

OPIS ZAŁOŻEŃ PRZEDSIĘWZIĘCIA INFORMATYCZNEGO O PUBLICZNYM ZASTOSOWANIU

Tytuł przedsięwzięcia	Platforma usług inteligentnych RF – bezpieczne i suwerenne środowisko usług sztucznej inteligencji dla Resortu Finansów (skrótowa nazwa: Platforma usług inteligentnych RF; akronim: PUIRF)		
Wnioskodawca	Minister Finansów i Gospodarki		
Beneficjent	Centrum Informatyki Resortu Finansów		
Partnerzy	nie dotyczy		
Źródło finansowania	Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 Priorytet FERC.02 Zaawansowane usługi cyfrowe Działanie FERC.02.01 Wysoka jakość i dostępność e-usług publicznych UE - 79,71% - 14 230 068,33 zł BP (część 19) – 20,29% - 3 622 231,67 zł		
Całkowity koszt przedsięwzięcia	17 852 300,00 zł		
Planowany okres realizacji przedsięwzięcia	01-2027 do 12-2028		
Osoba kontaktowa	Magdalena Kwiatek	magdalena.kwiatek@mf.gov.pl	532447791

1. POWODY PODJĘCIA PRZEDSIĘWZIĘCIA

1.1. Identyfikacja problemu i potrzeb

Resort Finansów nie posiada obecnie wewnętrznego, suwerennego rozwiązania sztucznej inteligencji umożliwiającego bezpieczne wykorzystanie dużych modeli językowych (LLM) w realizacji zadań służbowych. Jednocześnie zasoby wiedzy organizacyjnej są rozproszone w wielu systemach i repozytoriach, m.in. SharePoint, repozytoriach plików, poczcie elektronicznej oraz EZD. Brak narzędzi umożliwiających ich jednolite przeszukiwanie, analizę i wykorzystanie powoduje, że odnajdywanie informacji oraz przygotowywanie dokumentów jest czasochłonne i wymaga znacznego zaangażowania pracowników.

Rosnące zainteresowanie wykorzystaniem AI w pracy skutkuje korzystaniem z ogólnodostępnych usług opartych na LLM. Rozwiązania te nie zapewniają jednak pełnej kontroli nad przetwarzaniem danych ani gwarancji spełnienia wymagań bezpieczeństwa obowiązujących w Resorcie Finansów, w szczególności w odniesieniu do danych wrażliwych i objętych tajemnicą skarbową. Powoduje to ryzyka bezpieczeństwa, prawne i organizacyjne oraz ogranicza możliwość szerszego wykorzystania AI w działalności resortu.

Dodatkowo procesy wytwarzania i utrzymania oprogramowania nie są wspierane przez narzędzia AI działające w środowisku RF. Brakuje również rozwiązań umożliwiających bezpieczną analizę kodu źródłowego oraz dokumentacji technicznej, co ogranicza efektywność prac i utrudnia wykorzystanie wiedzy zgromadzonej w projektach informatycznych.

W ramach przedsięwzięcia powstanie system teleinformatyczny PUIRF, działający lokalnie, zapewniający bezpieczne środowisko udostępniania usług AI. PUIRF będzie obejmował dostęp

do modeli AI, mechanizmy kontroli dostępu i monitorowania wykorzystania usług. Na platformie uruchomiona zostanie usługa A2A wspierająca analizę i tworzenie dokumentów z wykorzystaniem zasobów wiedzy resortu. Wdrożenie tych produktów pozwoli usunąć wskazane ograniczenia, zapewni bezpieczne wykorzystanie AI oraz usprawni procesy pozyskiwania, analizy i wykorzystania informacji w Resorcie Finansów.

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
Pracownicy Resortu Finansów	• brak suwerennego narzędzia GenAI do realizacji zadań kluczowych, • czasochłonne wyszukiwanie informacji w rozproszonych źródłach wiedzy, • niska efektywność procesów tworzenia i analizy dokumentów, • brak możliwości bezpiecznego wykorzystania AI przy przetwarzaniu danych wrażliwych, • ograniczone możliwości ponownego wykorzystania wiedzy organizacyjnej, • brak narzędzi wspierających analizę kodu źródłowego i dokumentacji	Liczba pracowników Resortu Finansów – 64000 Liczba faktycznych użytkowników rok po zakończeniu projektu – 5000

1.2. Opis stanu obecnego

Obecnie w Resorcie Finansów:

- brak automatyzacji pracy z dokumentami (podsumowanie, streszczanie, tłumaczenie) w sposób bezpieczny bez udostępniania ich na zewnątrz,
- dokumenty tworzone ręcznie, na podstawie samodzielnego wyszukiwania w wielu źródłach,
- wiedza i dane rozproszone w wielu źródłach: np. SharePoint MF, Repozytorium plików MF, poczta e-mail oraz system obiegu dokumentów EZD PUW MF – brak wspólnej warstwy wyszukiwania semantycznego,
- uwierzytelnianie realizowane w oparciu o Active Directory; dane organizacyjne pracowników utrzymywane w odrębnym rejestrze pracowników,
- brak narzędzi generatywnej AI klasy korporacyjnej działających lokalnie; korzystanie z narzędzi publicznych rodziłoby ryzyko prawne i bezpieczeństwa danych,
- brak mechanizmów ponownego wykorzystania wiedzy i mierzenia produktywności pracy nad dokumentami,
- brak narzędzi do automatycznej weryfikacji kodu źródłowego aplikacji wytwarzanej na potrzeby resortu oraz ich dokumentacji.

2. EFEKTY PRZEDSIĘWZIĘCIA

W jaki sposób przedsięwzięcie realizuje Strategię Cyfryzacji Państwa?

Zgodnie z celami określonymi w Strategii Cyfryzacji Państwa – na 2035 r. 50% firm i 80% urzędów ma wykorzystywać technologie sztucznej inteligencji - w ramach płaszczyzny Państwo skoncentrowane na cyfryzacji procesów administracyjnych (2.2 Cyfryzacja procesów administracyjnych i postępowań sądowych) Cel 2.2.1 szczegółowy Procesy back-office w administracji publicznej są prowadzone cyfrowo, zapewnienie wprowadzenie automatyzacji i optymalizacji wykonywania procesów administracyjnych z wykorzystaniem rozwiązań sztucznej

inteligencji. Platforma usług inteligentnych RF – bezpieczne i suwerenne środowisko usług sztucznej inteligencji dla Resortu Finansów stanowi odpowiedź na rosnącą potrzebę uproszczenia i stwarzania bardziej efektywnej komunikacji wewnątrz jednostek Resortu Finansów oraz ułatwiania pracy pracownikom resortu, a także poprawę ich efektywności. Projekt poprzez udostępnienie usługi wewnątrz administracyjnej pozwoli na zautomatyzowanie rutynowych czynności pracowników Resortu Finansów, usprawni procesy decyzyjne oraz w następstwie ułatwi komunikację z obywatelami i między urzędami.

Projekt wpisuje się w obszary horyzontalne Strategii – przede wszystkim cyberbezpieczeństwo oraz koordynację cyfrowej transformacji – a także w płaszczyznę „państwo” (chmura obliczeniowa, cyfrowe procesy administracji) i „gospodarka i technologie” w zakresie sztucznej inteligencji.

Przedsięwzięcie wzmacnia suwerenność cyfrową państwa, w szczególności poprzez:

- kontrolę nad danymi – przetwarzanie danych wrażliwych wyłącznie w infrastrukturze resortu (on-premise), z izolacją danych departamentów (multi-tenant), autoryzacją oraz pełnym audytem zapytań i odpowiedzi;
- możliwość migracji danych dla usług – architektura API-first i otwarte formaty danych baz wiedzy umożliwiające przenoszenie zasobów oraz uniezależnienie od konkretnego dostawcy;
- ograniczenie zależności od pojedynczego dostawcy i dostawców spoza EOG – wykorzystanie modeli open-weight uruchamianych lokalnie (co najmniej 3 modele lokalne);
- zdolność administracji do utrzymania i rozwoju kluczowych usług – budowę kompetencji wewnętrznych CIRF, dokumentację techniczną i procedury utrzymania oraz zabezpieczony 5-letni plan utrzymania trwałości.

Jakie inne strategie, polityki publiczne lub wymagania strategiczne realizuje przedsięwzięcie?

Cele strategiczne Resortu Finansów: Cel 4.1. Wzmocnienie potencjału organizacji; Działanie 4.1.7. Budowa otoczenia wspierającego rozwój pracowników w obszarze AI; Cel 2.1. Wsparcie klientów w wykonywaniu obowiązków podatkowych i celnych; Działanie: 2.1.1. Cyfryzacja i automatyzacja usług

Dokument strategiczny: Kierunki działania i rozwoju Ministerstwa Finansów na lata 2025-2028

2.1. Cele i korzyści wynikające z przedsięwzięcia

Cel - 1	Zwiększenie automatyzacji procesów back-office poprzez budowę Platformy usług inteligentnych RF – bezpiecznego i suwerennego środowiska usług wewnątrzadministracyjnych (A2A) sztucznej inteligencji dla Resortu Finansów działającego lokalnie i obsługującego do 5 000 użytkowników.
Cel strategiczny	1. Strategia Cyfryzacji Państwa; Cyfryzacja procesów administracyjnych i postępowań sądowych Cel 1 Procesy back-office w administracji publicznej są prowadzone cyfrowo. 2. Przedsięwzięcie jest zgodne z kierunkami określonymi w dokumencie Polityka rozwoju sztucznej inteligencji w Polsce do 2030 roku opracowanym przez Ministerstwo Cyfryzacji oraz z obowiązującą Polityką dla rozwoju sztucznej inteligencji w Polsce od roku 2020. 3. Cele strategiczne Resortu Finansów: Cel 4.1. Wzmocnienie potencjału organizacji, Działanie 4.1.7. Budowa otoczenia wspierającego rozwój pracowników w obszarze AI; Dokument strategiczny: Kierunki działania i rozwoju Ministerstwa Finansów na lata 2025-2028. 4. Cele strategiczne Resortu Finansów: Cel 2.1. Wsparcie klientów w

	wykonywaniu obowiązków podatkowych i celnych, Działanie: 2.1.1. Cyfryzacja i automatyzacja usług; Dokument strategiczny: Kierunki działania i rozwoju Ministerstwa Finansów na lata 2025-2028.
Korzyść:	• zwiększenie efektywności operacyjnej (redukcja pracochłonności) • retencja i ponowne wykorzystanie wiedzy instytucjonalnej (szybki, semantyczny dostęp do wiedzy departamentów) • cyfryzacja i skalowanie procesu analizy dokumentów (jednolite, bezpieczne narzędzie GenAI on-premise) • podniesienie jakości i spójności dokumentów (standaryzacja, mniej błędów, krótszy obieg) • bezpieczna integracja środowiska (suwerenność danych i zgodność z prawem)
KPI:	KPI 1 - Liczba uruchomionych systemów teleinformatycznych w podmiotach wykonujących zadania publiczne KPI 2 - Instytucje publiczne otrzymujące wsparcie na opracowywanie usług, produktów i procesów cyfrowych KPI 3 - Liczba pracowników IT podmiotów wykonujących zadania publiczne objętych wsparciem szkoleniowym KPI 4 - Liczba pracowników podmiotów wykonujących zadania publiczne nie będących pracownikami IT, objętych wsparciem szkoleniowym KPI 5 - Użytkownicy nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych KPI 6 – Liczba unikalnych dokumentów tworzonych przez użytkowników platformy dziennie.
Wartość aktualna i docelowa KPI:	Wartość aktualna KPI 1 - 0 Wartość aktualna KPI 2 - 0 Wartość aktualna KPI 3 - 0 Wartość aktualna KPI 4 - 0 Wartość aktualna KPI 5 - 0 Wartość aktualna KPI 6 - 0 Wartość docelowa KPI 1 - 1 Wartość docelowa KPI 2 - 1 Wartość docelowa KPI 3 - 50 Wartość docelowa KPI 4 - 1000 Wartość docelowa KPI 5 - 5000 Wartość docelowa KPI 6 - 5000
Metoda pomiaru KPI	KPI 1: sposób kalkulacji: liczba systemów teleinformatycznych uruchomionych produkcyjnie; źródło danych: protokół odbioru systemu; częstotliwość: pomiar jednorazowy; termin pomiaru wartości docelowej: koniec okresu realizacji projektu (31.12.2028). KPI 2: sposób kalkulacji: liczba instytucji publicznych otrzymujących wsparcie; źródło danych: podpisana umowa o dofinansowanie projektu; częstotliwość: pomiar jednorazowy; termin pomiaru wartości docelowej: początek realizacji projektu. KPI 3: sposób kalkulacji: liczba unikalnych pracowników IT, którzy ukończyli szkolenia; źródło danych: listy obecności na szkoleniach (listy zgłoszonych osób); częstotliwość: po każdym zakończonym szkoleniu (narastająco); termin pomiaru wartości docelowej: 31.12.2028.

	KPI 4: sposób kalkulacji: liczba unikalnych pracowników niebędących pracownikami IT, którzy ukończyli szkolenia; źródło danych: listy obecności na szkoleniach (listy zgłoszonych osób); częstotliwość: po każdym zakończonym szkoleniu (narastająco); termin pomiaru wartości docelowej: 31.12.2028. KPI 5: sposób kalkulacji: liczba unikalnych zarejestrowanych użytkowników platformy; źródło danych: rejestr użytkowników / telemetria platformy; częstotliwość: raz w roku; termin pomiaru wartości docelowej: po każdym roku w okresie trwałości projektu. KPI 6: sposób kalkulacji: liczba unikalnych dokumentów tworzonych przez użytkowników platformy; źródło danych: telemetria platformy; częstotliwość: dziennie; termin pomiaru wartości docelowej: średnia dzienna za każdy dzień roboczy na koniec każdego kwartału w okresie trwałości projektu.
--	---

2.2. Udostępnione e-usługi

Lp.	Nazwa e-usługi	Typ	Zakres oddziaływania	Poziom dojrzałości e-usługi

2.3. Udostępnione informacje sektora publicznego i zdigitalizowane zasoby

Nie dotyczy

2.4. Produkty końcowe przedsięwzięcia

Nazwa produktu	Planowana data wdrożenia
Raport z inicjalnego testu prywatności	01-2027
Dokumentacja analityczna	01-2027
Środowisko/platforma inferencji AI	04-2027
Raport z badań UX i testów użyteczności	11-2027
System teleinformatyczny „Platforma usług inteligentnych RF” wraz z 8 komponentami: Portal PUI RF, Bezpieczeństwo PUI RF, Monitoring i Audytowalność PUI RF, Silniki LLM PUI RF, Bazy wiedzy PUI RF, Hub LLM PUI RF, Moduł ETL PUI RF, Konektory wiedzy PUI RF – wersja produkcyjna.	04-2028
API – wydzielona warstwa usług API dla portalu PUIRF dostępna pod adresem api.mf.gov.pl	04-2028
Raport z testów wydajności	04-2028
Materiały szkoleniowe	04-2028
Środowisko AI Governance	11-2028

Nazwa produktu	Planowana data wdrożenia
Raport z testów bezpieczeństwa	11-2028
Dokumentacja projektowa i powdrożeniowa	12-2028
Materiały informacyjno-promocyjne	12-2028

3. KAMIENIE MIŁOWE

Kamienie milowe	Planowany termin osiągnięcia
Projekt i PMO uruchomione	2027-01-31
PoC technologiczny w CIRF zakończony i odebrany	2027-04-30
Zakończona walidacja funkcjonalna Platformy usług Inteligentnych RF	2027-11-30
System teleinformatyczny „Platforma usług Inteligentnych RF” uruchomiony w wersji produkcyjnej i odebrany	2028-04-30
AI Governance wdrożony, audyt bezpieczeństwa zakończony	2028-11-30
Odbiór końcowy projektu zakończony	2028-12-31

4. KOSZTY

4.1. Koszty ogólne przedsięwzięcia wraz ze sposobem finansowania

Całkowity koszt przedsięwzięcia (netto oraz brutto), w tym	Netto 17 517 752,85 zł Brutto 17 852 300,00 zł	
Procent dofinansowania ze środków UE (brutto)	79,71%	
Procent dofinansowania ze środków z innych źródeł zagranicznych (brutto)		
Procent środków z budżetu państwa (brutto)	20,29%	
Podział całkowitego kosztu przedsięwzięcia na poszczególne lata (netto oraz brutto)	2027	Netto 10 008 814,31 zł Brutto 10 094 120,00 zł
	2028	Netto 7 508 938,54 zł Brutto 7 758 180,00 zł

4.2. Wykaz poszczególnych pozycji kosztowych

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
Oprogramowanie	Dokumentacja analityczna; Dokumentacja projektowa i powdrożeniowa; Środowisko/ platforma inferencji AI; API – wydzielona warstwa usług API dla portalu PUIRF dostępna pod adresem api.mf.gov.pl ; System teleinformatyczny „Platforma usług inteligentnych RF” wraz z 8 komponentami: Portal PUI RF, Bezpieczeństwo	13 485 600,00 zł	Koszty personelu merytorycznego zaangażowanego w realizację projektu. System będzie wytwarzany zasobami CIRF w tym: koordynatorzy budowy baz wiedzy dla 40 departamentów oraz zespół projektowy (25 specjalistów w pełnym zakresie wytworzenia gotowego rozwiązania).

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
	PUI RF, Monitoring i Audytowalność PUI RF, Silniki LLM PUI RF, Bazy wiedzy PUI RF, Hub LLM PUI RF, Moduł ETL PUI RF, Konektory wiedzy PUI RF – wersja produkcyjna.		
Infrastruktura	nie dotyczy	0,00 zł	Projekt nie obejmuje zakupu sprzętu IT, system będzie zbudowany na zasobach infrastrukturalnych CIRF.
Koszty UX i grafiki	Raport z badań UX i testów użyteczności	195 500,00 zł	Usługa zewnętrzna zorientowana na użytkownika (UX/UI)
Bezpieczeństwo	- Raport z inicjalnego testu prywatności; - Środowisko AI Governance; - Raport z testów bezpieczeństwa;	1 179 700,00 zł	Audyty, testy bezpieczeństwa zlecane podmiotom zewnętrznym. Testy będą wykonane również zasobami CIRF.
Wydajność rozwiązań	Raport z testów wydajności	216 000,00 zł	Testy zostaną wykonane zasobami CIRF.
Szkolenia	Materiały szkoleniowe	668 000,00 zł	Szkolenia będą realizowane zasobami własnymi CIRF. Uwzględniono również koszty zewnętrzne związane z organizacją szkoleń oraz wytworzenia materiałów. Materiały będą przygotowane w formatach dostępnych cyfrowo co daje gwarancję równych szans w procesie podnoszenia kompetencji zawodowych pracowników z niepełnosprawnościami.
Działania informacyjno-promocyjne	Materiały informacyjno-promocyjne	12 300,00 zł	Koszt zakupu tablicy informacyjnej, druk plakatów i materiałów informacyjnych.
Koszty zarządzania i wsparcia (w tym wynagrodzenia personelu wspomagającego)	Koszty zarządu (w tym kierowników projektu), asystentów, doradców prawnych,	2 095 200,00 zł	Koszty administracyjne oraz personelu wspomagającego.

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
	finansowych oraz koszty pośrednie.		

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

Całkowity koszt utrzymania trwałości przedsięwzięcia (brutto)	7 313 865,50 zł		Źródło finansowania
Podział całkowitego kosztu utrzymania trwałości przedsięwzięcia na poszczególne lata (netto oraz brutto)	2029	1 377 600,00 zł (brutto) (1 377 600,00 zł netto)	krajowe środki publiczne - budżet państwa
	2030	1 418 928,00 zł (brutto) (1 418 928,00 zł netto)	krajowe środki publiczne - budżet państwa
	2031	1 461 495,84 zł (brutto) (1 461 495,84 zł netto)	krajowe środki publiczne - budżet państwa
	2032	1 505 340,72 zł (brutto) (1 505 340,72 zł netto)	krajowe środki publiczne - budżet państwa
	2033	1 550 500,94 zł (brutto) (1 550 500,94 zł netto)	krajowe środki publiczne - budżet państwa

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

- 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 przedsięwzięcia

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
Brak otrzymania dofinansowania na realizację projektu	Duża	Średnie	Rzetelne przygotowanie dokumentacji oraz poszukiwanie alternatywnych źródeł finansowania.
Niska jakość / niekompletność danych źródłowych	Średnia	Wysokie	Walidacja i czyszczenie danych, narzędzia ETL/OCR, kryteria jakości, pilotaż
Złożoność integracji, zwłaszcza z EZD PUW MF	Duża	Średnie	Wczesna analiza API, PoC, dedykowany zespół integracyjny, bufor w harmonogramie
Zależność od komponentów open-source i zarządzanie ich aktualizacjami	Średnia	Średnie	Przypięcie wersji (digest), testy kontraktowe przy aktualizacji, kontrolowane okna zmian.
Przeciążenie współdzielonej infrastruktury GPU przez wiele usług i tryby agentowe	Duża	Średnie	Limity współbieżności i kolejkowanie, priorytetyzacja usług, monitoring zużycia zasobów, rozbudowa środowiska.
Opóźnienia legislacyjne (oczekiwanie na regulacje dotyczące AI)	Średnia	Wysokie	Realizacja w istniejącym otoczeniu prawnym; objęcie AI Governance; gotowość do dostosowania po wejściu regulacji.
Niska adopcja przez użytkowników	Duża	Średnie	Zarządzanie zmianą, szkolenia, sieć ambasadorów. Realne obniżenie barier wejścia i umożliwienie obsługi systemu przez zróżnicowaną grupę pracowników Resortu Finansów.
Brak wystarczających zasobów kadrowych do realizacji projektu	Średnia	Średnie	Odpowiednie zarządzanie zasobami ludzkimi (budowanie portfolio kandydatów); otwarcie rekrutacji w celu uzupełnienia kompetencji w zespołach
Przekroczenie harmonogramu realizacji projektu	Średnia	Niskie	Monitorowanie postępu rzeczowego i finansowanego projektu; cykliczne spotkania zespołu projektowego; współpraca z komitetem sterującym.

5.2. Ryzyka wpływające na utrzymanie efektów

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
Zmiana modelu wyszukiwania (embeddingu) wymuszająca ponowną indeksację	Duża	Niskie	Stabilizacja wyboru modelu; spójny model dla wprowadzania i zapytań; planowanie okien reindeksacji.
Utrata kadr i kompetencji utrzymaniowych	Duża	Średnie	Dokumentacja, szkolenia, redundancja kompetencji, umowy wsparcia.
Brak ciągłości finansowania utrzymania	Duża	Niskie	Zabezpieczenie kosztów utrzymania w budżetach dysponentów; plan 5-letni.
Zmiany regulacyjne (AI Act, RODO)	Średnia	Średnie	Monitoring prawny, elastyczna architektura, okresowe audyty zgodności.
Degradacja jakości odpowiedzi / halucynacje modeli	Średnia	Średnie	Grounding na danych, brak konfabulacji przy braku trafień, ewaluacja online/ offline, pętla informacji zwrotnej.

6. OTOCZENIE PRAWNE

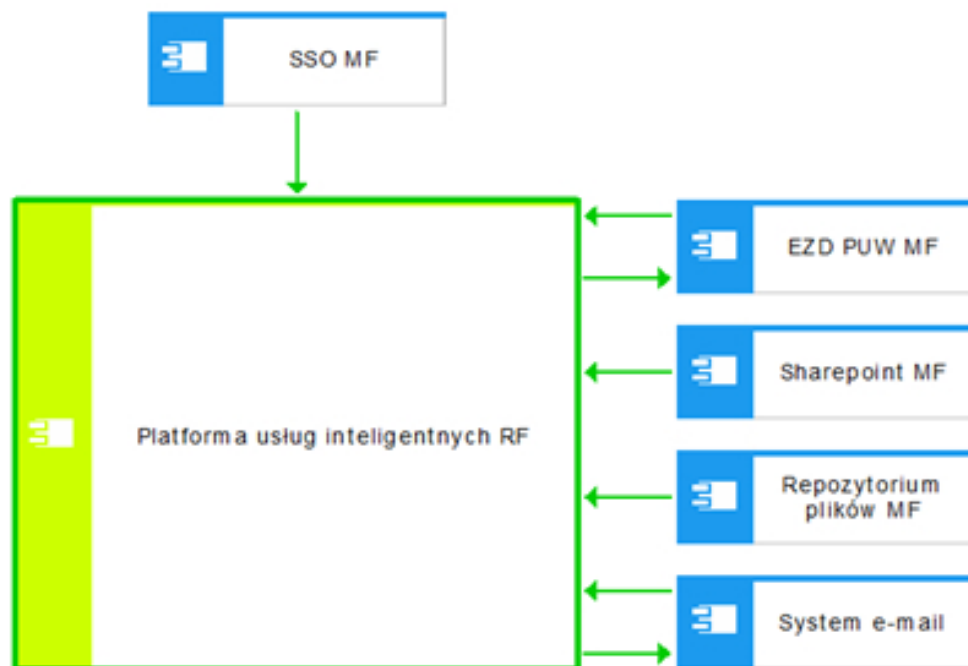
Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
1	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE - ogólne rozporządzenie o ochronie danych, RODO.	TAK /NIE		
2	Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000; t.j. Dz.U. z 2019 r. poz. 1781)	TAK /NIE		
3	Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne i Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla	TAK /NIE		

Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
	rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.			
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 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych.	TAK /NIE		
6	Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa	TAK /NIE		
7	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany wybranych rozporządzeń i dyrektyw UE - akt w sprawie sztucznej inteligencji, AI Act	TAK /NIE		
8	Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach	TAK /NIE		
9	Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych	TAK /NIE		
10	Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. - eIDAS	TAK /NIE		
11	Ustawa z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego	TAK /NIE		
12	Ustawa z dnia 29 sierpnia 1997 r. - Ordynacja podatkowa	TAK /NIE		
13	Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych	TAK /NIE		
14	Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych	TAK /NIE		
15	Ustawa z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego	TAK /NIE		
16	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/2854 z dnia 13 grudnia 2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz w sprawie	TAK /NIE		

Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
	zmiany 1 rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828 (akt w sprawie danych)			
17	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 z dnia 30 maja 2022 r. w sprawie europejskiego zarządzania danymi i zmieniające rozporządzenie (UE) 2018/1724 (akt w sprawie zarządzania danymi)	TAK /NIE		
18	Rozporządzenie Ministra Cyfryzacji z dnia 10 marca 2020 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników	TAK /NIE		
19	Rozporządzenie Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych	TAK /NIE		
20	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2026/1744 z dnia 8 lipca 2026 r. w sprawie zmiany rozporządzeń (UE) 2024/1689, (UE) 2018/1139 i (UE) 2023/1230 w odniesieniu do uproszczenia wdrażania zharmonizowanych przepisów dotyczących sztucznej inteligencji	TAK /NIE		
21	Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS2)	TAK /NIE		

7. ARCHITEKTURA

7.1. Widok kooperacji aplikacji



Legenda



Lista systemów wykorzystywanych w przedsięwzięciu

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
1	EZD PUW MF	Ministerstwo Finansów	Elektroniczne Zarządzanie Dokumentacją Podlaskiego Urzędu Wojewódzkiego (Ministerstwa Finansów) to system wspierający zarządzanie elektroniczną dokumentacją	Istniejący	

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			Ministerstwa Finansów. System wykorzystywany w szczególności do obiegu korespondencji wewnątrz organizacji ale nie tylko – istnieje możliwość przesyłania dokumentów międzyresortowo poprzez ePismo. System nie prowadzi rejestrów publicznych. Integracja z systemem poprzez API.		
2	Platforma usług inteligentnych RF	Ministerstwo Finansów	Platforma usług inteligentnych Resoru Finansów - bezpieczne i suwerenne środowisko usług sztucznej inteligencji dla Resortu Finansów to centralny system wspierający pracę zespołów RF poprzez dostarczenie usług inteligentnych. W systemie nie ma uruchomionych rejestrów publicznych. Główne komponenty/ moduły systemu: • Bazy wiedzy PUI RF – gromadzenie, wektoryzowanie, przeszukiwanie, udostępnianie dokumentów • Bezpieczeństwo PUI RF – autoryzacja i autentykacja użytkowników, audytowalność systemów • Hub LLM PUI RF – zarządzanie modelami AI, obsługa limitów, uprawnień, logów audytu oraz routingu do silnika	Planowany	

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			LLM • Konektory wiedzy PUI RF – obsługa komunikacji do i z systemów dziedzinowych • Moduł ETL PUI RF – przetwarzanie i transformacja danych • Monitoring i audytowalność PUI RF- monitoring parametrów SLA, dostęp do logów audytu • Portal PUIRF z uwzględnieniem obowiązujących standardów WCAG/ UX[AG27.1][AG27.2]- udostępnianie funkcjonalności dla użytkowników, zarządzanie dokumentami, zarządzanie i generowanie dokumentów, obsługa wnioskowania o dostępy, obsługa limitów użycia tokenów. Portal składa się z dwóch obszarów ai.mf.gov.pl (część informacyjna, niespersonalizowana dla niezalogowanych użytkowników) oraz moje.mf.gov.pl (część funkcjonalna, spersonalizowana dla zalogowanych użytkowników). • API – wydzielona warstwa usług API dla portalu PUIRF dostępna pod adresem api.mf.gov.pl i komunikująca się między innymi z silnikiem LLM. • Silniki LLM PUI RF – obsługa inferencji wywoływana przez API.		

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			System nie prowadzi rejestrów publicznych. System udostępnia usługi przez API.		
3	Repozytorium plików MF	Ministerstwo Finansów	Repozytoria plików Ministerstwa Finansów to system wspierający wymianę i składowanie dokumentów wewnątrz organizacji. System nie prowadzi rejestrów publicznych. Integracja z systemem przez API z uwzględnieniem ACL.	Istniejący	
4	Sharepoint MF	Ministerstwo Finansów	Sharepoint Ministerstwa Finansów to system wspierający zarządzanie dokumentami i współpracę zespołową na udostępnionych zasobach. System nie prowadzi rejestrów publicznych. Integracja z systemem przez API.	Istniejący	
5	SSO MF	Ministerstwo Finansów	System Single Sign-On Ministerstwa Finansów to system wspierający, udostępniający aplikacjom zewnętrznym i wewnętrznym funkcje uwierzytelniania klientów KAS w oparciu o różne metody logowania (węzeł krajowy, dane podatkowe, login i hasło, mObywatel). System nie prowadzi rejestrów publicznych. Integracja z systemem przez API.	Istniejący	
6	System e-mail	Ministerstwo Finansów	System e-mail @mf.gov.pl to system wspierający wymianę poczty	Istniejący	

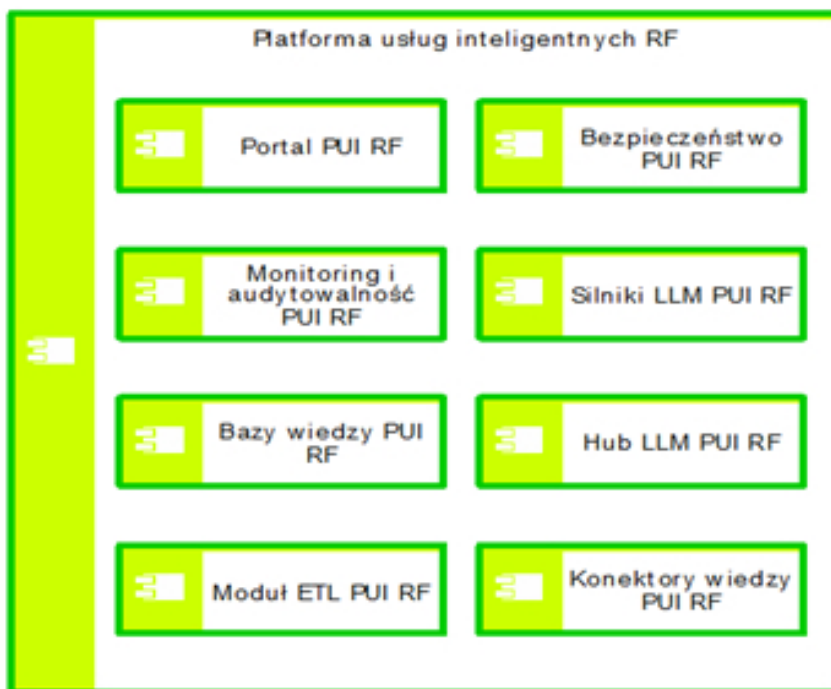
Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			elektronicznej Resortu Finansów. System nie prowadzi rejestrów publicznych. Integracja z systemem przez API.		

Lista przepływów

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
1	Platforma usług inteligentnych RF	EZD PUW MF	Zasilanie EZD dokumentami wygenerowanymi przez Platformę, w szczególności * znak pisma * dokument * metadane dokumentu	Odwołanie bezpośrednie	krytyczny dla sukcesu projektu	Usługa REST
2	EZD PUW MF	Platforma usług inteligentnych RF	Pobieranie danych (dokumentów) w szczególności * znak pisma * dokument * metadane dokumentu	Odwołanie bezpośrednie	krytyczny dla sukcesu projektu	Usługa REST
3	Platforma usług inteligentnych RF	System e-mail	Przygotowanie wkładu do odpowiedzi na wiadomości: * email nadawcy / odbiorcy * treść wiadomości * data wiadomości * załącznik	Odwołanie bezpośrednie	krytyczny dla sukcesu projektu	SMTP
4	Sharepoint MF	Platforma usług	Pobieranie danych	Odwołanie bezpośrednie	krytyczny dla sukcesu	Usługa REST (SharePoint)

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
		inteligentnych RF	(dokumentów) w szczególności: * plik (dokument) * data dokumentu * metadane dokumentu		projektu	REST API / Microsoft Graph)
5	System e-mail	Platforma usług inteligentnych RF	Pobieranie wiadomości: * email nadawcy / odbiorcy * treść wiadomości * data wiadomości * załącznik	Odwołanie bezpośrednie	krytyczny dla sukcesu projektu	IMAP
6	Repozytorium plików MF	Platforma usług inteligentnych RF	Pobieranie danych (dokumentów) w szczególności: * plik (dokument) * data dokumentu * metadane dokumentu	Odwołanie bezpośrednie	krytyczny dla sukcesu projektu	Usługa REST
7	SSO MF	Platforma usług inteligentnych RF	* dane użytkownika (imie, nazwisko, identyfikator, grupy AD)	Odwołanie bezpośrednie	krytyczny dla sukcesu projektu	Protokół OIDC / SAML 2.0

7.2. Kluczowe komponenty architektury rozwiązania



Legenda



7.3. Przyjęte założenia technologiczne

Lp.	Obszar	Założenie technologiczne
1.	Infrastruktura	Fizyczne serwery GPU.
2.	Sieć i bezpieczeństwo	Szyfrowanie danych w spoczynku i w tranzycie (TLS). Uwierzytelnianie przez Active Directory (SSO, MFA); izolacja danych departamentów (multi-tenant). Mechanizmy DLP, guardrails (ochrona przed prompt injection i wyciekiem danych), pełny audyt i logowanie.
3.	Standardy wymiany danych	Podejście API-first; integracje przez standardowe protokoły: REST/JSON, OAuth2/SAML (dla AD). Zasilanie danymi przez konektory ETL (SharePoint MF, repozytorium plików MF, e-mail,

Lp.	Obszar	Założenie technologiczne
		EZD PUW MF).
4.	Systemy operacyjne serwerowe	Środowisko serwerowe oparte na systemie operacyjnym z rodziny Linux (hosty kontenerów). Brak uzależnienia od konkretnego producenta – rozwiązania open-source.
5.	Bazy danych	Baza wektorowa do wyszukiwania semantycznego (RAG) oraz baza relacyjna na metadane, sesje i polityki. Preferowane rozwiązania open-source.
6.	Serwery aplikacji	Architektura kontenerowa/mikrouslugowa (Kubernetes).
7.	Portale	
8.	Inne	Modele open-weight (m.in. PLLuM/Bielik oraz wielojęzyczne).

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

7.5. Bezpieczeństwo

Planowany poziom zapewnienia bezpieczeństwa (w rozumieniu przepisów § 19 rozporządzenia 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 (Dz. U. poz. 773)) 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

Uwierzytelnianie przez Active Directory (SSO, MFA); autoryzacja oparta o role i strukturę organizacyjną (RBAC, dane z rejestru pracowników).

- Izolacja danych departamentów (multi-tenant) – użytkownik widzi wyłącznie wiedzę zgodną z uprawnieniami.
- Przetwarzanie danych wrażliwych lokalnie; do modelu chmurowego trafiają wyłącznie dane dopuszczone i zanonimizowane (mechanizmy DLP).
- Szyfrowanie danych w spoczynku i w transzycie.
- Pełny audyt i logowanie zapytań oraz odpowiedzi systemu.
- Zabezpieczenia przed prompt injection, wyciekami danych i halucynacjami (guardrails, weryfikacja źródeł w RAG).
- Zgodność z RODO, KRI, ustawą o KSC oraz AI Act.
- Cykliczne testy bezpieczeństwa (pentesty), zarządzanie podatnościami, kopie zapasowe i plan ciągłości działania (BCP/DR).

~~-dodatkowe zabezpieczenia powyżej wymogów KRI: należy wskazać uzasadnienie~~