**TABELA Z UWAGAMI WRAZ Z ODNIESIENIEM SIĘ DO UWAG**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Nazwa dokumentu:*** *projekt II tomu Rekomendacji Prezesa Urzędu Zamówień Publicznych dotyczących zamówień publicznych na systemy informatyczne pn. "OPZ i przygotowanie postępowania o udzielenie zamówienia publicznego na system informatyczny”* | | | | | |
| ***Lp.*** | ***Organ wnoszący uwagi*** | ***Jednostka redakcyjna, do której wnoszone są uwagi*** | ***Treść uwagi*** | ***Propozycja zmian zapisu*** | ***Odniesienie do uwagi*** |
| **1.** | **MC** | **Zagadnienia nr 6.2 oraz 6.3** | Przedstawione rekomendacje nie uwzględniają, poza tematyką związaną z usługami chmurowymi (zagadnienia nr 6.2 oraz 6.3), kwestii cyberbezpieczeństwa na żadnym z etapów przygotowywania zamówienia publicznego. Ze względu na coraz szersze wykorzystywanie systemów informatycznych do świadczenia usług, gromadzenia i przetwarzania danych, w tym danych osobowych, kwestie związane z bezpieczeństwem tych systemów i przetwarzanych danych nabierają coraz większego znaczenia i powinny być uwzględniane w przygotowywanych postępowaniach o zamówienie publiczne. Co więcej, z uwagi, że w najbliższych latach zaplanowane są liczne działania, których efektem będzie zwiększenie liczby zamówień publicznych na sprzęt i systemy informatyczne m.in. projekty zawarte w Krajowym Planie Odbudowy, w Polskim Ładzie oraz w nowej perspektywie finansowej UE na lata 2021-2027 (Fundusze Europejskie na Rozwój Cyfrowy) konieczne jest zapewnienie, aby zamawiający  uwzględniali wymagania cyberbezpieczeństwa na każdym etapie przygotowywania oraz oceniania ofert. W związku z powyższym, postuluje się uwzględnienie zagadnień cyberbezpieczeństwa we wszystkich tematach zamówień informatycznych, w szczególności na etapie analiz związanych z możliwością podziału zamówienia, czy określania kryteriów wyboru wykonawcy. W opinii MC uwzględnienie tematu cyberbezpieczeństwa w zamówieniu powinno być obligatoryjne. W tym kontekście należy zauważyć, że w całym dokumencie nie ma odniesienia do dostępnych już mechanizmów, np. klauzuli bezpieczeństwa państwa i rekomendacji Pełnomocnika Rządu ds. Cyberbezpieczeństwa, a zgodnie z art. 226 ust. 1 pkt 17 PZP zamawiający odrzuca ofertę, jeżeli obejmuje ona urządzenia informatyczne lub oprogramowanie wskazane w rekomendacji, o której mowa w [art. 33 ust. 4](https://sip.legalis.pl/document-view.seam?documentId=mfrxilrtg4ytkmzvgezdoltqmfyc4njvgi4dcojzgq) ustawy o krajowym systemie cyberbezpieczeństwa, stwierdzającej ich negatywny wpływ na bezpieczeństwo publiczne lub bezpieczeństwo narodowe. | **Uwaga uwzględniona.**  Do Rekomendacji dodano rozdział IX pt.: „ *Odpowiednie opisanie wymogów cyberbezpieczeństwa systemów informatycznych”,* w którym zawarto rekomendacje ogólne i szczegółowe dotyczące cyberbezpieczeństwa. Zrezygnowano jednak z wpisywania szczegółowych, konkretnych wymagań gotowych do przeniesienia do SWZ, bowiem takie wymagania w dużym stopniu zależą od specyfiki danego zamawiającego i mogą wymagać uwzględnieni a stanowisk różnych podmiotów, np. Prezesa Urzędu Ochrony Danych Osobowych, Urzędu Komisji Nadzoru Finansowego czy Pełnomocnika Rządu ds. Cyberbezpieczeństwa.Takie stanowiska mogą też zmieniać się w czasie. Dlatego niecelowe byłoby powtarzanie ich w rekomendacjach UZP.  Odnośnie rekomendacji Pełnomocnika Rządu ds. Cyberbezpieczeństwa - jeśli zostaną wydane rekomendacje Pełnomocnika dotyczące konkretnych produktów, zamawiający będą musieli uwzględnić je na etapie oceny ofert zgodnie z art. 226 ust. 1 pkt 17 PZP. Tom II rekomendacji UZP, których dotyczą uwagi, dotyczy jednak opisu przedmiotu zamówienia. | |
| **2.** | **MC** | **Definicje** | Definicje ujęte w projekcie dokumentu wymagają korekty i dlatego proponuje się nadanie im następującego brzmienia:  **a.** Chmura obliczeniowa/Cloud Computing – model przetwarzania umożliwiający powszechny i wygodny dostęp za pośrednictwem sieci do  wspólnej puli konfigurowalnych zasobów przetwarzania np. sieci, serwerów, pamięci masowych, aplikacji i usług (usługi w rozumieniu technicznym (ang. „services”) np. DNS, Active Directory, itp. a nie usługi w znaczeniu prawnym (np. w rozumieniu kodeksu cywilnego lub klasyfikacji zamówień publicznych), które są szybko udostępniane z katalogu usług przy minimalnym wysiłku ze strony zespołów zarządzania lub dostawcy usług.  Składa się z trzech podstawowych modeli usług, tj. SaaS, PaaS, IaaS. Jednocześnie należy zauważyć, że na rynku występują również modele usług w chmurze obliczeniowej: FaaS (Function as a Service), BaaS (Backend as a Service), DBaaS (Database as a Service), AIaaS (Artificial Intelligence as a Service), CaaS (Container as a Service), MaaS (Monitoring as a Service). W niedalekiej przyszłości możemy spodziewać się wprowadzenia na rynek nowych modeli usług, szeregu modeli wdrażania chmur (np. chmura prywatna, chmura wspólnotowa,  chmura publiczna, chmura hybrydowa, federacja chmur). Zatem proponuje się również uwzględnienie w przedmiotowym dokumencie modelu wdrożeniowego: federacja  Chmur. Zasadniczymi cechami chmury obliczeniowej są: samoobsługa na żądanie, szeroki dostęp do sieci, dynamiczne gromadzenie zasobów, szybkie i elastyczne przydzielanie i zwalnianie zasobów, mierzalność i optymalizacja usług. Stosowana jest zasada współdzielonej odpowiedzialności między dostawcą i odbiorcą usług chmurowych, a kluczowe technologie wykorzystywane do budowy tego modelu obejmują: szybkie i wydajne sieci rozległe, wydajne oraz relatywnie niedrogie serwery (uwzględniając ich liczbę) oraz wysokowydajną wirtualizację sprzętu,  **b.** On-premise – model budowy systemu informatycznego zakładający zainstalowanie (posadowienie) oprogramowania na konkretnych urządzeniach będących w bezpośredniej dyspozycji zamawiającego; w uproszczeniu –  systemy informatyczne on-premise to systemy, które nie opierają się na technologii chmury obliczeniowej. Oprogramowanie jest instalowane na infrastrukturze klienta, która pozostaje jego wyłączną własnością. Na kliencie spoczywa utrzymanie całego niezbędnego sprzętu,  **c**. SLA (umowa gwarancji świadczenia usługi) – umowa utrzymania ustalonego między klientem i usługodawcą, poziomu jakości usług. | **Brak podstaw do uwzględnienia uwagi z pkt a), b) c)** z następujących względów:  **Ad. a):** Zrezygnowano ze zmiany definicji Chmury obliczeniowej, ponieważ obecnie stosowana definicja została wprost przeniesiona z uchwały Rady Ministrów nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy "Wspólna Infrastruktura Informatyczna Państwa". Celowe wydaje się zachowanie spójności terminologicznej między rekomendacjami UZP a uchwałą Rady Ministrów.  **Ad. b):** Zrezygnowano ze zmiany definicji modelu On-premise, ponieważ proponowana modyfikacja mogłaby prowadzić do nieporozumień. Istotą modelu on-premise opisywanego w rekomendacjach jest wdrożenie systemu IT, które nie jest ściśle powiązane z konkretnym modelem prawnym dysponowania sprzętem. Zaznaczenie, że infrastruktura ma być własnością klienta, mogłoby prowokować pytania odbiorców rekomendacji np. o status dzierżawy sprzętu. Z kolei ostatnie zdanie mogłoby sugerować odbiorcom, że zamówienia w modelu on-premise nie mogą obejmować utrzymania sprzętu.  **Ad. c):** Zrezygnowano także z wprowadzenia zmienionej definicji SLA, ponieważ zaproponowana definicja wydaje się trudna do pogodzenia z terminologią stosowaną na gruncie prawa zamówień publicznych. Przykładowo, parametry SLA nie są tu „ustalane, nie zawsze usługodawca jest jednocześnie wykonawcą w rozumieniu PZP, a samo SLA w praktyce nigdy nie jest odrębną umową. Rekomendacje zostały jednak uzupełnione o problem określenia procedur na wypadek zaistnienia incydentów bezpieczeństwa, w tym potrzebę określenia SLA dla takich przypadków. | |
| **3.** | **MC** | **Zagadnienie 5.1** | Występujący w zagadnieniu 5.1. – model Time&Material nie został wcześniej zdefiniowany, w związku z powyższym taka definicja powinna zostać wprowadzona w części dotyczącej definicji. | **Uwaga uwzględniona.**  Rekomendacje w części „Definicje” zostały uzupełnione o definicję w brzmieniu: „model, w którym wynagrodzenie jest rozliczane na podstawie faktycznego czasu realizacji prac oraz stawki podanej w umowie i ewentualnie innych kosztów, których zasady zwrotu określa umowa”. | |
| **4.** | **MC** | **Rekomendacja 6.1** | Prezentowany w rekomendacji 6.1. – sposób zlikwidowania asymetrii informacyjnej między wykonawcami jest jak najbardziej słuszny, niemniej winno się znaleźć w nim zastrzeżenie, że zawarcie takich informacji może nastąpić, o ile nie będzie to zagrażało bezpieczeństwu systemu oraz świadczonych z jego wykorzystaniem usług. | **Uwaga uwzględniona.**  Rekomendacje zostały uzupełnione o wskazanie, że w przypadku informacji, których ujawnienie zagrażałoby bezpieczeństwu systemu lub usług świadczonych z jego wykorzystaniem, zamawiający powinien rozważyć postawienie wymagań dotyczących zachowania poufnego charakteru informacji (art. 18 ust. 4 PZP). | |
| **5.** | **MC** | **Rekomendacja 8.4** | W rekomendacji 8.4. (lokalizacja przetwarzania danych) –konieczne jest uwzględnienie zarówno odniesienia do kwestii związanych z cyberbezpieczeństwem, jak również z bezpieczeństwem państwa. | **Uwaga uwzględniona.**  Rekomendacje zostały uzupełnione o odesłanie do Standarów Cyberbezpieczeństwa Chmur Obliczeniowych. | |
| **6.** | **MC** | **Zagadnienie 6.1. pkt 2 oraz zagadnienie 6.3 pkt 2** | W zagadnieniu 6.1. w pkt 2 oraz w zagadnieniu 6.3 w pkt 2 – proponuje się doprecyzowanie „określenie wymagań dotyczących bezpieczeństwa” poprzez dodanie wyrazów „systemów informatycznych i informacji oraz ochrony prywatności w całym cyklu życia produktu”. | **Uwaga uwzględniona.**  Rekomendacje zostały doprecyzowane zgodnie z uwagą. | |
| **7.** | **MC** | **Zagadnienie 6.1. pkt 8 oraz zagadnienie 6.3 pkt 5** | W zagadnieniu 6.1. w pkt 8 oraz w zagadnieniu 6.3 w pkt 5 – celowe jest przywołanie nie tylko wskazania osób, ale również ról. | **Uwaga uwzględniona.**  Rekomendacje zostały doprecyzowane zgodnie z uwagą. | |
| **8.** | **MC** | **Ogólna** | Dokument nie podnosi kwestii dotyczących wyłączenia prawa PZP ze względu na bezpieczeństwo państwa. Warunki wykluczenia oferenta z postępowania są jednak szczegółowo opisane w ustawie - Prawo Zamówień Publicznych | **Brak podstaw do uwzględnienia uwagi** z następujących względów:  Tom II Rekomendacji dotyczy opisu przedmiotu zamówienia. Kwestia wyłączenia stosowania ustawy PZP nie mieści się w zakresie tematycznym Tomu II. | |
| **9.** | **MC** | **Ogólna** | Dokument wymaga ponownej analizy pod względem redakcyjnym, np. w tytule rozdziału VII jest INFORMATYCH, a powinno być INFORMATYCZNYCH. | **Uwaga uwzględniona.** | |