

Nazwa dokumentu: Opis założeń projektu informatycznego pn.: „ <i>Piaskownice AI – System regulacyjnych i technologicznych środowisk testowych dla sztucznej inteligencji</i> ”, wnioskodawca: Minister Cyfryzacji; beneficjent: Ministerstwo Cyfryzacji					
Lp.	Organ wnoszący uwagi	Jednostka redakcyjna, do której wnoszone są uwagi	Treść uwagi	Propozycja zmian zapisu	Odniesienie do uwagi
1.	RA IT	Uwaga ogólna	W celu zapewnienia jednoznacznej interpretacji zakresu projektu należy zweryfikować używanie zwrotu „Piaskownica AI” w kontekście konkretnego, jednego produktu projektu nazywanego „Piaskownica AI” od innych piaskownic AI, o których mowa w dokumencie, np. w produktach, kamieniach milowych.	Proszę o analizę i korektę opisu założeń	
2.	RA IT	1.1. Identyfikacja problemu i potrzeb	Dokument w pierwszej części mówi o rozwiązaniach typu <i>work-flow</i> , a dopiero w drugiej o projektowanej Piaskownicy AI, niezbędne jest doprecyzowanie w tym zakresie.	Proszę o analizę i korektę opisu założeń w pkt 1.1	
3.	RA IT	1.2. Opis stanu obecnego	W opisie stanu obecnego należy wskazać poziom gotowości fabryk do udostępniania danych i zasobów do realizacji powierzonych zadań.	Proszę o analizę i korektę opisu założeń	
4.	RA IT	2.1. Cele i korzyści wynikające z przedsięwzięcia	Na podstawie dokumentów przywołanych w „Celach”, a określonych jako regulacyjne dla piaskownic AI, nie wynika jakie cele wymagania są realizowane. W przypadku potrzeby przedstawienia szerszych wyjaśnień proszę o załączenie dodatkowego dokumentu. Możliwe jest również (należy mieć jednak na uwadze, że materiały przekazywane do KdsC mogą być publikowane na stronie KdsC) załączenie studium wykonalności ze wskazaniem konkretnych punktów dokumentu, które wyjaśniają poruszaną kwestię.	Proszę o analizę i wyjaśnienie	
5.	RA IT	2.1. Cele i korzyści wynikające z przedsięwzięcia	Brak wskaźników jakościowych Należy dodać mierniki rezultatów (mierzone do roku po zakończeniu projektu), np. czas obsługi wniosku, kompletność zgłoszeń, dostępność, SLA, czas utworzenia środowiska i satysfakcję użytkowników.	Proszę o analizę i korektę opisu założeń	
6.	RA IT	2.1. Cele i korzyści wynikające z przedsięwzięcia	Sformułowanie, że projekt zapewni zgodność z AI Act i RODO, może sugerować automatyczne potwierdzanie zgodności przez system. Należy doprecyzować, że system wspiera proces oceny zgodności, natomiast odpowiedzialność za ocenę, decyzję i rekomendację pozostaje po stronie uprawnionych ekspertów i organu.	Proszę o analizę i korektę opisu założeń	

7.	RA IT	2.1. Cele i korzyści wynikające z przedsięwzięcia	Nie wyjaśniono relacji między deklarowanym dostępem dla minimum 55 urzędów, 45 podmiotami uczestniczącymi oraz 300 użytkownikami. Należy zdefiniować jednostkę pomiaru każdego wskaźnika: instytucja, podmiot, konto użytkownika, użytkownik aktywny, zgłoszenie lub środowisko. Należy uwzględnić działanie arytmetyczne i metodologię: 55 + 45 podmiotów pomnożone przez 3 osoby daje 300 osób	Proszę o analizę i wyjaśnienie lub korektę opisu założeń	
8.	RA IT	2.4 Produkty końcowe przedsięwzięcia	Do usunięcia produkty dot. e-usług wymienionych w pkt 2.2	Proszę o analizę i korektę opisu założeń	
9.	RA IT	2.4. Produkty końcowe przedsięwzięcia	Dokument nie zawiera informacji o wystandaryzowaniu API dla projektowanych fabryk. Proszę o uzupełnienie nazwy produktu dot. „Interfejsu API”	Proszę o analizę i korektę opisu założeń	
10.	RA IT	2.4. Produkty końcowe przedsięwzięcia	Lista produktów nie zawiera jednoznacznego produktu odpowiadającego za kontrakty i integrację z Fabrykami AI oraz produktu związanego z wdrażanymi adapterami Należy dodać produkt „Dokumentacja integracyjna i kontrakty API Fabryk AI”, obejmujący katalog usług, modele danych, statusy, SLA, błędy i wersjonowanie oraz produkt dot. adapterów	Proszę o analizę i korektę opisu założeń	
11.	RA IT	2.4 Produkty końcowe w	Brak informacji czym jest "Komponent badawczy w postaci raportów z badań i ewaluacji piaskownic AI"	Proszę o analizę i wyjaśnienie	
12.	RA IT	3. Kamienie milowe	Harmonogram integracji Piaskownicy AI z Fabrykami AI nie zawiera terminów gotowości konkretnych dostawców i interfejsów. Należy przedstawić harmonogram gotowości testów integracyjnych, testów wydajnościowych i uruchomienia środowiska produkcyjnego.	Proszę o analizę i korektę opisu założeń	
13.	RA IT	4.2. Wykaz poszczególnych pozycji kosztowych	Należy doprecyzować informacje podane w drugiej kolumnie dla pozycji kosztowej „Oprogramowanie”, uwzględniając wszystkie produkty projektu, których koszt wliczono w tę pozycję kosztową. Należy mieć na uwadze, że wynagrodzenia pracowników merytorycznych (tj. bezpośrednio realizujących zadania związane z wytworzeniem i wdrożeniem/udostępnieniem produktów projektu), w tym zatrudnionych bez względu na formę zaangażowania i wynagrodzenia, co do zasady powinny być wykazane w innych pozycjach kosztowych, niż „Koszty zarządzania i wsparcia (w tym wynagrodzenia Personelu wspomagającego).	Proszę o analizę i korektę opisu założeń	

14.	RA IT	4.3. Koszty ogólne utrzymania wraz ze sposobem finansowania (okres 5 lat)	Występuje niespójność: dokument wskazuje okres utrzymania pięciu lat, ale podaje lata 2028–2033, czyli sześć lat kalendarzowych. Należy zweryfikować 5 letni okres utrzymania	Proszę o analizę i korektę opisu założeń	
15.	RA IT	5.1. Ryzyka wpływające na realizację przedsięwzięcia	Brakuje ryzyka niedostępności Fabryk AI, braku zasobów GPU i opóźnienia gotowości interfejsów. Należy dodać ryzyka dotyczące dostępności, limitów, SLA, zmian regulaminów dostępu i zależności od zewnętrznych operatorów.	Proszę o analizę i korektę opisu założeń	
16.	RA IT	5.1. Ryzyka wpływające na realizację przedsięwzięcia	Nie uwzględniono ryzyk specyficznych dla środowisk AI: prompt injection, data poisoning, model extraction i niekontrolowanego zużycia zasobów. Należy dodać ryzyka bezpieczeństwa modeli, danych i API oraz określić działania ograniczające i testy bezpieczeństwa. Należy wskazać kontrole dla prompt injection, data poisoning, model extraction, nadużycia API i nadmiernego zużycia zasobów.	Proszę o analizę i korektę opisu założeń	
17.	RA IT	5.2. Ryzyka wpływające na utrzymanie efektów	Brakuje ryzyka dezaktualizacji modeli, komponentów AI, bibliotek i procedur bezpieczeństwa. Należy określić proces zarządzania wersjami, aktualizacjami, podatnościami, wycofaniem modeli i ponowną walidacją.	Proszę o analizę i korektę opisu założeń	
18.	RA IT	7.1 Widok kooperacji aplikacji 7.2. Kluczowe komponenty architektury rozwiązania	Brak zarządzania uprawnieniami i brak wyjaśnienia w jaki sposób ma być zapewniona konkretna „objętość” projektowanej piaskownicy AI. Proszę o wyjaśnienie lub ew. uzupełnienie opisu systemu mając na uwadze, że Opis systemu powinien zawierać informacje dot. wszystkich poniższych aspektów: – pełną nazwę systemu (po pełnej nazwie sugerujemy użycie sformułowania „to system wspierający...”, co pozwoli na płynne przejście do kolejnej części opisu); w przypadku gdy opis dotyczy systemu wielokrotnego, należy pełną nazwę systemu poprzedzić sformułowaniem "System wielokrotny", – cel utworzenia systemu, – informację o prowadzonych w systemie rejestrach publicznych, jeśli nie jest to zawarte w celu, – opis głównych grup funkcjonalności (może być lista modułów z krótkimi opisami); – informacja o tym czy system wymienia dane z innymi systemami krajowymi lub zagranicznymi (czy system obsługuje takie procesy)	Proszę o analizę i wyjaśnienie lub ew. korektę opisu założeń	

			Opis: – powinien być sformułowany w czasie teraźniejszym, niezależnie od tego czy jest planowany, istniejący czy modyfikowany, – nie powinien zawierać odniesień do jakichkolwiek projektów czy przyszłych lub zrealizowanych działań, nie powinien zawierać odniesień do wyjątkowości systemu.		
19.	RA IT	7.1 Widok kooperacji aplikacji	Proszę o wyjaśnienie czy Piaskownica AI to tylko system do zarządzania klasyfikacji, obsługi przedsiębiorców i jednostek administracji, a w tym integrację z istniejącymi środowiskami AI, a nie ogólnie wskazaną fabryką. Ważnym jest wyszczególnienie wprost za co odpowiada projekt a za co wskazane komponenty z którymi następuje integracja, oraz dokładne wyszczególnienie właścicieli tych środowisk AI. Wspomniani właściciele muszą w jasny sposób wyrazić zgodę na zaproponowaną w projekcie koncepcję, tym samym potwierdzając realizację zaproponowanej koncepcji rozwiązania. Dlatego proszę o potwierdzenie, że wszystkie planowane i modyfikowane w projekcie procesy wymiany danych z systemami zostały uzgodnione z gestorami systemów, o ile jest to wymagane.	Proszę o analizę i wyjaśnienie, ew. korektę opisu założeń	
20.	RA IT	7.1. Widok kooperacji aplikacji – Węzeł Krajowy	Uwierzytelnienie użytkownika nie rozwiązuje problemu autoryzacji organizacyjnej i reprezentacji podmiotu. Należy opisać role, organizacje, pełnomocnictwa, użytkowników wieloorganizacyjnych, konta techniczne i administrację uprawnieniami.	Proszę o analizę i wyjaśnienie	
21.	RA IT	7.2. Kluczowe komponenty architektury rozwiązania	Proszę o wyjaśnienie dot. określenia RTO, RPO, procedury postępowania w przypadku awarii fabryki dla zintegrowanych podmiotów, zakresu odpowiedzialności i zachowania Piaskownicy AI podczas awarii Fabryki.	Proszę o analizę i wyjaśnienie	
22.	RA IT	7.2. Kluczowe komponenty architektury rozwiązania	Proszę o wyjaśnienie dot. sposobu informowania, które wersje modeli są tymi aktualnymi, jak system będzie informował użytkownika o wersji, statusie, właścicielu, licencji i aktualności modelu.	Proszę o analizę i wyjaśnienie	
23.	RA IT	7.2. Kluczowe komponenty architektury rozwiązania	W ramach projektowanego rozwiązania, brakuje informacji dot. automatyzacji środowiska testowego.	Proszę o analizę i korektę opisu założeń	

			Proszę o wyjaśnienie procesu, mechanizmu, zakresu automatyzacji i odpowiedzialności uczestników procesu. Należy opisać skrócie: nadawanie dostępu, konfigurację środowiska, limity i usuwanie zasobów.		
24.	RA IT	7.2. Kluczowe komponenty architektury rozwiązania	Wskazane komponenty nie obejmują repozytorium dokumentów, zarządzania testami, katalogu modeli, audytu i monitoringu. Należy uzupełnić model komponentów o brakujące funkcje oraz wskazać zależności i odpowiedzialności.	Proszę o analizę i korektę opisu założeń	
25.	RA IT	7.3. Przyjęte założenia technologiczne	OZPI w sposób szczątkowy opisuje infrastrukturę rozwiązania	Proszę o analizę i korektę opisu założeń	