

Załącznik nr 2
do zapytania o cenę w celu oszacowania wartości zamówienia
3/NCBR/2024

ZAMAWIAJĄCY:

AI Technika Sp. z o.o.
Ul. Włocławska 167
87-100 Toruń
KRS 0000841946
NIP 9562360955

OPIS PRZEDMIOTU ZAMÓWIENIA

AI Technika spółka z ograniczoną odpowiedzialnością realizuje projekt pt. *Opracowanie i wdrożenie innowacyjnej w skali świata usługi cyfrowej analizy pyłkowej miodów z wykorzystaniem technologii opartych na automatyzacji i sztucznej inteligencji do zastosowania w sektorze produkcji żywności funkcjonalnej* finansowany w ramach rządowego programu badań naukowych i prac rozwojowych: Program rządowy NUTRITECH - żywienie w świetle wyzwań poprawy dobrostanu społeczeństwa oraz zmian klimatu, organizowanego przez Narodowe Centrum Badań i Rozwoju.

Celem projektu jest realizacja prac badawczo-rozwojowych, których rezultatem będzie innowacja produktowa na skalę światową w postaci systemu cyfrowej analizy pyłkowej miodu bazującego na najnowocześniejszych rozwiązaniach w zakresie sztucznej inteligencji (w tym w szczególności autorską architekturę sztucznych sieci neuronowych). Rezultat będzie komercjalizowany w formie cyfrowego systemu dostępnego w formie usługi SaaS (Software as Service) poprzez przeglądarkę internetową lub poprzez technologię API, dzięki czemu możliwa będzie automatyzacja procesu przekazywania materiałów do systemu a także możliwość otrzymywania wyników w czasie rzeczywistym. Co więcej, mechanizmy związane z procesem analizy pyłkowej miodów w oparciu o procesy poznawcze, analityczne i klasyfikacyjne przy wykorzystaniu mechanizmów uczenia maszynowego będą stanowiły istotną nowość w dotychczasowym stanie technologicznym, przyczyniając się do istotnego rozwoju obszaru badań jakości miodów. Bezpośrednim odbiorcą rezultatu będą osoby działające w łańcuchu produkcji miodu oraz innych produktów pszczelich, w głównej mierze: producenci miodu (tj. pszczelarze indywidualni), przetwórcy miodu, miodowe firmy brokerskie, laboratoria, producenci i dystrybutorzy dodatków specjalistycznych służących do utrzymania gospodarki pasiecznej, czy producenci maszyn i urządzeń dla pszczelarstwa i przetworów.

W ramach realizacji projektu wnioskodawca planuje poniesienie wydatku w postaci zlecenia przygotowania aplikacji WEB wraz z API. W zakres planowanych prac wchodzi:

Projekt zakłada realizację następujących elementów:

1. Dokumentacja projektu
2. Implementacja serwera API
3. Implementacja aplikacji www – panel klienta
4. Implementacja aplikacji www – panel pracownika / laboranta
5. Implementacja aplikacji www
6. Serwer kolejujący próbki do usługi GPU
7. Generator raportów

Dokumentacja projektu

Wymagana jest pełna dokumentacja techniczna i biznesowa, obejmująca:

- Opis architektury systemu
- Specyfikację techniczną wszystkich komponentów
- Przewodniki dla użytkowników i administratorów
- Plan wdrożenia i utrzymania systemu
- Opis procesów analizy pyłkowej i zastosowanych algorytmów AI

Implementacja serwera API

Serwer API powinien umożliwiać:

- Składanie zleceń na analizę próbek
- Sprawdzanie statusu zleceń
- Pobieranie wyników analiz
- Obsługa zewnętrznego storage (macierz S3)
- Obsługę autoryzacji i autentykacji użytkowników
- Load balancer, Load balancer powinien zapewniać:
 - Równomierne rozłożenie obciążenia między serwery API i serwery aplikacji
 - Monitorowanie stanu zdrowia serwerów i przekierowywanie ruchu w przypadku awarii
 - Skalowalność systemu poprzez dodawanie i usuwanie serwerów w zależności od obciążenia
 - Wymagania technologiczne Load Balancer:
 - Protokół: HTTP/HTTPS
 - Algorytmy równoważenia obciążenia: Round Robin, Least Connections, IP Hash
 - Wsparcie dla SSL/TLS
 - Monitorowanie stanu zdrowia serwerów: HTTP health checks

Wymagania technologiczne API:

- REST API
- Format danych: JSON
- Bezpieczeństwo: OAuth 2.0 / JWT
- Skalowalność: Obsługa dużej liczby jednoczesnych zapytań

Implementacja aplikacji www – panel klienta

Panel klienta powinien oferować:

- Interfejs do składania zleceń na analizy
- Podgląd statusu zleceń
- Dostęp do wyników analiz i generowanych raportów
- Zarządzanie kontem użytkownika

Implementacja aplikacji www – panel pracownika / laboranta

Panel pracownika/laboranta powinien oferować:

- Interfejs do zarządzania zleceniami analiz
- Podgląd statusu i wyników analiz
- Narzędzia do ręcznej weryfikacji i korekty wyników
- Narzędzie do przypisywania próbek do cech (etykietowanie klas pod model AI)

Implementacja aplikacji www – backend (SaaS)

Backend systemu powinien obejmować:

- Obsługę logiki biznesowej

- Integrację z serwerem API
- Bezpieczeństwo danych i autoryzację użytkowników
- Skalowalność i wysoką dostępność systemu

Serwer kolejujący próbki do usługi GPU

Serwer kolejujący powinien zapewniać:

- Efektywne zarządzanie kolejką zleceń
- Wysyłanie zleceń do serwera GPU
- Monitorowanie statusu przetwarzania zleceń

Generator raportów

Generator raportów powinien umożliwiać:

- Definiowanie szablonów raportów
- Generowanie raportów w formacie PDF
- Automatyczne wysyłanie raportów do klientów

Wymagania dotyczące bezpieczeństwa

- Ochrona danych osobowych zgodnie z RODO
- Bezpieczeństwo komunikacji (HTTPS/TLS)
- Regularne audyty bezpieczeństwa
- Mechanizmy zapobiegania atakom (np. DDoS)

Wymagania NIS2

System musi być zgodny z Dyrektywą NIS2 (Network and Information Systems Directive 2), która określa środki na rzecz zapewnienia wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii Europejskiej. Wymagania obejmują:

- Zarządzanie ryzykiem: Opracowanie i wdrożenie strategii zarządzania ryzykiem, która identyfikuje, ocenia i minimalizuje ryzyka związane z cyberbezpieczeństwem.
- Bezpieczeństwo systemów i sieci: Wdrożenie odpowiednich środków technicznych i organizacyjnych, w tym mechanizmów monitorowania, detekcji i reagowania na incydenty.
- Zarządzanie incydentami: Opracowanie procedur zarządzania incydentami, w tym mechanizmów raportowania i reagowania na incydenty bezpieczeństwa.
- Kontynuacja działania: Zapewnienie ciągłości działania systemu, w tym planów odzyskiwania po awarii i testowania procedur awaryjnych.
- Zarządzanie łańcuchem dostaw: Identyfikacja i zarządzanie ryzykiem związanym z dostawcami oraz partnerami technologicznymi.

Standardy OWASP

System musi być zgodny ze standardami bezpieczeństwa OWASP (Open Web Application Security Project), w szczególności:

- OWASP: Identyfikacja i ochrona przed najczęściej występującymi zagrożeniami dla aplikacji webowych, w tym:
 - Injections (np. SQL, NoSQL, Command Injection)
 - Broken Authentication
 - Sensitive Data Exposure
 - XML External Entities (XXE)
 - Broken Access Control
 - Security Misconfiguration

- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging & Monitoring
- Bezpieczne kodowanie: Stosowanie zasad bezpiecznego kodowania zgodnych z wytycznymi OWASP, w tym unikanie podatności na ataki XSS, CSRF, i inne typowe zagrożenia.
- Bezpieczeństwo danych: Stosowanie mechanizmów szyfrowania danych zarówno w transzycie (TLS/SSL), jak i w spoczynku, zapewniając ochronę wrażliwych informacji przed nieautoryzowanym dostępem.
- Kontrola dostępu: Implementacja zaawansowanych mechanizmów kontroli dostępu, w tym uwierzytelnianie wieloskładnikowe (MFA) i role-based access control (RBAC).

Zasoby kadrowe

W zakresie zasobów kadrowych, podwykonawca powinien dysponować specjalistami z odpowiednim wykształceniem (wyższym lub technicznym)

Wymagania dotyczące zasobów kadrowych i doświadczenia

Podwykonawca powinien dysponować zespołem specjalistów z odpowiednim wykształceniem oraz doświadczeniem, aby zapewnić skuteczną realizację projektu cyfrowej analizy pyłkowej miodu. Wymagania dotyczące zasobów kadrowych obejmują:

Wykształcenie

- Specjaliści ds. Sztucznej Inteligencji i Uczenia Maszynowego: Wykształcenie wyższe (magisterskie lub inżynierskie) w dziedzinie informatyki, matematyki, fizyki lub pokrewnych. Doświadczenie w projektowaniu i wdrażaniu modeli AI/ML.
- Programiści Backend: Wykształcenie wyższe techniczne w dziedzinie informatyki, inżynierii oprogramowania lub pokrewnych. Znajomość technologii takich jak Python, Node.js, oraz doświadczenie w pracy z bazami danych SQL i NoSQL.
- Programiści Frontend: Wykształcenie wyższe techniczne w dziedzinie informatyki lub pokrewnych. Znajomość frameworków takich jak React lub Angular oraz doświadczenie w tworzeniu interfejsów użytkownika.
- Specjaliści ds. Bezpieczeństwa IT: Wykształcenie wyższe w dziedzinie informatyki, bezpieczeństwa informacji lub pokrewnych. Certyfikacje takie jak CISSP, CISM, CEH będą dodatkowym atutem.
- Administratorzy Systemów i Sieci: Wykształcenie wyższe techniczne w dziedzinie informatyki lub pokrewnych. Doświadczenie w zarządzaniu systemami rozproszonymi, znajomość narzędzi do monitorowania i zarządzania infrastrukturą IT.

Doświadczenie

- Realizacja dużych projektów: Firma powinna mieć udokumentowane doświadczenie w realizacji projektów obsługujących ponad 1000 użytkowników.
- Zarządzanie dużymi bazami danych: Doświadczenie w zarządzaniu i przetwarzaniu baz danych zawierających ponad 10 milionów wierszy.
- Rozwiązania rozproszone: Doświadczenie w tworzeniu rozwiązań rozproszonych zgodnych z wymaganiami NIS2, w tym:
 - Projektowanie i wdrażanie architektur mikroserwisowych
 - Zastosowanie load balancerów do równoważenia obciążenia
 - Zapewnienie wysokiej dostępności i skalowalności systemów
- Bezpieczeństwo: Udokumentowane doświadczenie w implementacji standardów bezpieczeństwa OWASP oraz zgodności z NIS2, w tym przeprowadzanie regularnych audytów bezpieczeństwa i testów penetracyjnych.

Spełnienie powyższych wymagań kadrowych i doświadczenia jest kluczowe dla zapewnienia, że podwykonawca posiada niezbędne kompetencje i zasoby do skutecznej realizacji projektu. Prosimy o przedstawienie odpowiednich referencji oraz szczegółowego opisu doświadczenia zespołu w odpowiedzi na to RFI.

.....
miejsowość, data

.....
*podpis i pieczęć osoby/osób uprawnionej
do reprezentowania oferenta*