

Nazwa dokumentu: Piaskownice AI - System regulacyjnych i technologicznych środowisk testowych dla sztucznej inteligencji

Lp.	Organ wnoszący uwagi	Jednostka redakcyjna, do której wnoszone są uwagi	Treść uwagi	Propozycja zmian zapisu	Odniesienie do uwagi
1.	MSWiA IOD	Pkt 2.4 Produkty końcowe przedsięwzięcia	W przypadku kreowania systemu, w którym będą umożliwiającego bezpieczne testowanie systemów sztucznej inteligencji, w tym wysokiego ryzyka, zgodnie z art. 27 AI Act powinno się przygotować ocenę skutków dla praw podstawowych – FRIA, w powiązaniu z DPIA o której mowa w art. 35 RODO.	Proponuje się rozważyć dodanie do dokumentów wymienianych jako produkty końcowe – Ocenę skutków dla praw podstawowych.	Wyjaśnienie. Obowiązek z art. 27 rozporządzenia 2024/1689 dotyczy podmiotów stosujących systemy AI wysokiego ryzyka w rozumieniu art. 6 ust. 2 i załącznika III. Przedmiotem przedsięwzięcia jest system teleinformatyczny do obsługi wniosków i organizacji procesu, który nie jest systemem AI wysokiego ryzyka, a charakter systemów testowanych w piaskownicy nie przenosi się na system służący jej obsłudze.
2.	MSWiA	Pkt 2.4 „Produkty końcowe przedsięwzięcia” oraz pkt 3 „Kamienie milowe” – privacy by design/privacy by default	Rekomendacje dotyczące wdrożenia zasad privacy by design i privacy by default mają zostać opracowane dopiero w grudniu 2028 r., podczas gdy system ma zostać uruchomiony w grudniu 2027 r. Opracowanie zasad dotyczących ochrony danych po zaprojektowaniu i wdrożeniu rozwiązania ogranicza możliwość rzeczywistego uwzględnienia ich w architekturze systemu.	Proponujemy zmianę harmonogramu oraz opis produktu: „Wymagania wynikające z zasad privacy by design i privacy by default zostaną określone przed zatwierdzeniem docelowej architektury rozwiązania i uwzględnione w wymaganiach projektowych. Przed uruchomieniem produkcyjnym zostanie przeprowadzona weryfikacja ich implementacji. Produkt końcowy w 2028 r. będzie stanowił raport podsumowujący doświadczenia i rekomendacje wynikające z eksploatacji rozwiązania.”	Uwaga uwzględniona. Rekomendacje dotyczące wdrożenia zasad privacy by design i privacy by default zostaną opracowane dopiero w grudniu 2027 r.
3.	MSWiA	Pkt 2.4 oraz pkt 3 – testy bezpieczeństwa i uruchomienie produkcyjne	Uruchomienie Piaskownicy AI, uzyskanie pozytywnego wyniku testów bezpieczeństwa, testów wydajności, badań UX oraz audytu WCAG zostało zaplanowane na ten sam termin – 31 grudnia 2027 r. Nie przewidziano czasu na usunięcie ewentualnych niezgodności wykrytych	Proponujemy zmianę kolejność kamieni milowych: „Uzyskanie pozytywnego wyniku testów bezpieczeństwa i testów wydajnościowych stanowi warunek uruchomienia produkcyjnego Piaskownicy AI. Harmonogram realizacji zapewni czas na usunięcie podatności i niezgodności	Uwaga uwzględniona. Kamienie milowe dotyczące testów bezpieczeństwa, wydajności, badań UX i audytu dostępności zostały przesunięte na 30 listopada 2027 r., a pozytywny wynik testów stanowi warunek uruchomienia produkcyjnego.

			podczas testów oraz wykonanie testów ponownych.	stwierdzonych podczas testów oraz na wykonanie testów ponownych przed dopuszczeniem systemu do eksploatacji.”	
4.	MSWiA	Pkt 2.4 i pkt 3 – API oraz Fabryki AI	System ma zostać uruchomiony w grudniu 2027 r., API w marcu 2028 r., a pełna integracja z Fabrykami AI dopiero w grudniu 2028 r.	Proponujemy uzupełnienie harmonogramu o etapy funkcjonalności: „W dniu uruchomienia systemu w grudniu 2027 r. dostępny będzie co najmniej zakres funkcjonalny obejmujący [...]. Do czasu udostępnienia docelowego API wymiana danych z dostawcami infrastruktury będzie realizowana poprzez [...]. Docelowa integracja automatyczna zostanie uruchomiona nie później niż w terminie [...]”.	Uwaga uwzględniona.
5.	MSWiA	Pkt 7.5 „Bezpieczeństwo”	Wskazanie, że system „nie podlega rygorom KRI”, bez podania uzasadnienia lub podstawy takiego stanowiska, jest niewystarczające w przypadku systemu teleinformatycznego wykorzystywanego do realizacji zadań publicznych. Jednocześnie pole dotyczące poziomu zapewnienia bezpieczeństwa pozostawiono jako „N/D”	Proponujemy usunąć zapis „system nie podlega rygorom KRI – N/D” i zastąpić go zapisem: „System zostanie zaprojektowany, wdrożony i eksploatowany zgodnie z wymaganiami Krajowych Ram Interoperacyjności mającymi zastosowanie do systemu. Szczegółowy zakres wymagań bezpieczeństwa zostanie określony na podstawie analizy ryzyka i klasyfikacji przetwarzanych informacji. Ewentualne wyłączenie zastosowania określonego wymagania wymaga wskazania podstawy prawnej i uzasadnienia.”	Uwaga uwzględniona. Zapis w pkt 7.5 zostanie zastąpiony brzmieniem zaproponowanym przez MSWiA.
6.	MSWiA	Pkt 7.5 „Bezpieczeństwo” – rejestrowanie i rozliczalność operacji	Dokument wskazuje na rejestrowanie zdarzeń związanych z obsługą piaskownic, jednak nie określa minimalnego zakresu logowania, okresu retencji ani zasad udostępniania logów uczestnikowi. W przypadku przetwarzania danych administracji publicznej możliwość odtworzenia operacji wykonanych na danych ma istotne znaczenie dla bezpieczeństwa i rozliczalności.	Proponujemy uzupełnienie dokumentu o wymagania dotyczące rejestrowania operacji wykonywanych na danych i zasobach uczestnika, obejmujące co najmniej identyfikację użytkownika, czas operacji, rodzaj wykonanej czynności, dostęp do danych, zmiany konfiguracji i zdarzenia administracyjne. Należy określić okres przechowywania logów, zasady ochrony ich integralności oraz możliwość ich udostępnienia uczestnikowi w przypadku incydentu lub kontroli.	Wyjaśnienie. Zakres logowania, retencja i ochrona integralności logów oraz zasady ich udostępniania zostaną określone na etapie realizacji projektu.

7.	MSWiA	Pkt 7.5 – obsługa incydentów bezpieczeństwa	W dokumencie nie określono zasad informowania uczestnika o incydencie dotyczącym jego danych lub środowiska ani podziału odpowiedzialności pomiędzy gestora Piaskownicy AI i dostawców Fabryk AI w takim przypadku. Jest to istotne, ponieważ system zakłada komunikację i wymianę danych pomiędzy odrębnymi komponentami i podmiotami.	Proponujemy dodać zapis: „Dla Piaskownicy AI zostanie określona procedura obsługi incydentów bezpieczeństwa obejmująca zasady wykrywania, rejestrowania, eskalacji i obsługi incydentów oraz informowania uczestnika o incydencie dotyczącym jego danych lub środowiska. Procedura określi również odpowiedzialność gestora systemu i dostawców infrastruktury technologicznej oraz kanały i terminy komunikacji.”	Wyjaśnienie. Procedura obsługi incydentów, w tym informowanie uczestnika i podział odpowiedzialności między gestora systemu a dostawców infrastruktury, zostanie określona na etapie realizacji projektu.
8.	MSWiA	Pkt 7.1–7.2 „Architektura” – podział odpowiedzialności	W dokumencie Komisja Rozwoju i Bezpieczeństwa Sztucznej Inteligencji (KRiBSI) została wskazana jako operator piaskownicy AI, Ministerstwo Cyfryzacji jako gestor systemu teleinformatycznego, natomiast środowiska technologiczne zapewniają dostawcy Fabryk AI. Architektura przewiduje wymianę zleceń i danych pomiędzy tymi systemami. Nie wskazano jednak szczegółowego podziału odpowiedzialności eksploatacyjnej i bezpieczeństwa.	Proponujemy dodanie zapisu: „Dla systemu Piaskownica AI zostanie określony model ról i odpowiedzialności obejmujący Ministerstwo Cyfryzacji, KRiBSI oraz podmioty zapewniające infrastrukturę technologiczną. Model określi odpowiedzialność za utrzymanie, zarządzanie tożsamością i dostępem (IAM), bezpieczeństwo, monitorowanie, obsługę incydentów, aktualizacje, podatności, kopie zapasowe, odtwarzanie, ciągłość działania, logowanie oraz ochronę danych i komunikacji pomiędzy komponentami.”	Wyjaśnienie. Model ról i odpowiedzialności obejmujący MC, KRiBSI oraz dostawców infrastruktury zostanie określony na etapie realizacji projektu. Dostawcy infrastruktury posiadają systemy zarządzania bezpieczeństwem informacji potwierdzone certyfikacją ISO 27001.
9.	MSWiA	Pkt 7 – izolacja danych i środowisk uczestników	Dokument przewiduje współdzielone środowiska testowe, zasoby obliczeniowe oraz dostęp do modeli AI dla wielu podmiotów. Nie opisano jednak szczegółowo zasad separacji danych, modeli, kodu i zasobów poszczególnych uczestników.	Proponujemy dodanie zapisu: „Środowiska poszczególnych uczestników Piaskownicy AI będą odseparowane w sposób uniemożliwiający nieuprawniony dostęp do danych, modeli, kodu, konfiguracji, logów i zasobów obliczeniowych innych uczestników. Mechanizmy izolacji będą podlegały weryfikacji i testom bezpieczeństwa przed udostępnieniem środowiska do eksploatacji.”	Wyjaśnienie. Środowiska poszczególnych uczestników będą od siebie odseparowane, a szczegółowe mechanizmy separacji i ich weryfikacja zostaną określone na etapie realizacji projektu.
10.	MSWiA	Pkt 7.1 – uwierzytelnianie i powiązanie użytkownika z podmiotem	Dokument zakłada wykorzystanie Węzła Krajowego do potwierdzania tożsamości użytkownika oraz REGON do walidacji danych podmiotu. Nie opisano natomiast sposobu weryfikacji uprawnienia konkretnej	Proponujemy dodanie zapisu: „System będzie zapewniał mechanizm weryfikacji uprawnienia użytkownika do działania w imieniu wskazanego podmiotu. Mechanizm obejmie obsługę reprezentacji	Wyjaśnienie. System zapewni mechanizmy umożliwiające weryfikację umocowania przedstawiciela wnioskodawcy, w szczególności na podstawie

			osoby do działania w imieniu przedsiębiorcy, JST lub innej jednostki.	ustawowej, pełnomocnictw oraz upoważnień, a także możliwość nadawania i odbierania ról użytkownikom w ramach podmiotu.”	pełnomocnictw. Szczegóły zostaną określone na etapie realizacji projektu.
11.	MSWiA	Pkt 7.3 „Sieć i bezpieczeństwo”	Obecny zapis ogranicza się do statycznych adresów publicznych, firewalla i VPN, co nie opisuje pełnego modelu bezpieczeństwa.	Proponujemy rozszerzenie zapis w pkt 7.3: „Bezpieczeństwo rozwiązania obejmie wielowarstwową ochronę dostępu i komunikacji, w tym uwierzytelnianie wieloskładnikowe tam, gdzie jest wymagane wynikiem analizy ryzyka, zarządzanie uprawnieniami, segmentację sieciową, szyfrowanie transmisji i danych przechowywanych, zarządzanie sekretami, rejestrowanie i monitorowanie zdarzeń, zarządzanie podatnościami oraz mechanizmy zapewnienia ciągłości działania i odtworzenia po awarii.”	Wyjaśnienie. Dobór zabezpieczeń będzie wynikał z analizy ryzyka oraz obowiązujących wymagań w zakresie cyberbezpieczeństwa i zostanie określony na etapie realizacji projektu.
12.	MSWiA	Pkt 7.4 oraz pkt 7.5 – lokalizacja przetwarzania danych	Dokument przewiduje wykorzystanie infrastruktury Fabryk AI oraz wymianę danych pomiędzy Piaskownicą AI a systemami dostawców tej infrastruktury. Nie wskazano jednak jednoznacznie lokalizacji przetwarzania i przechowywania danych uczestników ani zasad ewentualnego przekazywania danych pomiędzy poszczególnymi środowiskami. Z punktu widzenia jednostek administracji publicznej informacja ta może mieć zasadnicze znaczenie przy kwalifikowaniu danych do wykorzystania w Piaskownicy AI.	Proponujemy uzupełnienie dokumentu o wskazanie dopuszczalnych lokalizacji przetwarzania i przechowywania danych, w tym określenie, czy przetwarzanie będzie odbywało się wyłącznie na terytorium Polski, EOG czy również w innych lokalizacjach. Należy wskazać zasady przemieszczania danych pomiędzy komponentami Piaskownicy AI i infrastrukturą Fabryk AI oraz sposób zapewnienia zgodności tych operacji z wymaganiami dotyczącymi ochrony informacji.	Wyjaśnienie. System będzie utrzymywany na Rządowej Chmurze Obliczeniowej, a przetwarzanie i przechowywanie danych będzie odbywało się na terytorium RP lub EOG. Środowiska technologiczne partnerów zlokalizowane są na terytorium RP. Zasady przekazywania danych między komponentami zostaną określone na etapie realizacji projektu.
13.	MSWiA	Pkt 7.3–7.5 – dostęp uprzywilejowany do środowisk i danych uczestników	Dokument opisuje zarządzanie dostępem użytkowników do środowisk testowych, lecz nie określa zasad dostępu administracyjnego personelu operatora lub dostawców infrastruktury do środowisk i danych uczestników.	Proponujemy uzupełnienie dokumentu o zasady dostępu uprzywilejowanego do środowisk uczestników. Dostęp administracyjny powinien być ograniczony do niezbędnego zakresu, nadawany na czas określony, podlegać silnemu uwierzytelnieniu oraz pełnemu rejestrowaniu i rozliczalności. Należy również określić zasady dostępu personelu	Wyjaśnienie. Dostęp administracyjny personelu dostawców infrastruktury odbywa się zgodnie z ich politykami zarządzania dostępem, w zakresie adekwatnym do powierzonych zadań. Szczegółowe zasady dostępu uprzywilejowanego zostaną określone na etapie realizacji projektu.

				podmiotów zewnętrznych do danych uczestników.	
14.	MSWiA	Pkt 7.4 „Opis zasobów danych przetwarzanych w planowanym rozwiązaniu” oraz pkt 7.5 „Bezpieczeństwo”	Dokument wskazuje możliwość bezpiecznego przetwarzania w środowiskach eksperymentalnych danych, w tym danych wrażliwych, jednak nie określa jednoznacznie, czy w Piaskownicy AI dopuszczalne będzie przetwarzanie informacji niejawnych, informacji objętych tajemnicami prawnie chronionymi lub innych kategorii informacji wymagających szczególnej ochrony. W dokumencie nie wskazano również katalogu danych i informacji, których przetwarzanie w środowisku Piaskownicy AI jest niedopuszczalne. Brak takiego rozstrzygnięcia może prowadzić do niejednolitej kwalifikacji danych przez poszczególnych uczestników oraz do ryzyka przekazania do środowiska informacji, dla których nie zapewniono odpowiednich warunków technicznych, organizacyjnych lub prawnych.	Proponujemy uzupełnienie dokumentu o jednoznaczny katalog kategorii informacji dopuszczonych oraz niedopuszczonych do przetwarzania w Piaskownicy AI. W szczególności należy określić, czy dopuszczalne jest przetwarzanie informacji niejawnych, informacji objętych tajemnicami prawnie chronionymi oraz innych informacji wymagających podwyższonego poziomu ochrony. W przypadku wyłączenia określonych kategorii informacji należy wskazać to wprost w zasadach korzystania z Piaskownicy AI. Dla informacji dopuszczonych do przetwarzania należy określić wymagania techniczne, organizacyjne i prawne, jakie muszą zostać spełnione przed ich wprowadzeniem do środowiska testowego.	Wyjaśnienie. Katalog informacji dopuszczonych i niedopuszczonych do przetwarzania wraz z warunkami ich wprowadzenia do środowiska testowego zostanie określony w zasadach korzystania z piaskownicy na etapie realizacji projektu.
15.	MSWiA	Pkt 7.4 – zakończenie testów i usuwanie danych	Dokument nie określa zasad postępowania z danymi, modelami, kodem, kopiami roboczymi oraz innymi zasobami uczestnika po zakończeniu testów lub udziału w Piaskownicy AI. Brak określenia zasad retencji i usuwania danych może prowadzić do pozostawienia danych uczestnika w infrastrukturze Piaskownicy AI lub Fabryk AI po ustaniu celu ich przetwarzania.	Proponujemy uzupełnienie dokumentu o zapis: „Po zakończeniu testów lub udziału uczestnika w Piaskownicy AI dane, modele, kod, kopie robocze oraz inne zasoby uczestnika zostaną zwrócone, usunięte albo zarchiwizowane zgodnie z określonymi zasadami retencji. Zasady te powinny obejmować również kopie zapasowe, dane tymczasowe oraz zasoby znajdujące się w infrastrukturze dostawców Fabryk AI. Wykonanie procesu usunięcia danych powinno być możliwe do potwierdzenia uczestnikowi.”	Wyjaśnienie. Zasady postępowania z zasobami uczestnika po zakończeniu testów, w tym retencja i usuwanie danych, zostaną określone w zasadach korzystania z piaskownicy na etapie realizacji projektu, z uwzględnieniem obowiązków prawnych dotyczących przechowywania określonych kategorii danych.