywania, d) wyjaśnienia czy, a jeśli tak, to w jakim zakresie, administrator Rządowej Chmury Obliczeniowej będzie miał dostęp do danych przetwarzanych przez podmioty korzystające z tej chmury. | Uwaga uwzględniona. OSR projektu został uzupełniony o załącznik „Analiza ryzyka zagrożeń dla ochrony danych osobowych w ramach inicjatywy WIIP”. Analizę ryzyka sporządzono w oparciu katalog zagrożeń dla ochrony danych związanych z przetwarzaniem danych w chmurze, który został określony w Opinii 5/2012 w sprawie przetwarzania danych w chmurze obliczeniowej, sporządzonej w ramach Grupy Roboczej Artykułu 29 ds. Ochrony Danych oraz metodykę określoną zarządzeniem nr 5 Ministra Cyfryzacji z dnia 27 lutego 2019 r. w sprawie zatwierdzania do realizacji oraz zarządzania projektami, programami i portfelem projektów w resorcie cyfryzacji (Dz. Urz. Ministra Cyfryzacji z 2019 poz. 6). W pozostałym zakresie oceny skutków w rozumieniu art. 35 RODO dokonywane będą w każdym indywidualnym przypadku w związku z zawieranymi porozumieniami, gdyż w ramach uchwały mającej charakter kierunkowej zgody na realizację przedmiotowej inicjatywy nie jest możliwe szczegółowe uregulowanie wszystkich kwestii związanych z przetwarzaniem danych osobowych. |
| 9 | Prezes Urzędu Ochrony Danych Osobowych | § 4, § 7 | (…) Projektodawca winien jednoznacznie określić rolę poszczególnych podmiotów w procesie przetwarzania w Rządowej Chmurze Obliczeniowej. Zgodnie bowiem z § 4 ust. 1 projektu operatorem Rządowej Chmurze Obliczeniowej jest minister właściwy do spraw informatyzacji, który wszakże powierza realizację we własnym imieniu tego zadania jednostce nadzorowanej - Centralnemu Ośrodkowi Informatyki (§ 4 ust. 2 projektu). Powstaje zatem pytanie, jaki jest status Centralnego Ośrodka Informatyki w procesie przetwarzania w Rządowej Chmurze Obliczeniowej? (czy jest to podmiot przetwarzający w rozumieniu art. 26 rozporządzenia 2016/679, a jeśli tak, to czy jest to przetwarzanie przez podmiot przetwarzający na podstawie instrumentu prawnego, czy tez przetwarzanie przez podmiot przetwarzający na podstawie umowy). Co więcej - w proces przetwarzania w Rządowej Chmurze Obliczeniowej włączony jest też operator Rządowego Klastra Bezpieczeństwa (§ 4 ust. 4 projektu), którym jest minister właściwy do spraw informatyzacji (§ 7 ust. 4 projektu), który powierza realizację we własnym imieniu tego zadania jednostce nadzorowanej - Naukowej i Akademickiej Sieci Komputerowej - Państwowemu Instytutowi Badawczemu (§ 7 ust. 6 w zw. z ust. 5 projektu). W ocenie Prezesa Urzędu Ochrony Danych Osobowych przy takiej konstrukcji prawnej Rządowej Chmurze Obliczeniowej niespełniona jest zatem zasada przejrzystości z art. 5 ust. 1 lit. a rozporządzenia 2016/679. | Uwaga wyjaśniona. Minister właściwy ds. informatyzacji będzie pełnił rolę podmiotu przetwarzającego w rozumieniu art. 4 pkt 8 RODO. Przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora, a także inne szczegółowe kwestie, o których mowa w art. 28 ust. 3 RODO będą regulowane w porozumieniach zawieranych między poszczególnymi administratorami a podmiotem przetwarzającym. |
| 10 | Prezes Urzędu Ochrony Danych Osobowych | Uwaga ogólna | Nie umknęło uwadze organowi właściwemu w sprawie ochrony danych osobowych również to, ze w projekcie nie zostały określone procedury dotyczące przyłączenia, przeniesienia danych lub ewentualnego odłączenia się od Rządowej Chmury Obliczeniowej. Rodzi to ze strony Prezesa Urzędu Ochrony Danych Osobowych pytanie, czy podmiot korzystający z usług przetwarzania w Rządowej Chmurze Obliczeniowej, będący administratorem, w ogóle będzie miał możliwość zaniechania przetwarzania danych w tej chmurze i , czy zachowana zostanie jego realna kontrola nad procesem przetwarzania danych, których jest administratorem. Co więcej - Projektodawca winien przy budowie Rządowej Chmury Obliczeniowej mieć na względzie zasadę uwzględniania ochrony danych osobowych w fazie projektowania systemu teleinformatycznego (tzw. „privacy by design") - art. 25 ust. 1 rozporządzenia 2016/679. | Uwaga wyjaśniona. Uchwała ma charakter kierunkowej zgody na realizację przedmiotowej inicjatywy. Nie jest intencją projektodawcy określanie wszystkich technicznych procedur świadczenia usług oraz regulowanie zakresu odpowiedzialności usługodawcy i usługobiorcy, które będą przedmiotem osobnych umów i porozumień. Należy jednak wskazać, że na gruncie RODO kontrola administratora powinna dotyczyć głównie elementów funkcjonalnych, a nie technologicznych. |
| 11 | Prezes Urzędu Ochrony Danych Osobowych | Uwaga ogólna | (…) po przeprowadzeniu prawidłowej oceny skutków i uzupełnieniu projektu o sygnalizowane wyżej elementy, możliwe będzie rozstrzygniecie, czy projektowana Rządowa Chmura Obliczeniowa nie generuje ryzyk, o których mowa w opinii 5/2012 (Grupy Roboczej art. 29) w sprawie przetwarzania danych w chmurze obliczeniowej, to jest: - braku dostępności ze względu na brak interoperacyjności (uzależnienie od dostawcy). Jeżeli dostawca usługi w chmurze bazuje na zastrzeżonej technologii, dla klienta usługi może się okazać trudne przenoszenie danych i dokumentów między różnymi systemami opartymi na cloud computingu (możliwość przenoszenia danych) lub wymiana informacji z podmiotami korzystającymi z usług w chmurze zarządzanych przez innych dostawców (interoperacyjność), - braku integralności spowodowanego przez dzielenie się zasobami. Chmura obliczeniowa składa się z współdzielonych systemów i infrastruktur. Dostawcy usług w chmurze obliczeniowej przetwarzają dane osobowe wywodzące się z licznych źródeł - osób, których dane dotyczą i organizacji - i istnieje możliwość, ze mogą powstać sprzeczne interesy i/lub różne cele, - braku poufności w odniesieniu do wniosków z zakresu egzekwowania prawa składanych bezpośrednio do dostawcy usługi w chmurze obliczeniowej. Dane osobowe przetwarzane w chmurze mogą być przedmiotem wniosków z zakresu egzekwowania prawa pochodzących od organów egzekwowania prawa z państw członkowskich Unii Europejskiej oraz krajów trzecich, - braku możliwości interwencji ze względu na złożoność i dynamiczność łańcucha outsourcingu. Usługa w chmurze oferowana przez jednego dostawcy może być realizowana poprzez połączenie usług od szeregu innych dostawców, które mogą być dynamicznie dodawane lub usuwane, - braku możliwości interwencji (prawa osób, których dane dotyczą). Dostawca usługi w chmurze obliczeniowej może nie zapewnić niezbędnych środków i narzędzi mających pomóc administratorowi zarządzać danymi, np. w zakresie dostępu, usunięcia lub poprawienia danych, - braku odizolowania. Dostawca usługi w chmurze obliczeniowej może wykorzystywać swoją fizyczną kontrolę nad danymi od różnych klientów w celu łączenia danych. Jeżeli dostawcy usługi administrujący przetwarzaniem mieliby wystarczające prawa uprzywilejowanego dostępu, mogliby łączyć informacje od różnych klientów (administratorów), - braku informacji na temat przetwarzania (przejrzystości). Niewystarczające informacje na temat operacji przetwarzania w chmurze obliczeniowej stanowią zagrożenie dla administratorów, jak i dla osób, których dane dotyczą ponieważ mogą oni nie być świadomi potencjalnych zagrożeń i tym samym nie mogą podjąć środków, które uważają odpowiednie. | Uwaga uwzględniona. OSR do projektu uzupełniono o stosowną analizę ryzyka. |
| 12 | Prezes Urzędu Ochrony Danych Osobowych | § 5 ust 1, zał. 1 | Opisane w § 5 ust 1 projektu przyłączanie Centrów Przetwarzania Danych, dalej „CPD", do Rządowej Chmury Obliczeniowej nie może następować włącznie na podstawie pisemnych oświadczeń potwierdzających spełnienie minimalnych wymagań organizacyjnych i technicznych dla posiadaczy CPD oraz ich obiektów CPD przyłączonych do Rządowej Chmury Obliczeniowej. Zasadnym wydaje się, aby przed przyłączaniem przeprowadzony został niezależny audyt potwierdzający zgodność CPD z w/w wymaganiami. Warto również rozważyć wprowadzenia zapisu nakładającego konieczność przeprowadzania cyklicznie audytów spełniania wymagań; | Wyjaśnienie. Uchwała nie przewiduje konieczności uzyskania certyfikatów, biorąc pod uwagę, że właścicielami CPD są organy administracji, które ponadto zobligowane są do spełnienia wymogów określonych w KRI. Wymóg audytowania CPD nie wynika z przepisów RODO. Właściciele CPD będą ponosili odpowiedzialność za uchybienia w tym zakresie. |
| 13 | Prezes Urzędu Ochrony Danych Osobowych | Zał. 1 | Do - wskazanych w ust. 1 załącznika nr 1 do projektu - wykazu standardów celowym byłoby dopisać normę PN-ISO/IEC 27018 Praktyczne zasady ochrony danych identyfikujących osób (PII) w chmurach publicznych działających jako przetwarzający PIT. | Uwaga wyjaśniona.  Wymienione w zał. 1 normy np. dotyczące zarządzania bezpieczeństwem informacji odwołują się wprost do normy PN-ISO/IEC 27018 narzucając jej stosowanie. Z tego względu nie jest konieczne wprost wskazywanie normy dot. zasad ochrony danych identyfikujących osób (PII) w chmurach publicznych działających jako przetwarzający PIT. |