

Manila, 27 marca 2025 r.

ZAPYTANIE O OSZACOWANIE KOSZTÓW

Szanowni Państwo,

W związku z planowanym udzieleniem zamówienia publicznego na realizację usługi przyjmowania wniosków wizowych przez podmiot zewnętrzny na rzecz polskiego urzędu konsularnego na Filipinach w trybie zamówienia z wolnej ręki, Ambasada RP w Manili w ramach rozeznania rynku zwraca się z uprzejmą prośbą o wycenę usługi, przy założeniu opisanych poniżej wymagań dotyczących przedmiotu zamówienia.

I. Przedmiot zamówienia (zamówienie podstawowe):

Usługa przyjmowania wniosków wizowych w rozumieniu art. 43 Rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 810/2009 z dnia 13 lipca 2009 r. ustanawiającego Wspólnotowy Kodeks Wizowy, dalej jako: „Wspólnotowy Kodeks Wizowy” lub „WKW”, oraz zwrotu dokumentów i decyzji wizowych na terytorium Republiki Filipin na rzecz Zamawiającego – Ambasady RP w Manili. Maksymalną liczbę wniosków wizowych szacuje się na nie więcej niż 20 000 (słownie: dwadzieścia tysięcy) w okresie trwania umowy wynoszącym 2 lata.

Zamawiający przewiduje możliwość udzielenia zamówień podobnych do 50% wartości zamówienia podstawowego, stosownie do art. 214 ust. 1 pkt. 7 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (zwanej dalej Pzp), w szczególności w sytuacji zrealizowania przedmiotu zamówienia przed upływem terminu realizacji umowy, tj. przyjęcia maksymalnej liczby wniosków wizowych objętych przedmiotem zamówienia.

Poprzez wnioski wizowe należy rozumieć wnioski o wydanie wizy Schengen, wnioski o wydanie wizy krajowej oraz wnioski o ich ponowne rozpatrzenie.

Konieczne będzie uruchomienie przez Wykonawcę umowy 2 punktów przyjmowania wniosków wizowych (dalej: PPWW) w miejscowościach Manila i Cebu w celu przyjmowania wniosków wizowych oraz zwrotu dokumentów i decyzji wizowych.

Wymagane będzie świadczenie usług informacyjnych dla wnioskodawców w szczególności poprzez utworzenie i utrzymywanie dedykowanej stabilnej witryny internetowej, która powinna być dostępna w języku angielskim, jak i prowadzenie obsługi telefonicznej i e-mailowej klienta w językach angielskim i tagalog.

Strona internetowa musi umożliwiać umawianie spotkań w celu złożenia wniosku wizowego przez osoby fizyczne, z zastosowaniem zaawansowanych narzędzi informatycznych oraz identyfikacji biometrycznej, które uniemożliwią rejestrację spotkania przez osoby trzecie, osoby prawne czy algorytmy, a także umożliwi przyjmowanie opłaty serwisowej pobieranej od przyjętego wniosku

wizowego od wnioskodawcy. Opłata serwisowa od wnioskodawcy będzie pobierana w momencie dokonywania rejestracji przez wnioskodawcę poprzez stronę internetową.

Wykonawca musi dysponować własnymi narzędziami IT oraz możliwościami kadrowo-technologicznymi tak, aby całokształt prac związanych ze stroną internetową i systemem teleinformatycznym, jak bieżący nadzór, programowanie, modernizacja, dostosowanie systemów do nowych potrzeb, mógł być realizowany bez zbędnej zwłoki i nie był uzależniony od pomiotów zewnętrznych.

II. Wymagania ogólne:

Wykonawca zapewni w szczególności, że:

- nie prowadzi i nie będzie prowadził w okresie obowiązywania Umowy, działalności godzącej w interesy bądź wizerunek Rzeczypospolitej Polskiej;
- będzie prowadził outsourcing wizowy w zgodzie z przepisami prawa Rzeczypospolitej Polskiej, prawa Republiki Filipin oraz interesem publicznym;
- nie występuje i w okresie obowiązywania Umowy nie będzie występował konflikt interesów, czyli sytuacja, w której inna działalność prowadzona przez Wykonawcę lub jego powiązania mogłyby wpływać na jego bezstronność i rzetelność wykonywania Umowy;
- będzie stosował zabezpieczenia ochrony danych 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 dalej: „ogólne rozporządzenie o ochronie danych”, tj. przestrzegał przepisów ogólnego rozporządzenia o ochronie danych, przepisów określonych w załączniku X do Wspólnotowego Kodeksu Wizowego oraz odnośnych polskich przepisów o ochronie danych osobowych.

Wykonawca bierze pełną odpowiedzialność za działania i zaniechania personelu i innych osób zaangażowanych w realizację Umowy oraz będące następstwem działania i zaniechania skutki.

Wykonawca musi dysponować odpowiednim potencjałem osobowym, materiałowym, finansowym oraz technicznym pozwalającym na prawidłowe zrealizowanie przedmiotu zamówienia.

Wykonawca zobowiązuje się podjąć wszelkie niezbędne kroki organizacyjne celem sprawnej obsługi wnioskodawców, a w szczególności zapobiegania tworzenia się kolejek i wydłużania terminu umawiania wizyt.

Wykonawca musi zachować najwyższą staranność wynikającą z zawodowego charakteru prowadzonej działalności, zgodnie ze wszelkimi obowiązującymi przepisami, rzetelnie i terminowo, mając na względzie ochronę interesów polskich urzędów konsularnych w Republice Filipin.

III. Warunki niezbędne do udziału w postępowaniu

Na potwierdzenie spełnienia warunku udziału w postępowaniu dotyczącego zdolności technicznej lub zawodowej Zamawiający wymaga, aby Wykonawca:

wykazał się niezbędnym doświadczeniem, tj.

w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, wykonał, a w przypadku świadczeń okresowych lub ciągłych również należycie wykonuje co najmniej 2 usługi polegające na przyjmowaniu wniosków wizowych na rzecz 1 wybranej placówki dyplomatycznej albo konsularnej państwa Strefy Schengen, stosownie do dyspozycji art. 43 Wspólnotowego Kodeksu Wizowego (KW), niezależnie od tego, czy usługa była świadczona na podstawie umowy globalnej obejmującej wiele krajów, czy też umowy dotyczącej świadczenia usługi na rzecz tylko jednego kraju, wykonana/wykonywana usługa musi obejmować co najmniej 5000 (słownie: pięć tysięcy) wniosków wizowych przyjętych w okresie nie dłuższym niż 12 kolejnych miesięcy.

Zamawiający dopuszcza usługę świadczoną na podstawie umowy zawartej bezpośrednio z placówką dyplomatyczną albo konsularną, czy też na podstawie umowy zawartej z innym podmiotem (np. Ministerstwem Spraw Zagranicznych danego państwa Strefy Schengen lub innym urzędem tego państwa).

Nie dopuszcza się sumowania liczby wniosków realizowanych na rzecz kilku placówek dyplomatycznych lub konsularnych w danym państwie.

W przypadku usług wykonywanych Zamawiający wymaga, aby zrealizowana część usługi na dzień składania ofert wyniosła co najmniej 5000 przyjętych wniosków wizowych na rzecz jednego podmiotu w okresie nie dłuższym niż 12 kolejnych miesięcy.

W przypadku umów dłuższych niż 1 (słownie: jeden) rok Zamawiający będzie brał pod uwagę tylko jeden 12-miesięczny okres wskazany przez Wykonawcę.

wyказаł się dysponowaniem osobami zdolnymi do wykonania zamówienia, tj. wykazał, że dysponuje lub będzie dysponować co najmniej:

Koordynatorem w PPWW (Manila) i PPWW (Cebu) posiadającym co najmniej:

- a) 2-letnie doświadczenie w zarządzaniu zespołem pracowników.
- b) 1- roczne doświadczenie w obszarze wykonywania usługi polegającej na przyjmowaniu wniosków wizowych na rzecz placówki dyplomatycznej albo konsularnej państwa Strefy Schengen, stosownie do dyspozycji art. 43 Wspólnotowego Kodeksu Wizowego (KW).
- c) Znajomość języka angielskiego na poziomie co najmniej C1 zgodnie z Europejskim systemem opisu kształcenia językowego (CEFR) opracowanym przez Radę Europy (zamawiający dopuszcza potwierdzenie poziomu znajomości języka poprzez uzyskanie świadectwa ukończenia szkoły na poziomie szkoły średniej z wymaganym językiem jako wykładowym).

IV. PPWW musi spełniać następujące wymagania:

Musi znajdować się w obrębie centrum miasta z uwzględnieniem łatwego dla wnioskodawców dojazdu środkami transportu miejskiego, w bliskim sąsiedztwie stacji metra (o ile w danym mieście funkcjonuje) albo przystanków komunikacji miejskiej.

Musi zapewniać warunki do obsługi osób niepełnosprawnych i z ograniczeniami ruchowymi, tj. posiadać podjazd dla osób poruszających się na wózkach inwalidzkich oraz dla rodziców z wózkami z dziećmi, odpowiednio zaadaptowaną windę dla takich osób w przypadku PPWW usytuowanych na

piętrach budynku, co najmniej jedno stanowisko przystosowane do obsługi ww. osób oraz odpowiednio przystosowaną toaletę. PPWW muszą umożliwić obsługę kasową klienta.

Lokalizacje PPWW podlegają zatwierdzeniu przez Zamawiającego.

PPWW musi posiadać niedostępne dla osób postronnych pomieszczenia biurowe przeznaczone do przetwarzania danych wizowych (stanowiska do wprowadzenia wniosków wizowych do systemu elektronicznego oraz szyfrowania i zgrywania pakietów danych na nośnik), stanowiska przeznaczone do przygotowania wniosków wizowych wraz z paszportami do urzędów konsularnych, stanowiska przeznaczone do przygotowania odebranych z konsulatów paszportów do wydania Wnioskodawcom.

PPWW muszą być wyposażone w systemy przeciwpożarowe oraz ochraniane przez 24 godziny na dobę przy użyciu monitoringu (dozoru wizyjnego) i systemów alarmowych oraz, minimum w godzinach otwarcia PPWW, przy użyciu wyspecjalizowanej ochrony fizycznej.

Wejścia do pomieszczeń biurowych PPWW muszą być zabezpieczone przed dostępem osób nieuprawnionych przy użyciu elektronicznego systemu kontroli dostępu.

Pomieszczenia do przechowywania wniosków wizowych wraz z paszportami muszą być wyposażone w szafę pancerną i zabezpieczone przy użyciu elektronicznego systemu kontroli dostępu przed dostępem osób nieuprawnionych.

PPWW muszą posiadać wydzielone pomieszczenie serwerowni, w którym zlokalizowane będą urządzenia i serwery służące do utrzymania systemów informatycznych, podłączone do urządzenia gwarantującego zasilanie (UPS). Pomieszczenie to musi być zabezpieczone przed dostępem osób nieuprawnionych i objęte systemem monitoringu wizyjnego i systemem kontroli dostępu. Zamiast własnej serwerowni Zamawiający dopuszcza wykorzystanie przez Wykonawcę platformy chmury publicznej pod warunkiem, że przetwarzane dane będą przechowywane w lokalizacjach umieszczonych na terenie EOG (Europejski Obszar Gospodarczy) z gwarancją zmiany lokalizacji (w obrębie EOG) przetwarzania danych jedynie za pisemną zgodą Zamawiającego.

W poczekalni PPWW muszą zostać zapewnione poniższe warunki:

- klimatyzacja,
- bezpłatny dostęp do wody pitnej dla interesantów,
- bezpłatny dostęp do toalety przystosowanej dla osób niepełnosprawnych.

Zamawiający dopuszcza możliwość świadczenia przez PPWW dodatkowych, płatnych usług dla Wykonawcy w postaci między innymi:

- możliwości wykupienia podróznego ubezpieczenia medycznego, zgodnego z obowiązującymi wymogami wskazanymi przez Zamawiającego,
- możliwość wykupienia usługi kurierskiej (dostarczenie dokumentu paszportowego wnioskodawcy wraz z decyzją oraz ew. dokumentami),
- możliwość wykupienia usługi fotokopii dokumentów,
- możliwość wykupienia usługi wykonania fotografii,
- możliwość wykupienia usługi obsługi VIP wnioskodawców zarejestrowanych na złożenie

wniosków wizowych,

które stanowią wartość dodaną dla wnioskodawców, pod warunkiem, że Wykonawca nie będzie uzależniał przyjmowania wniosków wizowych od skorzystania z tych usług.

Zamawiający zastrzega sobie prawo zatwierdzenia podmiotów świadczących usługi dodatkowe w PPWW. Bez pisemnej zgody Zamawiającego, usługi nie mogą być świadczone w PPWW. Zamawiający zastrzega sobie prawo odwołania zgody na świadczenie danej usługi przez dany podmiot. Wykonawca ponosi odpowiedzialność za działanie jak i zaniechanie podwykonawców jak za własne.

Zamawiający dopuszcza wykorzystywanie PPWW dla obsługi placówek zagranicznych innych państw, w szczególności zobowiązanych do stosowania Wspólnotowego Kodeksu Wizowego, z zastrzeżeniem, że działalność taka nie może utrudniać wykonywania Umowy ani uchybiać wizerunkowi i godności Rzeczypospolitej Polskiej bądź polskiej placówki zagranicznej w Republice Filipin. Decyzja rozstrzygająca w powyższych sprawach należy do Zamawiającego.

Przy wykonywaniu czynności Wykonawca musi stosować przepisy ogólne rozporządzenia o ochronie danych oraz polskich przepisów o ochronie danych osobowych, przepisy określone w załączniku X do Wspólnotowego Kodeksu Wizowego.

V. Personel:

Wykonawca zobowiązuje się do przestrzegania odpowiednich przepisów prawa powszechnie obowiązującego, w szczególności przepisów prawa pracy odnośnie zatrudnianych przez Wykonawcę pracowników (m.in. zawieranie umów o pracę, przestrzeganie praw pracowniczych) lub przepisów prawa cywilnego odnośnie do osób działających na zlecenie Wykonawcy (m.in. zawieranie umów cywilnoprawnych) oraz przepisów podatkowych i dotyczących systemu ubezpieczeń społecznych.

Przy realizacji zadań wynikających z Umowy wykonywanych przez personel Wykonawca zapewni w szczególności:

- wykazanie, że personel nie był wcześniej karany i dysponuje niezbędnymi kwalifikacjami,
- bieżące przekazywanie Zamawiającemu informacji o tożsamości (imię, nazwisko, obywatelstwo, numer dokumentu tożsamości, data i miejsce urodzenia) osób, które mają wejść w skład personelu przed ich zatrudnieniem oraz konsultowanie zmian personelu, przed ich zatrudnieniem;
- odpowiednie przeszkolenie personelu gwarantujące należyte wykonywanie obowiązków,
- spośród personelu wyodrębni jednego koordynatora centralnego (PPWW w Manila) oraz koordynatora lokalnego (PPWW w Cebu), posiadających kwalifikacje określone w pkt III.
- aby personel podczas wykonywania obowiązków przestrzegał zasad poufności, także po odejściu ze stanowiska, czy po rozwiązaniu lub wygaśnięciu Umowy.

Wykonawca zobowiązuje się dołożyć również wszelkich starań dla utrzymania stabilności dysponowania personelem i zapobieżenia jego nadmiernej rotacji, zwłaszcza poprzez odpowiednią politykę płacową i politykę kadrową, odpowiadającą w szczególności stosownym filipińskim przepisom dotyczącym zatrudnienia.

VI. Dane osobowe

W związku z realizacją Umowy Administrator powierza Wykonawcy przetwarzanie danych osobowych w zakresie niezbędnym do jej prawidłowego wykonania. Strony zobowiązane są do podpisania Standardowych klauzul umownych, zgodnych ze wzorem przedstawionym przez Zamawiającego.

Wykonawca obowiązany jest przy wykonywaniu swoich czynności stosować przepisy ogólnego rozporządzenia o ochronie danych, polskie przepisy o ochronie danych osobowych oraz przepisy określone w załączniku X do Wspólnotowego Kodeksu Wizowego.

Wykonawca zobowiązuje się, przy przetwarzaniu danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych, zgodnie z wymaganiami zawartymi w art. 32 ogólnego rozporządzenia o ochronie danych. W odniesieniu do wykonywania swoich czynności, w zakresie ochrony danych osobowych, Wykonawca obowiązany jest w szczególności do:

- 1) nadania upoważnień do przetwarzania danych osobowych członkom swojego personelu, którzy będą przetwarzali powierzone dane osobowe w celu realizacji niniejszej Umowy;
- 2) stworzenia obiegu dokumentacji wizowej umożliwiającej upoważnionym pracownikom dostęp do danych osobowych adekwatny do zakresu ich obowiązków oraz stałego czuwania, aby dane nie były w szczególności czytane, kopiowane, zmieniane, czy usuwane bez upoważnienia, zwłaszcza podczas przekazywania ich Zamawiającemu;
- 3) zapewnienia odpowiednich środków służących śledzeniu obiegu akt każdego wniosku, wysyłanych do i z urzędu konsularnego;
- 4) zapewnienia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania ich w tajemnicy;
- 5) przekazywania danych według instrukcji udzielonych przez Zamawiającego:
 - elektronicznie, w zaszyfrowanej formie lub
 - bezpośrednio, w sposób zabezpieczony, uniemożliwiający dostęp do nich osób postronnych;
- 6) niezwłocznego przekazywania danych:
 - w przypadku danych przekazywanych fizycznie – niezwłocznie, jednak nie później niż w ciągu 2 dni roboczych od chwili ich przyjęcia,
 - w przypadku danych przekazywanych elektronicznie w postaci zaszyfrowanej – najpóźniej pod koniec dnia, w którym zostały pobrane.
- 7) usuwania danych natychmiast (nie później niż w ciągu 7 dni po ich przekazaniu) oraz zapewnienia przechowywania jedynie imienia i nazwiska oraz danych kontaktowych osoby ubiegającej się o wizę (w celu ustalenia terminu spotkania), a także numeru paszportu do chwili zwrotu paszportu osobie ubiegającej się o wizę i usunięcia tych danych po 5 dniach po zakończeniu usług związanych z przetwarzaniem danych osobowych, usunięcia lub zwrotu, zależnie od decyzji Zamawiającego, wszelkich danych osobowych oraz usunięcia wszelkich ich istniejących kopii, chyba że prawo Unii Europejskiej lub przepisy prawa obowiązujące Wykonawcę uniemożliwiają mu zwrot lub zniszczenie wszystkich lub części przekazanych danych osobowych. W tym przypadku Wykonawca gwarantuje, że zapewni poufność przekazanych danych osobowych i nie będzie ich już aktywnie przetwarzał;

- 8) zapewnienia wszystkich technicznych i organizacyjnych środków, zgodnie z wymaganiami zawartymi w art. 32 ogólnego rozporządzenia o ochronie danych, w tym środków bezpieczeństwa wymaganych do ochrony danych osobowych przed przypadkowym lub bezprawnym zniszczeniem, utratą, zmianą, niedozwolonym ujawnieniem lub udostępnieniem – szczególnie, gdy dotyczy to przechowywania akt i danych w pomieszczeniach Wykonawcy oraz przekazywania ich Zamawiającemu – oraz przed wszelkimi innymi formami bezprawnego przetwarzania danych osobowych; w szczególności do ochrony przetwarzanych danych powinny być zastosowane środki ochrony, takie jak nowoczesne systemy monitoringu CCTV, systemy alarmowe informujące o włamaniu, napadzie oraz pożarze, wyposażenie biura w patentowe szafy metalowe, szafy zwykle zamykane na zamek, wzmocnienia wejściowych i zapasowych drzwi oraz drzwi do głównych pomieszczeń, ochrona fizyczna obiektu, system kontroli dostępu itp.;
- 9) zabezpieczenia infrastruktury i sprzętu teleinformatycznego przed nieuprawnionym dostępem, ingerencją podmiotów trzecich oraz nieuprawnionymi działaniami personelu (np. korzystaniem z prywatnych komunikatorów, prywatnych skrzynek poczty elektronicznej, podłączeniem prywatnych nośników danych). Ponadto systemy teleinformatyczne służące do przetwarzania danych osobowych powinny gwarantować zapewnienie poufności, dostępności oraz integralności danych;
- 10) przetwarzania w imieniu Zamawiającego danych o osobach ubiegających się o wizę wyłącznie w celu realizacji Umowy;
- 11) dostarczania osobom ubiegającym się o wizę informacji wymaganych na mocy art. 37 Rozporządzenia (WE) Nr 767/2008 (Rozporządzenie w sprawie VIS);
- 12) spełnienia obowiązków wynikających z art. 28 ust. 3 pkt e) i f) ogólnego rozporządzenia o ochronie danych;
- 13) przedstawienia osobom ubiegającym się o wizę informacji o przetwarzaniu ich danych osobowych, o którym mowa w art. 13 i 14 ogólnego rozporządzenia o ochronie danych, w szczególności poprzez jej zamieszczenie na tablicach przed wejściem oraz w poczekalni wizowej PPWW, a także na dedykowanej witrynie internetowej, związanej z realizacją przedmiotu Umowy;
- 14) prowadzenia rejestru wszystkich kategorii czynności przetwarzania dokonywanych w związku z realizacją niniejszej Umowy, zgodnie z art. 30. ust 2 ogólnego rozporządzenia o ochronie danych;
- 15) przestrzegania warunków korzystania z usług innego podmiotu przetwarzającego, o którym mowa w art. 28 ust. 2 i 4 ogólnego rozporządzenia o ochronie danych;
- 16) przestrzegania standardów ochrony danych, co najmniej równorzędnych standardom określonym w ogólnym rozporządzeniu o ochronie danych;
- 17) wyznaczenia inspektora ochrony danych zgodnie z art. 37 ogólnego rozporządzenia o ochronie danych.

Wykonawca ponosi odpowiedzialność za ewentualne skutki działania niezgodnego z przepisami dotyczącymi ochrony danych osobowych.

Zamawiający zastrzega sobie prawo do kontroli realizacji wymogów określonych powyżej oraz przedstawiania zaleceń w celu przestrzegania warunków Umowy w przedmiotowym zakresie.

Zamawiający zastrzega możliwość dokonywania kontroli również przez osoby przez niego wskazane i upoważnione oraz organ nadzorczy, w rozumieniu art. 4 pkt 21 ogólnego rozporządzenia o ochronie danych, właściwy dla Administratora. Wykonawca zobowiązuje się do udostępnienia Zamawiającemu oraz organowi nadzorczemu, o którym mowa powyżej, wszelkich informacji, w tym dokumentów niezbędnych do wykazania spełnienia obowiązków określonych w art. 28 ogólnego rozporządzenia o ochronie danych.

Wykonawca zobowiązuje się do natychmiastowego (najpóźniej w ciągu 24 godzin) powiadomienia Administratora o stwierdzeniu jakichkolwiek prób lub faktów naruszenia bezpieczeństwa przetwarzanych danych osobowych. W przypadku stwierdzenia zdarzeń, o których mowa w zdaniu poprzedzającym, Wykonawca zobowiązuje się niezwłocznie umożliwić pracownikom Zamawiającego lub Ministerstwa Spraw Zagranicznych lub osobom działającym na ich zlecenie, przeprowadzenie kontroli procesu przetwarzania i ochrony danych osobowych, w tym w zakresie wdrożonych środków organizacyjnych i technicznych, o których mowa w art. 32 ogólnego rozporządzenia ochrony danych.

Wykonawca zobowiązuje się do przekazania Zamawiającemu imiennej listy upoważnionych członków personelu, którzy będą mieli dostęp do powierzonych danych osobowych w związku z realizacją Umowy, a także zobowiązuje się do uzyskania od swoich pracowników oświadczeń o zachowaniu w poufności danych osobowych, powierzonych przez Zamawiającego, do których będą mieli dostęp, zarówno w trakcie zatrudnienia ich przez Wykonawcę, jak i po jego ustaniu.

VII. Zabezpieczenie i utrzymanie systemów IT

Wykonawca zobowiązuje się podjąć wszelkie niezbędne zabezpieczenia techniczne strony internetowej oraz używanych systemów IT (w tym aplikacji mobilnych) celem zapewnienia ich płynnego działania oraz ochrony przed nieuprawnioną ingerencją ze strony osób trzecich, a w szczególności przed atakami hackerskimi.

VIII. Zakres funkcjonalny systemu rezerwacji spotkań w celu złożenia wniosków wizowych oraz działalność informacyjna.

Usługi informacyjne będą wykonywane przez pracowników Wykonawcy – bezpośrednio, telefonicznie, pocztą elektroniczną (e-mail) oraz poprzez stronę internetową.

Przed rezerwacją spotkania wnioskodawca wizowy ma obowiązek założyć i potwierdzić indywidualne konto. Sposób zabezpieczenia procesu rejestracji konta ma zagwarantować brak możliwości dokonania rejestracji przez osoby nieuprawnione.

Usługa rezerwacji spotkań polega, w szczególności na udostępnianiu on-line terminarza do zapisu na spotkanie w celu złożenia aplikacji wizowej w zaproponowanych terminach przez Zamawiającego. Wykonawca na wniosek Zamawiającego ma zapewnić możliwość kolejkowania zgłoszeń wnioskodawców. Zamawiający zastrzega sobie również możliwość samodzielnego prowadzenia terminarza spotkań.

Rejestracja spotkania ma miejsce wyłącznie poprzez uprzednio potwierdzone indywidualne konto. Sposób organizacji rejestracji spotkań on-line musi być w sposób efektywny zabezpieczony przed

udziałem osób trzecich, osób prawnych, botów, algorytmów lub innych czynników zewnętrznych, w szczególności poprzez zapewnienie technicznych możliwości weryfikacji tożsamości aplikującego w trakcie procesu zakładania konta oraz na poszczególnych etapach rejestracji terminu spotkania wizowego. Zastosowane przez Wykonawcę środki technologiczne i informatyczne muszą być przez niego regularnie aktualizowane i dostosowane do bieżących uwarunkowań.

System on-line umożliwia użytkownikom poprzez konto indywidualne uzyskanie niezbędnych informacji o spotkaniu, wyszukiwanie dostępnych terminów, planowanie i pomyślną rezerwację terminu spotkania. Użytkownik będzie miał możliwość zmiany lub odwołania terminu spotkania.

Wykonawca zapewnia Zamawiającemu konto administracyjne w systemie umożliwiające zarządzanie terminarzem oraz dostępem do wszystkich danych, które zostały wprowadzone lub posłużyły użytkownikom do rezerwacji terminu spotkania. Wykonawca zapewni Zamawiającemu oraz MSZ RP pełny dostęp do systemu rejestracji spotkań wizowych celem sprawowania nadzoru nad realizacją umowy. Wykonawca zapewni ułatwiony wgląd oraz możliwość weryfikacji każdego etapu procesu, w tym danych dot. czasu logowania, rejestrowania spotkań, danych dot. płatności itp.

Wykonawca zapewnia Wnioskodawcom automatyczną informację o zmianie statusu spotkania oraz możliwość weryfikacji etapu rozpatrywania wniosku wizowego. Wykonawca będzie do wnioskodawcy wysyłał drogą elektroniczną komunikat o dokonaniu zapisu na spotkanie, przypomnieniach o terminie, odwołaniu spotkania poprzez e-mail, sms oraz indywidualne konto użytkownika w systemie. System musi informować o zmianach statusu lub danych w koncie użytkownika.

Wykonawca jest zobowiązany do zapewnienia zasobów o charakterze technicznym, informatycznym i kadrowym, które pozwolą na skuteczną i bezpieczną pod kątem ochrony danych osobowych, rejestrację terminu na złożenie wniosków wizowych oraz będą skutecznie przeciwdziałać ingerencji osób trzecich, algorytmów, botów lub innych czynników zewnętrznych w proces rejestracji spotkań, w szczególności poprzez zapewnienie technicznych możliwości weryfikacji tożsamości aplikującego w trakcie procesu zakładania konta oraz na poszczególnych etapach rejestracji terminu spotkania wizowego.

Wykonawca zobowiązany jest do zapewnienia, że wszelkie dane osobowe przetwarzane przez niego, jako administratora w związku z obsługą systemu rejestracji na złożenie wniosków będą przetwarzane w centrach przetwarzania danych znajdujących się na terenie Europejskiego Obszaru Gospodarczego.

Zamawiający zastrzega sobie prawo do testowania systemu zabezpieczeń przed nieautoryzowanym dostępem osób trzecich i algorytmów.

IX. Zamówienie z prawem opcji:

Zamawiający zastrzega sobie możliwość uruchomienia, w ramach usługi świadczonej zgodnie z wymaganiami dla zamówienia podstawowego, dodatkowej funkcjonalności w zakresie weryfikacji tożsamości wnioskodawcy – wideo-weryfikacji, na podstawie art. 441 Pzp (prawo opcji).

Wykonawca rozpocznie świadczenie usługi w ramach prawa opcji w terminie uzgodnionym

z Zamawiającym, nie dłuższym jednak niż 30 dni od dnia otrzymania pisemnego zlecenia od Zamawiającego.

Proces weryfikacji Wnioskodawcy w prawie opcji polegać będzie na weryfikacji przez Wykonawcę adresu e-mail i filipińskiego numeru telefonu wnioskodawcy, oraz wymagać będzie zastosowania systemu umożliwiającego weryfikację w czasie rzeczywistym tożsamości osoby zapisującej się na złożenie wniosku wizowego (wideo-weryfikacja) – dot. rejestracji spotkania/przełożenia/anulowania spotkania wizowego w systemie Wykonawcy.

W procesie weryfikacji obsługiwany będzie paszport wnioskodawcy.

1. System musi posiadać bazę referencyjną dokumentów (SPECIMEN) z krajów wyszczególnionych w *Publicznym rejestrze on-line autentycznych dokumentów tożsamości i dokumentów podróży* (PRADO), znajdującym się na oficjalnym portalu Rady UE i Rady Europejskiej (<https://www.consilium.europa.eu/prado/pl/prado-start-page.html>), która umożliwia sprawdzenie za zgodność ze wzorem przedstawionego przez wnioskodawcę paszportu.
2. W sytuacji, gdy wnioskodawca posługuje się paszportem, który nie posiada chipa RFID lub nie ma możliwości zweryfikowania certyfikatu danego kraju, którym zostały podpisane dane, należy wprowadzić dodatkowy element weryfikacji poprzez zastosowanie przelewu zwrotnego kartą bankową wnioskodawcy albo członka najbliższej rodziny lub jego opiekuna prawnego.
3. W sytuacji gdy wnioskodawca posługuje się paszportem z chipem RFID, gdzie dane zostały podpisane ważnym certyfikatem danego kraju, nie należy dokonywać weryfikacji poprzez przelew zwrotny.
4. Weryfikacja paszportu użytego do identyfikacji oraz danych na nich zapisanych przebiega automatycznie.
5. System musi obsługiwać odczyt danych z paszportu przez interfejs NFC oraz odczyt danych przez OCR zawartych w MRZ.
6. Weryfikacji mogą być poddawane wszystkie dane znajdujące się w paszporcie (wraz ze zdjęciem) lub wybrane przez Zamawiającego.
7. Podczas weryfikacji wnioskodawcy powinny być prezentowane w czasie rzeczywistym wskazówki pomagające w robieniu zdjęć.
8. System powinien zapewniać kontrolę jakości obrazu podczas przechwytywania wideo i selfie oraz ich kompresję podczas transferu.
9. Mechanizm porównawczy dokonuje weryfikacji z uwzględnieniem normalizacji wszystkich znaków, tj. ignoruje wielkość liter i pomija znaczenie znaków diakrytycznych lub z pominięciem normalizacji, w zależności od ustawionego parametru systemu.
10. Algorytm weryfikujący powinien posiadać funkcjonalność pozwalającą stwierdzić czy Wnioskodawcą jest osoba, a nie np. bot, tj. wykrywać i blokować próby oszukania systemu poprzez prezentację zdjęć przez automat/skrypt lub podstawioną osobę. Oznacza to, że w ramach procesu uwierzytelniania wykonywana jest kontrola:

- „liveness detection”, która wykrywa, czy wnioskodawca jest prawdziwą „żywą” osobą,

- „liveness face matching”, która porównuje twarz pomiędzy zdjęciem referencyjnym a klatkami wideo z nagrań na żywo.

11. Algorytm weryfikujący powinien sprawdzać co najmniej:

- zgodność ze wzorem przedstawionego paszportu,
- datę ważności paszportu,
- czy kraj wydania paszportu (według MRZ lub wzoru graficznego) jest tym oczekiwanym,
- czy data wystawienia paszportu jest zgodna z pierwszą datą wystawienia uznanego wzoru,
- czy model graficzny paszportu jest poprawny w stosunku do MRZ,
- czy obliczenia sumy kontrolnej MRZ są prawidłowe,
- czy format alfanumeryczny MRZ jest prawidłowy, zgodnie z normą ICAO i specyfiką kraju,
- czy znaki paska MRZ są prawidłowo wyrównane i czy czcionka jest prawidłowa,
- czy w przypadku dokumentu, który powinien zawierać kod dwuwymiarowy (2DDOC) jest on obecny i zgodny z oczekiwanym standardem,
- czy podpis w 2DDOC jest ważny,
- czy dana strona paszportu zawiera zdjęcie i czy jest ono we właściwym miejscu,
- czy wszystkie zabezpieczenia widoczne w paszporcie są zgodne i obecne,
- czy analizowany paszport nie jest czarno-białą kserokopią.

12. Algorytm weryfikujący powinien wykonywać kontrolę spójności pomiędzy danymi wejściowymi, wprowadzonymi na początku procesu, a danymi wyodrębnionymi z analizowanego paszportu oraz między danymi w różnych częściach dokumentu jak MRZ i VIZ (strefa wizualna), a pobranymi z chipa poprzez NFC.

X. Pobieranie danych biometrycznych

Przedmiotem zamówienia jest również pobieranie od wnioskodawców i dostarczanie placówce zagranicznej danych biometrycznych niezbędnych do wydania wizy.

Wykonawca wyposaży we własnym zakresie PPWW w sprzęt i oprogramowanie niezbędne do pobierania identyfikatorów biometrycznych (odcisków linii papilarnych), skanowania zdjęć i wykonywania zdjęć twarzy bezpośrednio na miejscu wraz z ich wydrukiem w formacie zgodnym z wymogami WKW oraz zautomatyzowanej/maszynowej rejestracji wszystkich danych alfanumerycznych zawartych we wniosku wizowym.

Sprzęt i oprogramowanie winno zostać przygotowane i skonfigurowane przez Wykonawcę w taki sposób, aby dane biometryczne (odciski linii papilarnych) pobierane w procesie wizowym spełniały kryteria określone w decyzji Komisji Europejskiej nr 2009/756/WE z dnia 9 października 2009 r.

ustanawiającej specyfikacje dotyczące rozdzielczości oraz korzystania z odcisków palców do identyfikacji i weryfikacji biometrycznej w wizowym systemie informacyjnym (Dz.Urz.U.E.L Nr 270, str. 14).

Urządzenie biometryczne:

- musi posiadać certyfikat FBI stwierdzający zgodność ze specyfikacją FBI jakości rejestrowanych obrazów odcisków palców dla potrzeb AFIS (FBI Electronic Fingerprint Transmission Specification (EFTS)/Appendix F IAFIS Image Quality Specification).
- musi spełniać kryteria normy ISO/IEC 19794-4:2005 (Biometric data interchange formats – Part 4: Finger image data), odnoszące się do pobierania obrazów odcisków palców, w szczególności punktu 7. („Image acquisition requirements”) lub równoważne.
- jakość zebranych obrazów odcisków palców musi spełniać wymagania normy ISO/IEC 19794-4:2005 oraz standardu ANSI/NIST-ITL 1-2000 (Data Format for the Interchange of Fingerprint, Facial, Scarmark & Tattoo (SMT) Information) lub równoważne.
- urządzenie musi umożliwiać rejestrację zeskanowanych obrazów płaskich odcisków palców z rozdzielczością 500 ppi $\pm$ 5ppi (w pionie oraz w poziomie) w 8-bitowej skali szarości (256 odcieni).
- urządzenie musi być dostosowane do pracy w temperaturze otoczenia w zakresie od 5 do 40 st. C oraz przy wilgotności względnej w zakresie od 20 do 80%.
- urządzenie musi być dostosowane do ciągłej pracy przez 12 godzin na dobę w całym okresie użytkowania.
- urządzenie musi być wyposażone w elementy (np. diody LED, piktogramy rąk i palców, wyświetlacz LCD) wspomagające pracę operatora poprzez informowanie o bieżącym kroku procesu pobierania odcisków palców oraz wyniku oceny jakości zebranego obrazu.
- oprogramowanie dostarczone z urządzeniem musi umożliwiać korzystanie z urządzenia w trybie zwykłego użytkownika, nieposiadającego uprawnień administratora w systemie operacyjnym komputera PC.
- urządzenie wraz z dostarczonym oprogramowaniem musi posiadać funkcję automatycznej kontroli jakości skanowanych obrazów odcisków oraz funkcję automatycznego zebrania odcisków, gdy jakość zostanie przez nie oceniona, jako wystarczająca.
- urządzenie wraz z dostarczonym oprogramowaniem musi posiadać funkcję redukcji negatywnego wpływu nadmiernie suchej lub wilgotnej skóry na jakość zebranych odbitek palców.
- urządzenie wraz z dostarczonym oprogramowaniem musi posiadać funkcję automatycznej detekcji deformacji obrazu, spowodowanych niepożądanym przemieszczeniem palca podczas skanowania, informującą w razie potrzeby użytkownika o tym fakcie.

Wykonawca zobowiązuje się do pobierania identyfikatorów biometrycznych z jakością umożliwiającą utrzymanie poziomu błędów IQ (Insufficient Quality Percentage) nie wyższego niż 2,5 % dla danych biometrycznych przesyłanych do Systemu Centralnego Wizowego Systemu Informacyjnego. Powyższy poziom jakości pobierania identyfikatorów biometrycznych powinien być utrzymywany przez cały okres świadczenia usługi przez każdy PPWW z osobna.

Na prośbę Wykonawcy Zamawiający przeprowadzi testy jakości przekazanych próbek pobieranych

identyfikatorów biometrycznych w środowisku testowym Wizowego Systemu Informacyjnego oraz poinformuje Wykonawcę o wynikach tychże testów.

Pobrane dane biometryczne wraz z danymi alfanumerycznymi będą przekazywane do urzędu konsularnego w postaci pakietów danych, zapisanych na nośnikach zewnętrznych. Jako nośnik zewnętrzny dopuszcza się użycie płyt optycznych jednokrotnego zapisu, jednowarstwowych i jednostronnych (single-sided, single-layered).

Przetwarzanie i przekazywanie danych do placówki zagranicznej musi uwzględniać wymogi zawarte we Wspólnotowym Kodeksie Wizowym oraz w ogólnym rozporządzeniu o ochronie danych, w szczególności musi zostać zapewnione, aby dane przekazywane nie były czytane, kopiowane, zmienione czy kasowane bez upoważnienia.

Dane mogą być przekazywane do placówki zagranicznej jedynie w formie zaszyfrowanej, o poziomie bezpieczeństwa nie gorszym, niż w przypadku zastosowania standardu Advanced Encryption Standard (AES) (FIPS PUB 197) z użyciem klucza kryptograficznego 256-bit lub równoważne.

Pakiety danych wymienione w pkt. 4.7 będą zawierały w szczególności dane alfanumeryczne w postaci plików w formacie XML, oraz dane biometryczne w formacie NIST, zgodnym ze standardem ANSI/NIST-ITL 1-2000 lub równoważne.

Dane biometryczne zapisane w formacie NIST będą zawierały następujące informacje:

- Opis transakcji – rekord logiczny Type-1,
- Dane tekstowe zawierające dodatkową informację związaną z rodzajem transakcji – rekord logiczny Type -2,
- Zeskanowane obrazy płaskich odcisków dla poszczególnych 10-iu palców po segmentacji w rozdzielczości 500 dpi – rekordy logiczne Type-4.

XI. Podwykonawca

Zamawiający dopuszcza wykonywanie Umowy przez Podwykonawców, z tym że zastrzega, iż następujące kluczowe czynności muszą być wykonywane przez Wykonawcę (nie mogą być wykonywane przez Podwykonawców):

- 1) przyjmowanie wniosków wizowych;
- 2) pobieranie danych biometrycznych;
- 3) pobieranie i przekazywanie do Zamawiającego opłat wizowych;
- 4) odbieranie od Zamawiającego paszportów i decyzji wizowych.
- 5) bieżące utrzymanie, modyfikacja oraz aktualizacja wykorzystywanych dla realizacji usługi wyspecjalizowanych narzędzi informatycznych;
- 6) centrum kontaktu z klientem.

Wykonawca ponosi odpowiedzialność wobec Zamawiającego za działania lub zaniechania Podwykonawców jak za działania i zaniechania własne.

Ustanowienie Podwykonawcy wymaga każdorazowej pisemnej zgody Zamawiającego. Zamawiający zastrzega sobie prawo do odwołania zgody na wykonywanie Umowy przez danego Podwykonawcę. W

przypadku konieczności powierzenia Podwykonawcy przetwarzania danych osobowych Wykonawca zobowiązany jest do wystąpienia do Administratora o wyrażenie pisemnej zgody. Po uzyskaniu zgody Wykonawca zawiera odrębną Umowę dotyczącą powierzenia danych osobowych z Podwykonawcą, która zasadniczo przewiduje takie same obowiązki w odniesieniu do ochrony danych osobowych, jakie zostały określone w Standardowych klauzulach umownych podpisanych przez Wykonawcę i Administratora.

Wymagania co do wyceny:

Prosimy o przedstawienie proponowanej całkowitej ceny netto EUR (bez podatku) dla całości przedmiotu umowy oraz opłaty netto EUR (bez podatku) za przyjęcie 1 wniosku wizowego zgodnie z poniższym formularzem, z rozróżnieniem ceny za wykonanie zamówienia podstawowego i zamówienia z prawem opcji.

Na potrzeby niniejszej wyceny należy przyjąć maksymalną przewidywaną liczbę wniosków tj. 20 000 zarówno w wariantcie zamówienia podstawowego jak i w wariantcie z prawem opcji.

WNIOSKI WIZOWE		
Szacunkowa maksymalna ilość przyjętych wniosków wizowych w okresie trwania umowy	Cena jednostkowa EUR netto rozumiana jako opłata pobierana od jednego przyjętego wniosku wizowego	Wartość EUR netto za przyjęte wnioski wizowe w okresie trwania umowy
A	B	$C = A \times B$
20 000		
Usługa przyjmowania wniosków wizowych w wariantcie z prawem opcji		
Szacunkowa maksymalna ilość przyjętych wniosków wizowych w okresie trwania umowy	Cena jednostkowa EUR netto rozumiana jako opłata pobierana od jednego przyjętego wniosku wizowego	Wartość EUR netto za przyjęte wnioski wizowe w okresie trwania umowy
A	B	$C = A \times B$
20 000		

Termin złożenia wyceny:

Uprzejmie prosimy o przesłanie wyceny usługi w terminie do 4 kwietnia 2025 r. na adres mailowy: manila.amb.sekretariat@msz.gov.pl

Osoba uprawniona do kontaktu: p. Agnieszka Dyszlewska, Konsul RP w Manili.

Informacja dodatkowa:

Informujemy, że przedmiotowe zapytanie o wycenę **nie stanowi oferty w rozumieniu art. 66 Kodeksu cywilnego**, ani też nie jest ogłoszeniem o zamówieniu w rozumieniu ustawy Prawo zamówień publicznych. Ma ono na celu wyłącznie rozeznanie cenowe rynku wśród podmiotów świadczących usługi przyjmowania wniosków wizowych w Republice Filipin oraz uzyskanie wiedzy na temat szacunkowych kosztów związanych z planowanym zamówieniem publicznym.

Informacja dotycząca przetwarzania danych osobowych przez Ambasadę RP w Manili

Niniejsza informacja stanowi wykonanie obowiązku określonego w art. 13 i art. 14 rozporządzenia 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, zwanego dalej „RODO”.

1. Administratorem, w rozumieniu art. 4 pkt 7 RODO, danych osobowych jest Minister Spraw Zagranicznych z siedzibą w Polsce, w Warszawie, Al. J. Ch. Szucha 23, natomiast wykonującym obowiązki administratora jest Kierownik Ambasady RP w Manili, **adres:** 9th Floor, Del Rosario Law Centre, 21st Drive corner 20th Drive, Bonifacio Global City, City of Taguig 1630, Metro Manila.
2. W MSZ i placówkach zagranicznych powołano Inspektora Ochrony Danych (IOD).
Dane kontaktowe IOD:
adres siedziby: Al. J. Ch. Szucha 23, 00-580 Warszawa
adres e-mail: iod@msz.gov.pl
3. Zakres przetwarzanych danych obejmuje dane wskazane w ofercie przesłanej przez Oferenta, w szczególności:
 - a) imię i nazwisko,
 - b) służbowy adres e-mail,
 - d) służbowy numer telefonu.
4. Dane osobowe zostały przekazane przez Oferenta w związku z odpowiedzią na zapytanie o szacowanie kosztów lub bezpośrednio.
5. Dane osobowe będą przetwarzane na podstawie art. 6 ust. 1 lit. c RODO, w celu przygotowania postępowania o udzielenie zamówienia publicznego, którego przedmiotem jest usługa

przyjmowania wniosków wizowych, w związku z art. 44 ust. 2-4 oraz art. 162 pkt. 4 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.

6. Dane osobowe będą przetwarzane do czasu ustania celu przetwarzania, o którym mowa w pkt 5, a następnie będą przechowywane w celach archiwalnych, zgodnie z przepisami ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach oraz przepisami wewnętrznymi MSZ i placówki zagranicznej wynikającymi z przepisów ww. ustawy.
7. Dane podlegają ochronie na podstawie przepisów RODO i mogą być udostępniane innym osobom i podmiotom na podstawie przepisów prawa. Dostęp do danych posiadają uprawnieni pracownicy MSZ i placówki zagranicznej.
8. Dane osobowe nie będą przekazywane do państwa trzeciego, ani do organizacji międzynarodowych.
9. Osobie, której dane dotyczą przysługują prawa do kontroli przetwarzania danych, określone w art. 15-19 RODO, w szczególności prawo dostępu do treści swoich danych i ich sprostowania, prawo do usunięcia danych oraz ograniczenia przetwarzania, o ile będą miały zastosowanie.
10. Dane osobowe nie będą przetwarzane w sposób zautomatyzowany, który będzie miał wpływ na podejmowanie decyzji mogących wywołać skutki prawne lub w podobny sposób istotnie na nie wpłynąć. Dane nie będą poddawane profilowaniu.
11. Osoba, której dane dotyczą ma prawo wniesienia skargi do organu nadzorczego na adres:
Prezes Urzędu Ochrony Danych Osobowych
ul. Stawki 2
00-193 Warszawa