

OPIS ZAŁOŻEŃ PROJEKTU INFORMATYCZNEGO

Tytuł projektu	Piaskownice AI – System regulacyjnych i technologicznych środowisk testowych dla sztucznej inteligencji		
Wnioskodawca	Minister Cyfryzacji		
Beneficjent	Ministerstwo Cyfryzacji		
Partnerzy	Ministerstwo Rozwoju i Technologii (MRiT), Urząd Ochrony Danych Osobowych (UODO), Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (NASK-PIB), Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie – Akademickie Centrum Komputerowe Cyfronet (Cyfronet), Instytut Chemii Bioorganicznej PAN - Poznańskie Centrum Superkomputerowo-Sieciowe (PCSS)		
Źródło finansowania	1) Budżet państwa część 27 – Informatyzacja 2) Dofinansowanie UE - Program Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC) II oś Działanie 2.1. Wysoka jakość i dostępność e-usług		
Całkowity koszt projektu	35 000 000,00 zł		
Planowany okres realizacji projektu	09-2026 do 12-2028		
Osoba kontaktowa	Aleksandra Tomaszewska	Aleksandra.Tomaszewska@cyfra.gov.pl	880120947

1. POWODY PODJĘCIA PROJEKTU

1.1. Identyfikacja problemu i potrzeb

Projekt odpowiada na problem braku kompleksowego systemu umożliwiającego bezpieczne testowanie systemów sztucznej inteligencji w Polsce dla przedsiębiorców i dla jednostek administracji publicznych. Obecnie brak jest jednolitego środowiska pozwalającego na praktyczne testowanie systemów AI w warunkach zbliżonych do rzeczywistych, przy jednoczesnym wsparciu procesu osiągania zgodności z przepisami prawa, w tym AI Act. Projekt odpowiada również na problem ograniczonej gotowości administracji publicznej do wykorzystywania technologii AI wynikający z braku odpowiedniej infrastruktury, środowisk testowych oraz wsparcia eksperckiego. W efekcie wdrażanie rozwiązań AI wiąże się z wysokim ryzykiem regulacyjnym i organizacyjnym, co ogranicza rozwój innowacji oraz praktyczne wykorzystanie AI w sektorze publicznym. Brak jest również narzędzi (e-usług) wspierających funkcjonowanie systemu piaskownic, umożliwiających m.in. elektroniczną obsługę procesu zgłoszeń, komunikację uczestników z operatorem piaskownicy oraz monitorowanie procesu testowania systemów AI. Mając na względzie powyższe oraz biorąc pod uwagę konieczność wypełnienia AI Act zidentyfikowano potrzebę stworzenia bezpiecznego środowiska wspierającego proces osiągania zgodności z prawem, rozwój i testowanie systemów AI, który zwiększy poziom przygotowania administracji publicznej do wykorzystania technologii AI oraz przyczyni się do rozwoju nowoczesnych usług cyfrowych w Polsce oraz stworzenie narzędzi wspierających funkcjonowanie tego środowiska. Planowany system Piaskownica AI stanowi cyfrową warstwę obsługi tych procesów. Mechanizmy workflow są jego funkcjonalnością i wspierają obsługę zgłoszeń, ich weryfikację i ocenę, komunikację z uczestnikami, prowadzenie spraw, monitoring oraz raportowanie. System integruje się również z zewnętrznymi

środowiskami Fabryk AI wykorzystywanymi w ścieżce technologicznej.

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
Przedsiębiorcy	1. Brak wystarczającego dostępu przedsiębiorców do wiedzy eksperckiej w zakresie interpretacji wymogów i obowiązków wynikających z AI Act. 2. Brak cyfrowej obsługi procedury piaskownicy regulacyjnej dla MŚP i startupów rozwijających systemy AI wysokiego ryzyka, ze skróceniem czasu obsługi wniosku dzięki automatyzacji procesów oceny i monitoringu. 3. Brak jednolitego, transparentnego interfejsu dostępu do procedury piaskownicy zgodnej z art. 57 AI Act, z elektronicznym śledzeniem statusu sprawy oraz komunikacją z operatorem piaskownicy. 4. Brak wystarczającej pewności prawnej dla MŚP i startupów rozwijających systemy AI wysokiego ryzyka z uwagi na brak praktycznego wsparcia w osiągnięciu zgodności z przepisami. 5. Brak możliwości praktycznego testowania zgodności systemów AI z wymaganiami AI Act w warunkach nadzorowanych przez regulatora. 6. Brak ustandaryzowanego procesu iteracyjnego testowania i wprowadzania zmian w systemach AI w oparciu o rekomendacje regulatora. 7. Ograniczona możliwość interakcji z administracją publiczną w trybie cyfrowym w zakresie procedury piaskownicy AI.	ok. 19 tys.
Administracja publiczna (Jednostki samorządu terytorialnego i jednostki sektora finansów publicznych)	1. Niewystarczający dostęp do technologii AI z uwagi na utrudniony dostęp do infrastruktury testowej, 2. Wysokie koszty zakupu własnej infrastruktury. 3. Brak samodzielnych zdolności do budowania własnych modeli językowych oraz gotowych komponentów AI (chatboty, asystenci, OCR). 4. Brak dostępu do współdzielonej, bezpiecznej infrastruktury testowej AI umożliwiającej eksperymentowanie z rozwiązaniami AI bez ryzyka dla systemów produkcyjnych. 5. Rozproszenie działań związanych z wdrażaniem AI oraz brak wspólnych standardów i środowisk testowych. 6. Brak możliwości testowania gotowych komponentów AI (np. modeli językowych,	ok. 4,6 tys.

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
	chatbotów, OCR) przed ich wdrożeniem w procesach administracyjnych. 7. Ograniczone zasoby kadrowe i kompetencyjne w zakresie projektowania i wdrażania systemów AI. 8. Brak narzędzi umożliwiających bezpieczne przetwarzanie danych (w tym danych wrażliwych) w środowiskach eksperymentalnych zgodnie z RODO.	
Operator piaskownicy AI, tj. Komisja Rozwoju i Bezpieczeństwa Sztucznej Inteligencji	1. Brak narzędzi informatycznych umożliwiających kompleksową obsługę piaskownicy AI, w tym przyjmowanie zgłoszeń, ocenę uczestników, monitoring testów oraz raportowanie do Komisji Europejskiej zgodnie z art. 57 AI Act. 2. Brak integracji procesów i danych oraz ograniczona automatyzacja raportowania i analizy danych. 3. Trudności w zapewnieniu jednolitego standardu obsługi piaskownicy na poziomie krajowym.	1

1.2. Opis stanu obecnego

Przepisy ustawy z dnia 3 lipca 2026 r. o systemach sztucznej inteligencji (Dz. U. poz. 1003) dotyczące piaskownic regulacyjnych weszły w życie 11.08.2026 r. Ustawa powierza prowadzenie piaskownic regulacyjnych Komisji Rozwoju i Bezpieczeństwa Sztucznej Inteligencji. Obecnie nie istnieje system teleinformatyczny umożliwiający złożenie oraz obsługę wniosku o dostęp do piaskownicy regulacyjnej - nie istnieje warstwa back-office obsługująca pełen cykl życia uczestnictwa w piaskownicy. Ocena formalna i merytoryczna wniosków, kwalifikacja uczestników oraz cykliczne raportowanie do Komisji Europejskiej (art. 57 ust. 16 AI Act) prowadzone są poza systemem, z wykorzystaniem poczty elektronicznej i arkuszy kalkulacyjnych, co nie skaluje się do liczby uczestników przewidzianych w docelowym modelu piaskownicy. Przedsiębiorcy, w szczególności MŚP i startupy rozwijające systemy AI wysokiego ryzyka, nie mają dziś dostępu do ujednoliconego, cyfrowego interfejsu zgłoszenia do procedury piaskownicy regulacyjnej zgodnej z art. 57 AI Act, ani do elektronicznego śledzenia statusu sprawy i komunikacji z operatorem. Brak jest również narzędzi wspierających iteracyjne testowanie systemów AI w warunkach nadzorowanych przez regulatora. Administracja publiczna i jednostki samorządu terytorialnego nie dysponują dostępem do współdzielonej, bezpiecznej infrastruktury obliczeniowej umożliwiającej testowanie i adaptację rozwiązań AI bez ryzyka dla systemów produkcyjnych. Polskie modele językowe (PLLuM) oraz gotowe komponenty AI (chatboty, asystenci, OCR) wytwarzane w innych projektach krajowych nie są dostępne w trybie self-service dla urzędów. Wdrażanie rozwiązań AI w administracji wiąże się z wysokimi kosztami zakupu własnej infrastruktury oraz z ryzykiem regulacyjnym i organizacyjnym, co ogranicza praktyczne wykorzystanie technologii w sektorze publicznym. Obecnie Fabryki AI są w realizacji, a harmonogram ich uruchomienia jest dostosowany do harmonogramu realizacji projektu.

2. EFEKTY PROJEKTU

2.1. Cele i korzyści wynikające z projektu

Cel - 1	Umożliwienie przedsiębiorcom, administracji publicznej oraz rządowej możliwości testowania systemów AI w kontrolowanych warunkach poprzez wytworzenie i wdrożenie systemu informatycznego obsługującego polską piaskownicę AI, w szczególności dwóch e-usług zgłoszeniowych w ramach portalu stanowiącego centralny punkt dostępu do piaskownicy AI. Odstępstwa od stosowania przepisów przyznaje Komisja Rozwoju i Bezpieczeństwa Sztucznej Inteligencji w drodze decyzji, w granicach katalogu określonego w art. 91 ust. 3 ustawy z dnia 3 lipca 2026 r. o systemach sztucznej inteligencji, wyłącznie w ścieżce regulacyjnej.
Cel strategiczny	1. Strategia na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030); Cel szczegółowy III: „Skuteczne państwo i instytucje służące wzrostowi oraz włączeniu społecznemu i gospodarczemu”, Obszar: E-państwo (Cyfryzacja). Cel wynikający ze strategii, polegający na udostępnieniu cyfrowego punktu dostępu do piaskownicy AI oraz e-usług zgłoszeniowych o wysokim stopniu dojrzałości, realizuje założenia rozwoju e-usług publicznych i sprawnego, cyfrowego państwa. 2. Polityka dla rozwoju sztucznej inteligencji w Polsce od roku 2020 (uchwała nr 196 Rady Ministrów z dnia 28 grudnia 2020 r.). Cel wynikający ze strategii - dokument wprost wskazuje piaskownice regulacyjne i testowe jako narzędzie realizacji celów rozwoju AI w administracji i gospodarce. 3. Europejska strategia w zakresie sztucznej inteligencji (European AI Strategy). Cel wynikający ze strategii - projekt wspiera cel budowy zaufanego, bezpiecznego ekosystemu AI oraz zwiększania konkurencyjności europejskiego rynku rozwiązań opartych na AI. 4. Plan działania na rzecz kontynentu AI (AI Continent Action Plan). Cel wynikający ze strategii - projekt wpisuje się w kierunek rozbudowy europejskiej infrastruktury AI (m.in. fabryk AI), na której oparta jest udostępniana piaskownica technologiczna.
Korzyść:	Wdrożenie systemu Piaskownica AI niesie za sobą konkretne korzyści zwłaszcza dla przedsiębiorców (MŚP, startupów) i administracji publicznej oraz rządowej. 1. Zwiększenie dostępności do wiedzy eksperckiej – wsparcie przedsiębiorców wiedzą ekspercką z zakresu zgodności z prawem polskim i regulacjami unijnymi (AI Act) – tym samym obniżenie barier ze względu na obowiązki compliance z prawem unijnym i ustawą je wdrażającą. 2. Szybka obsługa wniosku dzięki automatyzacji. 3. Dostęp do środowiska testowego dla min. 55 urzędów, bez konieczności zakupu własnej infrastruktury. 4. Dostęp do API polskich modeli językowych (w tym PLLuM) i gotowych komponentów AI (chatbotów, asystentów AI, wsparcia w OCR). 5. System Piaskownica AI tworzy jednolity punkt dostępu do wiedzy wpływającej prosto od regulatora na temat standardów prawnych dotyczących realizacji przedsięwzięć w zakresie AI. Rozwiązanie niesie za sobą także podniesienie transparentności procedur, jak i spełnienie

	obowiązków dotyczących cyfryzacji raportowania do KE (por. Art. 57 ust. 16 AI Act), co w dłuższej perspektywie podnosi konkurencyjność gospodarek polskiej i ogólnie ujmując, unijnej. System wspiera proces osiągania i oceny zgodności z wymaganiami AI Act i RODO. System nie dokonuje automatycznej oceny zgodności. Ocena, rekomendacje i rozstrzygnięcia pozostają po stronie właściwych ekspertów i organów.
KPI:	Wskaźniki produktu: 1. Instytucje publiczne otrzymujące wsparcie na opracowywanie usług, produktów i procesów cyfrowych [szt.] 2. Liczba podmiotów wspartych w zakresie rozwoju usług, produktów i procesów cyfrowych [szt.] 3. Liczba usług publicznych udostępnionych on-line o stopniu dojrzałości co najmniej 4 – transakcja [szt.] 4. Wartość usług, produktów i procesów cyfrowych opracowanych dla przedsiębiorstw [PLN] 5. Liczba udostępnionych usług wewnątrzadministracyjnych (A2A) [szt.] 6. Liczba uruchomionych systemów teleinformatycznych w podmiotach wykonujących zadania publiczne [szt.] Wskaźniki rezultatu: 7. Użytkownicy nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych [użytkownicy/rok] 8. Liczba podmiotów, które wzięły udział w procesie piaskownic regulacyjnych [szt.] 9. Liczba etapów procesu piaskownicy regulacyjnej obsługiwanych w systemie teleinformatycznym [szt.] 10. Poziom satysfakcji użytkowników systemu Piaskownica AI [%]
Wartość aktualna i docelowa KPI:	1. Wartość aktualna: 0 2. Wartość aktualna: 0 3. Wartość aktualna: 0 4. Wartość aktualna: 0 5. Wartość aktualna: 0 6. Wartość aktualna: 0 7. Wartość aktualna: 0 8. Wartość aktualna: 0 9. Wartość aktualna: 0 10. Wartość aktualna: 0 1. Wartość docelowa: 3 2. Wartość docelowa: 3 3. Wartość docelowa: 1 4. Wartość docelowa: 20 826 764,11 5. Wartość docelowa: 2 6. Wartość docelowa: 1 7. Wartość docelowa: 300 8. Wartość docelowa: 45 9. Wartość docelowa: 4 10. Wartość docelowa: 70
Metoda pomiaru KPI	1. Metoda\spół sposób pomiaru: weryfikacja podpisanego porozumienia/umowy o dofinansowanie Źródło danych\pomiaru: podpisane porozumienie/umowa o dofinansowanie Częstotliwość pomiaru: jednorazowo po podpisaniu porozumienia/umowy o dofinansowanie.

2.
Metoda\spółób pomiaru: weryfikacja podpisanego porozumienia/umowy o dofinansowanie
Źródło danych\pomiaru: podpisane porozumienie/umowa o dofinansowanie
Częstotliwość pomiaru: jednorazowo po podpisaniu porozumienia/umowy o dofinansowanie
3.
Metoda\spółób pomiaru: testy wdrożonych usług
Źródło danych\pomiaru: raport z testów
Częstotliwość pomiaru: jednorazowo najpóźniej w ostatnim dniu realizacji projektu
4.
Metoda\spółób pomiaru: oszacowanie nakładów ex-ante
Źródło danych\pomiaru: umowa in-house z Wykonawcą, faktury
Częstotliwość pomiaru: jednorazowo w dniu podpisania umowy in-house z Wykonawcą
5.
Metoda\spółób pomiaru: testy wdrożonych usług
Źródło danych\pomiaru: raport z testów
Częstotliwość pomiaru: jednorazowo najpóźniej w ostatnim dniu realizacji projektu
6.
Metoda\spółób pomiaru: raport z wdrożenia systemu
Źródło danych\pomiaru: protokół odbioru potwierdzający wdrożenie
Częstotliwość pomiaru: jednorazowo najpóźniej w ostatnim dniu realizacji projektu
7.
Metoda\spółób pomiaru: odczyt z raportu systemowego; produkty projektu zostaną udostępnione w ciągu pierwszych 12 miesięcy licząc od miesiąca następującego po miesiącu zakończenia projektu co najmniej 55 urzędom i co najmniej 45 podmiotom. Zgodnie z definicją wskaźnika "Użytkownicy nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych" obowiązującą w FERC "Użytkownicy odnoszą się do klientów nowo opracowanych lub zmodernizowanych publicznych usług i produktów oraz do pracowników instytucji publicznej korzystających z nowo opracowanych lub znacząco zmodernizowanych procesów cyfrowych (...). Jeżeli nie można zidentyfikować poszczególnych użytkowników, ten sam klient/osoba korzystająca z usługi online kilka razy w ciągu roku nie jest uznawana za podwójne liczenie". Zgodnie z tą definicją we wskaźniku liczone są osoby, a nie urzędy czy instytucje. Przyjęto założenie, że z każdej instytucji/urzędu skorzysta średnio po 3 osoby (pracownicy), co daje wartość wskaźnika 300 ((55 urzędów+45 podmiotów) x 3 osoby = 300 osób).
Źródło danych\pomiaru: raport na podstawie danych z systemu
Częstotliwość pomiaru: w ciągu pierwszych 12 miesięcy licząc od miesiąca następującego po miesiącu zakończenia projektu
8.
Metoda\spółób pomiaru: odczyt z raportu systemowego
Źródło danych\pomiaru: raport na podstawie danych z systemu
Częstotliwość pomiaru: co 6 miesięcy przez kolejnych 12 miesięcy od momentu zakończenia realizacji projektu
9.
Metoda\spółób pomiaru: odczyt z raportu systemowego
Źródło danych\pomiaru: złożenie zgłoszenia, ocena wniosku, monitorowanie

	przebiegu testów, przygotowanie sprawozdania rocznego dla Komisji Europejskiej Częstotliwość pomiaru: przez kolejnych 12 miesięcy od momentu zakończenia realizacji projektu 10. Metoda\spół sposób pomiaru: poziom satysfakcji użytkowników systemu Piaskownica AI mierzony jako % użytkowników oceniających system co najmniej na poziomie zadowolającym w pięciostopniowej skali (1. bardzo niezadowolony, 2. niezadowolony, 3. ani zadowolony, ani niezadowolony, 4. zadowolony, 5. bardzo zadowolony) Źródło danych\pomiaru: wypełnione ankiety Częstotliwość pomiaru: w ciągu pierwszych 12 miesięcy licząc od miesiąca następującego po miesiącu zakończenia projektu
--	--

2.2. Udostępnione e-usługi

Lp.	Nazwa e-usługi	Typ	Zakres oddziaływania	Poziom dojrzałości e-usługi
1	Zgłoszenie do ścieżki technologicznej (e-usługa)	A2A	Administracja publiczna (Jednostki samorządu terytorialnego i jednostki sektora finansów publicznych) (rocznie ok 55 transakcji)	Transakcja
2	Zgłoszenie do ścieżki regulacyjnej (e-usługa)	A2A A2B	Przedsiębiorcy Administracja publiczna (Jednostki samorządu terytorialnego i jednostki sektora finansów publicznych) Operator piaskownicy AI, tj. Komisja Rozwoju i Bezpieczeństwa Sztucznej Inteligencji (rocznie ok 100 transakcji)	Transakcja

2.3. Udostępnione informacje sektora publicznego i zdigitalizowane zasoby

Nie dotyczy

2.4. Produkty końcowe projektu

Nazwa produktu	Planowana data wdrożenia
Raport z inicjalnego testu prywatności	01-2027
Opis Architektury systemu Piaskownica AI	07-2027
Raport z weryfikacyjnego testu prywatności	09-2027
System Piaskownica AI System wraz z dwiema e-usługami w ramach istniejącego, ograniczonego funkcjonalnie API platform dostępowych Fabryk AI	12-2027
Mapa sektorów priorytetowych i materiały informacyjne dla przedsiębiorców	12-2027
Raport Bezpieczeństwa systemu Piaskownica AI oraz e-Uслуг Dokument potwierdzający realizację testów bezpieczeństwa Systemu	12-2027
Raport Testów systemu Piaskownica AI oraz e-Uслуг Dokument potwierdzający realizację testów UAT oraz testów wydajności rozwiązania w ramach Systemu	12-2027
Raport z badań UX e-Uслуг Dokument prezentujący wyniki testów użyteczności projektowanych oraz wdrażanych usług w ramach Systemu	12-2027
Raport z audytu WCAG systemu Piaskownica AI oraz e-Uслуг Dokument podsumowujący wyniki oceny dostępności rozwiązania pod kątem standardów WCAG.	12-2027
Rekomendacje w zakresie wdrożenia zasady privacy by design i privacy by default (art. 25 RODO) w architekturze systemów informatycznych i środowisk	12-2027
Dokumentacja integracyjna oraz kontrakty API dla dostawców zasobów i usług AI (w tym Fabryk AI) wraz z docelowym wystandaryzowanym Interfejsem API (adapтеры Fabryk AI dostosowane do specyfiki projektu)	03-2028
Zestaw narzędzi prawnych, regulacyjnych i informacyjnych piaskownic AI	03-2028
Materiały szkoleniowe	03-2028
Dokumentacja biznesowo-techniczna systemu Piaskownica AI oraz e-Uслуг Dokumentacja biznesowo-techniczna Systemu w zakresie architektury rozwiązania oraz analizy biznesowo-systemowej	06-2028
Dokumentacja użytkownika systemu Piaskownica AI oraz e-Uслуг Instrukcja korzystania z rozwiązania	06-2028
Środowisko technologiczne oparte na infrastrukturze fabryk AI	12-2028
Opis środowisk i ekosystemu w środowiskach AI (Infrastruktura PCSS, PLGrid)	12-2028
Komponent badawczy w postaci raportów z badań i ewaluacji piaskownic AI	12-2028

3. KAMIENIE MIŁOWE

Kamienie milowe	Planowany termin osiągnięcia
Zakończony inicjalny test prywatności	2027-01-31

Kamienie milowe	Planowany termin osiągnięcia
Opracowano docelową architekturę systemu Piaskownica AI	2027-07-01
Zakończony weryfikacyjny test prywatności	2027-09-30
Uzyskany pozytywny wynik testów bezpieczeństwa	2027-11-30
Uzyskany pozytywny wynik testów wydajności	2027-11-30
Uzyskany pozytywny wynik badań UX	2027-11-30
Uzyskano pozytywny wynik audytu dostępności WCAG	2027-11-30
Uruchomiono system Piaskownica AI	2027-12-31
Uruchomiono e-usługę zgłoszenia do ścieżki regulacyjnej	2027-12-31
Uruchomiono e-usługę zgłoszenia do ścieżki technologicznej	2027-12-31
Opracowanie mapy sektorów priorytetowych i materiałów informacyjnych dla przedsiębiorców	2027-12-31
Opracowanie zbioru rekomendacji w zakresie wdrożenia zasady privacy by design i privacy by default (art. 25 RODO) w architekturze systemów informatycznych i środowisk	2027-12-31
Publikacja zestawu narzędzi prawnych i regulacyjnych piaskownic AI	2028-03-31
Opracowano materiały szkoleniowe dotyczące systemu Piaskownica AI	2028-03-31
Udostępniono interfejs API Piaskownicy AI	2028-03-31
Opracowano dokumentację biznesowo-techniczną systemu Piaskownica AI	2028-06-30
Opracowano dokumentację użytkownika systemu Piaskownica AI	2028-06-30
Uzyskany pozytywny wynik testów integracyjnych między systemem Piaskownica AI oraz Fabrykami AI	2028-06-30
Uzyskany pozytywny wynik testów wydajnościowych mechanizmu integracji między systemem Piaskownica AI oraz Fabrykami AI	2028-09-30
Zakończono proces integracji Fabryk AI z systemem Piaskownica AI - uruchomienie produkcyjne	2028-12-29
Wyskalowanie środowisk i rozszerzenie ekosystemu w środowiskach AI (Infrastruktura PCSS, PLGrid)	2028-12-29
Zakończono badania i ewaluację projektu - Zakończenie prac nad raportem końcowym z badań „Mapa potencjału innowacji AI przedsiębiorstw”	2028-12-31

4. KOSZTY

4.1. Koszty ogólne projektu wraz ze sposobem finansowania

Całkowity koszt projektu (netto oraz brutto), w tym	Netto 31 956 825,51 zł Brutto 35 000 000,00 zł	
Procent dofinansowania ze środków UE (brutto)	79,71%	
Procent środków z budżetu państwa (brutto)	20,29%	
Podział całkowitego kosztu projektu na poszczególne lata (netto oraz brutto)	2026	Netto 5 364 890,57 zł Brutto 5 561 908,57 zł
	2027	Netto 17 053 385,78 zł Brutto 19 139 894,96 zł
	2028	Netto 9 538 549,16 zł Brutto 10 298 196,47 zł

4.2. Wykaz poszczególnych pozycji kosztowych

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
Oprogramowanie	Pozycja ta obejmuje: - Wytworzenie oprogramowania systemu eksploatacji Piaskownic AI (MC zlecenie dla COI) - 11 880 196,95 PLN - Wykonanie środowiska opartego na infrastrukturze fabryk AI (PCSS, Cyfronet) - 7 473 350,00 PLN - Wykonanie analiz eksperckich i opracowań w zakresie wykorzystania Piaskownic i AI wraz z doradztwem na rzecz przedsiębiorców (MRiT) - 1 680 000,00 PLN Wykonanie analiz	26 390 146,95 zł	Oprogramowanie jest niezbędne do osiągnięcia celów projektu zarówno pod względem umożliwienia przedsiębiorcom i administracji publicznej testowania rozwiązań, jak również uzyskania wsparcia w zakresie zgodności regulacyjnej z AI Act. Wskazana wartość nie dotyczy zakupu gotowej aplikacji ani samego wykonania dwóch formularzy e-usług. Obejmuje kompleksowe wytworzenie, wdrożenie i przygotowanie do eksploatacji systemu Piaskownica AI, będącego centralnym systemem obsługującym procesy ścieżki regulacyjnej i technologicznej wraz z połączeniem systemu ze środowiskiem Fabryk AI (komponent oprogramowania łączący infrastrukturę z systemem i e-usługami – konfiguracja i uruchomienie środowiska testowego). W ramach tej pozycji

Nazwa pozycji kosztowej	Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
eksperckich w zakresie przetwarzania i ochrony danych osobowych (UODO) - 2 500 000,00 PLN Wykonanie prac badawczych dot. wykorzystania i rozwoju sztucznej inteligencji w Polsce (NASK) - 2 856 600,00 PLN Produkty: - Opis Architektury systemu Piaskownica AI - System Piaskownica AI - Zestaw narzędzi prawnych, regulacyjnych i informacyjnych piaskownic AI - Dokumentacja integracyjna oraz kontrakty API dla dostawców zasobów i usług AI (w tym Fabryk AI) wraz z docelowym wystandaryzowanym Interfejsem API (adaptery Fabryk AI dostosowane do specyfiki projektu) - Dokumentacja biznesowo-techniczna systemu Piaskownica AI oraz e-Usług - Dokumentacja użytkownika systemu Piaskownica AI oraz e-Usług - Środowisko technologiczne oparte na infrastrukturze		uwzględniono w szczególności: analizę biznesową i systemową; projekt architektury rozwiązania; implementację dwóch e-usług i mechanizmów back-office; obsługę procesu przyjmowania, weryfikacji i prowadzenia spraw; mechanizmy uwierzytelnienia i autoryzacji użytkowników; integracje z systemami zewnętrznymi, w tym Węzłem Krajowym, REGON i systemami Dostawców Fabryk AI; przygotowanie i implementację interfejsów API; monitoring, raportowanie i rejestrację zdarzeń; automatyzację testów; konfigurację procesów CI/CD i wdrożeniowych; dokumentację biznesowo-techniczną i użytkownika; działania zapewniające bezpieczeństwo rozwiązania już na etapie projektowania i wytwarzania. Kalkulację kosztu po stronie MC wykonano na podstawie rzeczywistej pracochłonności zespołu COI - łącznie 5 877 dni roboczych (MD). Dla komponentów oprogramowania łączących system z infrastrukturą Fabryk AI założono dla każdego podmiotu pracę 5 etatów przy wytworzeniu oprogramowania – 4 przez cały okres projektu, 1 etat przez 24 miesiące. Ponadto ujęto koszty merytorycznego doradztwa, analiz eksperckich i prac badawczych istotnych ze względu na innowacyjny charakter projektu i niezbędnych do osiągnięcia jego celów.

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
	fabryk AI - Opis środowisk i ekosystemu w środowiskach AI (Infrastruktura PCSS, PLGrid). - Mapa sektorów priorytetowych i materiały informacyjne dla przedsiębiorców - Rekomendacje w zakresie wdrożenia zasady privacy by design i privacy by default (art. 25 RODO) w architekturze systemów informatycznych i środowisk - Komponent badawczy w postaci raportów z badań i ewaluacji piaskownic AI		
Infrastruktura	Zestawy komputerowe dla pracowników PCSS i Cyfronet	183 250,00 zł	Zakup sprzętu komputerowego niezbędnego do realizacji prac programistycznych zaplanowanych przez partnerów projektu.
Koszty UX i grafiki	Raport z badań UX e-Usług Raport z audytu WCAG systemu Piaskownica AI oraz e-Usług	397 740,01 zł	Niezbędne do prawidłowego działania i uzyskania efektywnej realizacji usług od strony użytkowników końcowych.
Bezpieczeństwo	Raport z testów prywatności Raport Bezpieczeństwa systemu Piaskownica AI oraz e-Usług	427 665,00 zł	Realizacja zadań niezbędna w celu zapewnienia bezpieczeństwa funkcjonowania e-usług i platformy.
Wydajność rozwiązań	Raport Testów systemu Piaskownica AI oraz eUsług	997 065,96 zł	Testy pozwalające na uzyskanie zakładanej wydajności i efektywności działania e-usług.
Szkolenia	Materiały	179 250,00 zł	Szkolenia personelu oraz

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
	szkoleniowe		warsztaty dla interesariuszy projektu umożliwiające uzyskanie zaplanowanych efektów.
Działania informacyjno-promocyjne	Materiały informacyjno-promocyjne	1 354 850,00 zł	Działania informacyjno-promocyjne obejmujące prace związane z poinformowaniem i zachęceniem grup docelowych użytkowników do korzystania z e-usług. Działania te pozwolą na przyciągnięcie i zachęcenie odpowiedniej liczby użytkowników do korzystania e-usług opracowywanych w projekcie. Promocja niezbędna, aby osiągnąć założone wskaźniki realizacji celów projektu oraz aby wypełnić obowiązki informacyjno-promocyjne.
Koszty zarządzania i wsparcia (w tym wynagrodzenia personelu wspomagającego)	Pozycja ta obejmuje: Koszty zarządzania i wsparcia - 2 780 312,45 PLN Koszty pośrednie - 2 289 719,63 PLN	5 070 032,08 zł	Koszty obejmujące zarówno zarządzanie projektem jak i wartość kosztów pośrednich (stawka ryczałtowa 7% kosztów bezpośrednich).

4.3. Koszty ogólne utrzymania wraz ze sposobem finansowania (okres 5 lat)

Całkowity koszt utrzymania trwałości projektu (brutto)	24 230 759,00 zł		Źródło finansowania
Podział całkowitego kosztu utrzymania trwałości projektu na poszczególne lata (netto oraz brutto)	2029	4 554 676,00 zł (brutto) (3 702 989,00 zł netto)	krajowe środki publiczne - budżet państwa
	2030	4 759 636,00 zł (brutto) (3 869 623,00 zł netto)	krajowe środki publiczne - budżet państwa
	2031	4 864 349,00 zł (brutto) (3 954 755,00 zł netto)	krajowe środki publiczne - budżet państwa
	2032	4 971 364,00 zł (brutto) (4 041 759,00 zł netto)	krajowe środki publiczne - budżet państwa

	2033	5 080 734,00 zł (brutto) (4 130 678,00 zł netto)	krajowe środki publiczne - budżet państwa
--	------	---	---

4.4. Planowane koszty ogólne realizacji (w przypadku projektu współfinansowanego – wkład krajowy z budżetu państwa) oraz koszty utrzymania projektu:

- zostaną pokryte w ramach budżetów odpowiednich dysponentów części budżetowych bez konieczności występowania o dodatkowe środki z budżetu państwa
- ~~- będą powodować konieczność przyznania dodatkowych kwot~~

5. GŁÓWNE RYZYKA

5.1. Ryzyka wpływające na realizację projektu

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
Nieterminowa realizacja prac wytwórczych	Średnia	Średnie	1. Stałe monitorowanie kamieni milowych i postępu projektu 2. Priorytetyzowanie potrzeb i wdrażanie wg priorytetów 3. Uzgodnienie z kierownictwem MC roadmap-y na okres realizacji projektu
Wdrożenie zmian legislacyjnych w obszarze RODO i AI Act wpływające na zakres oceny zgodności	Średnia	Wysokie	1. Stały monitoring zmian legislacyjnych w zakresie RODO przez UODO 2. Stały monitoring zmian legislacyjnych w zakresie aktu w sprawie sztucznej inteligencji i wydanych do niego aktów wykonawczych przez Ministerstwo Cyfryzacji we współdziałaniu z UODO w zakresie zmian obejmujących ochronę danych osobowych 3. Opracowanie wytycznych i szablonów w formie modułowej, umożliwiającej ich aktualizację bez przebudowy całego systemu oceny
Opóźnienie powołania i uruchomienia Komisji Rozwoju i Bezpieczeństwa Sztucznej Inteligencji (KRiBSI)	Duża	Średnie	1. Monitorowanie ustawowych terminów powołania przewodniczącego Komisji i zwołania jej pierwszego posiedzenia 2. Przygotowanie dokumentacji operacyjnej piaskownicy przed powołaniem Komisji, tak aby przejęcie zadań nie wymagało przerwy w działaniu
Niepełne	Średnia	Wysokie	Odpowiednia analiza architektury i

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
oszacowanie odpowiedniej infrastruktury			infrastruktury wraz z opracowaniem procedur wdrożenia oczekiwanego rozwiązania pozwoli na zaplanowanie zasobów gwarantujących płynność prac
Brak wystarczających zasobów kadrowych do realizacji projektu	Średnia	Niskie	1. Wcześniejsze przygotowanie planu zasobów projektu i alokacji, zastępowalność w projekcie 2. Zapewnienie ciągłości kompetencyjnej 3. Powołanie zespołów dedykowanych wyłącznie dla tego projektu (nierealizujących prac w innych projektach)
Brak akceptacji systemu ze strony użytkowników zewnętrznych	Mała	Niskie	1. Działania promocyjne 2. Bliska współpraca z Interesariuszami w zakresie produktów wytwarzanych w ramach projektu
Niezrealizowanie harmonogramu realizacji projektu	Średnia	Niskie	Stałe monitorowanie kamieni milowych i postępu projektu w ujęciu iteracyjnym, KS będą się odbywać z regularną częstotliwością
Niewdrożenie komponentów informatycznych	Duża	Wysokie	1. Stałe monitorowanie kamieni milowych i postępu projektu w ujęciu iteracyjnym, KS będą się odbywać z regularną częstotliwością 2. Bliska współpraca z Interesariuszami.
Nieosiągnięcie wskaźnika efektu projektu	Średnia	Średnie	Zarządzanie zakresem, zamykanie zakresów etapów i ich potwierdzanie
Nieosiągnięcie wskaźników produktu oraz celu projektu	Średnia	Średnie	Zarządzanie zakresem, zamykanie zakresów etapów i ich potwierdzanie
Niepełne zidentyfikowanie infrastruktury sprzętowej co przekłada się na proces zakupowy	Średnia	Niskie	Zdefiniowanie wymagań wydajnościowych na wczesnym etapie projektu (tj. analizy do systemu informatycznego)
Nieprzetestowanie w pełni środowiska modeli i dostępu do danych	Średnia	Średnie	Potrzeba testowania modeli, dostępu do danych, niskopoziomowej analizy
Niezrealizowanie	Duża	Średnie	Regularna kontrola postępu

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
harmonogramu gotowości infrastruktury fabryk AI			przygotowań infrastruktury AI
Zmiany po stronie partnerów projektu lub dostawców usług zewnętrznych wpływające na harmonogram	Średnia	Wysokie	Porozumienia o partnerstwie określające zakres, harmonogram i budżet każdego partnera wraz z zasadami zgłaszania zmian. Cykliczny przegląd postępu prac partnerów na Komitecie Sterującym. Bieżąca komunikacja z EuroHPC JU w zakresie harmonogramu udostępnienia fabryk AI.
Brak wystarczających zasobów (GPU, interfejsów), co będzie skutkowało niedostępnością lub brakiem gotowości Fabryk AI	Duża	Niskie	1. Monitorowanie poziomu zużycia zasobów oraz popytu na przewidywane usługi piaskownicy technologicznej dla administracji publicznej. 2. Zapewnienie mechanizmów ograniczających zużycie zasobów przez jednego użytkownika do odpowiedniego poziomu. 3. Zwiększenie zasobów obsługujących piaskownicę technologiczną lub wdrożenie systemu priorytetyzacji oraz ograniczeń przydziału dostępu do Fabryk AI i dostępnych zasobów.
Brak identyfikacji i oceny ryzyk właściwych dla rozwiązań AI takich jak prompt injection, data poisoning, model extraction i niekontrolowanego zużycia zasobów	Średnia	Niskie	1. Ustanowienie na poziomie projektu odpowiednich procesów zarządzania jakością, tj. procesów dotyczących wdrażania technologii AI w ramach piaskownicy technologicznej i modeli dostępnych poprzez API. 2. Zapewnienie w procesie wdrażania modeli AI dostępnych poprzez API analizę ryzyka obejmującą identyfikację i ocenę ryzyk z zakresu bezpieczeństwa, w tym dotyczących prompt injection, model extraction, data poisoning, nadużycia API czy nadmiernego zużycia zasobów. 3. Monitorowanie i kontrolowanie procesów wdrażania modeli AI w ramach piaskownicy technologicznej AI dla administracji publicznej, w tym przeprowadzenie testów bezpieczeństwa.
Niewystarczające	Średnia	Niskie	1. Monitorowanie i zarządzanie

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
zabezpieczenie modeli AI			procesem zmian w ramach piaskownicy technologicznej AI dla administracji publicznej, w tym monitorowanie i zarządzanie procesami wdrażania modeli AI. 2. Przeprowadzenie testów bezpieczeństwa przed udostępnieniem modeli AI poprzez API w ramach piaskownicy technologicznej dla administracji publicznej.
Niewłaściwa ochrona danych i interfejsów API	Duża	Niskie	1. Wbudowanie w procesy wdrażania technologii w ramach piaskownicy technologicznej AI dla administracji publicznej elementu związanego z testami bezpieczeństwa. 2. Monitorowanie i okresowa weryfikacja poziomu zabezpieczeń, zgodnie z praktykami odpowiednich standardów zabezpieczeń dla Fabryk AI.

5.2. Ryzyka wpływające na utrzymanie efektów

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
Brak zidentyfikowanych środków na utrzymanie systemu	Duża	Średnie	Szczegółowe planowanie kosztów utrzymania i bieżąca ich aktualizacja
Brak wystarczających zasobów kadrowych do realizacji projektu	Średnia	Średnie	1. Zapewnienie zastępowalności kadr 2. Prowadzenie szczegółowej dokumentacji projektu umożliwiającej szybkie wdrożenie dodatkowych osób
Problemy z wydajnością systemu na etapie jego eksploatacji	Średnia	Niskie	Cykliczne monitorowanie wydajności systemu na etapie jego eksploatacji oraz podejmowanie działań optymalizacyjnych w kontekście wydajności systemu
Brak zainteresowania odbiorców ostatecznych	Mała	Niskie	Monitorowanie poziomu wykorzystania produktów projektu. Na podstawie zebranych informacji planowane będą działania zaradcze, np.: dostosowujące

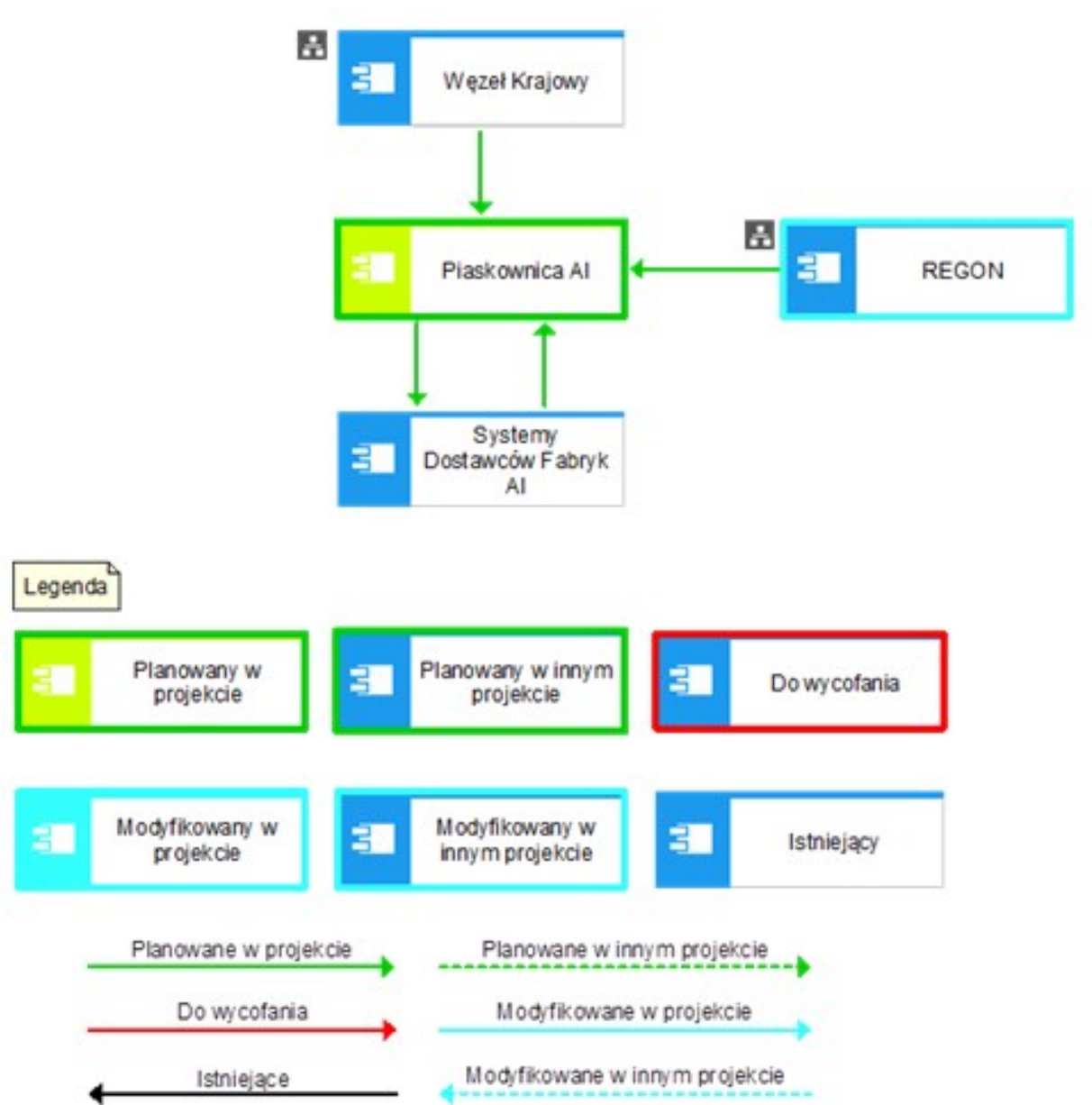
Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
projektu korzystaniem z funkcjonalności systemu			produkty do zmieniających się wymagań odbiorców, działania informacyjne i promocyjne.
Niewystarczające zainteresowanie przedsiębiorców oraz administracji publicznej i JST udziałem w piaskownicy	Średnia	Wysokie	Działania informacyjne i promocyjne.
Dezaktualizacja modeli AI	Mała	Średnie	1. Opracowanie zasad związanych z aktualizacją modeli AI w ramach piaskownicy technologicznej dla administracji publicznej. 2. Analiza potrzeb zgłaszanych przez administrację publiczną oraz adekwatne planowanie prac wdrożeniowych w zakresie modeli AI dostępnych poprzez API. 3. Zapewnienie właściwego procesu zarządzania wersjami, aktualizacjami, podatnościami, a także szerzej procesem zarządzania usługą, zgodnie z wybranymi praktykami, np. ITIL.
Dezaktualizacja komponentów AI	Mała	Średnie	1. Opracowanie zasad związanych z aktualizacją komponentów AI w ramach piaskownicy technologicznej dla administracji publicznej. 2. Analiza potrzeb zgłaszanych przez administrację publiczną oraz adekwatne planowanie prac wdrożeniowych w zakresie komponentów AI dostępnych poprzez API. 3. Zapewnienie właściwego procesu zarządzania wersjami, aktualizacjami, podatnościami, a także szerzej procesem zarządzania usługą, zgodnie z wybranymi praktykami, np. ITIL.
Dezaktualizacja bibliotek i procedur bezpieczeństwa	Średnia	Niskie	Zarządzanie bezpieczeństwem i zmianami zgodnie z wdrożonymi systemami bezpieczeństwa i jakości w Fabrykach AI (Cyfronet i PCSS), w tym realizacja okresowych przeglądów, np. ramach certyfikacji lub innych powiązanych działań dotyczących zarządzania zmianą i bezpieczeństwem

6. OTOCZENIE PRAWNE

Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
1	Ustawa z dnia 3 lipca 2026 r. o systemach sztucznej inteligencji Dz.U. 2026 poz. 1003	TAK/NIE		
2	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji)	TAK/NIE		
3	Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne	TAK/NIE		
4	Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych	TAK/NIE		
5	Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa	TAK/NIE		
6	Rozporządzenie 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)	TAK/NIE		
7	Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych	TAK/NIE		
8	Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych	TAK/NIE		
9	Ustawa z dnia 26 maja 2023 r. o aplikacji mObywatel	TAK/NIE		
10	Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej	TAK/NIE		
11	Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach	TAK/NIE		

7. ARCHITEKTURA

7.1. Widok kooperacji aplikacji



Lista systemów wykorzystywanych w projekcie

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
1	Piaskownica AI	Ministerstwo Cyfryzacji	Piaskownica AI to system wspierający obsługę wniosków o dostęp do	Planowany	N\D

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			dwóch ścieżek: ścieżki regulacyjnej i ścieżki technologicznej. Celem systemu jest zapewnienie kompleksowej obsługi procesu udostępniania piaskownic AI, w tym przyjmowania, weryfikacji i oceny wniosków o dostęp do piaskownic, tworzenia oraz prowadzenia piaskownic AI, a także zarządzania zleceniami dotyczącymi konfiguracji i zapewnienia środowisk technologicznych. Rozwiązanie umożliwia obsługę wniosków składanych w ramach e-usług, obejmujących dostęp do piaskownic regulacyjnych oraz technologicznych. Rozwiązanie wspiera również rejestrację zdarzeń wynikających z procesu obsługi piaskownic AI, zarządzanie użytkownikami oraz komunikację z podmiotami zapewniającymi infrastrukturę technologiczną. System zapewnia także możliwość pobierania danych na potrzeby raportowe i sprawozdawcze. W systemie nie są prowadzone rejestry publiczne. Główne grupy funkcjonalności systemu obejmują: - uwierzytelnianie użytkowników; - obsługę złożonych w		

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			ramach e-Uслуг wniosków o dostęp do piaskownic AI; - zarządzanie piaskownicami AI oraz rejestracja zdarzeń wynikających z procesu obsługi piaskownic AI oraz wspierający prowadzenie piaskownic; - komunikację systemu Piaskownica AI z Fabrykami AI, tj. zlecenia grantów obliczeniowych, monitorowanie i obsługę środowisk. System wymienia dane z innymi systemami krajowymi w zakresie obsługi e-usług, komunikacji z Fabrykami AI oraz zarządzania zleceniami dotyczącymi konfiguracji i zapewnienia środowisk technologicznych.		
2	REGON	Główny Urząd Statystyczny	System Krajowego rejestru urzędowego podmiotów gospodarki narodowej REGON służy do prowadzenia rejestru REGON, w tym do rejestracji podmiotów gospodarki narodowej, tj. osób prawnych, jednostek organizacyjnych niemających osobowości prawnej, osób fizycznych prowadzących działalność gospodarczą (w tym osób prowadzących indywidualne gospodarstwa rolne) skutkującej nadaniem numeru identyfikacyjnego REGON oraz udostępniania danych rejestru, w tym za	Modyfikowany	N\D

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			pośrednictwem usługi sieciowej. System REGON składa się z modułów: * CRR (Centralny Rejestr Regon) - centralny komponent systemu - zawiera bazę danych przechowującą dane o podmiotach gospodarki narodowej oraz informacje o ich zmianach, * BPR (Baza Publikacyjna REGON) - realizuje takie funkcje jak: tworzenie wyciągów z rejestru REGON dla uprawnionych instytucji w zakresie zmian danych, jakie miały miejsce w ciągu ostatniego miesiąca, zasilanie danymi systemu Bazy Jednostek Statystycznych (BJS), opracowywanie sprawozdań i raportów, udostępnianie danych rejestru podmiotom trzecim na podstawie wniosków o udostępnienie danych. * BIR (Baza Internetowa REGON) - przechowuje tworzoną na bieżąco replikę danych z modułu CRR (zakres replikowanych danych nie obejmuje danych objętych tajemnicą statystyczną) w celu ich bieżącego przeglądania i wyszukiwania na podstawie zadanych kryteriów przez sieć INTERNET. Zakres funkcji wyszukiwania jest zależny od typu użytkownika. * Bazy Systemowej – przechowuje informacje wspólne, pomocnicze dla pozostałych modułów, w		

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			tym logi z aktywności użytkowników w systemie. REGON pobiera dane z systemów: CRP KEP Ministerstwa Finansów, SIO Ministerstwa Edukacji Narodowej, KRS Ministerstwa Sprawiedliwości, CEIDG Ministerstwa Rozwoju i Technologii w zakresie niezbędnym do dokonywania wpisów w rejestrze określonych podmiotów / cech, oraz zwraca numery identyfikacyjne REGON do tych systemów. Integruje się z krajowymi systemami teleinformatycznymi.		
3	Systemy Dostawców Fabryk AI	Dostawcy usług AI	System Dostawców Fabryk to system wspierający zapewnianie infrastruktury technologicznej dla piaskownic AI, w tym dostęp do środowisk testowych, zasobów obliczeniowych oraz gotowych rozwiązań opartych na sztucznej inteligencji. Celem systemu jest umożliwienie korzystania z infrastruktury obliczeniowej i technologicznej udostępnianej przez Fabryki AI na potrzeby testowania, weryfikacji i rozwoju rozwiązań AI w ramach piaskownic technologicznych. System umożliwia integrację infrastruktury obliczeniowej Fabryk AI z systemem piaskownic AI	Istniejący	N\D

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			oraz ścieżką technologiczną, zapewniając obsługę procesów związanych z udostępnianiem środowisk testowych, konfiguracją dostępu oraz wykorzystaniem mocy obliczeniowej. W ramach systemu udostępniane są również gotowe rozwiązania AI, w tym modele językowe, takie jak PLLuM, oraz inne wybrane rozwiązania AI. W systemie nie są prowadzone rejestry publiczne. Główne grupy funkcjonalności systemu obejmują: - zarządzanie dostępem do środowisk testowych – obsługa konfiguracji dostępu użytkowników i podmiotów do środowisk piaskownic AI; - udostępnianie zasobów obliczeniowych – zapewnianie dostępu do mocy obliczeniowej niezbędnej do testowania i uruchamiania rozwiązań AI; - integrację z systemem Piaskownica AI – wymianę informacji i obsługę procesów technologicznych pomiędzy infrastrukturą Fabryk AI a systemem Piaskownica AI; - obsługę ścieżki technologicznej – wspieranie procesów technicznych związanych z wykorzystaniem infrastruktury oraz rozwiązań AI w środowiskach piaskownic;		

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			- udostępnianie gotowych rozwiązań AI – zapewnianie dostępu do wybranych modeli i narzędzi AI, w tym modeli językowych oraz rozwiązań wytwarzanych w ramach ekosystemu AI. System wymienia dane z innymi systemami krajowymi w zakresie niezbędnym do integracji infrastruktury obliczeniowej Fabryk AI z systemem Piaskownica AI oraz obsługi procesów realizowanych w ramach ścieżki technologicznej.		
4	Węzeł Krajowy	Ministerstwo Cyfryzacji	Węzeł Krajowy to system wspierający proces uwierzytelniania użytkowników korzystających z usług online świadczonych przez podmioty publiczne. System pełni rolę pośrednika pomiędzy systemami identyfikacji elektronicznej a systemami udostępniającymi usługi elektroniczne, umożliwiając bezpieczne przekazywanie potwierdzeń tożsamości. Celem systemu jest zapewnienie jednolitego, bezpiecznego i interoperacyjnego mechanizmu uwierzytelniania użytkowników usług online administracji publicznej poprzez wykorzystanie różnych środków identyfikacji elektronicznej. Główne grupy funkcjonalności:	Istniejący	N\D

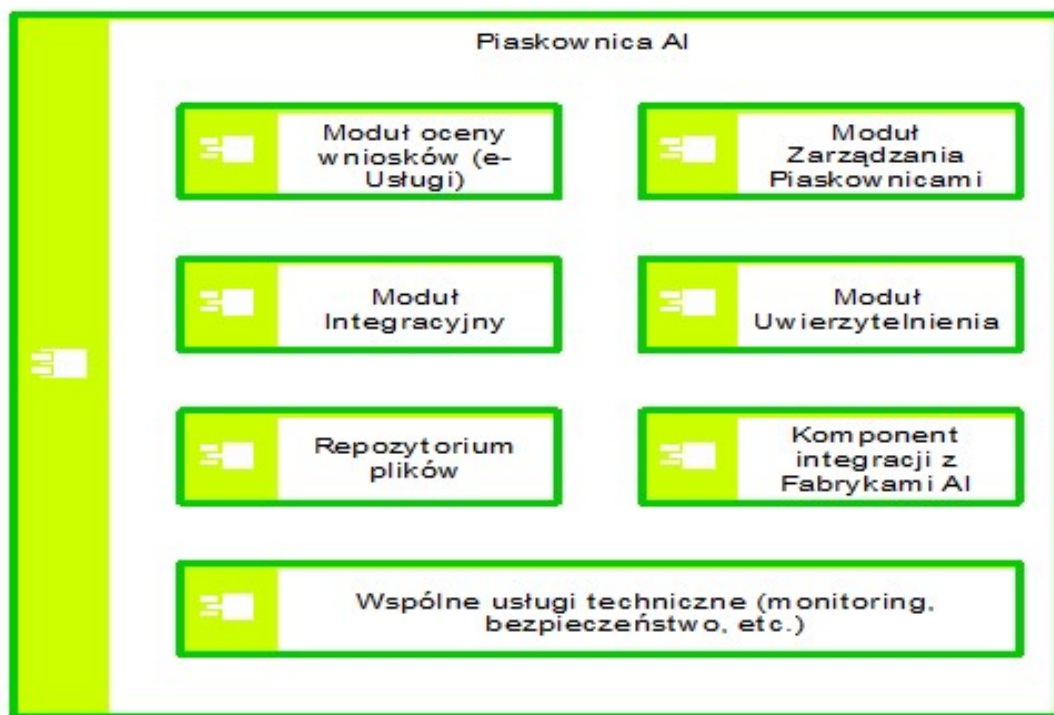
Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			– pośredniczenie w procesie uwierzytelniania użytkowników usług online, – integracja z systemami identyfikacji elektronicznej, – przekazywanie potwierdzeń tożsamości do systemów świadczących usługi elektroniczne, – zapewnienie bezpiecznej wymiany danych identyfikacyjnych, Integracje System jest zintegrowany z krajowymi systemami teleinformatycznymi.		

Lista przepływów

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
1	REGON	Piaskownica AI	Dane identyfikacyjne podmiotu gospodarczego (nazwa, adres, forma prawna, numer REGON) pobierane w celu uzupełnienia i walidacji danych podmiotu w formularzu zgłoszeniowym	tryb odwołań bezpośrednich	realizowalny inną metodą	protokół SOAP
2	Węzeł Krajowy	Piaskownica AI	Potwierdzenie tożsamości oraz dane identyfikacyjne użytkownika	tryb odwołań bezpośrednich	realizowalny inną metodą	protokół SOAP

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
			przekazywane po uwierzytelnieniu, wykorzystywane do utworzenia konta i powiązania z podmiotem			
3	Piaskownica AI	Systemy Dostawców Fabryk AI	Zlecenia w zakresie konfiguracji oraz zarządzania środowiskami ścieżki technologicznej piaskownicy AI	tryb odwołań bezpośrednich	realizowalny inną metodą	SOAP, REST
4	Systemy Dostawców Fabryk AI	Piaskownica AI	Dane o statusach realizacji zleceń oraz dane raportowe w zakresie wykorzystanych oraz dostępnych mocy obliczeniowych systemów	tryb odwołań bezpośrednich	realizowalny inną metodą	SOAP, REST

7.2. Kluczowe komponenty architektury rozwiązania



Legenda



7.3. Przyjęte założenia technologiczne

Lp.	Obszar	Założenie technologiczne
1.	Infrastruktura	Infrastruktura Rządowej Chmury Obliczeniowej (RChO). System Piaskownica AI będzie uruchomiony w Rządowej Chmurze Obliczeniowej. Infrastruktura systemu centralnego obejmuje warstwę dostępową i zabezpieczającą, warstwę frontendową, backendową, bazodanową oraz komponenty monitoringu i obserwowalności. Dla realizacji procesu wytwórczego i utrzymaniowego przewidziane są odrębne środowiska deweloperskie, testowe, preprodukcyjne i produkcyjne. Komunikacja pomiędzy komponentami będzie realizowana z wykorzystaniem mechanizmów sieciowych i zabezpieczeń właściwych dla RChO, w tym kontroli dostępu sieciowego, firewalli oraz VPN. Założenia technologiczne przewidują

Lp.	Obszar	Założenie technologiczne
		wykorzystanie m.in. systemu Linux, PostgreSQL, Spring Boot, Docker oraz narzędzi monitoringu i logowania, takich jak Zabbix, Loki i Grafana. Infrastruktura systemu Piaskownica AI jest odrębna od infrastruktury wykonawczej wykorzystywanej w ścieżce technologicznej. Projekt nie zakłada budowy nowej infrastruktury HPC/GPU ani zakupu dedykowanych zasobów obliczeniowych dla usług AI. Środowiska testowe i zasoby obliczeniowe będą zapewniane przez partnerów infrastrukturalnych – Cyfronet i PCSS – w ramach infrastruktury Fabryk AI.
2.	Sieć i bezpieczeństwo	Pojedyncze statyczne publiczne adresy IP na potrzeby komunikacji publicznej; ograniczony na poziomie firewall'a dostęp pomiędzy infrastrukturami; VPN
3.	Standardy wymiany danych	HTTPS, REST, JSON
4.	Systemy operacyjne serwerowe	Linux
5.	Bazy danych	Postgresql
6.	Serwery aplikacji	Spring Boot, Docker
7.	Portale	rozwiązania CMS (content management system)
8.	Inne	Zabbix, Loki, Grafana

7.4. Opis zasobów danych przetwarzanych w planowanym rozwiązaniu

Czy nowy system będzie tworzył zasoby danych o charakterze rejestru publicznego?

TAK/NIE

Czy nowy system będzie przetwarzał (używał, zmieniał) zawartość innych rejestrów publicznych?

TAK/NIE

Lp.	Rejestr publiczny	Opis	Zakres przetwarzania
1	Krajowy rejestr urzędowy podmiotów gospodarki narodowej (REGON)	Krajowy rejestr urzędowy podmiotów gospodarki narodowej (REGON) obejmuje: osoby prawne, jednostki organizacyjne niemające osobowości prawnej, osoby fizyczne prowadzące działalność gospodarczą, a także osoby prowadzące indywidualne gospodarstwa rolne oraz jednostki lokalne wymienionych wcześniej podmiotów. Rejestr REGON zawiera zbiór podmiotów i ich referencyjnych danych, spośród wszystkich rejestrów	Piaskownica AI pobiera z rejestru dane identyfikacyjne podmiotu (nazwa, adres, forma prawna, numer REGON) w celu uzupełnienia i walidacji danych podmiotu w formularzu zgłoszeniowym do ścieżki regulacyjnej oraz technologicznej. Projekt nie przewiduje zmiany zawartości rejestru ani wprowadzania do niego danych.

Lp.	Rejestr publiczny	Opis	Zakres przetwarzania
		podmiotów polskiej administracji publicznej.	

7.5. Bezpieczeństwo

Planowany poziom zapewnienia bezpieczeństwa (w rozumieniu przepisów §20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności [...] (Dz. U. 2012, poz. 526 z późn. zm.) w zakresie dot. systemu zarządzania bezpieczeństwem informacji:

- ~~-system nie podlega rygorom KRI – należy wyjaśnić czy istnieją inne normy bezpieczeństwa, które będą spełnione przez system zgodnie z wymogami KRI~~
- ~~-dodatkowe zabezpieczenia powyżej wymogów KRI: należy wskazać uzasadnienie~~