**Wykonawcy/**

**uczestnicy postępowania**

**Odpowiedzi na zapytania wykonawców dotyczące treści SWZ**

Dotyczy postępowania o udzielenie zamówienia publicznego: Utrzymanie, wsparcie techniczne i rozwój Systemu Monitorowania Funduszu Sprawiedliwej Transformacji (SM FST) na potrzeby wdrażania FST w ramach FEDS 2021-2027. Działając na podstawie art. 284 ust. 2 ustawy z dnia 11 września 2019r. Prawo zamówień publicznych (Dz.U.2024.1320), Zamawiający przekazuje treść zapytań wraz z wyjaśnieniami dotyczących zapisów Specyfikacji Warunków Zamówienia. W związku z powyższym, Zamawiający udziela wyjaśnień, które poniżej.

# Pytanie nr 1

Każdy mikroserwis w systemie jest definiowany przy użyciu Helm Chartów, które określają wszystkie niezbędne zasoby Kubernetes, takie jak Deployment, Service, czy Ingress. Pliki te są przechowywane w dedykowanym katalogu w repozytorium GitLab, co ułatwia zarządzanie konfiguracją i wdrażanie nowych wersji mikroserwisów. Czy Wykonawca otrzyma dotychczas używane Helm Charty?

**Odpowiedź na pytanie:**

Zamawiający nie posiada dostępu do plików przechowywanych w dedykowanym katalogu w repozytorium GitLab, tym samym nie ma możliwości ich udostępnienia Wykonawcy.

# Pytanie nr 2

Czy Wykonawca musi przygotować dedykowany mechanizm weryfikacji poprawności migracji danych, który zagwarantuje brak ich utraty lub uszkodzenia? Jeśli tak, to jakie metody weryfikacji są wymagane (np. checksumy, raporty porównawcze)?

**Odpowiedź na pytanie:**

Tak, na Wykonawcy spoczywa ciężar przygotowania dedykowanego mechanizmu weryfikacji poprawności migracji danych, obejmującego checksumy dla integralności, raporty porównawcze liczby i zawartości rekordów, testy integralności relacji, walidację biznesową oraz raportowanie błędów, tak aby zagwarantować brak utraty lub uszkodzenia danych.

# Pytanie nr 3

Czy Zamawiający przewiduje określone procedury walidacji poprawności przeniesionych danych?

**Odpowiedź na pytanie:**

Wymagane/przewidywane są następujące procedury:

* Spójności danych: Porównanie danych źródłowych i docelowych w bazach i repozytoriach (np. liczba rekordów, wartości kluczowe).
* Testy integralności: Weryfikacja kluczy obcych, relacji i zależności między tabelami.
* Testy funkcjonalne: Sprawdzenie działania funkcji biznesowych na przeniesionych danych.
* Automatyczna walidacja: Skrypty walidujące dane zgodnie z ustalonymi regułami.
* Testy użytkownika: Udział Zamawiającego w akceptacji poprawności przeniesionych danych na środowisku testowym.

# Pytanie nr 4

Czy infrastruktura AWS, na której obecnie działa system, będzie w całości odtwarzana na nowym środowisku Wykonawcy, czy dopuszcza się różnice w konfiguracji, pod warunkiem spełnienia wymagań SLA i wydajnościowych?

**Odpowiedź na pytanie:**

Zgodnie z pkt P-3 Opisu Przedmiotu Zamówienia po zawarciu Umowy Zamawiający przekaże w uzgodnionym z Wykonawcą terminie oraz w uzgodniony sposób: kod źródłowy Systemu i kopie baz danych wraz z repozytorium plików oraz dokumentację systemu. Ww. zostaną przekazane w takim kształcie w jakim Zamawiający otrzyma je od obecnego Wykonawcy.

Nowy Wykonawca będzie odpowiedzialny za pełną konfigurację środowisk, w tym za samodzielne przygotowanie konfiguracji m. in. Kubernetes (np. Deployment, Service, ConfigMap, Ingress), pipeline'y CI/CD, Helm Charty jak również konfigurację np. Terrafroma lub innych analogicznych narzędzi.

# Pytanie nr 5

Czy Zamawiający dostarczy szczegółowe scenariusze testowe do weryfikacji działania systemu po

migracji, czy Wykonawca jest odpowiedzialny za ich opracowanie?

**Odpowiedź na pytanie:**

Zamawiający nie dostarczy szczegółowych scenariuszy testowych do weryfikacji działania systemu po migracji. Wykonawca samodzielnie opracuje scenariusze testowe i będzie odpowiedzialny za poprawność zrealizowanych prac.

# Pytanie nr 6

Czy system po migracji musi przejść pełną weryfikację bezpieczeństwa i wydajnościową, jeśli środowisko docelowe ulegnie zmianie?

**Odpowiedź na pytanie:**

Tak, Zamawiający potwierdza, że system po migracji musi przejść pełną weryfikację pod kątem bezpieczeństwa jak i wydajności.

# Pytanie nr 7

Jakie są wymagania dotyczące automatycznego skalowania zasobów w kontekście przewidywanych szczytów obciążenia?

**Odpowiedź na pytanie:**

Wymagania dotyczące automatycznego skalowania zasobów obejmują wykorzystanie mechanizmów takich jak Horizontal Pod Autoscaler (HPA) i Vertical Pod Autoscaler (VPA) w Kubernetes oraz AWS EC2 Auto Scaling, skalowanie na podstawie prognoz historycznych i bieżących metryk (np. CPU, pamięć, kolejki RabbitMQ), a także zapewnienie wysokiej dostępności poprzez równoważenie obciążenia i działanie w wielu strefach dostępności (Multi-AZ). Dodatkowo wymagane jest ustawienie minimalnych i maksymalnych zasobów, utrzymanie rezerwy na szczyty obciążenia oraz regularne testy obciążeniowe w celu optymalizacji parametrów skalowania i zapewnienia wydajności w dynamicznych warunkach.

# Pytanie nr 8

Czy Zamawiający identyfikował już potencjalne ryzyka techniczne, które Wykonawca powinien

uwzględnić w swojej ofercie?

**Odpowiedź na pytanie:**

Tak, Zamawiający zidentyfikował potencjalne ryzyka techniczne, takie jak obciążenie infrastruktury przez API umożliwiające import dużych zbiorów danych, szczególnie przy jednoczesnym korzystaniu przez wielu użytkowników, oraz wpływ nowego modułu eksportu danych w czasie rzeczywistym do CST2021 na zasoby systemowe (CPU, pamięć, przepustowość sieci). Wykonawca powinien uwzględnić konieczność dostawienia dodatkowych węzłów w klastrze Kubernetes (K8s), aby zapewnić odpowiednią skalowalność i wydajność systemu podczas szczytów obciążenia.

# Pytanie nr 9

Czy logi systemowe są przechowywane w centralnym repozytorium, czy rozproszone pomiędzy

serwisy?

**Odpowiedź na pytanie:**

Aktualnie logi systemowe przez krótki okres są przechowywane rozproszone w poszczególnych serwisach i mikroserwisach. Wszystkie logi są następnie zbiorczo przesyłane i przechowywane w centralnym repozytorium w Datadog, co umożliwia ich analizę i monitorowanie w jednym miejscu.

Wykonawca będzie musiał zaproponować własne rozwiązanie dla przechowywania i zarządzania logami, które zapewni skuteczność, zgodność z wymaganiami oraz skalowalność w zależności od infrastruktury, na której system będzie wdrożony.

# Pytanie nr 10

Czy Wykonawca będzie odpowiedzialny za utrzymanie środowiska CI/CD, czy takie procesy pozostaną po stronie Zamawiającego?

**Odpowiedź na pytanie:**

Tak, Wykonawca będzie w pełni odpowiedzialny za utrzymanie środowiska CI/CD.

Wykonawca będzie musiał samodzielnie zaprojektować, wdrożyć oraz zarządzać procesami CI/CD, zgodnie z wymaganiami systemu i najlepszymi praktykami, zapewniając ich efektywność, bezpieczeństwo i niezawodność.

# Pytanie nr 11

Czy Zamawiający wymaga narzędzi do wizualizacji metryk i raportów (np. Grafana, Kibana)?

**Odpowiedź na pytanie:**

Tak, Zamawiający wymaga narzędzi do wizualizacji metryk i raportów, takich jak Grafana lub Kibana. W szczególności wymagane są miesięczne raporty uwzględniające wizualizacje kluczowych metryk, takich jak wydajność systemu, zużycie zasobów, liczba przetworzonych danych oraz statystyki błędów.

# Pytanie nr 12

Czy monitoring systemu (np. Prometheus, Datadog) jest już wdrożony, czy Wykonawca będzie musiał go skonfigurować i dostosować?

**Odpowiedź na pytanie:**

Tak, monitoring systemu obejmujący Prometheus, Datadog, Kibana, Amazon CloudWatch jest już wdrożony w obecnym środowisku. Jednakże Wykonawca będzie musiał zaproponować własne rozwiązanie, odpowiednio je skonfigurować i wdrożyć od początku, zgodnie z wymaganiami oraz specyfiką nowej infrastruktury i oczekiwaniami Zamawiającego.

# Pytanie nr 13

Czy Wykonawca będzie odpowiedzialny za wprowadzanie aktualizacji systemu, w tym frameworków i bibliotek, na których opiera się SM FST?

**Odpowiedź na pytanie:**

Tak, wykonawca będzie odpowiedzialny za wprowadzanie aktualizacji systemu, w tym frameworków i bibliotek, instalując, konfigurując i aktualizując certyfikaty oraz komponenty programistyczne niezbędne do działania SM FST. Wykonawca musi również dostosowywać system do nowych wersji przeglądarek w ciągu 30 dni roboczych od ich wydania oraz zapewniać zgodność zewnętrznych platform i komponentów, takich jak Profil Zaufany czy Szafir, aby zagwarantować prawidłowe działanie mechanizmów uwierzytelniania i podpisywania dokumentów.

# Pytanie nr 14

Czy rozważano możliwość migracji do innej platformy chmurowej, np. Azure lub Google Cloud? Jeśli tak, jakie zmiany w architekturze byłyby konieczne?

**Odpowiedź na pytanie:**

Nie, możliwość migracji do innej platformy chmurowej, takiej jak Azure lub Google Cloud, nie była rozważana, jednak nie jest ona zabroniona.

Jeśli taka migracja miałaby zostać przeprowadzona, konieczne byłoby przeprowadzenie dokładnej analizy, ponieważ wedle wiedzy Zamawiającego wszystkie wiodące chmury (AWS, Azure, Google Cloud) oferują analogiczne usługi, takie jak konteneryzacja, orkiestracja (np. Kubernetes), bazy danych, systemy kolejkowe, monitoring czy cache. Jednak różnice w implementacji, konfiguracji i integracji tych usług mogą wymagać potencjalnej zmiany usług specyficznych dla AWS, takich jak S3, RDS czy ElastiCache, na ich odpowiedniki na innych platformach (np. Azure Blob Storage, Google Cloud SQL).

# Pytanie nr 15

Czy Zamawiający identyfikował ryzyka związane z migracją lub wsparciem technicznym (np. utrata danych, opóźnienia)?

**Odpowiedź na pytanie:**

Ryzyka związane z migracją lub wsparciem technicznym, takie jak utrata danych lub opóźnienia, są w pełni po stronie Wykonawcy. To Wykonawca jest odpowiedzialny za cały proces migracji, w tym zabezpieczenie danych, minimalizację ryzyka oraz zapewnienie płynnego przejęcia wsparcia technicznego zgodnie z wymaganiami Zamawiającego.

# Pytanie nr 16

W jaki sposób zarządzana jest zgodność wersji bibliotek takich jak Npgsql.PostgreSQL, Autofac czy Hangfire w długoterminowym utrzymaniu systemu?

**Odpowiedź na pytanie:**

Zarządzanie zgodnością wersji bibliotek w długoterminowym utrzymaniu systemu realizowane jest poprzez regularne audyty i testy regresyjne, kontrolę wersji w plikach zarządzania pakietami (NuGet), planowe aktualizacje zgodnie z wytycznymi producentów, monitorowanie bezpieczeństwa zależności oraz proaktywne dostosowywanie systemu do nowych wersji w harmonogramie utrzymania.

# Pytanie nr 17

Jak realizowana jest obsługa wyjątków i błędów w komunikacji synchronicznej (REST) i asynchronicznej

(RabbitMQ, AMQP)?

**Odpowiedź na pytanie:**

W komunikacji synchronicznej (REST) obsługa błędów realizowana jest poprzez walidację danych wejściowych, zwracanie odpowiednich kodów http z komunikatami błędów oraz rejestrowanie wyjątków w centralnym systemie logowania. W komunikacji asynchronicznej (RabbitMQ, AMQP) błędy obsługiwane są za pomocą walidacji wiadomości, mechanizmów retry, Dead Letter Queue (DLQ) oraz centralnego logowania i monitoringu kolejek w czasie rzeczywistym.

# Pytanie nr 18

Jakie mechanizmy testowania dostępności WCAG zostały zaimplementowane, aby zapewnić zgodność

z tym standardem?

**Odpowiedź na pytanie:**

W ramach testowania tych funkcjonalności przeprowadzono testy manualne i automatyczne:

* Testy nawigacji klawiaturą.
* Testy z użyciem czytników ekranu: Użycie narzędzi takich jak NVDA, JAWS lub VoiceOver w celu przetestowania systemu pod kątem dostępności dla osób niewidomych.
* Testy z użytkownikami z niepełnosprawnościami: Zaangażowanie osób z różnymi niepełnosprawnościami w proces testowania.
* Testy kontrastu i widoczności.
* Testy responsywności i użyteczności na różnych urządzeniach.
* Testy funkcjonalne z różnymi przeglądarkami i systemami operacyjnymi.

# Pytanie nr 19

Czy system wspiera pełne tłumaczenie interfejsu na inne języki, czy tylko wybrane elementy?

**Odpowiedź na pytanie:**

Tak, system wspiera pełne tłumaczenie interfejsu na inne języki.

# Pytanie nr 20

Jakie są scenariusze awaryjne, które wymagają interwencji manualnej w przypadku problemów z

Kubernetes?

**Odpowiedź na pytanie:**

Sytuacje awaryjne w Kubernetes, które mogą wymagać interwencji manualnej, obejmują m.in. problemy z przydzielaniem zasobów, awarie podów, błędy komponentów kontrolnych, problemy z siecią, Persistent Volumes (PV), nieefektywne skalowanie podów, błędy konfiguracji Ingress/Load Balancer, awarie narzędzi CI/CD oraz problemy z rejestracją usług.

Obecna konfiguracja Kubernetes nie jest dostępna Zamawiającemu i nie zostanie przekazana Wykonawcy. Wykonawca będzie musiał we własnym zakresie opracować i wdrożyć konfigurację Kubernetes, jeśli zdecyduje się na jego użycie.

# Pytanie nr 21

Czy Zamawiający przewiduje zwiększenie się liczby błędów w najbliższych miesiącach, czy są planowane jakieś duże wdrożenia które mogą mieć na to wpływ ? Może są jakieś inne czynniki jakie należy wziąć pod uwagę przy wycenie pracochłonności na najbliższe 9 miesięcy, które mogą zwiększyć zaangażowanie Wykonawcy w prace przy wsparciu technicznym?

**Odpowiedź na pytanie:**

Zamawiający przewiduje możliwość zwiększenia liczby błędów w najbliższych miesiącach, ponieważ może zostać wdrożony mechanizm zasilania Wspólnej Bazy Danych Centralnego Systemu Teleinformatycznego danymi SM FST (każdy uczestnik i podmiot otrzymujący wsparcie w projektach będzie przesyłany z wykorzystaniem usług sieciowych do bazy danych CST2021, w celu umożliwienia raportowania z wykorzystaniem SR2021). Standardowe zagrożenia związane z integracją z nowym systemem obejmują problemy z kompatybilnością, nieprzewidziane błędy w wymianie danych, opóźnienia w synchronizacji czy problemy z wydajnością, które mogą generować zwiększoną liczbę zgłoszeń.

Dodatkowo udostępniony został moduł integracyjny dla systemów zewnętrznych, którego wykorzystanie przez różne podmioty może znacząco zwiększyć zarówno liczbę zgłoszeń dotyczących wsparcia, jak i zapotrzebowanie na zasoby infrastrukturalne, co należy uwzględnić przy wycenie pracochłonności na najbliższe miesiące.

***Odpowiedzi na pytania są integralną częścią SWZ są wiążące dla wszystkich wykonawców***

*Termin składania i otwarcia ofert oraz termin związania ofertą nie ulega zmianie.*