

OPIS ZAŁOŻEŃ PRZEDSIĘWZIĘCIA INFORMATYCZNEGO O PUBLICZNYM ZASTOSOWANIU

Tytuł przedsięwzięcia	AI-SDLC: wsparcie procesów wytwarzania oprogramowania przez narzędzia AI w Centrum e-Zdrowia		
Wnioskodawca	Minister Zdrowia		
Beneficjent	Centrum e-Zdrowia		
Partnerzy	Nie dotyczy		
Źródło finansowania	Fundusze Europejskie na Rozwój Cyfrowy, Działanie FERC.02.01 Wysoka jakość i dostępność e-usług publicznych. Budżet państwa cz. 46 - Zdrowie		
Całkowity koszt przedsięwzięcia	27 651 973,08 zł		
Planowany okres realizacji przedsięwzięcia	01-2027 do 08-2029		
Osoba kontaktowa	Jarosław Rostkowski	j.rostkowski@cez.gov.pl	602416698

1. POWODY PODJĘCIA PRZEDSIĘWZIĘCIA

1.1. Identyfikacja problemu i potrzeb

CeZ realizuje procesy wytwarzania, rozwoju, utrzymania i zapewniania jakości oprogramowania w wielu projektach, wykorzystując rozproszone repozytoria kodu, narzędzia CI/CD, systemy zadaniowe, dokumentację oraz narzędzia jakości i bezpieczeństwa. Brakuje jednej, kontrolowanej i audytowalnej warstwy wykorzystania AI w całym cyklu życia oprogramowania. Powoduje to niejednolite praktyki analizy kodu, testowania i dokumentowania, rozproszenie wiedzy, wydłużony onboarding, trudności w wykrywaniu podatności i długu technicznego oraz brak porównywalnych danych o jakości procesów. Rośnie również ryzyko niekontrolowanego korzystania z zewnętrznych modeli AI i przekazywania do nich danych CeZ. Obecne użycie narzędzi AI nie pokrywa obszaru wytwarzania oprogramowania (SDLC), zatem projektowane rozwiązanie wypełni istniejącą lukę kontrolną.

Odpowiedzią będzie wewnątrzadministracyjna e-usługa A2A „e-Koordynator SDLC AI”, udostępniana przez system AI-SDLC zespołom CeZ, w tym pracownikom z niepełnosprawnościami i właścicielom biznesowym systemów e-zdrowia. Zapewni ona kontrolowane wsparcie AI w analizie wymagań i kodu, przeglądzie zmian, testowaniu, dokumentowaniu, zarządzaniu wiedzą, onboardingu i raportowaniu jakości, przy pozostawieniu decyzji uprawnionym użytkownikom.

Przedsięwzięcie obejmuje budowę trzech systemów: AI-SDLC – koordynującego procesy SDLC i udostępniającego e-usługę; AI-Gateway – będącego kontrolowanym punktem dostępu do modeli AI; oraz CeZ AI – realizującego zadania wymagające podwyższonej kontroli nad kodem i danymi. Trzy zbudowane systemy zostaną zintegrowane z trzema istniejącymi systemami CeZ:

Repozytoria kodu i narzędzia CI/CD CeZ, Baza wiedzy i zadań CeZ oraz Systemy bezpieczeństwa CeZ. Zintegracja umożliwi kontrolowaną wymianę danych, zadań i wyników analiz. Zintegrowane systemy pozostaną źródłami prawdy w swoich obszarach. Sześć systemów i współdzielona infrastruktura tworzą Platformę AI-SDLC.

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
Centrum e-Zdrowia	• Sztuczna inteligencja wchodzi do procesu wytwórczego bez jednej, kontrolowanej bramy – jej użycie pozostaje nieujednolicone i nieewidencjonowane, poza kontrolą dostępu i nadzorem nad danymi przekazywanymi do modeli. • Niejednolity, zależny od wykonawców przegląd zmian w kodzie (code review) prowadzi do niespójności standardami i nadmiernego obciążenia doświadczonych specjalistów w sytuacji braków kadrowych dla specjalistycznych dziedzin • Niewystarczające i nierównomierne, zależne od wykonawcy pokrycie testami (testowanie) obniżająca jakość i niezawodność portfela systemów. • Brak skorelowanej analizy bezpieczeństwa w procesie wytwórczym ze względu na zależność sposobu realizacji standardów od zespołu stale powiększając fragmentację systemów i rejestrów e-zdrowia • Rozproszenie wiedzy projektowej (dokumentowanie i zarządzanie wiedzą) wpływające na opóźnienia we wdrażaniu nowych rozwiązań w sektorze. • Narastający dług techniczny i duplikacja komponentów (zarządzanie zależnościami) – podnoszą koszt utrzymania i stan niespójności architektonicznej. • Brak porównywalnych, mierzalnych danych o jakości i bezpieczeństwie procesu (raportowanie jakości) – utrudnia priorytetyzację ryzyk i decyzje zarządcze - skutecznie ograniczając możliwości restrukturyzacji i konsolidacji systemów dzielących tożsame zakresy funkcjonalne i potrzeby techniczne.	1
Ministerstwo Zdrowia	• Ograniczone tempo wdrażania zmian wymaganych przepisami powoduje opóźnienia realizacji polityki publicznej w cyfryzacji ochrony zdrowia i wpływa na zaufanie opinii publicznej wobec e-zdrowia. • Niewystarczający nadzór nad ryzykiem jakościowym i bezpieczeństwa systemów – wpływa na spowolnienie propagacji rozwiązań IT mających bezpośredni wpływ na jakość i czas decyzji zarządczych w sektorze ochrony zdrowia • Rosnący koszt utrzymania systemów e-zdrowia – obciąża budżet przy rosnącej	1

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
	liczbie systemów, a obecne rozproszenie procesów koszty zwiększa.	
Podmioty administracji publicznej i instytucje sektora ochrony zdrowia (AOTMiT, URPL, GIF, NFZ, CMJ, NCK, CEM, NIL, NIA, KRDL)	• Wydłużona reakcja na zmiany i incydenty w systemach centralnych wywołuje opóźnienia i spadek jakości realizacji zadań publicznych przez instytucje sektora • Ograniczona spójność architektury wykorzystywanych systemów wpływa na rosnące koszty ich utrzymania oraz ograniczenia możliwości ich rozwoju względem potrzeb instytucji realizujących zadania publiczne w sektorze ochrony zdrowia	10
Podmioty wykonujące działalność leczniczą oraz personel medyczny	• Opóźnienia we wdrażaniu zmian w systemach e-zdrowia – utrudniają codzienną pracę i obsługę świadczeń oraz ograniczają możliwość wsparcia tych podmiotów (szczególnie w zakresie procesów restrukturyzacji, konsolidacji czy obsługi inwestycji). • Ograniczona niezawodność narzędzi obsługujących e-recepty, e-skierowania, dokumentację medyczną i zdarzenia medyczne skutkuje większymi kosztami obsługi, zwiększonymi kolejkami oraz zmniejszeniem jakości dostępu do świadczeń przez nie udzielanych. • Zwiększone obciążenie organizacyjne placówek przy incydentach – przenosi koszt zakłóceń na personel.	25000
Usługobiorcy	• Ograniczona niezawodność dostępu do e-usług zdrowotnych i zasoby kadrowe wobec zwiększających się wymagań i zagrożeń informatycznych prowadzi do czasowych niedostępności w realizacji usług, dostępie do danych medycznych oraz informacji ubezpieczeniowej w kraju i za granicą. • Wolniejsza adaptacja systemów do potrzeb dostępności wpływa na mniejszą jakość lub opóźnienia w zakresie wdrażania rozwiązań dedykowanych dla osób ze szczególnymi potrzebami.	37332500
Pracownicy Centrum e-Zdrowia (zespoły wytwórcze)	• Przegląd zmian w kodzie (code review) i kontrola jakości spoczywają na najbardziej doświadczonych specjalistach – obciążają ich pracą powtarzalną i odciągają od zadań strategicznych merytorycznie, zwłaszcza przy brakach kadrowych w wąskich dziedzinach. • Procesy onboardingu, a także związane z odtworzeniem kontekstu projektowego (kod,	536

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
	zależności, decyzje) wymaga nieefektywnego przeszukiwania wielu rozproszonych źródeł oraz wiedzy ograniczonej ilości ekspertów i weryfikacji zróżnicowanych pomiędzy nimi standardów i założeń – ograniczając efektywność czasowo-finansową oraz przedłużając procesy wytwórcze w czasie. • Tworzenie i ocena testów oraz analiza bezpieczeństwa realizowane są ręcznie i w sposób niejednolity w zespołach zwiększając nakład pracy i przesuwają wykrywanie błędów na późne etapy. • Praktyki i narzędzia różnią się między zespołami i wykonawcami – utrudniają współpracę, przechodzenie między projektami i utrzymanie jednolitej jakości.	
Pracownicy Ministerstwa Zdrowia (Właściciele biznesowi systemowych, inicjatorzy, eksperci dla systemów IT obsługiwanych przez CeZ)	• Definiowanie i uzgadnianie wymagań oraz ocena ich wykonalności wymagają wielu iteracji z zespołami technicznymi – spowalniają inicjowanie i przygotowanie zmian. • Komunikacja z zespołami technicznymi jest utrudniona brakiem wspólnego kontekstu i jednolitego opisu potrzeb – wydłuża uzgodnienia i zwiększa liczbę nieporozumień. • Tempo rozwoju cyfrowego sektora przy jednoczesnym stale rosnącym zakresie zadań publicznych jednostki uniemożliwia jej komunikację i nadzór właścicielski nad systemami, powierzonymi CeZ, w tym efektywną komunikację biznesowo-techniczną.	50

1.2. Opis stanu obecnego

CeZ prowadzi procesy wytwarzania, rozwoju, utrzymania i zapewniania jakości oprogramowania w wielu równoległych projektach informatycznych. Proces wytwórczy obejmuje m.in. analizę wymagań, projektowanie, implementację, testowanie, code review, wdrożenia, utrzymanie, obsługę zmian oraz dokumentowanie rozwiązań technicznych i architektonicznych. Zespoły korzystają z narzędzi repozytoryjnych do kontroli wersji kodu, systemów zgłoszeniowych, narzędzi CI/CD, dokumentacji technicznej oraz narzędzi kontroli jakości i bezpieczeństwa. Obecne środowisko rozwoju oprogramowania ma charakter rozproszony i nie zapewnia jednej, kontrolowanej warstwy wspierającej zespoły w sposób jednolity, audytowalny i zgodny z wymaganiami bezpieczeństwa, ochrony danych, zarządzania jakością oraz zarządzania kosztami utrzymania.

Wiedza o systemach, modułach, zależnościach, decyzjach projektowych, standardach implementacyjnych i przyczynach zmian jest przechowywana w wielu miejscach: w kodzie źródłowym, historii commitów, pull requestach, zgłoszeniach, dokumentacji projektowej, architektonicznej oraz w wiedzy indywidualnych ekspertów. Utrudnia to szybkie odtworzenie

kontekstu projektowego, aktualizację dokumentacji, porównywanie jakości między projektami oraz ograniczanie ryzyka utraty wiedzy przy zmianach kadrowych.

Stan oczekiwany zakłada wdrożenie objęcie wykorzystania sztucznej inteligencji w procesach wytwarzania i utrzymania oprogramowania jednolitą, audytowalną warstwą kontroli - platformą AI-SDLC o horyzontalnym zastosowaniu w CeZ, wspierającą systemy odpowiedzialne za działanie e-usług zdrowotnych. Platforma ma wspierać bezpieczne, audytowalne i powtarzalne wykorzystanie AI w kolejnych fazach cyklu życia oprogramowania – analizie wymagań, projektowaniu, implementacji, testowaniu, dokumentowaniu, wdrożeniu i utrzymaniu – przy zachowaniu kontroli nad danymi, uprawnieniami, jakością wyników, rejestrowaniem działań oraz zgodnością z wymaganiami bezpieczeństwa i zarządzania systemami publicznymi.

2. EFEKTY PRZEDSIĘWZIĘCIA

W jaki sposób przedsięwzięcie realizuje Strategię Cyfryzacji Państwa?

Przedsięwzięcie wpisuje się w kierunki Strategii Cyfryzacji Polski do 2035 r. poprzez wzmacnianie zdolności administracji publicznej do utrzymania i rozwoju kluczowych usług cyfrowych, podnoszenie bezpieczeństwa cyfrowego, rozwój wykorzystania sztucznej inteligencji w administracji oraz zwiększanie suwerenności cyfrowej państwa. Przedsięwzięcie wzmacnia suwerenność cyfrową wszystkich obsługiwanych przez Centrum e-Uслуг oraz wpływa na wzrost ich jakości, spójności i interoperacyjności w architekturze informacyjnej państwa. Ponadto realizacja projektu wspiera automatyzację weryfikacji jakości i bezpieczeństwa kodu oraz budowę współdzielonej bazy wiedzy, co ułatwia audytowalność, inwentaryzację zasobów i bezpieczną adopcję otwartych standardów i oprogramowania w administracji publicznej.

Zakres przedsięwzięcia wpisuje się przede wszystkim w:

Cel 1.4.3: Architektura Informacyjna Państwa stanowi powszechną i ugruntowaną metodę strategicznego zarządzania informatyzacją państwa

Cel 2.3.1: Publiczne systemy teleinformatyczne i rejestry publiczne są interoperacyjne;

Cel 3.2.4: Sztuczna inteligencja oraz inne nowe technologie cyfrowe są wykorzystywane w sposób bezpieczny i skuteczny dla poprawy jakości opieki nad pacjentem

Cel 4.2.1: Rozwój gospodarki, przemysłu cyfrowego i dobrostanu społecznego jest wspierany przez sprawny i skoordynowany ekosystem sztucznej inteligencji;

Cel 4.6.1: Polska administracja publiczna w większym stopniu wykorzystuje otwarte oprogramowanie.

Przedsięwzięcie przyczynie się do osiągnięcia wskaźnika efektywności określonego dla Strategii nr 15: „Odsetek urzędów administracji publicznej wykorzystujących technologie sztucznej inteligencji”

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

Przedsięwzięcie wpisuje się w realizację celów wynikających z następujących dokumentów strategicznych:

- Strategia na rzecz Odpowiedzialnego Rozwoju
- Polityka rozwoju sztucznej inteligencji w Polsce do 2030 r
- Program Zdrowa Przyszłość. Ramy strategiczne rozwoju systemu ochrony zdrowia na lata 2021-2027
- Program rozwoju e-zdrowia w Polsce na lata 2022 – 2027.

Realizacja postulatów ze wskazanych polityk nastąpi poprzez wdrożenie horyzontalnego systemu back-office wspierającego procesy wytwarzania i utrzymania e usług, wykorzystanie narzędzi sztucznej inteligencji w sposób kontrolowany i audytowalny oraz rozwój

ustrukturyzowanego wykorzystania danych w procesach decyzyjnych. Projekt przyczynia się do zwiększenia efektywności działania administracji, poprawy jakości systemów e zdrowia oraz standaryzacji i interoperacyjności procesów, zgodnie z kierunkami rozwoju e państwa, e zdrowia i wykorzystania AI w administracji publicznej.

2.1. Cele i korzyści wynikające z przedsięwzięcia

Cel - 1	Usprawnienie działania Centrum e-Zdrowia oraz zwiększenie jakości e-usług publicznych w zakresie e-Zdrowia
Cel strategiczny	Strategia Cyfryzacji Państwa – zakres przedsięwzięcia wpisuje się w cele szczegółowe: Cel 1.4.3: Architektura Informacyjna Państwa stanowi powszechną i ugruntowaną metodę strategicznego zarządzania informatyzacją państwa Cel 2.3.1: Publiczne systemy teleinformatyczne i rejestry publiczne są interoperacyjne; Cel 3.2.4: Sztuczna inteligencja oraz inne nowe technologie cyfrowe są wykorzystywane w sposób bezpieczny i skuteczny dla poprawy jakości opieki nad pacjentem Cel 4.2.1: Rozwój gospodarki, przemysłu cyfrowego i dobrostanu społecznego jest wspierany przez sprawny i skoordynowany ekosystem sztucznej inteligencji; Cel 4.6.1: Polska administracja publiczna w większym stopniu wykorzystuje otwarte oprogramowanie. Strategia na rzecz Odpowiedzialnego Rozwoju do 2020 (z perspektywą do 2030 r.) – Zakres przedsięwzięcia wpisuje się w cel szczegółowy III – skuteczne państwo i instytucje służące włączeniu społecznemu i gospodarstwu – Obszar: E-państwo.. Zdrowa Przyszłość. Ramy strategiczne rozwoju systemu ochrony zdrowia na lata 2021-2027. Zakres przedsięwzięcia wpisuje się w Cel 3.3 [Innowacje] Rozwój i upowszechnianie stosowania nowoczesnych i nowatorskich rozwiązań w ochronie zdrowia. Program rozwoju e-zdrowia w Polsce na lata 2022 – 2027. Zakres przedsięwzięcia wpisuje się w cel szczegółowy programu: Cel 4.2 Rozwój usług back- office. Polityka rozwoju sztucznej inteligencji w Polsce do 2030 r. Zakres przedsięwzięcia wpisuje się w Cel 4.1 Cel i działania dla rozwoju AI w administracji, cel szczegółowy nr 3: Sprawne Państwo wykorzystujące rozwiązania sztucznej inteligencji.
Korzyść:	- Sprawniejsze funkcjonowanie Centrum e-Zdrowia – szybsze, bardziej przewidywalne i tańsze dostarczanie oraz utrzymanie systemów, utrzymywane w okresie eksploatacji - Wyższa jakość i bezpieczeństwo publicznych e-usług zdrowotnych, wynikające z wcześniejszego eliminowania wad i długu technicznego, odczuwane przez obywateli i podmioty sektora - Krótszy cykl od potrzeby biznesowej do wdrożenia zmiany oraz lepsza współpraca właścicieli biznesowych z zespołami, utrzymywana w kolejnych latach - Poprawa efektywności oraz jakości realizowanych usług cyfrowych w obszarze ochrony zdrowia. - Ograniczenie ryzyka niekontrolowanego użycia narzędzi sztucznej inteligencji. - Zwiększenie kontroli i audytowalności nowoczesnych rozwiązań AI stosowanych w procesach back-office administracji publicznej. - Wzmocnienie odporności i suwerenności cyfrowej – niezależność od

	pojedynczego dostawcy i gotowość do stosowania modeli krajowych i europejskich w kluczowych procesach rozwojowych dla sektora - Wzmocnienie zdolności do bezpiecznego utrzymania i rozwoju systemów teleinformatycznych, będących fundamentem publicznych e-usług zdrowia.
KPI:	KPI 1: Instytucje publiczne otrzymujące wsparcie na opracowanie usług, produktów i procesów cyfrowych. KPI 2: Liczba udostępnionych usług wewnątrzadministracyjnych A2A. KPI 3: Liczba uruchomionych systemów teleinformatycznych w podmiotach wykonujących zadania publiczne. KPI 4: Udział repozytoriów zintegrowanych z AI-SDLC, należących do systemów zakwalifikowanych do wdrożenia w portfolio CeZ
Wartość aktualna i docelowa KPI:	KPI 1: Wartość aktualna (2026): 0 szt KPI 2: Wartość aktualna (2026): 0 szt KPI 3: Wartość aktualna (2026): 0 szt KPI 4: Wartość aktualna (2026): 0 % KPI 1: Wartość docelowa (2027):1 szt KPI 2 Wartość docelowa (2029):1 szt KPI 3: Wartość docelowa (2029): 1 szt KPI 4: Wartość docelowa (2029): 50%
Metoda pomiaru KPI	KPI 1: Źródło danych: Podpisane porozumienie o dofinansowanie projektu w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 Działanie FERC.02.01 Wysoka jakość i dostępność e-usług publicznych Termin i częstotliwość pomiaru: Styczeń 2027, jednorazowo Metoda i sposób pomiaru: wskaźnik zostanie zmierzony poprzez potwierdzenie objęcia CeZ wsparciem w ramach projektu dofinansowanego ze środków FERC. KPI 2: Źródło danych: Osiągnięcie wskaźnika produktów zostanie stwierdzone na podstawie protokołu odbioru. Termin i częstotliwość pomiaru: sierpień 2029, jednorazowo Metoda i sposób pomiaru: wskaźnik zostanie zmierzony poprzez potwierdzenie udostępnienia jednej usługi wewnątrzadministracyjnej A2A w ramach projektu. Wartość docelowa została przyjęta na poziomie 1 szt., ponieważ projekt zakłada uruchomienie jednej platformy AI-SDLC jako rozwiązania back-office wspierającego procesy wytwarzania i utrzymania oprogramowania w CeZ. KPI 3: Źródło danych: Protokół odbioru końcowego wdrożenia systemu.

	Termin i częstotliwość pomiaru: sierpień 2029, jednorazowo Metoda i sposób pomiaru: wskaźnik zostanie zmierzony poprzez potwierdzenie uruchomienia systemu teleinformatycznego AI-SDLC w CeZ. Wartość docelowa została przyjęta na poziomie 1 szt., ponieważ projekt obejmuje wdrożenie jednej platformy AI-SDLC jako rozwiązania back-office wspierającego procesy SDLC. KPI 4: Źródło danych: Wykaz repozytoriów objętych wdrożeniem na podstawie rejestru integracji oraz protokołów wdrożenia systemu AI-SDLC obejmujący zintegrowane repozytoria systemowe. Termin i częstotliwość pomiaru: sierpień 2029, jednorazowo Metoda i sposób pomiaru: Wskaźnik potwierdzi faktyczne objęcie platformą AI-SDLC repozytoriów należących do systemów zakwalifikowanych do wdrożenia w portfolio CeZ. Osiągnięcie wskaźnika będzie oznaczało, że platforma AI-SDLC została zintegrowana z istotną częścią środowiska wytwórczego CeZ, co umożliwi stosowanie jednolitych mechanizmów analizy kodu, kontroli jakości, bezpieczeństwa, testowania i raportowania w projektach objętych wdrożeniem. Wartość docelowa na poziomie 50% zakwalifikowanych projektów z portfolio systemów CeZ została przyjęta jako realistyczna dla pierwszego etapu wdrożenia platformy AI-SDLC po uruchomieniu usługi. Integracją zostaną objęte przede wszystkim repozytoria najważniejszych systemów CeZ - których kwalifikacja odbędzie się w pierwszej fazie projektu (KM1) poprzez wykorzystanie kryteriów jakościowych - t.j. możliwości adaptacji w czasie, braku ograniczeń prawno-formalnych i kryteriów jakościowych dla potencjału wykorzystania mechanizmów automatycznej analizy kodu, jakości, bezpieczeństwa i testowania dla ich obecnego standardu wytwórczego. Centrum e-Zdrowia zarządza obecnie ponad 50 systemami dziedzinowymi, rejestrami publicznymi, systemami Ministerstwa Zdrowia i podmiotów ochrony zdrowia oraz systemami umożliwiającymi udzielanie i weryfikację świadczeń przez personel medyczny.
Cel - 2	Zwiększenie wykorzystania zmodernizowanych procesów cyfrowych SDLC przez zespoły CeZ w celu poprawy jakości e-usług publicznych
Cel strategiczny	Strategia Cyfryzacji Państwa – zakres przedsięwzięcia wpisuje się w cele szczegółowe: Cel 1.4.3: Architektura Informacyjna Państwa stanowi powszechną i ugruntowaną metodę strategicznego zarządzania informatyzacją państwa Cel 2.3.1: Publiczne systemy teleinformatyczne i rejestry publiczne są interoperacyjne; Cel 3.2.4: Sztuczna inteligencja oraz inne nowe technologie cyfrowe są wykorzystywane w sposób bezpieczny i skuteczny dla poprawy jakości opieki nad pacjentem Cel 4.2.1: Rozwój gospodarki, przemysłu cyfrowego i dobrostanu społecznego jest wspierany przez sprawny i skoordynowany ekosystem sztucznej inteligencji; Cel 4.6.1: Polska administracja publiczna w większym stopniu wykorzystuje otwarte oprogramowanie. Strategia na rzecz Odpowiedzialnego Rozwoju do 2020 (z perspektywą do 2030 r.) – Zakres przedsięwzięcia wpisuje się w cel szczegółowy III –

	skuteczne państwo i instytucje służące włączeniu społecznemu i gospodarczemu – Obszar: E-państwo. Zdrowa Przyszłość. Ramy strategiczne rozwoju systemu ochrony zdrowia na lata 2021-2027. Zakres projektu przedsięwzięcia wpisuje się w Cel 3.3 [Innowacje] Rozwój i upowszechnianie stosowania nowoczesnych i nowatorskich rozwiązań w ochronie zdrowia. Program rozwoju e-zdrowia w Polsce na lata 2022 – 2027. Zakres projektu przedsięwzięcia wpisuje się w następujące cele szczegółowe programu: Cel 4.2 Rozwój usług back office. Polityka rozwoju sztucznej inteligencji w Polsce do 2030 r. Zakres projektu przedsięwzięcia wpisuje się w Cel 4.1 Cel i działania dla rozwoju AI w administracji, cel szczegółowy nr 3: Sprawne Państwo wykorzystujące rozwiązania sztucznej inteligencji.
Korzyść:	- Wzrost zdolności organizacyjnej i odporności kadrowej CeZ, przekładająca się na lepszą jakość i dostępność usług e-zdrowia - Wyższa jakość oraz spójność wytwarzania i utrzymania systemów w całym portfolio CeZ przez zwiększenie efektywności pracy zespołów poprzez wykorzystanie wspólnego, kontrolowanego środowiska wspierającego analizę kodu, code review, testowanie, dokumentację, bezpieczeństwo, onboarding i raportowanie jakości. - Ograniczenie rozproszenia narzędzi i praktyk stosowanych w różnych zespołach oraz poprawa spójności realizacji procesów SDLC. - Krótszy i bardziej przewidywalny czas dostarczania oraz utrzymania zmian w systemach e-zdrowia, przekładający się na ciągłość i niezawodność usług.
KPI:	KPI 1: Użytkownicy nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych KPI 2: Liczba pracowników IT podmiotów wykonujących zadania publiczne objętych wsparciem szkoleniowym (kobiety) KPI 3: Liczba pracowników IT podmiotów wykonujących zadania publiczne objętych wsparciem szkoleniowym (mężczyźni) KPI 4: Liczba pracowników podmiotów wykonujących zadania publiczne niebędących pracownikami IT, objętych wsparciem szkoleniowym (kobiety) KPI 5: Liczba pracowników podmiotów wykonujących zadania publiczne niebędących pracownikami IT, objętych wsparciem szkoleniowym (mężczyźni) KPI 6: Liczba procesów SDLC objętych wdrożeniem platformy AI-SDLC. KPI 7: Odsetek zmian w kodzie objętych automatyczną analizą jakości (code review) w projektach wspartych przez platformę AI-SDLC
Wartość aktualna i docelowa KPI:	KPI 1: Wartość aktualna (2026): 0 osób KPI 2: Wartość aktualna (2026): 0 osób KPI 3: Wartość aktualna (2026): 0 osób KPI 4: Wartość aktualna (2026): 0 osób KPI 5: Wartość aktualna (2026): 0 osób KPI 6: Wartość aktualna (2026): 0 procesów KPI 7: Wartość aktualna (2026): 0 % KPI 1:

	Wartość docelowa (2030): 300 osób KPI 2: Wartość docelowa (2029): 50 osób KPI 3: Wartość docelowa (2029): 50 osób KPI 4: Wartość docelowa (2029): 25 osób KPI 5: Wartość docelowa (2029): 25 osób KPI 6: Wartość docelowa (2029): minimum 5 procesów SDLC obejmujących np. analizę kodu, code review, testowanie, analizę bezpieczeństwa, dokumentowanie, onboarding i raportowanie jakości KPI 7: Wartość docelowa (2030): 50%
Metoda pomiaru KPI	KPI 1: Źródło danych: Rejestr użytkowników systemu, logi systemowe. Termin pomiaru: sierpień 2030, jednorazowo Metoda i sposób pomiaru: Wskaźnik zostanie zmierzony na podstawie liczby unikalnych użytkowników korzystających z platformy AI-SDLC po uruchomieniu rozwiązania. Wartość docelowa 300 osób została oszacowana na podstawie przewidywanej skali wykorzystania platformy przez zespoły CeZ oraz osoby zaangażowane w procesy wytwarzania, utrzymania, testowania, dokumentowania, bezpieczeństwa i zarządzania jakością oprogramowania po roku od uruchomienia rozwiązania. KPI 2: Źródło danych: Listy uczestników szkoleń. Termin pomiaru: sierpień 2029, jednorazowo Metoda i sposób pomiaru: wskaźnik zostanie zmierzony na podstawie list obecności poprzez zliczenie kobiet będących pracownikami IT, które ukończą szkolenie lub zostaną objęte wsparciem szkoleniowym w ramach projektu. KPI 3: Źródło danych: Listy uczestników szkoleń. Termin pomiaru: sierpień 2029, jednorazowo Metoda i sposób pomiaru: wskaźnik zostanie zmierzony na podstawie list obecności poprzez zliczenie mężczyzn będących pracownikami IT, którzy ukończą szkolenie lub zostaną objęte wsparciem szkoleniowym w ramach projektu. KPI 4: Źródło danych: Listy uczestników szkoleń. Termin pomiaru: sierpień 2029, jednorazowo Metoda i sposób pomiaru: wskaźnik zostanie zmierzony na podstawie list obecności poprzez zliczenie kobiet niebędących pracownikami IT, które ukończą szkolenie lub zostaną objęte wsparciem szkoleniowym w ramach projektu. KPI 5: Źródło danych: Listy uczestników szkoleń.

	Termin pomiaru: sierpień 2029, jednorazowo Metoda i sposób pomiaru: wskaźnik zostanie zmierzony na podstawie list obecności poprzez zliczenie mężczyzn niebędących pracownikami IT, którzy ukończą szkolenie lub zostaną objęte wsparciem szkoleniowym w ramach projektu. KPI 6: Źródło danych: Rejestr procesów objętych wdrożeniem, dokumentacja konfiguracji workflow. Termin pomiaru: sierpień 2029, jednorazowo Metoda i sposób pomiaru: Wskaźnik mierzy liczbę procesów cyklu życia oprogramowania SDLC, które zostaną objęte funkcjonalnościami platformy AI-SDLC po uruchomieniu rozwiązania. Jego osiągnięcie potwierdzi faktyczne wdrożenie AI-SDLC w kluczowych procesach cyklu życia oprogramowania oraz doprowadzenie do realnej modernizacji procesów pracy zespołów CeZ poprzez objęcie ich wsparciem platformy AI-SDLC. Przyjęta wartość docelowa na poziomie minimum 5 procesów SDLC wynika z konieczności zapewnienia kompleksowego wsparcia technologicznego dla kluczowych etapów cyklu życia oprogramowania w Centrum e-Zdrowia. Wybrane procesy (analiza kodu, code review, testowanie, analiza bezpieczeństwa, dokumentowanie, onboarding i raportowanie jakości) stanowią filary fazy realizacji oraz stabilizacji systemu, odpowiadając na zidentyfikowane potrzeby w zakresie automatyzacji i kontroli jakości. KPI 7: Źródło danych: Raport z weryfikacji pull request z przypisaną rolą AI/human Termin i częstotliwość pomiaru: sierpień 2030, co pół roku. Metoda i sposób pomiaru: Wartość docelowa na poziomie 50% zmian w kodzie objętych automatyczną analizą jakości została przyjęta jako realistyczna dla pierwszego etapu wdrożenia platformy AI-SDLC po uruchomieniu usługi, a jednocześnie znacząco wpływająca na jakość kodu dla najważniejszych systemów CeZ. Ich kwalifikacja odbędzie się w pierwszej fazie projektu (KM1) poprzez wykorzystanie kryteriów jakościowych - t.j. możliwości adaptacji w czasie, braku ograniczeń prawno-formalnych i kryteriów jakościowych dla potencjału wykorzystania mechanizmów automatycznej analizy kodu, jakości, bezpieczeństwa i testowania dla ich obecnego standardu wytwórczego.
--	--

2.2. Udostępnione e-usługi

Lp.	Nazwa e-usługi	Typ	Zakres oddziaływania	Poziom dojrzałości e-usługi
1	e-Koordynator SDLC AI - wewnętrzna e-usługa A2A wspierająca współpracę pomiędzy CeZ a właścicielami biznesowymi systemów informatycznych. Usługa zapewnia zautomatyzowane, wspomagane	A2A	Centrum e-Zdrowia Ministerstwo Zdrowia Podmioty administracji publicznej i instytucje sektora ochrony zdrowia (AOTMiT, URPL,	Personalizacja

Lp.	Nazwa e-usługi	Typ	Zakres oddziaływania	Poziom dojrzałości e-usługi
	sztuczną inteligencją definiowanie, porządkowanie, analizę i obsługę potrzeb biznesowych, potrzeb wdrożeniowych oraz zmian architektonicznych w całym cyklu życia rozwiązań informatycznych.		GIF, NFZ, CMJ, NCK, CEM, NIL, NIA, KRDL) Podmioty wykonujące działalność leczniczą oraz personel medyczny Pracownicy Centrum e-Zdrowia (zespoły wytwórcze) Pracownicy Ministerstwa Zdrowia (Właściciele biznesowi systemowych, inicjatorzy, eksperci dla systemów IT obsługiwanych przez CeZ) (rocznie ok 534156 transakcji)	

2.3. Udostępnione informacje sektora publicznego i zdigitalizowane zasoby

Rodzaj informacji/zasobów	Planowana data udostępnienia	Szacowana liczba obiektów objętych digitalizacją (udostępnianiem informacji)

Czy wszystkie zdigitalizowane zasoby objęte przedsięwzięciem będą udostępniane bezpłatnie?
TAK/NIE

2.4. Produkty końcowe przedsięwzięcia

Nazwa produktu	Planowana data wdrożenia
Dokumentacja opisująca metodykę kwalifikacji projektów do poziomów AI-SDLC, obejmująca krytyczność, złożoność, ryzyko kompetencyjne, dług techniczny i wymagania bezpieczeństwa oraz raport z inicjalnego testu prywatności platformy AI-SDLC obejmującej wszystkie budowane systemy.	03-2027
Dokumentacja opisująca baseline metryk jakości, bezpieczeństwa, testów, długu technicznego, onboardingu i przepływu pracy dla projektów objętych wdrożeniem	06-2027
Infrastruktura platformy AI-SDLC	05-2028

Nazwa produktu	Planowana data wdrożenia
System teleinformatyczny AI-Gateway	05-2028
System teleinformatyczny AI-SDLC	05-2028
System teleinformatyczny CeZ-AI	05-2028
Raport z testów wydajnościowych pilotażu	05-2028
Raport z testów bezpieczeństwa pilotażu	05-2028
Raport z testów UX pilotażu	05-2028
Dokumentacja techniczna integracji z systemem „Repozytoria kodu i narzędzia CI/CD” - wsparcie tworzenia testów jednostkowych i analizy pokrycia testami, analiza pull requestów i zgodności kodu ze standardami CeZ	09-2028
Dokumentacja techniczna integracji z systemami bezpieczeństwa CeZ - analiza reużywalności, duplikacji, długu technicznego, kandydatów do refaktoryzacji	02-2029
Dokumentacja techniczna integracji z systemem „Baza wiedzy i zadań CeZ” - baza wiedzy projektowej i onboardingowej dla wybranych systemów krytycznych, oparta o kontrolowany RAG, dashboard jakości, długu technicznego, onboardingu i przepływu pracy	05-2029
Materiały szkoleniowe	05-2029
Materiały informacyjno-promocyjne	05-2029
Dokumentacja techniczna i analityczna platformy AI-SDLC	08-2029
Raport z testów wydajnościowych pełnego rozwiązania Platformy AI-SDLC obejmującej wszystkie budowane systemy	08-2029
Raport z testów bezpieczeństwa pełnego rozwiązania Platformy AI-SDLC obejmującej wszystkie budowane systemy	08-2029
Raport z testów UX pełnego rozwiązania Platformy AI-SDLC obejmującej wszystkie budowane systemy	08-2029
Polityka skalowania i bezpiecznego wykorzystania AI w SDLC CeZ, wraz z katalogiem danych zakazanych, zasadami audytu i odpowiedzialności	08-2029
Dokumentacja zawierająca model trwałości, utrzymania, rozwoju i kosztów AI-SDLC po zakończeniu finansowania zewnętrznego	08-2029

3. KAMIENIE MIŁOWE

Kamienie milowe	Planowany termin osiągnięcia
KM1. Zatwierdzona dokumentacja inicjująca projekt w tym potwierdzenie przeprowadzenia inicjalnego testu prywatności, model governance i kryteria kwalifikacji projektów	2027-03-31
KM2. Zatwierdzona dokumentacja zawierająca pomiar baseline i wybrane projekty do poziomów wdrożenia AI-SDLC	2027-06-30

Kamienie milowe	Planowany termin osiągnięcia
KM3. Rozstrzygnięte postępowania na główne komponenty: AI-Gateway narzędzia jakości, bezpieczeństwa, integrację i szkolenia	2027-09-30
KM4. Przeprowadzone weryfikacyjne testy prywatności platformy	2027-12-31
KM5. Odebrane pilotażowe wersje systemów AI-Gateway, CeZ AI i AI-SDLC oraz dokumentacja zawierająca polityki bezpiecznego użycia AI w SDLC	2028-05-31
KM6. Uzyskane pozytywne wyniki testów oprogramowania (bezpieczeństwa, wydajności i UX)	2028-05-31
KM7. Odebrane wdrożenie integracji z systemem „Repozytoria kodu i narzędzi CI/CD CeZ” w pierwszej grupie projektów: testy, analiza Peer Review, jakość kodu, bezpieczeństwo komponentów	2028-09-30
KM8. Odebrane wdrożenie integracji z systemami bezpieczeństwa CeZ wraz z integracją do platformy	2029-02-28
KM9. Odebrane wdrożenie integracji z systemem „Baza wiedzy i zadań CeZ” wraz z integracją do platformy i dashboardem zarządczym	2029-05-31
KM10. Odebrana baza wiedzy projektowej i odebrane wdrożenie modułu onboardingu dla systemów krytycznych	2029-05-31
KM11. Wydana decyzja o zakresie selektywnego skalowania na podstawie KPI i wyników wdrożenia	2029-06-30
KM12. Odebranie wdrożonej polityki skalowania i bezpiecznego wykorzystania platformy AI-SDLC na projekty zakwalifikowane do poziomu pełnego i ograniczonego, zdefiniowany model trwałości, przekazanie do utrzymania i raport efektów	2029-08-31

4. KOSZTY

4.1. Koszty ogólne przedsięwzięcia wraz ze sposobem finansowania

Całkowity koszt przedsięwzięcia (netto oraz brutto), w tym	Netto 23 441 634,68 zł Brutto 27 651 973,08 zł	
Procent dofinansowania ze środków UE (brutto)	79,71%	
Procent dofinansowania ze środków z innych źródeł zagranicznych (brutto)	20,29%	
Procent środków z budżetu państwa (brutto)		
Podział całkowitego kosztu przedsięwzięcia na poszczególne lata (netto oraz brutto)	2027	Netto 5 261 170,82 zł Brutto 6 107 599,04 zł
	2028	Netto 8 904 306,57 zł Brutto 10 360 951,54 zł
	2029	Netto 9 276 157,29 zł Brutto 11 183 422,50 zł

4.2. Wykaz poszczególnych pozycji kosztowych

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
Oprogramowanie	1. Koszty wytworzenia oprogramowania 2. Koszty integracji z istniejącymi systemami 3. Koszty subskrypcji	21 413 676,70 zł	Koszty związane z zapewnieniem ekspertów odpowiedzialnych za przygotowanie dokumentacji, wytworzenie oprogramowania z uwzględnieniem wytycznych WCAG, integrację z istniejącymi systemami, przeprowadzenie testów, konfigurację i wdrożenie. Koszty subskrypcji dla narzędzi AI coding assistance oraz tokenów u dostawców chmurowych LLM.
Infrastruktura	Zapewnienie infrastruktury dla AI-Gateway oraz RAG (Retrieval-Augmented Generation)	1 994 676,74 zł	Środki umożliwią zapewnienie infrastruktury w zakresie serwerów, przestrzeni dyskowej w architekturze HA (Active-Passive) w ramach rozbudowy istniejącej infrastruktury CeZ.
Koszty UX i grafiki	Zapewnienie dostępności	51 225,00 zł	Środki na przeprowadzenie audytu zgodności interfejsu

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
	cyfrowej (WCAG)		użytkownika z wymaganiami dostępności cyfrowej.
Bezpieczeństwo	Testy i audyt bezpieczeństwa wszystkich komponentów platformy AI-SDLC	335 803,84 zł	Środki umożliwią przeprowadzenie testów i audytu bezpieczeństwa wszystkich komponentów platformy AI-SDLC m.in. komponentu AI-Gateway w zakresie autoryzacji, kontroli, DLP, anonimizacji, deanonimizacji czy blokowania informacji wrażliwych.
Wydajność rozwiązań	Uwzględnione w kosztach wytworzenia oprogramowania	0,00 zł	Koszty badań wydajnościowych nie zostały wyodrębnione jako odrębna pozycja budżetowa, ponieważ zgodnie z przyjętym rachunkiem kosztów projektu stanowią integralny element procesu wytworzenia wdrażanych komponentów platformy AI-SDLC.
Szkolenia	Szkolenia specjalistyczne dla specjalistów IT oraz pracowników nie IT	907 040,12 zł	Koszty specjalistycznych szkoleń realizowane przez wyspecjalizowanych dostawców szkoleń obejmujące pełen workflow procesów wytwórczych (SDLC) oraz koszty przygotowania wewnętrznych materiałów szkoleniowych (z uwzględnieniem wytycznych WCAG) dla szkoleń i onboardingów.
Działania informacyjno-promocyjne	Przeprowadzenie działań informacyjno-promocyjnych	167 027,40 zł	Środki umożliwią przeprowadzenie Działań informacyjno-promocyjnych, również tych wynikających z wymagań programowych FERC
Koszty zarządzania i wsparcia (w tym wynagrodzenia personelu wspomagającego)	Realizacja działań związanych z zarządzaniem projektem oraz wsparciem organizacyjnym.	2 782 523,28 zł	Koszty obejmują zarządzanie projektem, nadzór merytoryczny i wsparcie administracyjne (w tym ekspertów ds. zgodności prawnej, ochrony danych i compliance) tj. 973 515,70 zł oraz koszty pośrednie (7% od kwalifikowanych całkowitych kosztów bezpośrednich), tj. 1 809 007,58 zł.

4.3. Koszty ogólne utrzymania wraz ze sposobem finansowania

(okres 5 lat)

Całkowity koszt utrzymania trwałości przedsięwzięcia (brutto)	16 135 421,24 zł		Źródło finansowania
Podział całkowitego kosztu utrzymania trwałości przedsięwzięcia na poszczególne lata (netto oraz brutto)	2029	216 014,38 zł (brutto) (211 775,02 zł netto)	krajowe środki publiczne - budżet państwa
	2030	3 300 918,18 zł (brutto) (2 907 970,08 zł netto)	krajowe środki publiczne - budżet państwa
	2031	3 340 501,69 zł (brutto) (2 947 553,59 zł netto)	krajowe środki publiczne - budżet państwa
	2032	3 366 535,64 zł (brutto) (2 973 587,54 zł netto)	krajowe środki publiczne - budżet państwa
	2033	3 393 115,36 zł (brutto) (3 000 167,26 zł netto)	krajowe środki publiczne - budżet państwa
	2034	2 518 335,99 zł (brutto) (2 129 631,39 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 możliwości dofinansowania projektu z FERC	Średnia	Średnie	- opracowanie kompletnej i zgodnej z kryteriami dla oceny działania 2.1 Wysoka jakość i dostępność e-usług publicznych wyboru projektów w

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
			programie Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 dokumentacji na podstawie, której przeprowadzona będzie ocena Wniosku o dofinansowanie, - realizacja Projektu ze środków budżetu państwa
Zmiana składu zespołu projektowego	Duża	Średnie	- bieżące reagowanie na zmianę składu zespołu- systematyczne planowanie i monitorowanie prac zespołu - prowadzenie repozytorium projektowego, w którym umieszczane są wszelkie informacje o stanie, poszczególnych zadań oraz dokumentach związanych z nimi, - wykorzystanie systemu motywowania.
Zmiany prawne wpływające na zakres i sposób realizacji projektu	Średnia	Niskie	- monitorowanie zmian legislacyjnych na poziomie krajowym i UE oraz projektowanie rozwiązań w sposób elastyczny i modułowy, umożliwiający ich dostosowanie do nowych wymagań. - zapewnienie bieżącej współpracy z jednostkami odpowiedzialnymi za kształtowanie regulacji i interpretację przepisów.
Opóźnienia wynikające z potencjalnych negatywnych wyników testów (akceptacyjnych, bezpieczeństwa)	Duża	Wysokie	- dobór doświadczonej kadry (szczególnie dla obszarów: analiza, development, testy). - monitorowanie jakości oprogramowania, - bieżąca współpraca z departamentem bezpieczeństwa. - wykonanie testów wewnętrznych testów bezpieczeństwa.
Opóźnienia w procesie postępowań zakupowych (np. zaskarżenia KIO, etc.).	Średnia	Wysokie	- wprowadzenie szczegółowego harmonogramu postępowań zakupowych, uwzględniającego możliwe opóźnienia i kluczowe terminy, aby zminimalizować ryzyko przekroczenia czasu. - regularne monitorowanie statusu postępowań i szybkie reagowanie na wykryte przeszkody, np. poprzez dedykowaną osobę odpowiedzialną za koordynację procesu zakupowego.
Ograniczona dostępność lub	Duża	Średnie	- zastosowanie modelu hybrydowego (chmurowe i lokalne) wykorzystywania

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
niedostępność wybranych chmurowych modeli AI spowodowana decyzjami dostawców usług lub legislatorów (np. decyzje polityczne w krajach dostawców, nowe regulacje na poziomie UE)			modeli AI - monitorowanie regulacji mających wpływ na dostępność modeli AI dla polskich podmiotów publicznych - dostosowanie elastyczności mechanizmu wykorzystywania różnych chmurowych modeli AI do bieżącego zagrożenia
Opóźnienia lub wzrost kosztów w stosunku do planów wynikający z nowatorskiego charakteru projektu – pierwszy tego rodzaju w Centrum e-Zdrowia	Średnia	Średnie	- pozyskanie, analiza i wykorzystanie dostępnych doświadczeń innych podmiotów publicznych - zaproszenie do konsultacji podmiotów publicznych i komercyjnych z kompetencjami w obszarze praktycznej implementacji modeli AI z możliwością współpracy w roli inżyniera kontraktu
Brak pozytywnej weryfikacji narzędzia przez instytucję regulującą kwestie AI w instytucjach publicznych np. KRIBSI	Duża	Niskie	- bieżące monitorowanie regulacji mających wpływ na zakres projektu - konsultacje z ekspertami prawnymi w celu szybkiego identyfikowania i reagowania na zmiany w przepisach dotyczących AI.
Powstanie długu technologicznego w zakresie dostępności i wykluczenie cyfrowe użytkowników z niepełnosprawnościami w następstwie wdrożenia niedostępnego cyfrowo narzędzia AI	Mała	Średnie	- dodanie i cykliczne uzupełnianie bazy kontekstowej platformy o standardy dostępności, które będą w zestawie wymagań do odpowiedzi generowanych przez narzędzia AI

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
Wystąpienie wycieku informacji wrażliwych do operatora chmury zewnętrznej i dalej do służb obcych państw, albo do innych podmiotów trzecich może skutkować zagrożeniami poufności danych wrażliwych	Duża	Wysokie	zastosowanie w systemie AI-Gateway mechanizmów anonimizowania danych i blokowania przesyłu danych wrażliwych
Wystąpienie halucynacji i zła jakość generowanych odpowiedzi	Średnia	Średnie	- ugruntowanie danych (grounding) - brak konfabulacji przy braku trafień (zapobieganie halucynacjom przez eliminację wymyślania nieprawdziwych informacji, gdy system nie zna odpowiedzi), testy - mechanizm informacji zwrotnej (feedback).
Wystąpienie dryftu wdrożonych modeli LLM	Średnia	Średnie	- Wdrożenie procedur aktualizowania i monitorowania aktualności baz kontekstowych platformy - mechanizm informacji zwrotnej (feedback).

5.2. Ryzyka wpływające na utrzymanie efektów

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
Brak zabezpieczenia środków finansowych na utrzymanie po zakończeniu realizacji projektu	Średnia	Wysokie	- analiza kosztów utrzymania i rozwoju oraz zabezpieczenie odpowiednich środków budżetowych - uwzględnienie aspektu kosztów utrzymania w projektowaniu systemu.
- brak możliwości zatrudnienia osób o odpowiednich kompetencjach niezbędnych do	Średnia	Średnie	Zapewnienie odpowiednich środków budżetowych

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
utrzymania efektów projektu			
Błędy działania systemu niewykryte na etapie testowania	Średnia	Niskie	- wdrożenie odpowiednich procedur dotyczących testów akceptacyjnych oraz wymóg testowania zmian na środowisku testowym przed- wprowadzeniem na produkcję/ wprowadzenie procedur odtworzenia systemu oraz systematycznego tworzenia kopii zapasowych
Duże zwwyżki kosztów korzystania z zewnętrznych silników chmurowych AI	Duża	Wysokie	- wdrożenia mechanizmów monitorowania i raportowania kosztów wykorzystania usług AI - zdefiniowanie i stosowanie limitów zużycia (progi alarmowe) oraz alertów budżetowych po ich osiągnięciu dla poszczególnych komponentów systemu i dla użytkownika mierzone w zdefiniowanych interwałach (np. miesięcznie) - optymalizacja wykorzystania modeli (m.in. dobór tańszych modeli dla prostych zapytań, umożliwienie przełączenia zapytań chmurowych na wybrane tańsze modele, ograniczanie liczby tokenów) - hybrydowy model wdrożenia, połączenie onprem z chmurą – umożliwienie przełączenia zapytań na model lokalny - system AI-Gateway przygotowany do generowania danych dla mechanizmów showback/chargeback - przygotowanie zasad automatycznego ograniczania użycia

6. OTOCZENIE PRAWNE

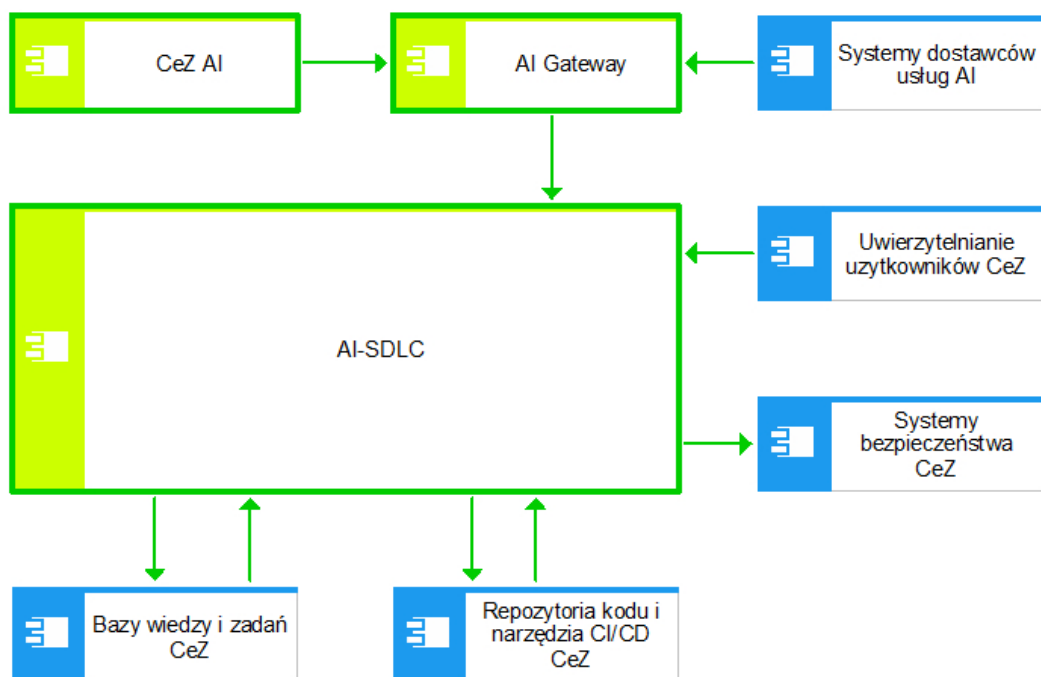
Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
1	Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia	TAK/NIE		

Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
2	Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa	TAK /NIE		
3	Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych	TAK /NIE		
4	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		
5	Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego	TAK /NIE		
6	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		
7	Uchwała Nr 92 Rady Ministrów z dnia 10 marca 2026 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej	TAK /NIE		
8	Standard Cyberbezpieczeństwa Chmur Obliczeniowych - na podstawie przepisu § 3 uchwała Nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa”	TAK /NIE		
9	Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne	TAK /NIE		
10	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		
11	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 z dnia 30 maja 2022 r. w sprawie europejskiego zarządzania danymi	TAK /NIE		

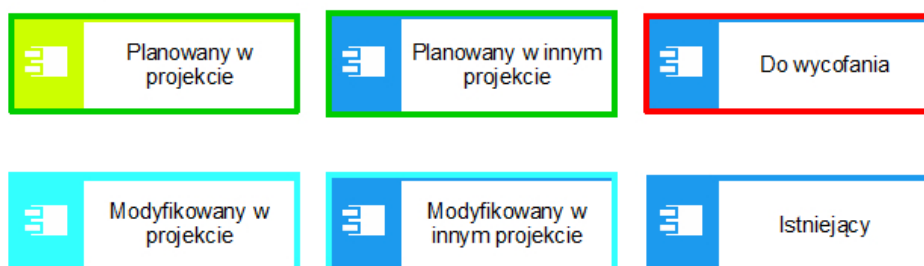
Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
	(Akt w sprawie zarządzania danymi)			
12	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/2854 z dnia 13 grudnia 2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania (Akt w sprawie danych)	TAK/NIE		
13	Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych	TAK/NIE		
14	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji (Akt w sprawie sztucznej inteligencji)	TAK/NIE		
15	Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej	TAK/NIE		
16	Rozporządzenie Ministra Cyfryzacji z dnia 29 czerwca 2020 r. w sprawie profilu zaufanego i podpisu zaufanego	TAK/NIE		
17	Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach	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	AI-SDLC	Centrum e-Zdrowia	AI-SDLC (system wsparcia cyklu życia oprogramowania z wykorzystaniem AI) to system wspierający analizę wymagań i kodu, przegląd zmian, testowanie,	Planowany	

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			dokumentowanie, onboarding i raportowanie jakości. Celem utworzenia systemu jest koordynacja działania procesów SDLC (a wykorzystujących wsparcie AI). Jest to system wewnętrzny nie przetwarzający danych publicznych i nie udostępniający usług interoperacyjnych. System AI-SDLC zarządza możliwością aktywacji modeli AI na potrzeby wsparcia zadań implementacyjnych na rzecz zespołów rozwijających rozwiązania aplikacyjne w CeZ. Komponentem systemu jest RAG.		
2	AI-Gateway	Centrum e-Zdrowia	AI Gateway to system, który umożliwia bezpieczne korzystanie z modeli AI podczas tworzenia i rozwoju oprogramowania. Celem powstania systemu jest kontrola dostępu do modeli (oraz właściwe przekierowanie), oraz ochrona danych wrażliwych a także monitorowanie ich wykorzystania (aspekty użycia, aspekty kosztowe). Komponenty systemu: Konfiguracja dostępu do usług AI, Zarządzanie dostępem do usług AI, Audyt dostępu i wykorzystania usług AI.	Planowany	
3	Repozytoria kodu i narzędzia CI/CD CeZ	Centrum e-Zdrowia	Repozytoria kodu i narzędzia CI/CD CeZ to system wspierający działanie zespołów wytwórczych oraz utrzymaniowych w	Istniejący	

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			zakresie wytwarzania oprogramowania. Cel powstania systemu – realizacja zadań powierzonych w zakresie wytworzenia funkcjonalności na rzecz usług biznesowych powierzonych do realizacji Centrum e-Zdrowia przez Ministerstwo Zdrowia. System zawiera kanoniczne składowe zgodne z najlepszymi praktykami rynkowymi w ramach wytwarzania i rozwoju oprogramowania.		
4	Bazy wiedzy i zadań CeZ	Centrum e-Zdrowia	Baza wiedzy i zadań CeZ to system wspierający obsługę wszystkich procesów dokumentowania pracy oraz informacji. Cel powstania systemu – ciągłość działania, transparentność. Kluczowe składowe wykorzystują rozwiązania rynkowe do tego specjalizowane (komponenty): Confluence, Jira, Enterprise Architect	Istniejący	
5	Systemy dostawców usług AI	Usługodawca - Podmiot dostarczający usługi AI	Systemy Dostawców Usług AI to zaawansowane zewnętrzne (a dostępne w modelu usługowej) platformy oferujące inteligentne rozwiązania oparte na sztucznej inteligencji. Umożliwiają one automatyzację procesów, analizę danych, przetwarzanie obrazu oraz personalizację usług. Nie wyróżnia się komponentów z racji	Istniejący	

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			wykorzystania systemu w modelu SaaS.		
6	CeZ AI	Centrum e-Zdrowia	CeZ AI to system wspierający wytworzenie rekomendacji na podstawie przekazanych danych wejściowych z wykorzystaniem algorytmów AI. Cel powstania to zagwarantowanie bezpiecznego przetwarzania informacji, które nie mogą być przekazane do systemów dostawców usług AI. System umożliwia analizę danych, wsparcie realizacji procesów. System oparty jest o komponent Lokalny LLM.	Planowany	
7	Systemy bezpieczeństwa CeZ	Centrum e-Zdrowia	Systemy bezpieczeństwa CeZ to narzędzia i systemy utrzymywane i zarządzane przez CeZ monitorujące infrastrukturę CeZ oraz MZ jak i systemy biznesowe. W skład systemów wchodzi: • DAM - Database Activity Monitoring (monitorowanie bezpieczeństwa i aktywności w bazach danych); • WAF - Web Application Firewall (zapora sieciowa dedykowana ochronie aplikacji webowych); • System zarządzania dostępem sieciowym (CeZ) – NAC; • System ochrony stacji końcowych (CEZ) – EDR - Endpoint Detection and Response (ochrona stacji roboczej); • System monitorowania,	Istniejący	

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			analizy i zarządzania zdarzeniami związanymi • z bezpieczeństwem - SIEM (Security Information and Event Management); • Usługa monitorowania zagrożeń oraz artefaktów cyberbezpieczeństwa dla sektora ochrony zdrowia(usługa typu Cyber Threat Intelligence); • Platforma elearningowa do umieszczania treści edukacyjnych z zakresu cyberbezpieczeństwa; • System zarządzania uprawnieniami uprzywilejowanymi oraz nagrywaniem sesji (system typu Privileged Access Management); • System zarządzania logami oraz ich retencją celem optymalizacji zdarzeń przesyłanych do systemów klasy SIEM (system klasy Data Lake); • System ochrony DNS (system klasy DNS firewall / secure DNS); • Narzędzie do automatyzacji testów penetracyjnych; • Platforma wspomagająca analizę i testowanie kodu pod kątem bezpieczeństwa na etapie produkcji.		
8	Uwierzytelnianie użytkowników CeZ.	Centrum e-Zdrowia	System klasy IAM zapewniający usługę uwierzytelniania i autoryzacji użytkowników CeZ. Cel powstania systemu to uspołniony model uwierzytelnienia i autoryzacji użytkowników w ramach pracy na infrastrukturze	Istniejący	

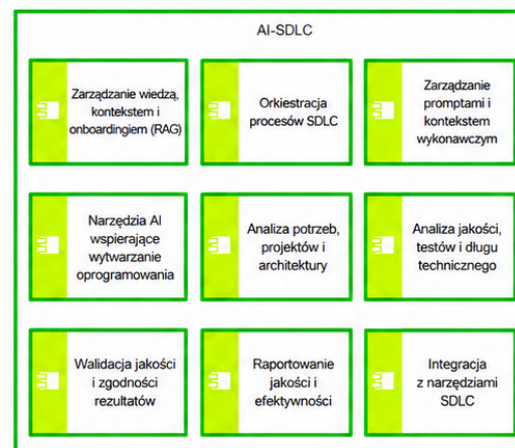
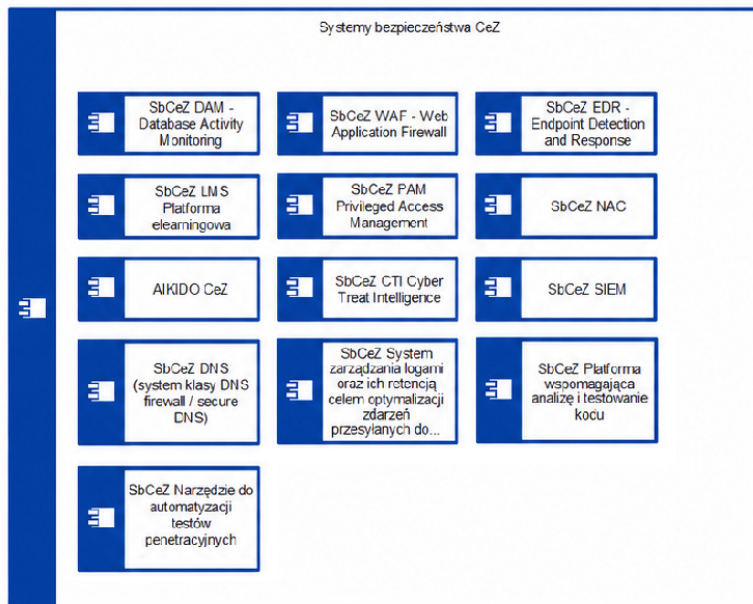
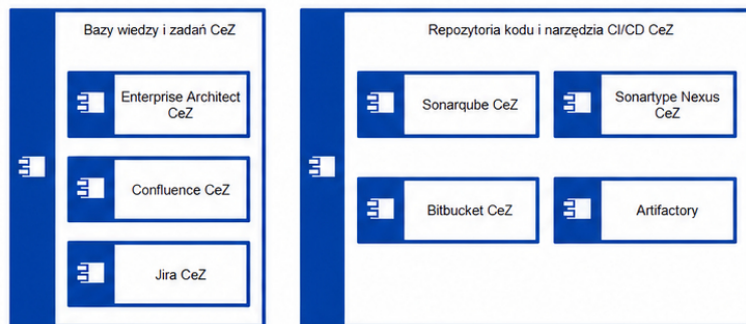
Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			techniczno-systemowo-narzędziowej CeZ.		

Lista przepływów

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
1	AI-Gateway	AI-SDLC	Rekomendacja realizacyjnaT	tryb odwołań bezpośrednich	Krytyczny dla sukcesu przedsięwzięcia	REST API / wewnętrzne API /
2	CeZ AI	AI-Gateway	Rekomendacja realizacyjna	Tryb odwołań bezpośrednich	Krytyczny dla sukcesu przedsięwzięcia	REST API / wewnętrzne API /
3	Systemy dostawców usług AI	AI-Gateway	Rekomendacja realizacyjna	Tryb odwołań bezpośrednich	Krytyczny dla sukcesu przedsięwzięcia	REST API
4	Baza wiedzy i zadań CeZ	AI-SDLC	Dokumentacja, zadania	Tryb odwołań bezpośrednich	Krytyczny dla sukcesu przedsięwzięcia	REST API / wewnętrzne API / metodą
5	AI-SDLC	Systemy Bezpieczeństwa CeZ	Kod źródłowy, skrypt testu automatycznego, skrypt konfiguracyjny, skrypt uruchomieniowy, konfiguracja, uruchomienie modelu, wynik modelu	Tryb odwołań bezpośrednich	Krytyczny dla sukcesu przedsięwzięcia	REST API / wewnętrzne API /
6	Repozytoria kodu i narzędzia CI/CD CeZ	AI-SDLC	Kod źródłowy, konfiguracja, skrypty, testy automatyczne	Tryb odwołań bezpośrednich	Krytyczny dla sukcesu przedsięwzięcia	REST API / wewnętrzne API /
7	AI-SDLC	Baza wiedzy i zadań CeZ	Dokumentacja, zadanie	Tryb odwołań bezpośrednich	Krytyczny dla sukcesu przedsięwzięcia	REST API / wewnętrzne API /
8	Uwierzytelnienie	AI-SDLC	Użytkownik, role,	Tryb odwołań bezpośrednich	Krytyczny dla sukcesu	OIDC / OAuth2

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
	użytkownicy CeZ		uprawnienia, tożsamość, autoryzacja i autentykacja		przedsięwzięcia	
9	AI-SDLC	Repozytoria kodu i narzędzia CI/CD CeZ	Kod źródłowy, dokumentacja w kodzie, gałąź kodu, zadanie w narzędziach CI/CD, skrypt testu automatycznego, skrypt konfiguracyjny, skrypt uruchomieniowy, konfiguracja	Tryb odwołań bezpośrednich	Krytyczny dla sukcesu przedsięwzięcia	REST API / wewnętrzne API /

7.2. Kluczowe komponenty architektury rozwiązania



Legenda



7.3. Przyjęte założenia technologiczne

Lp.	Obszar	Założenie technologiczne
1.	Infrastruktura	Platforma AI-SDLC, AI-Gateway, warstwa integracyjna, baza metadanych, repozytorium wektorowe i dashboard będą uruchomione w infrastrukturze on-premises CeZ. Domyślne wykorzystanie modeli AI będzie realizowane w chmurze wyłącznie przez AI-Gateway. Architektura przewiduje możliwość uruchamiania lokalnych modeli AI on-premises. Elementy obszaru pod pełną kontrolą CeZ z uwzględnieniem dużych modeli chmurowych (LLM), dla których zabezpieczeniem będą: - mechanizmy bezpieczeństwa zaimplementowane w AI-Gateway, które dla usług chmurowych (LLM) zapewniają uwierzytelnianie i autoryzację, kontrolę uprawnień, szyfrowanie transmisji, separację sieciową, kontrolę ruchu wychodzącego,

Lp.	Obszar	Założenie technologiczne
		DLP, maskowanie i blokowanie danych niedozwolonych, rejestrowanie zapytań i wyników, audyt oraz kontrolę, - zastosowanie RAG (Retrieval-Augmented Generation) jako źródeł wiedzy wewnętrznej do budowania kontekstów, które będą przechowywały wyłącznie wiedzę z repozytoriów projektowych z wyłączeniem jakichkolwiek danych wrażliwych czy osobowych, - dopuszczone zostaną wyłącznie komponenty i dostawcy spełniające wymagania bezpieczeństwa, ochrony danych, własności intelektualnej oraz AI Act, - usługi chmurowe (LLM) dostarczane przez podmioty zewnętrzne będą mogły być wykorzystywane wyłącznie w modelach Business lub Enterprise, zapewniających odpowiedni poziom bezpieczeństwa oraz zapewniające niewykorzystywanie danych CeZ do trenowania modeli publicznych.
2.	Sieć i bezpieczeństwo	Dostęp do modeli AI odbywa się wyłącznie przez AI-Gateway. Zabronione jest bezpośrednie korzystanie z modeli chmurowych z pominięciem AI-Gateway. Wymagane są mechanizmy TLS, separacja sieciowa, kontrola egress, filtrowanie ruchu, logowanie, DLP, maskowanie danych i blokowanie danych zakazanych. Elementy obszaru pod pełną kontrolą CeZ. W CeZ obowiązuje od 2017 r. System Zarządzania Bezpieczeństwem Informacji zgodny z ISO:27001 i podlega corocznej certyfikacji. Aktualny certyfikat zgodności z kwietnia 2026r.
3.	Standardy wymiany danych	Integracje będą realizowane preferencyjnie przez REST API, webhooki, import raportów technicznych oraz bezpieczne kanały HTTPS. Dla uwierzytelniania i autoryzacji przyjęto OIDC/OAuth2 z wykorzystaniem Keycloak. Elementy obszaru pod pełną kontrolą CeZ.
4.	Systemy operacyjne serwerowe	Zakłada się wykorzystanie standardowych systemów serwerowych dopuszczonych w CeZ, preferencyjnie systemów Linux dla komponentów aplikacyjnych, integracyjnych, modeli lokalnych i usług pomocniczych. Elementy obszaru pod pełną kontrolą CeZ.
5.	Bazy danych	Zakłada się wykorzystanie relacyjnej bazy metadanych oraz repozytorium wektorowego uruchomionych on-premises. Technologia powinna umożliwiać szyfrowanie danych, backup, monitoring, odtworzenie, audyt i skalowanie. Elementy obszaru pod pełną kontrolą CeZ.
6.	Serwery aplikacji	Komponenty aplikacyjne powinny być uruchamiane w modelu kontenerowym lub równoważnym, zgodnym ze standardami infrastrukturalnymi CeZ, z możliwością automatyzacji wdrożeń, monitorowania i skalowania. Elementy obszaru pod pełną kontrolą CeZ.
7.	Portale	Rozwiązanie nie będzie portalem publicznym. Udostępniony zostanie interfejs back-office dla uprawnionych użytkowników CeZ oraz API techniczne dla integracji z narzędziami SDLC. Elementy obszaru pod pełną kontrolą CeZ.
8.	Inne	Architektura musi umożliwiać zmianę dostawcy modelu AI bez przebudowy całego rozwiązania. Wymagane jest wersjonowanie

Lp.	Obszar	Założenie technologiczne
		polityk, audyt użycia AI, mierzenie kosztów, human-in-the-loop dla wyników wpływających na decyzje projektowe oraz brak trenowania modeli zewnętrznych na danych CeZ, o ile nie zostanie to odrębnie dopuszczone formalnie i kontraktowo. Planowane jest zapewnienie zgodności systemu z wytycznymi WCAG oraz uwzględnienie standardów dostępności w przeglądach kodu realizowanych przez platformę.

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~~

- dodatkowe zabezpieczenia powyżej wymogów KRI: należy wskazać uzasadnienie

Dla AI-SDLC, AI Gateway i komponentów przyjmuje się podwyższony poziom zapewnienia bezpieczeństwa. Rozwiązanie działa w SZBI zgodnym z ISO/IEC 27001 (m.in w oparciu o wskazane w pkt 7.3 dokumenty systemowe, polityki, procedury) a ISO 42001 i KRI uzupełnia o mechanizmy bezpieczeństwa AI w SDLC.

AI-SDLC to rozwiązanie horyzontalne, wewnątrzadministracyjne. Nie tworzy rejestru publicznego, nie przetwarza danych medycznych, lecz przetwarza dane techniczne, projektowe i organizacyjne: kod, konfiguracje, dokumentację, metadane i wyniki analiz. Dane mogą obejmować informacje wewnętrzne, sekrety i podatności, dlatego dostęp zależy od roli, klasy danych, krytyczności i ryzyka.

Analiza obejmie ryzyka IT oraz AI: przekazanie kodu, sekretów lub danych zakazanych do modeli AI, błędne rekomendacje, podatny kod, ujawnienie informacji dostawcy, obejście AI Gateway, podatności komponentów AI, zależność od dostawców oraz zmianę warunków licencji, kosztów lub usług, Analiza ryzyka zakłada mechanizmy bezpieczeństwa minimalizujące specyficzne dla rozwiązań AI zagrożenia.

Dostęp do AI będzie realizowany wyłącznie przez AI Gateway jako punkt kontroli, autoryzacji, audytu i egzekwowania polityk. Stosowane będą role, minimalne uprawnienia, separacja środowisk, kontrola egress, szyfrowanie, DLP, filtrowanie promptów i odpowiedzi, blokowanie danych zakazanych, kontrola sekretów i logowanie.

Rozwiązanie obejmie monitoring, rejestrowanie zdarzeń i audyt użycia AI. Incydenty będą obsługiwane zgodnie z zasadami CeZ, w tym wyciek danych w promptach, ujawnienie sekretów, nieautoryzowany dostęp do modelu, obejście AI Gateway albo naruszenie integralności repozytorium.

Dostawcy usług, modeli, komponentów AI i integracji spełnią wymagania bezpieczeństwa, ochrony danych, zgodności, audytowalności, ciągłości działania i zarządzania podatnościami, w

tym zakaz trenowania modeli na danych CeZ bez podstawy, zgłaszanie incydentów, przenoszalność danych i ograniczenie vendor lock-in.