[working translation of Polish language version into English, in case of discrepancies between Polish and English version, Polish version shall prevail]

WKIP.MAN.260.1.2025
WKIP.307.2.2025

Manila, 27 March 2025 r.

REQUEST FOR COST ESTIMATION

In connection with the planned award of a public contract for the provision of the service of accepting visa applications by an external entity for the Polish consular office in the Philippines under the single-source procurement procedure, the Embassy of the Republic of Poland in Manila, as part of its market research, kindly requests a quote for the service, assuming the requirements described below regarding the subject of the contract.

I. Subject of the contract (basic contract):
The service of accepting visa applications within the meaning of Article 43 of Regulation (EC) No. 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing the Community Code on Visas, hereinafter referred to as the "Community Code on Visas" or "CCV", and the return of visa documents and decisions on the territory of the Republic of the Philippines to the Ordering Party – the Embassy of the Republic of Poland in Manila. The maximum number of visa applications is estimated at no more than 20,000 (say: twenty thousand) during the term of the agreement of 2 years.

The Contracting Authority provides for the possibility of awarding contracts similar to 50% of the value of the basic contract, pursuant to Article 214(1)(7) of the Public Procurement Law of 11 September 2019 (hereinafter referred to as the PPL), in particular in the event of completion of the subject of the contract before the expiry of the contract performance deadline, i.e. acceptance of the maximum number of visa applications covered by the subject of the contract.

Visa applications should be understood as applications for Schengen visas, applications for national visas and applications for their reconsideration.

It will be necessary for the Contractor to launch 2 visa application points (hereinafter: VACs) in Manila and Cebu in order to receive visa applications and return visa documents and decisions.

It will be required to provide information services to applicants, in particular by creating and maintaining a dedicated stable website, which should be available in English, as well as providing telephone and e-mail support to the client in English and Tagalog.

The website must allow for appointments for the purpose of submitting a visa application by natural persons, using advanced IT tools and biometric identification, which will prevent the registration of the appointment by third parties, legal entities or algorithms, and will also allow the acceptance of the

service fee charged on the accepted visa application from the applicant. The service fee will be charged to the applicant at the time of registration by the applicant through the website.

The contractor must have its own IT tools as well as human and technological capabilities so that all work related to the website and the ICT system, such as ongoing supervision, programming, modernization, adaptation of systems to new needs, can be carried out without undue delay and is not dependent on external entities.

II. General requirements:

The Contractor shall ensure in particular that:

1. does not and will not conduct during the term of the Agreement any activity detrimental to the interests or image of the Republic of Poland;
2. will conduct visa outsourcing in accordance with the laws of the Republic of Poland, the laws of the Republic of the Philippines and the public interest;
3. there is and will not be a conflict of interest during the term of the Contract, i.e. a situation in which other activities conducted by the Contractor or its connections could affect its impartiality and reliability of the performance of the Contract;
4. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, hereinafter referred to as the "General Data Protection Regulation", i.e. complies with the provisions of the General Data Protection Regulation, the provisions set out in Annex X to the Community Code on Visas and the relevant Polish legislation on the protection of personal data.

The Contractor takes full responsibility for the actions and omissions of the staff and other persons involved in the performance of the Contract and the consequences resulting from the acts and omissions.

The contractor must have the appropriate human, material, financial and technical potential to properly perform the subject of the contract.

The Contractor undertakes to take all necessary organizational steps to efficiently serve the applicants, and in particular to prevent the formation of queues and extend the deadline for making appointments.

The Contractor must exercise the utmost diligence resulting from the professional nature of the conducted activity, in accordance with all applicable regulations, reliably and on time, with a view to protecting the interests of Polish consular offices in the Republic of the Philippines.

III. Conditions necessary to participate in the procedure

To confirm the fulfilment of the condition of participation in the procedure concerning technical or professional capacity, the Contracting Authority requires that the Contractor:

Has demonstrated the necessary experience, i.e.

within the last 3 years before the expiry of the deadline for submission of tenders, and if the period of conducting business activity is shorter - during this period, performed, and in the case of periodic or continuous services also duly performs at least 2 services consisting in accepting visa applications for the benefit of 1 selected diplomatic or consular mission of a Schengen Area country, in accordance with the disposition of Article 43 of the Community Code on Visas (CCV), Regardless of whether the service was provided on the basis of a global agreement covering many countries or an agreement for the provision of a service to only one country, the service performed/performed must include at least 5000 (say: five thousand) visa applications accepted over a period of no more than 12 consecutive months.

The contracting authority allows the service to be provided on the basis of a contract concluded directly with a diplomatic or consular mission, or on the basis of an agreement concluded with another entity (e.g. the Ministry of Foreign Affairs of a given Schengen Area country or another office of that country).

It is not allowed to add up the number of applications processed for several diplomatic or consular missions in a given country.

In the case of services performed, the Ordering Party requires that the part of the service provided as at the date of submission of offers amounts to at least 5000 accepted visa applications for one entity in a period not longer than 12 consecutive months.

In the case of contracts longer than 1 (in words: one) year, the Ordering Party will take into account only one 12-month period indicated by the Contractor.

demonstrated that it has at its disposal persons capable of performing the contract, i.e. it has demonstrated that it has or will have at least:

Coordinator at the VAC (Manila) and VAC (Cebu) with at least:

1. 2 years of experience in managing a team of employees.
2. 1- one year of experience in the area of providing a service consisting in accepting visa applications for a diplomatic or consular mission of a Schengen Area country, in accordance with the disposition of Article 43 of the Community Code on Visas (CCV).
3. Knowledge of English at least at C1 level in accordance with the Common European Framework of Reference for Languages (CEFR) developed by the Council of Europe (the contracting authority allows confirmation of the level of language proficiency by obtaining a secondary school leaving certificate with the required language as the language of instruction).

IV. The VAC must meet the following requirements:

It must be located within the city centre, taking into account easy access for applicants by public transport, in close proximity to a metro station (if there is one in a given city) or public transport stops.

It must provide conditions for serving people with disabilities and mobility limitations, i.e. have a ramp for people in wheelchairs and for parents with prams with children, a properly adapted lift for such people in the case of VACs located on the floors of the building, at least one stand adapted to serve the above-mentioned people and a properly adapted toilet. The VACs must enable cash service for the customer.

The locations of the VAC are subject to approval by the Ordering Party.

The VAC must have office rooms inaccessible to third parties for the processing of visa data (workstations for entering visa applications into the electronic system and for encrypting and downloading data packets to a carrier), workstations for preparing visa applications with passports to consular offices, workstations for preparing passports collected from consulates to be issued to Applicants.

The VACs must be equipped with fire protection systems and protected 24 hours a day using monitoring (video surveillance) and alarm systems and, at least during the opening hours of the VAC, with the use of specialized physical protection.

Entrances to the office premises of the VAC must be secured against unauthorized access using an electronic access control system.

The rooms for storing visa applications and passports must be equipped with an armored cabinet and secured with an electronic access control system against unauthorized access.

The VACs must have a separate server room where devices and servers used to maintain IT systems will be located, connected to a device guaranteeing power supply (UPS). This room must be protected against unauthorized access and covered by a video surveillance system and an access control system. Instead of its own server room, the Ordering Party allows the Contractor to use a public cloud platform, provided that the processed data will be stored in locations located in the EEA (European Economic Area) with a guarantee of a change of location (within the EEA) of data processing only with the written consent of the Ordering Party.

The following conditions must be provided in the VAC waiting room:

1. air conditioning
2. free access to drinking water for visitors,
3. free access to a toilet adapted for the disabled.

The Ordering Party allows for the possibility of providing additional, paid services for the Contractor by the VAC in the form of, among others:

1. the possibility of purchasing travel medical insurance, in accordance with the applicable requirements indicated by the Ordering Party,
2. the possibility of purchasing a courier service (delivery of the applicant's passport document together with the decision and possible documents),
3. the possibility of purchasing the photocopy service of documents,
4. the possibility of purchasing a photo service,
5. the possibility of purchasing the VIP service for applicants registered to submit visa applications,

which constitute an added value for the applicants, provided that the Contractor will not make the acceptance of visa applications dependent on the use of these services.

The Ordering Party reserves the right to approve entities providing additional services in the VAC. Without the written consent of the Ordering Party, services cannot be provided in the VAC. The Ordering Party reserves the right to revoke the consent to the provision of a given service by a given entity. The Contractor is responsible for the actions and omissions of subcontractors as for its own.

The Contracting Authority allows the use of VACs for the service of foreign missions of other countries, in particular those obliged to apply the Community Code on Visas, with the proviso that such activity may not hinder the performance of the Agreement or violate the image and dignity of the Republic of Poland or the Polish foreign mission in the Republic of the Philippines. The decision in the above matters rests with the Ordering Party.

When performing its activities, the Contractor must apply the provisions of the General Data Protection Regulation and the Polish regulations on the protection of personal data, the provisions set out in Annex X to the Community Code on Visas.

V. Personnel:

The Contractor undertakes to comply with the relevant provisions of generally applicable law, in particular the provisions of the labour law with regard to the employees employed by the Contractor (i.a. concluding employment contracts, observance of employee rights) or the provisions of civil law with respect to persons acting on behalf of the Contractor (m.in. concluding civil law contracts) as well as tax regulations and regulations concerning the social security system.

When performing the tasks resulting from the Contract performed by the Contract, the Contractor shall ensure in particular:

1. demonstrate that the staff has no previous criminal record and has the necessary qualifications,
2. providing the Ordering Party with information about the identity (name, surname, citizenship, number of the identity document, date and place of birth) of persons who are to be included in the staff on an ongoing basis before their employment and consulting changes in personnel before their employment;
3. appropriate training of staff to ensure the proper performance of duties,
4. from among the staff, it will select one central coordinator (VAC in Manila) and a local coordinator (VAC in Cebu), with the qualifications specified in point III.
5. that the staff comply with the principles of confidentiality during the performance of their duties, also after leaving the position or after the termination or expiration of the Agreement.

The Contractor also undertakes to make every effort to maintain the stability of staff disposition and to prevent excessive staff turnover, in particular through appropriate wage and personnel policies, corresponding in particular to the relevant Philippine employment laws.

VI. Personal data

In connection with the performance of the Agreement, the Administrator entrusts the Contractor with the processing of personal data to the extent necessary for its proper performance. The Parties are obliged to sign Standard Contractual Clauses, in accordance with the template presented by the

Ordering Party.

The Contractor is obliged to apply the provisions of the General Data Protection Regulation, the Polish regulations on the protection of personal data and the provisions set out in Annex X to the Community Code on Visas.

The Contractor undertakes, when processing personal data, to secure them by applying appropriate technical and organizational measures ensuring an adequate level of security corresponding to the risk associated with the processing of personal data, in accordance with the requirements contained in Article 32 of the General Data Protection Regulation. With regard to the performance of its activities in the field of personal data protection, the Contractor is obliged, in particular, to:

1. authorize the members of its staff to process personal data who will process the entrusted personal data for the purpose of the performance of this Agreement;
2. creating a circulation of visa documentation enabling authorized employees to access personal data adequate to the scope of their duties and constant vigilance so that the data is not read, copied, changed or deleted without authorization, especially when transferring them to the Ordering Party;
3. provide adequate means to trace the circulation of the file of each application sent to and from the consular office;
4. ensure that persons authorised to process personal data undertake to keep them confidential;
5. transfer of data according to the instructions given by the Ordering Party:
   - electronically, in encrypted form, or
   - indirectly, in a secured manner, preventing access to them by third parties;
6. prompt submission of data:
   - in the case of data provided physically – immediately, but not later than within 2 working days from the moment of their acceptance,
   - in the case of data transmitted electronically in encrypted form, at the latest at the end of the day on which they were collected.
7. delete the data immediately (no later than within 7 days after their submission) and ensure that only the name and surname and contact details of the applicant are stored (in order to arrange the date of the appointment), as well as the passport number until the passport is returned to the applicant and deleted after 5 days after the end of services related to the processing of personal data, delete or return, depending on the Ordering Party's decision, all personal data and delete any existing copies thereof, unless the European Union law or the provisions of law applicable to the Contractor prevent the Contractor from returning or destroying all or part of the personal data provided. In this case, the Contractor guarantees that it will ensure the confidentiality of the personal data provided and will not actively process it anymore;
8. ensure all technical and organizational measures, in accordance with the requirements of Article 32 of the General Data Protection Regulation, including security measures required to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or disclosure – especially when it concerns the

storage of files and data in the Contractor's premises and their transfer to the Ordering Party – and against any other forms unlawful processing of personal data; in particular, to protect the processed data, security measures should be used, such as modern CCTV monitoring systems, alarm systems informing about burglary, assault and fire, equipping the office with patent metal cabinets, ordinary lockable cabinets, reinforcements of entrance and spare doors and doors to main rooms, physical protection of the facility, access control system, etc.;

9. securing ICT infrastructure and equipment against unauthorized access, interference of third parties and unauthorized activities of personnel (e.g. use of private communicators, private e-mail boxes, connection of private data carriers). In addition, ICT systems used for the processing of personal data should guarantee the confidentiality, availability and integrity of data;
10. processing data on visa applicants on behalf of the Ordering Party only for the purpose of performing the Agreement;
11. provide visa applicants with the information required under Article 37 of Regulation (EC) No 767/2008 (VIS Regulation);
12. comply with the obligations under Article 28(3)(e) and (f) of the General Data Protection Regulation;
13. provide visa applicants with information on the processing of their personal data, as referred to in Articles 13 and 14 of the General Data Protection Regulation, in particular by posting it on the boards in front of the entrance and in the Visa Lounge of the Visa Advisory Board, as well as on a dedicated website related to the implementation of the subject of the Agreement;
14. keep a record of all categories of processing activities carried out in connection with the performance of this Agreement, in accordance with Article 30(2) of the General Data Protection Regulation;
15. compliance with the terms and conditions of use of the services of another processor referred to in Article 28(2) and (4) of the General Data Protection Regulation;
16. comply with data protection standards at least equivalent to those set out in the General Data Protection Regulation;
17. designate a data protection officer in accordance with Article 37 of the General Data Protection Regulation.

The Contractor is responsible for the possible consequences of acting contrary to the provisions on the protection of personal data.

The Ordering Party reserves the right to control the implementation of the requirements set out above and to present recommendations in order to comply with the terms of the Agreement in this respect. The Ordering Party reserves the right to carry out inspections also by persons indicated and authorized by the Ordering Party and the supervisory authority, within the meaning of Article 4(21) of the General Data Protection Regulation, competent for the Administrator. The Contractor undertakes to provide the Ordering Party and the supervisory authority referred to above with all information, including documents necessary to demonstrate compliance with the obligations set out in Article 28 of the General Data Protection Regulation.

The Contractor undertakes to immediately (within 24 hours at the latest) notify the Administrator of any attempts or facts to breach the security of the processed personal data. In the event of finding the events referred to in the preceding sentence, the Contractor undertakes to immediately enable the employees of the Ordering Party or the Ministry of Foreign Affairs or persons acting on their behalf, to carry out control of the processing and protection of personal data, including in the scope of the implemented organizational and technical measures referred to in Article 32 of the General Data Protection Regulation.

The Contractor undertakes to provide the Employer with a list of names of authorized staff members who will have access to the entrusted personal data in connection with the performance of the Contract, and also undertakes to obtain from its employees statements on maintaining the confidentiality of personal data entrusted by the Employer, to which they will have access, both during their employment by the Contractor and after its termination.

VII. Securing and maintaining IT systems

The Contractor undertakes to take all necessary technical security measures for the website and the IT systems used (including mobile applications) to ensure their smooth operation and protection against unauthorized interference by third parties, in particular against hacker attacks.

VIII. Functional scope of the appointment booking system for the purpose of submitting visa applications and information activities.

Information services will be provided by the Contractor's employees – directly, by phone, e-mail and via the website.

Before booking an appointment, the visa applicant is required to create and confirm an individual account. The method of securing the account registration process is to guarantee that unauthorized persons cannot register.

The appointment booking service consists, in particular, in providing on-line access to the schedule for registration for a meeting in order to submit a visa application on the dates proposed by the Ordering Party. At the request of the Contracting Authority, the Contractor is to ensure the possibility of queuing applicants' applications. The Ordering Party also reserves the right to keep a schedule of meetings on its own.

Registration of the meeting takes place only through a previously confirmed individual account. The method of organizing the registration of online meetings must be effectively secured against the participation of third parties, legal persons, bots, algorithms or other external factors, in particular by ensuring technical possibilities of verifying the identity of the applicant during the process of creating an account and at individual stages of registration of a visa appointment. The technological and IT measures used by the Contractor must be regularly updated and adapted to the current conditions.

The on-line system allows users to obtain the necessary information about the meeting through an individual account, search for available dates, plan and successfully book an appointment. You will have the option to change or cancel the appointment.

The Contractor provides the Contracting Authority with an administrative account in the system enabling the management of the schedule and access to all data that has been entered or used by users to book a meeting. The Contractor will provide the Ordering Party and the Ministry of Foreign Affairs of the Republic of Poland with full access to the visa appointment registration system in order to supervise the performance of the contract. The contractor will provide facilitated insight and the ability to verify each stage of the process, including login time data, meeting registration, payment data, etc.

The Contractor provides Applicants with automatic information about the change in the status of the appointment and the possibility of verifying the stage of visa application consideration. The Contractor will send an electronic message to the applicant about signing up for a meeting, reminders about the date, cancellation of the meeting via e-mail, text message and an individual user account in the system. The system must inform you about changes in the status or data in the user's account.

The Contractor is obliged to provide technical, IT and human resources that will allow for effective and secure registration of the date for submitting visa applications in terms of personal data protection and will effectively counteract the interference of third parties, algorithms, bots or other external factors in the meeting registration process, in particular by ensuring technical possibilities to verify the identity of the applicant during the registration process account and at the various stages of registration for a visa appointment.

The Contractor is obliged to ensure that all personal data processed by it as the controller in connection with the operation of the registration system for the submission of applications will be processed in data processing centres located in the European Economic Area.

The Ordering Party reserves the right to test the security system against unauthorized access by third parties and algorithms.

IX. Contract with the right of option:

The Contracting Authority reserves the right to launch, as part of the service provided in accordance with the requirements for the basic contract, an additional functionality in the field of verification of the applicant's identity – video-verification, pursuant to Article 441 of the Public Procurement Law (right of option).

The Contractor shall commence the provision of the service under the right of option on the date agreed with the Employer, but not later than 30 days from the date of receipt of the written order from the Employer.

The process of verification of the Applicant in the right of option will consist in the verification by the Contractor of the e-mail address and Filipino phone number of the applicant, and will require the use of a system enabling real-time verification of the identity of the person signing up for the application (video-verification) – regarding the registration of the appointment/postponement/cancellation of the visa appointment in the Contractor's system.

The applicant's passport will be supported in the verification process.

1. The system must have a reference database of documents (SPECIMEN) from countries listed in *the Public Online Register of Authentic Identity and Travel Documents* (PRADO), located on the official website of the Council of the EU and the European Council (https://www.consilium.europa.eu/prado/pl/prado-start-page.html), which allows the passport presented by the applicant to be checked for compliance with the specimen.
2. In a situation where the applicant uses a passport that does not have an RFID chip or it is not possible to verify the certificate of a given country with which the data was signed, an additional element of verification should be introduced by using a return transfer with the bank card of the applicant or a member of the immediate family or his/her legal guardian.
3. If the applicant uses a passport with an RFID chip, where the data has been signed with a valid certificate of a given country, verification by return transfer should not be carried out.
4. Verification of the passport used for identification and the data stored on them is automatic.
5. The system must support reading passport data via NFC interface and OCR reading data contained in MRZ.
6. All data in the passport (including a photo) or selected by the Ordering Party can be verified.
7. During the verification process, applicants should be presented with real-time tips to help them take photos.
8. The system should provide image quality control when capturing video and selfies and compressing them during transfer.
9. The comparison mechanism performs verification taking into account the normalization of all characters, i.e. it ignores the case and omits the meaning of diacritics or bypasses normalization, depending on the set system parameter.
10. The verification algorithm should have a functionality that allows to determine whether the Applicant is a person and not, for example, a bot, i.e. detect and block attempts to cheat the system by presenting photos by an automaton/script or a substituted person. This means that as part of the authentication process, a check is performed:

    - "liveness detection", which detects whether the applicant is a real, "live" person,

    - "Liveness Face Matching", which compares the face between the reference photo and the video frames from the live recordings.

11. The verification algorithm should check at least:

    - compliance with the specimen of the presented passport,

    - passport expiration date,

    - whether the country of issue of the passport (according to the MRZ or graphic design) is the expected one,

    - whether the date of issue of the passport is consistent with the first date of issue of the recognized specimen,

- whether the graphic model of the passport is correct in relation to the MRZ,

- whether the MRZ checksum calculations are correct,

- whether the alphanumeric format of MRZ is correct, in accordance with the ICAO standard and the specificity of the country,

- whether the MRZ bar characters are correctly aligned and whether the font is correct,

- in the case of a document that should contain a two-dimensional code (2DDOC), whether it is present and compliant with the expected standard,

- whether the signature in 2DDOC is valid,

- whether the passport page contains a photo and whether it is in the right place,

- whether all security features visible in the passport are consistent and present,

- whether the analysed passport is not a black and white photocopy.

12. The verification algorithm should perform a consistency check between the input data entered at the beginning of the process and the data extracted from the analyzed passport, and between the data in different parts of the document such as MRZ and VIZ (visual zone) and downloaded from the chip via NFC.

X. Collection of biometric data

The subject of the contract is also the collection of biometric data necessary to issue a visa from applicants and providing the foreign mission with biometric data.

The Contractor will equip the VAC on its own with the hardware and software necessary to collect biometric identifiers (fingerprints), scan photos and take photos of the face directly on site along with their printing in a format compliant with the requirements of the Emergency Service and automated/machine registration of all alphanumeric data included in the visa application.

The hardware and software should be prepared and configured by the Contractor in such a way that the biometric data (fingerprints) collected during the visa process meet the criteria set out in the European Commission Decision No. 2009/756/EC of 9 October 2009 laying down specifications for the resolution and use of fingerprints for biometric identification and verification in the Visa Information System (OJ L 270, p. 14).

Biometric device:

- it must be certified by the FBI for compliance with the FBI Electronic Fingerprint Transmission Specification (EFTS)/Apendix F IAFIS Image Quality Specification.
- it shall comply with the criteria of ISO/IEC 19794-4:2005 (Biometric data interchange formats – Part 4: Finger image data) relating to the collection of fingerprint images, in particular point 7. ("Image aquisition requirements") or equivalent.

- the quality of the fingerprint images collected must meet the requirements of ISO/IEC 19794-4:2005 and ANSI/NIST-ITL 1-2000 (Data Format for the Interchange of Fingerprint, Facial, Scarmark & Tattoo (SMT) Information) or equivalent.
- Your device must be capable of capturing scanned flat fingerprint images at 500 ppi ± 5ppi (vertical and horizontal) in 8-bit grayscale (256 shades).
- the device must be adapted to work at ambient temperatures ranging from 5 to 40 degrees Celsius and at relative humidity ranging from 20 to 80%.
- The appliance must be designed for continuous operation for 12 hours a day throughout its lifetime.
- The device must be equipped with elements (e.g. LEDs, hand and finger pictograms, LCD display) supporting the operator's work by informing about the current step of the fingerprinting process and the result of the assessment of the quality of the collected image.
- the software supplied with the device must allow the device to be used in normal user mode, without administrator rights in the operating system of the PC.
- The device and the supplied software must have a function of automatic quality control of scanned fingerprint images and a function of automatic collection of fingerprints when the quality is assessed by them as sufficient.
- The device and the supplied software must have a function to reduce the negative impact of excessively dry or damp skin on the quality of the collected fingerprints.
- The device and the supplied software must have the function of automatic detection of image deformations caused by unwanted movement of the finger during scanning, informing the user about this fact if necessary.

The Contractor undertakes to collect biometric identifiers with a quality that allows to maintain an IQ (Insufficient Quality Percentage) error rate not higher than 2.5% for biometric data sent to the Central Visa Information System. The above level of quality of biometric identifier collection should be maintained throughout the entire period of service provision by each VAC separately.

At the request of the Contractor, the Ordering Party will carry out quality tests of the submitted samples of collected biometric identifiers in the test environment of the Visa Information System and will inform the Contractor about the results of these tests.

The collected biometric data together with alphanumeric data will be transferred to the consular office in the form of data packets saved on external carriers. As an external medium, it is allowed to use write-once, single-layered and single-sided optical discs.

The processing and transmission of data to a mission abroad must take into account the requirements of the Community Code on Visas and the General Data Protection Regulation, in particular it must be ensured that the data transmitted is not read, copied, altered or deleted without authorisation.

Data may be transferred to a foreign mission only in encrypted form, with a level of security not worse than in the case of using the Advanced Encryption Standard (AES) (FIPS PUB 197) using a 256-bit cryptographic key or equivalent.

The data packets listed in section 4.7 shall include, in particular, alphanumeric data in the form of XML files, and biometric data in NIST format, in accordance with the ANSI/NIST-ITL 1-2000 standard or equivalent.

Biometric data saved in NIST format will include the following information:

- Description of the transaction – Type-1 logical record,
- Text data containing additional information related to the type of transaction – logical record Type -2,
- Scanned images of flat prints for each 10 fingers segmented at 500 dpi – Type-4 logical records.

XI. Subcontractor

The Employer allows the Contract to be performed by Subcontractors, however, it stipulates that the following key activities must be performed by the Contractor (they cannot be performed by Subcontractors):

1. accepting visa applications;
2. Collection of biometric data;
3. collection and transfer of visa fees to the Ordering Party;
4. collecting passports and visa decisions from the Ordering Party.
5. ongoing maintenance, modification and update of specialized IT tools used for the implementation of the service;
6. customer contact center.

The Contractor shall be liable to the Employer for the acts or omissions of the Subcontractors as for its own acts and omissions.

The appointment of a Subcontractor requires the written consent of the Ordering Party in each case. The Ordering Party reserves the right to revoke the consent to the performance of the Agreement by a given Subcontractor. If it is necessary to entrust the Subcontractor with the processing of personal data, the Contractor is obliged to apply to the Administrator for written consent. After obtaining the consent, the Contractor concludes a separate Personal Data Entrustment Agreement with the Subcontractor, which generally provides for the same obligations with respect to the protection of personal data as specified in the Standard Contractual Clauses signed by the Contractor and the Controller.

Requirements for valuation:

Please provide the proposed total net price of EUR (excluding tax) for the entire subject of the contract and the net fee of EUR (excluding tax) for the acceptance of 1 visa application in accordance with the form below, distinguishing between the price for the performance of the basic contract and the contract with the right of option.

For the purposes of this valuation, the maximum expected number of applications, i.e. 20,000, should be assumed, both in the basic contract variant and in the option variant.

VISA APPLICATIONS		
Estimated maximum number of accepted visa applications during the term of the contract	**The net unit price of EUR understood as the fee charged from one accepted visa application**	**The net value of EUR for accepted visa applications during the term of the contract**
A	B	C = A x B
20 000		
Option visa application service		
Estimated maximum number of accepted visa applications during the term of the contract	**EUR net unit price understood as a fee charged per accepted visa application**	**The net value of EUR for accepted visa applications during the term of the contract**
A	B	C = A x B
20 000		

Deadline for submitting the valuation:
We kindly ask you to send a quote for the service by April 4, 2025 to the following e-mail address: manila.amb.sekretariat@msz.gov.pl
Contact person: Ms. Agnieszka Dyszlewska, Consul of the Republic of Poland in Manila.

Additional information:

Please be advised that the said request for valuation **does not constitute an offer within the meaning of Article 66 of the Civil Code,** nor is it a contract announcement within the meaning of the Public Procurement Law. Its purpose is solely to assess the price of the market among entities providing visa application services in the Republic of the Philippines and to obtain knowledge of the estimated costs associated with the planned public contract.

Information on the processing of personal data by the Embassy of the Republic of Poland in Manila

This information is the implementation of the obligation set out in Articles 13 and 14 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, hereinafter referred to as the "GDPR".

1. The controller, within the meaning of Article 4(7) of the GDPR, of personal data is the Minister of Foreign Affairs with its registered office in Poland, Warsaw, Al. J. Ch. Szucha 23, while the controller is the Head of the Embassy of the Republic of Poland in Manila, **address:** 9th Floor, Del RosarioLaw Centre, 21st Drive corner 20th Drive, Bonifacio Global City, City of Taguig 1630, Metro Manila.
2. A Data Protection Officer (DPO) has been appointed in the Ministry of Foreign Affairs and foreign missions.

   Contact details of the DPO:

   registered office address: Al. J. Ch. Szucha 23, 00-580 Warsaw

   adres e-mail: iod@msz.gov.pl
3. The scope of processed data includes the data indicated in the offer sent by the Bidder, in particular:
   name and surname,
   b) business e-mail address,
   d) business telephone number.
4. The personal data has been provided by the Tenderer in connection with the response to the request for cost estimation or directly.
5. Personal data will be processed on the basis of Article 6(1)(c) of the GDPR, in order to prepare the public procurement procedure, the subject of which is the service of accepting visa applications, in connection with Article 44(2)-(4) and Article 162(4) of the Act of 27 August 2009 on public finance.
1. Personal data will be processed until the purpose of processing referred to in point 5 ceases to exist, and then they will be stored for archival purposes, in accordance with the provisions of the Act of 14 July 1983 on the national archival resources and archives and the internal regulations of the Ministry of Foreign Affairs and the foreign mission resulting from the provisions of the above-mentioned Act.
2. The data is protected under the GDPR and may be made available to other persons and entities under the law. Access to the data is granted to authorized employees of the Ministry of Foreign Affairs and the foreign mission.
3. Personal data will not be transferred to a third country or to international organizations.
4. The data subject has the rights to control the processing of data, specified in Articles 15-19 of the GDPR, in particular the right to access the content of their data and rectify them, the right to delete data and limit processing, if applicable.

5. Personal data will not be processed in an automated manner that will affect the making of decisions that may have legal effects or similarly significantly affect them. The data will not be subject to profiling.
6. The data subject has the right to lodge a complaint with the supervisory authority at the following address: President of the Office for Personal Data Protection
   Stawki 2
   00-193 Warsaw