Załącznik do KARTY OCENY ZAŁOŻEŃ PROJEKTU INFORMATYCZNEGO NR P471

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nazwa dokumentu:** Opis założeń projektu informatycznego pn. **„mLekarz – kompleksowa cyfryzacja procesów obsługi członków Okręgowej Izby Lekarskiej w Warszawie”** - wnioskodawca: Minister Zdrowia, beneficjent: Okręgowa Izba Lekarska w Warszawie | | | | | |
| **Lp.** | **Organ wnoszący uwagi** | **Jednostka redakcyjna, do której**  **wnoszone są uwagi** | **Treść uwagi** | **Propozycja zmian zapisu** | **Odniesienie do uwagi** |
|  | **MC** | Uwaga ogólna | Proszę o informację, jakie jest uzasadnienie dla rozdzielenia projektów „mLekarz – kompleksowa cyfryzacja procesów obsługi członków Okręgowej Izby Lekarskiej w Warszawie” i „Wirtualny Dziekanat Stażu Podyplomowego – pilotażowy system cyfrowej obsługi lekarzy stażystów w Okręgowej Izbie Lekarskiej  w Warszawie”? |  | Pierwotne rozdzielenie projektów „mLekarz – kompleksowa cyfryzacja procesów obsługi członków Okręgowej Izby Lekarskiej w Warszawie” oraz „Wirtualny Dziekanat Stażu Podyplomowego - pilotażowy system cyfrowej obsługi lekarzy stażystów w Okręgowej Izbie Lekarskiej w Warszawie” było decyzją strategiczną, wynikającą z zasad zarządzania ryzykiem regulacyjnym i organizacyjnym. Procesy objęte projektem mLekarz oraz Wirtualny Dziekanat mają charakter trwały i systemowy, wynikający z ustawowych zadań izb lekarskich. Na etapie przygotowania projektu w przestrzeni publicznej pojawiały się informacje o możliwych zmianach w modelu stażu podyplomowego, co uzasadniało ostrożne podejście projektowe. Aktualnie utrzymanie stażu podyplomowego zostało potwierdzone, co zmniejsza ryzyko regulacyjne. Staż podyplomowy pozostaje stałym elementem ścieżki zawodowej lekarza i powinien być obsługiwany w sposób zintegrowany z pozostałymi procesami systemu mLekarz.  W związku z powyższym podjęto decyzję o połączeniu zakresów obu inicjatyw w ramach jednego projektu systemowego mLekarz, przy zachowaniu modułowego podejścia do realizacji. Pozwala to na zapewnienie spójnej architektury, jednolitego modelu danych oraz efektywnego wykorzystania infrastruktury. |
|  | **MC** | Uwaga ogólna | Z projektu wynika, że będą w ramach jego realizacji przetwarzane dane osobowe. Lista systemów wykorzystywanych w projekcie obejmuje 20 pozycji. Z uwagi na powyższe opis założeń wymaga uzupełnienia o ocenę skutków dla ochrony danych osobowych, o której mowa w art. 35 RODO i uzupełnienia ryzyk wpływających na realizację projektu np.: podatności dotyczących bezpieczeństwa dla nowego systemu, które mogą mieć wpływ na bezpieczeństwo danych w systemie lub osób, których te dane dotyczą. |  | Projekt mLekarz zakłada przetwarzanie danych osobowych oraz integrację z wieloma systemami zewnętrznymi, dlatego ochrona danych i bezpieczeństwo informacji zostały uwzględnione już na etapie projektowania rozwiązania, zgodnie z art. 35 RODO oraz zasadami privacy by design i security by design. Projekt nie przewiduje wprowadzania nowych źródeł danych ani rozszerzania zakresu przetwarzanych kategorii danych osobowych – przetwarzanie dotyczy wyłącznie danych już wykorzystywanych przez samorząd lekarski w ramach realizacji ustawowych zadań. W pierwszym etapie realizacji projektu przewidziano opracowanie dokumentacji analizy procesów, obejmującej identyfikację przepływów danych oraz wymagań bezpieczeństwa.  Na podstawie wyników tej analizy zaplanowano przeprowadzenie inicjalnego testu prywatności, w tym wykonanie oceny skutków dla ochrony danych osobowych (DPIA) lub innej adekwatnej formy oceny – w zależności od zidentyfikowanego poziomu ryzyka. |
|  | **MC** | 5.1. Ryzyka wpływające na realizację projektu | Jako ryzyko wpływając na utrzymanie efektów wskazano Ryzyko naruszeń bezpieczeństwa danych (dane osobowe i medyczne), jako środek zaradczy wskazano: Wdrożenie polityk bezpieczeństwa, certyfikowanych rozwiązań, regularne testy penetracyjne i audyty RODO. | W ocenie MC konieczne jest wdrożenie procesu zarządzania tymi ryzykami np. stosowanie zasady privacy by design na każdym etapie projektu, zaangażowanie w prace nad projektem IOD MZ, identyfikowanie podatności dot. bezpieczeństwa dla systemu oraz prowadzenie regularnych audytów oprócz RODO także audytów bezpieczeństwa. | Projekt przewiduje stosowanie zasady security by design oraz privacy by design na wszystkich etapach realizacji projektu. Ponadto w ramach prac projektowych przewidziano zaangażowanie Ministerstwa Zdrowia jako konsultanta, w szczególności w zakresie zgodności projektowanych rozwiązań z wymaganiami dotyczącymi przetwarzania danych oraz bezpieczeństwa informacji. |
|  | **MFiPR** |  | Tytuł projektu: „mLekarz – kompleksowa cyfryzacja procesów obsługi członków Okręgowej Izby Lekarskiej w Warszawie” oraz jego opis świadczą o tym, że projektowane e-usługi będą miały zasięg regionalny. Natomiast zgodnie ze wskazaniem zapisów programu w FERC wdrażane w programie e-usługi muszą mieć charakter ogólnokrajowy. | Należy rozważyć poszerzenie zakresu projektu oraz włączenie pozostałych regionalnych izb lekarskich jako partnerów. | Informacja o skalowalności projektu na inne Okręgowe Izby Lekarskie została dodana do pkt 1.1. Identyfikacja problemu i potrzeb: Projekt zakłada wdrożenie systemu mLekarz w OIL w Warszawie oraz przygotowanie go jako rozwiązania skalowalnego, gotowego do wdrożenia w innych OIL w Polsce, w celu upowszechnienia jednolitego standardu cyfrowej obsługi.  W celu zapewnienia uniwersalności użytkowej, organizacyjnej i technicznej systemu mLekarz, Wnioskodawca przewiduje utworzenie Rady interesariuszy projektu, z udziałem przedstawicieli wybranych okręgowych izb lekarskich, w tym dużych izb (powyżej 15 tys. członków), średnich izb (od 4 do 15 tys. członków) oraz małych izb (poniżej 4 tys. członków), która będzie pełniła funkcję doradczą w zakresie skalowalności i wdrożenia systemu mLekarz w innych OIL w Polsce.  Tytuł zostanie zmieniony w celu podkreślenia ogólnokrajowego charakteru projektu: mLekarz – kompleksowa cyfryzacja procesów obsługi lekarzy. |
|  | **MFiPR** | 2.2 Udostępnione e-usługi | Dwie usługi: 10 Obsługa klubu i inicjatyw integracyjnych oraz 11. Umawianie się na wizyty oraz multichannel dla kontaktów w OIL  Warszawa mają wpisany poziom dojrzałości dwustronna interakcja. Natomiast w FERC zapisano, że dofinansowane może być wdrożenie usług na 4 poziomie tj. transakcja.  Koszty planowane na wdrożenie tych usług nie mogą być zatem kwalifikowalne w projekcie planowanym do zgłoszenia w działaniu 2.1 FERC. | Proszę o przeanalizowanie poziomu obydwu planowanych usług. Jeżeli we wniosku pozostanie wpisany aktualnie poziom usług, należy wtedy wyliczyć koszty z nimi związane i wpisać je jako niekwalifikowalne, czyli takie, które beneficjent będzie musiał ponieść we własnym zakresie. | Zmieniono opis usług w celu spełniania wymogu transakcji:   1. Elektroniczna rejestracja i obsługa uczestnictwa w klubie i inicjatywach integracyjnych (np. Klub Lekarza Przedsiębiorcy, wydarzenia sportowe, spotkania środowiskowe)   Elektroniczne umawianie wizyt stacjonarnych, wideo i tele w OIL Warszawa |
|  | **MFiPR** | 2.1 Cele i korzyści wynikające z projektu | 1) Podano, iż wartość docelowa wskaźnika „Liczba usług publicznych udostępnionych on-line o stopniu dojrzałości co najmniej 4 – transakcja” wynosi 9 szt., podczas gdy w tabeli nr 2.2 wykazano 11 usług A2B, A2C.  2) Nazwa wskaźnika „Liczba użytkowników nowych publicznych usług cyfrowych” powinna zostać skorygowana zgodnie z nazwą wskaźnika określoną w dz. 2.1 FERC, tj. „Użytkownicy nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych”.  3) Należy wyjaśnić różnice między KPI 4 i 5, tj.:  KPI 4: Liczba użytkowników nowych publicznych usług cyfrowych.  KPI 5: Liczba spraw załatwionych całkowicie online w ciągu 12 miesięcy  Z opisu KPI wynika, że KPI 4 dotyczy: monitoringu rejestru użytkowników w systemie mLekarz, statystyk rejestracji i aktywności kont, analiz logowań.  Natomiast KPI 5 dotyczy: statystyk zamkniętych spraw w systemie mLekarz/CMS, analizy  workflow z oznaczeniem „100% zakończona elektronicznie”.  Jednocześnie, wartości docelowe obu wskaźników są takie same, tj. wynoszą 10 000.  Na podstawie ww. opisu trudno stwierdzić, jaka jest różnica między wskaźnikami. | 1) Proszę o weryfikację liczby e-usług podanych w tabelach 2.1 i 2.2. Wartości powinny być spójne w obu miejscach.  2) Proszę o korektę nazwy wskaźnika zgodnie z nazwą określoną w dz. 2.1 FERC. Jednocześnie wskaźnik powinien spełniać warunki jego definicji opracowanej przez IZ FERC.  3) Wnioskodawca powinien w pierwszej kolejności wybrać wskaźnik „Użytkownicy nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych”, który powinien spełniać warunki definicji, tj. dotyczyć użytkowników uruchomionych e-usług, tj. obywateli lub przedsiębiorców.  Wnioskodawca może określić dodatkowo wskaźnik własny, jednak różnica pomiędzy ww. wskaźnikiem a wskaźnikiem własnym powinna być jasna. Obecnie tak nie jest, także dlatego, że wartości docelowe obu zaproponowanych wskaźników są takie same.  Proszę o weryfikację obu wskaźników i odpowiednią korektę zgodnie z powyższymi zaleceniami. | 1. Zaktualizowano liczbę usług o stopniu dojrzałości co najmniej 4  2. Nazwę wskaźnika zmieniono zgodnie z treścią uwagi  3. W wyniku doprecyzowania metodologii pomiaru wskaźników efektywności projektu pozostawiono bez zmian wartość KPI 4, natomiast dokonano korekty wartości KPI 5: Zmiana wartości KPI 5 z 10 000 na 30 000 wynika z doprecyzowania metodologii liczenia wskaźnika, decyzji o realizacji wszystkich e-usług na poziomie dojrzałości 4 (transakcja) oraz połączenia projektu mLekarz z Wirtualnym Dziekanatem, obsługującym lekarzy odbywających staż podyplomowy. Wskaźnik mierzy liczbę spraw załatwionych całkowicie online, a nie liczbę użytkowników, przy czym jeden użytkownik realizuje w ciągu roku kilka spraw administracyjnych. Przyjęta wartość 30 000 odpowiada konserwatywnemu założeniu 3 spraw rocznie na użytkownika w okresie pilotażowym i pozostaje spójna z zakresem oraz efektywnością projektowanego systemu. |
|  | **MSWiA** | pkt 7.4 Opis zasobów danych przetwarzanych w planowanym rozwiązaniu | W tabeli w pkt nr 5 dotyczącym rejestru PESEL w kolumnie opis wydaje się zasadnym zastąpienie użytego opisu:  „Państwowy rejestr powszechny, zawierający dane identyfikacyjne wszystkich obywateli Polski oraz cudzoziemców zameldowanych na pobyt  stały lub czasowy” na opis:  „Rejestr gromadzący dane obywateli polskich zamieszkujących na terytorium Rzeczypospolitej Polskiej lub poza granicami Rzeczypospolitej Polskiej w związku z ubieganiem się o polski dokument tożsamości oraz cudzoziemców zamieszkujących na terytorium Rzeczypospolitej Polskiej, a także dane osób obowiązanych na podstawie odrębnych przepisów do posiadania numeru PESEL.”.  Propozycja doprecyzowania wynika z przepisów ustawy z dnia 24 września 2010 r. o ewidencji ludności (Dz. U. z 2025 r. poz. 274). | Propozycja zawarta w treści uwagi. | Opis został zmieniony zgodnie z propozycją zawartą w treści uwagi. |
|  | **MSWiA** | pkt 7.4 Opis zasobów danych przetwarzanych w planowanym rozwiązaniu | W pkt 6 tabeli wskazany został Rejestr PESEL obywateli Ukrainy. Wskazaną w tabeli nazwę rejestru należy zastąpić nazwą rejestr obywateli Ukrainy (ROU).  Rejestr obywateli Ukrainy prowadzi się w systemie teleinformatycznym, o którym mowa w art. 55 ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych, ale jest to rejestr odrębny od Rejestru Dowodów Osobistych i rejestru PESEL, prowadzony na podstawie przepisów ustawy z dnia 12 marca 2022 r. o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego Państwa (Dz. U. z 2025 r. poz. 337, z późn. zm.). Wobec powyższego nie jest zasadne w opisie rejestru wskazanie, iż rejestr obywateli Ukrainy jest częścią rejestru PESEL. | Propozycja zawarta w treści uwagi. | Nazwa rejestru została zastąpiona zgodnie z propozycją zawartą w treści uwagi. |
|  | **RA IT** | Uwaga ogólna | Czy mLekarz będzie skalował swoje produkty na inne okręgowe izby lekarskie? | Proszę o analizę i wyjaśnienie lub korektę opisu założeń | Informacja o skalowalności projektu na inne Okręgowe Izby Lekarskie została dodana do pkt 1.1. Identyfikacja problemu i potrzeb: Projekt zakłada wdrożenie systemu mLekarz w Okręgowej Izbie Lekarskiej w Warszawie oraz przygotowanie go jako rozwiązania skalowalnego i replikowalnego, gotowego do wdrożenia w innych OIL w Polsce.  W celu zapewnienia uniwersalności użytkowej, organizacyjnej i technicznej systemu mLekarz, Wnioskodawca przewiduje utworzenie Rady interesariuszy projektu, z udziałem przedstawicieli wybranych okręgowych izb lekarskich, w tym dużych izb (powyżej 15 tys. członków), średnich izb (od 4 do 15 tys. członków) oraz małych izb (poniżej 4 tys. członków), która będzie pełniła funkcję doradczą w zakresie skalowalności i wdrożenia systemu mLekarz w innych OIL w Polsce.  Nawiązując do uwagi zarówno RA IT, jak i Ministerstwa Cyfryzacji dotyczącej uzasadnienia rozdzielenia projektów „mLekarz – kompleksowa cyfryzacja procesów obsługi członków Okręgowej Izby Lekarskiej w Warszawie” oraz „Wirtualny Dziekanat Stażu Podyplomowego - pilotażowy system cyfrowej obsługi lekarzy stażystów w Okręgowej Izbie Lekarskiej w Warszawie”, pierwotne rozdzielenie projektów było decyzją strategiczną, wynikającą z zasad zarządzania ryzykiem regulacyjnym i organizacyjnym. Procesy objęte projektem mLekarz oraz Wirtualny Dziekanat mają charakter trwały i systemowy, wynikający z ustawowych zadań izb lekarskich. Na etapie przygotowania projektu w przestrzeni publicznej pojawiały się informacje o możliwych zmianach w modelu stażu podyplomowego, co uzasadniało ostrożne podejście projektowe. Aktualnie utrzymanie stażu podyplomowego zostało potwierdzone, co zmniejsza ryzyko regulacyjne. Staż podyplomowy pozostaje stałym elementem ścieżki zawodowej lekarza i powinien być obsługiwany w sposób zintegrowany z pozostałymi procesami systemu mLekarz.  W związku z powyższym podjęto decyzję o połączeniu zakresów obu inicjatyw w ramach jednego projektu systemowego mLekarz, przy zachowaniu modułowego podejścia do realizacji. Pozwala to na zapewnienie spójnej architektury, jednolitego modelu danych oraz efektywnego wykorzystania infrastruktury. |
|  | **RA IT** | 2.1. Cele i korzyści wynikające z projektu | Zaproponowane mierniki nie mierzą tych korzyści. | Proszę o analizę i wyjaśnienie lub korektę opisu założeń | Dodano wskaźnik własny:  **KPI 9:** Odsetek spraw z automatycznym pobraniem lub weryfikacją danych z systemów zewnętrznych  Jednostka: %  Wartość bazowa: 0%  Wartość docelowa: 70%  Metoda pomiaru: logi integracyjne FINN / RPWDL / SMK  **Domyka korzyść integracyjną**, której obecnie nie mierzy żaden KPI |
|  | **RA IT** | 2.1. Cele i korzyści wynikające z projektu | Należy uzupełnić listę wskaźników o wskaźnik rezultatu związany z wdrożeniem produktów projektu w innych okręgowych izbach lekarskich. | Proszę o analizę i wyjaśnienie lub korektę opisu założeń | Dodano wskaźnik:  **KPI 10:** Opracowanie i zatwierdzenie dokumentacji umożliwiającej udostępnienie i wdrożenie systemu mLekarz w innych okręgowych izbach lekarskich w Polsce.  Wartość bazowa: 0 Wartość docelowa: 1  Sposób pomiaru: potwierdzenie opracowania i zatwierdzenia dokumentacji architektonicznej systemu mLekarz oraz sporządzenia raportu z konsultacji Rady interesariuszy projektu. |
|  | **RA IT** | 2.2. Udostępnione e-usługi | Część usług jest atomowymi wydarzeniami, które mogą być częścią innych usług. Można odnieść wrażenie, że usługi zostały sztucznie rozdzielone. | Proszę o analizę i wyjaśnienie lub korektę opisu założeń | W odpowiedzi na uwagę dotyczącą możliwego atomowego charakteru części e-usług, dokonano ponownej analizy katalogu e-usług pod kątem zakresu merytorycznego, interesariuszy oraz relacji organizacyjnych. W wyniku analizy wprowadzono doprecyzowania oraz korekty porządkujące opis usług. Analiza ta została przeprowadzona również w kontekście połączenia zakresów projektów mLekarz oraz Wirtualny Dziekanat, co skutkowało ujęciem w katalogu e-usług procesów związanych z obsługą stażu podyplomowego.  **Połączenie e-usług 1 i 3**  E-usługi dotyczące: (1) obsługi wniosków o przyznanie prawa wykonywania zawodu lekarza/lekarza dentysty w trybach W-2, W-2A–D, W-4, W-4A oraz (3) obsługi wniosków o odtworzenie PWZ i ponowny wpis lekarzy figurujących w archiwum FINN (W-6), zostały ujęte jako jedna e-usługa pod nazwą:  **„Obsługa wniosków o przyznanie i odtworzenie prawa wykonywania zawodu lekarza/lekarza dentysty (PWZ)”**.  Połączenie jest uzasadnione tożsamością typu sprawy administracyjnej (status PWZ), realizacją przez ten sam organ (OIL Warszawa) oraz tym samym głównym interesariuszem (lekarz). E-usługa obejmuje obsługę wniosków dotyczących przyznania prawa wykonywania zawodu lekarza i lekarza dentysty w trybach W-2, W-2A–D, W-4 i W-4A oraz odtworzenia PWZ i ponownego wpisu lekarzy figurujących w archiwum FINN (W-6). Usługa umożliwia elektroniczne składanie wniosków i załączników, automatyczną weryfikację przynależności oraz danych w systemie FINN, a także generowanie uchwał i wydawanie decyzji z podpisem elektronicznym. Podstawową relacją realizacji usługi jest A2C (lekarz – OIL Warszawa), przy czym w przypadku wniosków o przyznanie PWZ występuje dodatkowo relacja A2A lokalna po stronie administracji OIL. |
|  | **RA IT** | 2.4. Produkty końcowe projektu | Zaskakujące jest najpierw wykonanie integracji systemów (Integracje systemowe - FINN, RPWDL, SMK, Węzeł krajowy, V-Desk, ERP IZBA) a dopiero potem dostarczenie pierwszej wersji systemu mLekarz. | Proszę o analizę i wyjaśnienie lub korektę opisu założeń | Integracje z systemami zewnętrznymi (FINN, RPWDL, SMK, Węzeł Krajowy, V-Desk, ERP IZBA) stanowią w projekcie mLekarz element determinujący model danych oraz sposób realizacji kluczowych procesów biznesowych, dlatego ich realizacja została zaplanowana na wczesnym etapie projektu. Na tym etapie integracje obejmują przede wszystkim ustalenie i weryfikację interfejsów (API), mechanizmów uwierzytelniania oraz scenariuszy wymiany danych. Działania te mają charakter przygotowawczy i projektowy oraz są niezbędne do zapewnienia, że wersja systemu mLekarz (beta) będzie mogła funkcjonować w rzeczywistym środowisku integracyjnym.  Jednocześnie projekt zakłada etapowe uruchamianie integracji, w tym możliwość uruchomienia wybranych integracji przed wdrożeniem wersji beta, w ramach bazowej wersji systemu obsługującej kluczowe procesy, przy zachowaniu ograniczonego zakresu funkcjonalnego.  W punkcie 5.1 „Ryzyka wpływające na realizację projektu” zidentyfikowano ryzyko trudności integracyjnych z istniejącymi systemami. W odpowiedzi na to ryzyko przewidziano wczesne testy integracyjne, etapowe uruchamianie integracji oraz zaangażowanie dostawców systemów zewnętrznych już na etapie projektowania rozwiązania. |
|  | **RA IT** | 2.4. Produkty końcowe projektu | Czym jest produkt „model utrzymania systemu”? Jeśli są to założenia utrzymania systemu, to powinny być znane na początku projektu. | Proszę o analizę i wyjaśnienie lub korektę opisu założeń | Model utrzymania systemu jest zestawem polityk, procedur i innych dokumentów opisujących zasady utrzymania systemu teleinformatycznego mLekarz. Model ten zostanie stworzony na bazie projektu systemu i w harmonogramie został umiejscowiony bezpośrednio po jego dostarczeniu.  Dodatkowo, model utrzymania systemu w kontekście finansowym został ujęty w pkt 5.2. dotyczącym ryzyk wpływających na utrzymanie efektów. |
|  | **RA IT** | 2.4. Produkty końcowe projektu | Czas pomiędzy dostarczeniem raportów prywatności, UX, bezpieczeństwa, wydajności a wersją finalną systemu mLekarz wynosi od 0 do 2 miesięcy. To za mało by wprowadzić ewentualne korekty w przypadku negatywnych testów. | Proszę o analizę i wyjaśnienie lub korektę opisu założeń | Harmonogram został skorygowany zgodnie z uwagą – raporty z testów prywatności, UX, bezpieczeństwa i wydajności są obecnie planowane na kilka miesięcy przed wersją finalną systemu mLekarz, co zapewnia wystarczający czas na wprowadzenie ewentualnych korekt i ponowną weryfikację przed decyzją Go-Live.  Jednocześnie projekt zakłada uwzględnienie zasad security by design i privacy by design już na etapie analizy procesów, poprzez identyfikację przepływów danych oraz wymagań bezpieczeństwa. |
|  | **RA IT** | 5.1. Ryzyka wpływające na realizację projektu | Projekt zakłada modyfikacje systemu FINN - Centralny Rejestr Lekarzy i Lekarzy Dentystów – nie oszacowano ryzyka dostępu do systemu, modyfikacji w trakcie działania. | Proszę o analizę i wyjaśnienie lub korektę opisu założeń | Zmodyfikowano ten pkt (ryzyko nr 2) i dodano oprócz dostawców również gestorów systemu.  W celu ograniczenia ryzyk w projekt zostanie włączony przedstawiciel Naczelnej Izby Lekarskiej jako administrator danych oraz gestor systemu FINN, pełniący rolę koordynatora uzgodnień z dostawcami oraz łącznika w zakresie komunikacji i synchronizacji działań z pozostałymi Okręgowymi Izbami Lekarskimi. |
|  | **RA IT** | 7.3. Przyjęte założenia technologiczne | Założenia są tak lakonicznie, że nie można się do nich odnieść. Zdecydowanie potrzeba więcej szczegółów dotyczących technologii rozwiązania. | Proszę o analizę i korektę opisu założeń | Założenia technologiczne zostały uszczegółowione. Poniżej opis. |
|  | **RA IT** | 7.4. Opis zasobów danych przetwarzanych w planowanym rozwiązaniu | Należy zweryfikować opis rejestru PESEL dla obywateli Ukrainy. | Proszę o analizę i korektę opisu założeń | Opis zweryfikowano i zmieniono |

Założenia technologiczne:

|  |  |
| --- | --- |
| **Obszar** | **Założenie technologiczne** |
| Infrastruktura | System będzie oparty na skalowalnej i wysokodostępnej infrastrukturze teleinformatycznej, opartej o wirtualizację i konteneryzację, zapewniającej odporność na awarie oraz możliwość dynamicznego skalowania w odpowiedzi na zmienne obciążenia. Zakłada się eliminację pojedynczych punktów awarii (SPOF) na wszystkich poziomach – od warstwy sprzętowej, przez wirtualizację, aż po warstwę aplikacyjną. Infrastruktura będzie przygotowana do pracy w trybie ciągłym (24/7), z uwzględnieniem procedur odtwarzania po awarii (Disaster Recovery) oraz scenariuszy awarii częściowej i degradacji usług. Warstwa kontenerowa będzie zarządzana przez orkiestrator z automatycznym rozkładaniem obciążeń i samonaprawą usług. Konfiguracja infrastruktury będzie utrzymywana jako kod (IaC), co umożliwi powtarzalne odtwarzanie środowisk oraz kontrolę zmian. |
| Sieć i bezpieczeństwo | Całość komunikacji i przetwarzania danych będzie realizowana zgodnie z obowiązującymi standardami bezpieczeństwa, ochrony danych oraz regulacjami prawnymi. Architektura sieciowa będzie oparta na silnej segmentacji, separacji stref bezpieczeństwa oraz zasadzie minimalnych uprawnień (least privilege). Uwzględnione zostaną integracje z systemami zewnętrznymi o różnym poziomie dojrzałości technicznej, w tym systemami znajdującymi się poza strefami DMZ lub nieposiadającymi nowoczesnych mechanizmów uwierzytelniania. Projekt zakłada stosowanie mechanizmów kontroli ruchu, inspekcji, buforowania i izolowania komunikacji, tak aby ograniczyć ryzyko propagacji incydentów bezpieczeństwa pomiędzy strefami. Dane będą szyfrowane in-rest oraz in-transit. Model bezpieczeństwa będzie realizowany w podejściu Zero Trust, z centralnym uwierzytelnianiem (SSO/MFA) i egzekwowaniem polityk dostępu w oparciu o role i kontekst. Zdarzenia bezpieczeństwa i logi będą konsolidowane w SIEM, a ruch krytyczny dodatkowo chroniony mechanizmami IDS/IPS oraz WAF dla interfejsów webowych i API. |
| Standardy wymiany danych | Integracje z systemami zewnętrznymi będą realizowane w oparciu o uznane standardy interoperacyjności (Krajowe Ramy Interoperacyjności) i formaty danych powszechnie stosowane w administracji publiczne oraz dostępne systemach integrowanych w ramach projektu. Wymiana danych będzie projektowana w sposób maksymalnie odporny na niespójności, opóźnienia oraz niejednoznaczność semantyczną po stronie systemów zewnętrznych. Architektura integracyjna zakłada możliwość adaptacji do systemów legacy, systemów o niskiej jakości API lub opartych na nietypowych mechanizmach komunikacji. Istotnym elementem będzie normalizacja danych, wersjonowanie interfejsów oraz jednoznaczne kontrakty integracyjne, minimalizujące wpływ zmian po stronie partnerów integracyjnych na stabilność systemu centralnego. Interfejsy integracyjne będą publikowane przez bramę API (API Gateway) z mechanizmami autoryzacji, limitowania (rate limiting) i rejestrowania wywołań. Dla integracji asynchronicznych przewiduje się kolejki lub broker wiadomości, a standardowe formaty wymiany będą obejmować m.in. JSON/REST oraz SOAP/XML tam, gdzie wymaga tego otoczenie. |
| Systemy operacyjne serwerowe | Środowiska serwerowe będą oparte na stabilnych i długoterminowo wspieranych (LTS) platformach systemowych klasy produkcyjnej z rodziny Linux zapewniających możliwość spełnienia wymagań audytowych i certyfikacyjnych. Projekt uwzględnia zarządzanie cyklem życia systemów operacyjnych, w tym polityki aktualizacji, testów bezpieczeństwa oraz zgodności z obowiązującymi regulacjami. Środowisko systemowe będzie przygotowane do automatyzacji zarządzania, monitorowania stanu oraz szybkiego odtwarzania w przypadku awarii. Obrazy systemowe będą ustandaryzowane i utwardzone zgodnie z uznanymi benchmarkami (np. CIS), a konfiguracja zarządzana centralnie narzędziami automatyzacji. Aktualizacje będą wdrażane w kontrolowanych oknach serwisowych z wykorzystaniem środowisk testowych oraz mechanizmów rollback, aby ograniczyć ryzyko przestojów. |
| Bazy danych | Architektura bazodanowa będzie projektowana z uwzględnieniem różnorodności danych (transakcyjne, referencyjne, audytowe, historyczne) oraz ich krytyczności. Szczególny nacisk zostanie położony na integralność danych, odporność na błędy logiczne oraz możliwość odtworzenia stanu systemu na określony moment w czasie. Dla kluczowych baz przewiduje się wysoką dostępność (replikacja/klaster) oraz kopie zapasowe umożliwiające odtworzenie do punktu w czasie (PITR) zgodnie z wymaganiami RPO/RTO. Warstwa bazodanowa będzie objęta audytem dostępu, szyfrowaniem oraz monitoringiem wydajności, w tym procedurami okresowej optymalizacji i archiwizacji danych. W miarę możliwości stosowane będą bazy danych otwartoźródłowe. |
| Serwery aplikacji | Warstwa aplikacyjna będzie oparta na architekturze umożliwiającej niezależny rozwój i wdrażanie poszczególnych komponentów (konteneryzacja, mikroserwisy, szyna integracyjna), przy zachowaniu spójności całego ekosystemu. Projekt zakłada odporność na częściowe niedostępności komponentów oraz możliwość stopniowej degradacji funkcjonalności zamiast całkowitego zatrzymania systemu. Istotnym elementem będzie obserwowalność systemu – możliwość monitorowania stanu aplikacji, przepływu danych oraz identyfikacji problemów w czasie rzeczywistym. Wdrażanie będzie realizowane w modelu CI/CD z automatycznymi testami i strategią bezprzerwowych wdrożeń (blue-green/canary) tam, gdzie jest to uzasadnione. Każdy komponent będzie posiadał jasno zdefiniowane limity zasobów, polityki autoskalowania oraz mechanizmy circuit breaker/retry dla połączeń zależnych. |
| Portale | Portale użytkownika będą projektowane z myślą o różnych grupach odbiorców – zarówno użytkownikach końcowych, jak i administratorach czy operatorach systemu. Szczególny nacisk zostanie położony na dostępność, ergonomię oraz odporność na błędy użytkownika. Rozwiązanie będzie uwzględniało konieczność pracy w środowiskach o ograniczonej przepustowości, czasowych przerwach w dostępności usług (PWA) oraz potrzebę zachowania spójnego doświadczenia użytkownika nawet w warunkach obniżonej dostępności części systemu. Portale będą wspierały jednokrotne logowanie (SSO) i federację tożsamości, z rozdzieleniem uprawnień użytkownika i administratora na poziomie aplikacji. Interfejsy będą responsywne i zgodne z WCAG 2.1 AA, a dla funkcji krytycznych przewiduje się tryb ograniczonej funkcjonalności offline z synchronizacją po odzyskaniu łączności. |
| Inne | Całość rozwiązania będzie projektowana w oparciu o podejście długofalowe, uwzględniające nie tylko aktualne wymagania, ale również przyszły rozwój systemu, zmiany regulacyjne oraz ewolucję otoczenia technologicznego. Architektura umożliwi stopniową modernizację, wymianę komponentów oraz integrację z nowymi systemami bez konieczności przebudowy całości. Projekt uwzględnia konieczność transparentności, audytowalności, jednoznacznej odpowiedzialności komponentów oraz możliwości pracy w warunkach podwyższonego ryzyka operacyjnego. Dokumentacja architektury i decyzji projektowych (ADR) będzie prowadzona na bieżąco, a standardy kodowania i bezpieczeństwa będą egzekwowane w procesie wytwórczym (DevSecOps). Założenia obejmują również zarządzanie kosztami i pojemnością (FinOps/Capacity Management) oraz regularne przeglądy techniczne w celu utrzymania zgodności i aktualności komponentów. |