Opis przedmiotu zamówienia

I. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa oraz wdrożenie oprogramowania do automatyzacji procesów rejestracji korespondencji przychodzącej w ministerstwie.

W ramach przedmiotu zamówienia Wykonawca zrealizuje dostawę oraz wdrożenie oprogramowania do automatyzacji procesów rejestracji korespondencji przychodzącej z kanałów e-mail w systemie Elektronicznego Zarządzania Dokumentacją (EZD PUW) Zamawiającego wraz ze świadczeniem usług wsparcia oraz instruktażem wdrożeniowym w zakresie robotyzacji procesów biznesowych w technologii RPA (Robotic Process Automation).

II. Szczegółowy zakres zamówienia

W ramach realizacji zamówienia Wykonawca zobowiązany będzie do:

1. **Wdrożenia** Platformy do robotyzacji, rozumianej jako spójne połączenie zbioru komponentów IT, w tym: oprogramowania infrastrukturalnego, narzędzi do budowy i zarządzania robotami programowymi, a także reguł zarządzania nimi, zgodnie z poniższymi zasadami:
    a. opracowanie harmonogramu wdrożenia;
    b. instalacja i konfiguracja Platformy na środowisku Zamawiającego przez Wykonawcę pod nadzorem Zamawiającego;
    c. przeprowadzenie testów bezpieczeństwa przez Zamawiającego;
    d. przygotowanie i dostarczenie dokumentacji powdrożeniowej dot. obsługi Platformy;
    e. opracowania i dostarczenie podręczników użytkownika i administratora w języku polskim.
2. **Opracowania i uruchomienia Robota** nadzorowanego, przeznaczonego do zautomatyzowania zadań wykonywanych obecnie przez Kancelarię Główną MRiT**,** przez co rozumiemy zaprojektowanie, wytworzenie, wdrożenie, przetestowanie i stabilizację na środowisku produkcyjnym, zgodnie z poniższymi zasadami:
    a. analizę przedwdrożeniową procesu biznesowego, w tym: projektu funkcjonalnego / projektu realizacji Robota (PFR/PRR),
    b. instalację i uruchomienie robota na środowisku testowym,
    c. przygotowanie scenariuszy testowych,
    d. przeprowadzenie testów akceptacyjnych z udziałem Zamawiającego,
    e. uruchomienie produkcyjne obejmujące co najmniej instalację i walidację robota na środowisku produkcyjnym,
    f. dostarczenie dokumentacji Robota, scenariuszy testowych oraz instrukcji użytkowania Robota,
    g. instruktaż z obsługi Robota.
3. **Dostarczenia subskrypcji oprogramowania na platformę do robotyzacji na okres 12 miesięcy.**
   Licencję należy dostarczyć do Zamawiającego w dniu następnym po podpisaniu protokołu odbioru Robota.
4. **Dostarczenia subskrypcji na robota nadzorowanego na okres 12 miesięcy**
   Licencje należy dostarczyć do Zamawiającego w dniu następnym po podpisaniu protokołu odbioru Robota.

5. **Dostarczenia subskrypcji oprogramowania pozwalającego na obsługę wytworzonych robotów programowych, możliwość zmiany kodu robota programowego i tworzenia kodu dla robotów programowych oraz testowanie procesów dla co najmniej 2 użytkowników**
   Licencje należy dostarczyć do Zamawiającego w dniu następnym po podpisaniu protokołu odbioru Robota w porozumieniu z Zamawiającym co do szczegółowego terminu.

6. **Świadczeniu usług utrzymaniowych Robota, w tym co najmniej:**
   a. zapewnienie usługi wsparcia i asysty technicznej dla oprogramowania na zasadach określonych przez producenta oprogramowania w wersji Premium Support, obejmujące systemy: produkcyjny i dewelopersko/testowy;
   b. wykonanie analizy i diagnozy oraz określenie miejsca wystąpienia błędu/usterki/awarii, a następnie jej usunięcie w określonym czasie w zależności od rodzaju;
   c. raportowanie błędów w czasie rzeczywistym i cyklicznym;
   d. wsparcie przy wykonaniu dodatkowych prac konfiguracyjnych i administracyjnych;
   e. zapewnienie dostępu do wszystkich aktualizacji i rozszerzeń oprogramowania UI Path w ramach zakupionych licencji, a także wsparcie przy ich wprowadzaniu;
   f. świadczenie usługi konsultacyjno-doradczej, miesięcznie przez okres 12 miesięcy w ilości nie więcej niż 40 godzin od daty podpisania protokołu odbioru dot. instalacji i konfiguracji oprogramowania a także obsługi robota na infrastrukturze Zamawiającego.

7. **Przeprowadzenia instruktażu wdrożeniowego**
   1. Przeprowadzenie instruktażu wdrożeniowego w formie stacjonarnej lub online w celu podniesienia kompetencji i wiedzy pracowników Zamawiającego dla grupy składających się maksymalnie z 5 osób w ilości co najmniej 20 godzin szkoleniowych. Warsztaty powinny obejmować m.in.:
      a. obsługę narzędzia zarządzającego pracą Robota,
      b. zarządzanie kodem Robota,
      c. zastosowanie dobrych praktyk przy zarządzaniu narzędziem,
      d. obsługę narzędzia deweloperskiego,
      e. omówienie zasad działania integracji, sposobów komunikacji pomiędzy poszczególnymi komponentami narzędzia, a także ich utrzymanie i rozwój.
   2. Instruktaż dla wskazanego pracownika IT w celu poprawnej instalacji i aktualizacji oprogramowania na infrastrukturze Zamawiającego,
   3. Przeprowadzenie przedmiotowych warsztatów w oparciu o materiały szkoleniowe przygotowane przez Wykonawcę w języku polskim.

8. **Wykonania Dokumentacji powdrożeniowej**
   Wykonawca opracuje dokumentację w języku polskim i dostarczy ją Zamawiającemu w wersji elektronicznej - w edytowalnym formacie DOC i formacie PDF, w przypadku dokumentów tekstowych oraz w przypadku diagramów/schematów w innych formatach, zapewniających ich import do repozytorium będącym w posiadaniu Zamawiającego (BPMN i/lub EA). Cała dokumentacja będzie podlegała akceptacji Zamawiającego.

Platforma do robotyzacji dostarczona przez Wykonawcę musi realizować podstawowe (minimalne) wymagane funkcjonalności zawarte w tabeli poniżej:

F01	Robot musi być zarządzany z centralnego narzędzia, zarządzającego Platformą Robotów, zainstalowanego w infrastrukturze Zamawiającego. Zamawiający nie dopuszcza rozwiązania chmurowego ani nie dopuszcza rozwiązania, które będzie wysyłać przetwarzane dane poza infrastrukturę Zamawiającego.

F02	Środowisko do zarządzania Platformą Robotów musi być szyfrowane protokołem TLS (HTTPS) min. 1.2
F03	Proponowane narzędzie powinno charakteryzować się bezproblemową integracją z technologiami firmy Microsoft, w tym między innymi pakietem Microsoft Office.
F04	Rozwiązanie musi umożliwiać budowę Robotów w modelu wizualnym (drag & drop).
F05	Oferowane rozwiązanie nie może wymagać stałego połączenia z Internetem podczas wykonywania automatyzacji/pracy Robota.
F06	Oferowane narzędzie posiada funkcjonalność tworzenia komponentów wielokrotnego użytku zapewniającą używanie tego samego scenariusza automatyzacji oraz kodu w scenariuszach Robota nadzorowanego.
F07	Rozwiązanie musi wykorzystywać jedno wspólne, spójne narzędzie do budowania automatyzacji nadzorowanych.
F08	Rozwiązanie musi zapewniać w pełni wizualne budowanie czynności Robota w interfejsie graficznym z wykorzystaniem gotowych komponentów umieszczanych na diagramie metodą przeciągnij i upuść, bez konieczności kodowania kroków Robota w językach programowania. Poprzez powyższe Zamawiający rozumie graficzne przedstawienie zadań za pomocą diagramu blokowego zapewniającego użytkownikom biznesowym używanie narzędzia do robotyzacji i zarządzania procesami.
F09	Rozwiązanie musi posiadać nagrywarkę przebiegu procesu przyspieszającą budowanie scenariusza pracy Robota i zapewniać edycję każdego kroku bez konieczności ponownego nagrywania. Nagrywarka musi działać na wszystkich technologiach, które podlegać będą automatyzacji stosowanych przez Zamawiającego.
F10	Rozwiązanie musi zapewniać uruchamianie w trakcie działania Robota dowolnego dodatkowego kodu napisanego za pomocą dedykowanej aktywności wspieranej przez producenta oprogramowania i opisanej w oficjalnej dokumentacji dostępnej publicznie w szczególności w językach wykorzystywanych przez Zamawiającego. Dodatkowy kod do uruchomienia musi być widoczny na diagramie w formie wizualnej jako osobny komponent. Screen Scraping nie jest akceptowalny jako metoda połączenia z GUI.
Szczegółowe wymagania funkcjonalne Robota	
F11	**Skanowanie i identyfikacja danych** • Robot musi skanować wielopoziomową strukturę folderów na wskazanym zasobie (Microsoft Outlook lub dysk sieciowy) • Obsługiwane formaty plików: .msg, .eml, .mht, .xml, .pdf. • Mechanizm ignorowania plików już przetworzonych • Prawidłowa obsługa polskich znaków niezależnie od kodowania.
F12	**Parsowanie i walidacja e-mail** • Ekstrakcja danych: nadawca, odbiorca, data, temat oraz treść korespondencji. • Identyfikacja i wypakowanie załączników. • Korekta tematów: Robot powinien usuwać znaki oraz skracać zbyt długie tematy lub dodawać parametry, aby dostosować je do wymogów EZD PUW.
F13	**Integracja z systemem EZD PUW** • Automatyczne logowanie: Obsługa poświadczeń oraz zatwierdzanie ewentualnych popup'ów systemowych. • Tworzenie tzw. koszulki: Rejestracja wiadomości z automatycznym wypełnieniem metadanych koszulki (na podstawie nazwy folderu i treści z maila). • Załączniki: Dodawanie wyekstrahowanych załączników do koszulki w EZD PUW.
F14	**Przekazywanie i zarządzanie plikami** • Automatyczne przesłanie zarejestrowanej koszulki na sekretariat właściwego departamentu zgodnie ze ścieżką obiegu.

	• Po zakończeniu pracy: przeniesienie pliku do folderu „Przetworzone” (z datą) lub w razie błędu do innego dedykowanego (np. „Do_weryfikacji”).
F15	**Obsługa błędów, monitorowanie i raportowanie** • Mechanizm Retry: W przypadku błędu komunikacji z EZD PUW, Robot musi ponowić próbę określoną liczbę razy przed skierowaniem sprawy do obsługi manualnej. • Raportowanie: Po każdym uruchomieniu robot generuje raport (CSV/Excel) zawierający statystyki (liczba sukcesów/błędów, czas wykonania) i zapisuje go w historii (min. 90 dni). • Powiadomienia: Wysyłanie alertów e-mail do pracowników Kancelarii w przypadku wystąpienia błędów krytycznych.
F16	**Wymagania techniczne i konfiguracja** • Harmonogram: Robot musi pracować co najmniej według ustalonego harmonogramu (np. 3 razy dziennie: 9:00, 12:00, 15:00) z możliwością zwiększenia częstotliwości do trybu co godzinę (cykliczne skanowanie) lub na aktywowanie pracownika Kancelarii. • Konfigurowalność: Kluczowe parametry (ścieżki folderów, dane dostępowe, mapowanie folder-departament) muszą być edytowalne w zewnętrznym pliku konfiguracyjnym bez konieczności zmiany kodu. • Skalowalność: Rozwiązanie powinno umożliwiać późniejszą rozbudowę o automatyzację innych wpływów: np. z ePUAP, eDOR.
F17	**Wskaźniki jakości (SLA)** Oczekiwana skuteczność poprawnego przetwarzania maili i dokumentów przez Robota powinna kształtować się na poziomie min. 98%.

III. Termin realizacji zamówienia

Wykonawca zobowiązuje się do zrealizowania Przedmiotu zamówienia w następujących terminach:

1. przygotowanie harmonogramu wdrożenia technologii RPA obejmującego:
    a. instruktaż;
    b. instalację narzędzia;
    c. testów aplikacji;
    d. stworzenie Robota;
    e. testów Robota na środowisku produkcyjnym,

w terminie do **5 dni roboczych** od dnia podpisania Umowy;

2. wdrożenie platformy na środowisku produkcyjnym – do **10 dni roboczych** od dnia udostepnienia środowiska przez Zamawiającego;
3. instruktaż dla administratorów i użytkowników – do **10 dni roboczych** od dnia podpisania Umowy;
4. testy bezpieczeństwa platformy – do **14 dni roboczych** od wdrożenia platformy na środowisku produkcyjnym;
5. uruchomienie Robota na środowisku produkcyjnym po testach akceptacyjnych – do **25 dni roboczych** od dnia podpisania Umowy.

IV. Gwarancja

Wykonawca udziela Zamawiającemu gwarancji na okres 12 miesięcy od dnia podpisania protokołu odbioru wdrożenia Robota na prawidłowe działanie wdrożonego Robota nadzorowanego.

V. Usługi Wsparcia

Usługi wsparcia producenta – w zakresie środowiska RPA.

W zakresie Platformy Wykonawca zapewni wsparcie na warunkach określonych przez producenta oprogramowania.

W ramach wsparcia Wykonawca zobowiązany będzie do obsługi zgłoszeń serwisowych (*błąd krytyczny, błąd niekrytyczny / zgłoszenie bez błędu*) w dni robocze w godzinach 8 – 16. Przez Zgłoszenie rozumie się poinformowanie Wykonawcy o zaistniałym wydarzeniu przez administratora lub innego upoważnionego przedstawiciela Zamawiającego na wskazany nr telefonu lub na e-mail.

Usługi wsparcia w zakresie Robota

Czas usunięcia ***błędu krytycznego*** wynosi 1 dzień roboczy od momentu przesłania Zgłoszenia przez Zamawiającego, przy czym jako błąd (usterka krytyczna) Zamawiający rozumie oprogramowanie, które nie działa lub zaistniał błąd w środowisku produkcyjnym powodujący niezgodne funkcjonowanie oprogramowania z dokumentacją oprogramowania, które zakłóca działanie wszystkich bądź kluczowych funkcjonalności systemu, wskutek czego znacząco utrudnia lub uniemożliwia realizację prac przez Zamawiającego. Do błędów krytycznych zalicza się również wszelkie zidentyfikowane w trakcie trwania umowy podatności bezpieczeństwa.

Podatność bezpieczeństwa to zidentyfikowana i zdefiniowana przez Zamawiającego wada oprogramowania lub brak odpowiedniego zabezpieczenia, które według Zamawiającego w sposób bezpośredni lub pośredni zagrażają bezpieczeństwu zasobów Zamawiającego. Do podatności bezpieczeństwa zaliczamy w szczególności podatności opisane w ramach aktualnych wersji projektów OWASP TOP 10.

Czas usunięcia ***błędu niekrytycznego*** wynosi 5 dni roboczych od momentu przesłania Zgłoszenia przez Zamawiającego, przy czym jako błąd niekrytyczny Zamawiający rozumie błąd, w wyniku zaistnienia którego dane funkcjonalności systemu nie są dostępne dla Zamawiającego i nie jest możliwe zastosowanie obejścia, nie powodujący znaczących utrudnień, o których mowa w definicji błędu krytycznego.

Czas usunięcia ***zgłoszenia bez błędu*** wynosi 30 dni roboczych od momentu przesłania Zgłoszenia przez Zamawiającego, przy czym jako zgłoszenie bez błędu Zamawiający rozumie pytania dotyczące oprogramowania i konsultacje.

VI. Bezpieczeństwo Platformy

1. Dostarczona Platforma zostanie przetestowana przez Zamawiającego pod kątem spełnienia wymogów bezpieczeństwa.
2. Wykonawca dostarczy dokumentację Platforma niezbędną do przeprowadzenia testów bezpieczeństwa.
3. Platforma musi zapewniać mechanizmy zabezpieczające przed podatnościami bezpieczeństwa, w szczególności z aktualnej listy TOP 10 wg organizacji OWASP (OWASP TOP 10 Web Application Security Risk oraz OWASP TOP 10 Desktop Application Security Risk) oraz podatnościami opisywanymi w zaktualizowanym OWASP Testing Guide.
4. Platforma musi posiadać mechanizmy walidacji danych wejściowych i wyjściowych w szczególności pod kątem ataków typu cross-site scripting (XSS) oraz injection (SQL, code, shell).
5. Platforma musi zapewniać bezpieczeństwo komunikacji danych poprzez silne szyfrowanie za pomocą algorytmów, które są powszechnie uznawane za bezpieczne i pozbawione są powszechnie znanych błędów.

6. Platforma musi zapewnić mechanizmy zabezpieczające przed podatnościami związanymi z kontrolą dostępu (np. niezabezpieczone bezpośrednie odwołania do obiektów, nieograniczony dostęp URL, nieograniczony dostęp użytkowników do funkcji, eskalacje uprawnień, niewłaściwe zarządzanie sesją użytkownika).
7. Platforma musi zapewniać mechanizmy zabezpieczające przed podatnościami wynikającymi z nieodpowiedniego zarządzania błędami oraz nadmiarowym ujawnieniem informacji o infrastrukturze.
8. Platforma musi zapewniać mechanizmy pełnego monitorowania i logowania zdarzeń.
9. W ramach prac utrzymaniowych Wykonawca jest odpowiedzialny za monitorowanie, wykrywanie i usuwanie pojawiających się luk bezpieczeństwa w Platformie.
10. Platforma musi korzystać wyłącznie z aktualnych i wolnych od znanych podatności bezpieczeństwa komponentów oraz bibliotek programistycznych przez cały okres wsparcia producenta.
11. Każdy z elementów Platformy (baza danych, systemy operacyjne, serwery webowe/aplikacyjne oraz inne dostarczone przez Wykonawcę komponenty informatyczne itd.) musi być poddany procesowi utwardzania (hardeningu) zgodnie z powszechnie dostępnymi w sieci Internet zaleceniami producenta w celu uzyskania maksymalnej możliwej odporności systemu na ataki.
12. Wymagania bezpieczeństwa dla systemu, wymienione w ww. punktach, muszą być spełnione bez wykorzystywania w tym celu infrastruktury MRiT.