

Long Term Arrangement for PCI Compliant Telemarketing Solution

Table of Contents

| | |
|------------------------------------------------------------------------------|-----------|
| 1. Background | 2 |
| 2. Purpose and Objectives | 2 |
| 3. Scope of Works | 2 |
| 4. Deliverables | 6 |
| 5. Payment Terms | 7 |
| 6. UNICEF Standards on Travel | 7 |
| 7. Data Processing Agreement and PCI SCC Provisions attachment | 7 |
| 8. Duration | 7 |
| 9. Project Management | 7 |
| 10. Qualifications or Specialized Knowledge/Experience Required | 7 |
| 11. Evaluation Process and Methods | 7 |
| 11.1. TECHNICAL EVALUATION (70% weight) | 8 |
| 11.2. FINANCIAL EVALUATION (30% weight) | 10 |
| 11.3. AWARD RECOMMENDATION | 10 |
| 12. IMPORTANT: Additional Submission Instruction | 10 |
| 13. Appendix to the TOR | 12 |
| Appendix 1 – Detail on the Acquisition Rates for Telemarketing Channel | 12 |
| Appendix 2 – Class I System UNICEF Security Requirements | 13 |
| Appendix 3 - Data Processing Agreement and PCI SCC Provisions | 17 |

1. Background

UNICEF promotes the rights and wellbeing of children everywhere, working with partners including National Committees in [190 countries and territories](#). UNICEF is a voluntary-funded organization, meaning it does not receive assessments from the United Nations and raises funds in both public and private sectors. Private sector fundraising is led by UNICEF's division for Private Sector Fundraising and Partnerships (PFP) with Head Quarter in Geneva, Switzerland.

From the private sector, UNICEF raises funds from individuals, businesses, and foundations. Individual pledge donors have been a successful UNICEF fundraising mechanism for the country offices through various channels, including the telemarketing channel. UNICEF offices across the world have established Telephone-for-fundraising (i.e. telemarketing) activity to grow the donors' database and it has been showing promising result.

These campaigns have allowed to increase and maintain loyalty of monthly donors who provide their support so that UNICEF can continue to carry out actions for children. On average, 121,000 new donors are recruited annually adding to the 589,000 already existing donors. PANs (Primary Account Number) are collected when a donor signs up to donate using a debit or credit card, and when they update their card information. Further detail on the number of donors obtained through the telemarketing channel can be seen under Appendix 1 of this TOR. The data listed in Appendix 1 is the status as of 2022.

UNICEF has obligations to its donors to protect their cardholder data and is seeking a superior solution that aligns with the requirements of the Payment Card Industry Data Security Standards (PCI-DSS). UNICEF's strategy is to transfer UNICEF's Card Holder Data (CHD) footprint from internal environments to PCI compliant third-party service providers.

2. Purpose and Objectives

UNICEF is seeking to work with one or more qualified vendor/s through a Long Term Arrangement/s (LTA/s) to provide an easy-to-implement Telemarketing solution that connects to the local Payment Gateway/Payment Service Provider/Tokenization Provider for tokenization and payment processing as well as with UNICEF's internal CRM systems ensuring PCI compliance of UNICEF's Telemarketing channel.

The vendor/s that have been awarded the LTA/s, i.e. LTA vendor/s, shall provide services in one, two or all of the four regions/LOTs* identified below:

- LOT1: Asia Region
- LOT2: Europe Region
- LOT3: South America Region
- LOT4: Africa Region

*Definition of "LOTs": Following the scope of this TOR, the Telemarketing solution is expected to be procured and operated under the above LOTs which are differentiated based on the regions. **Interested vendors can propose to provide services for one or more of the LOT/s, clearly indicating the service area coverage above that they are interested in. Proposal for each LOT must be submitted separately.**

The Long Term Arrangements (LTAs) to commence after the initial implementation and System acceptance by UNICEF and shall be valid for an initial period of up to 3 years, with potential extension for two (2) additional periods of two (2) years each (3+2+2 years) at the discretion of UNICEF and subject to satisfactory performance and UNICEF's needs. The LTAs shall be a mutual agreement between UNICEF and the LTA vendors to provide the required services and software solutions at agreed rates/fees over a period of time.

Once the LTAS is in place, UNICEF will operationalize the engagement of the telemarketing solution through the issuance of Institutional Contracts. UNICEF shall provide specific deliverables and time frames for each requirement as required using the terms and conditions agreed in the LTA and the agreed rates/fees stated in the LTA will be used to calculate the contract amount.

UNICEF reserves the right to rescind the Arrangement during that period should performance not meet its requirements. Under an LTA, UNICEF does not warrant that any quantity of services or Software Solutions (SAAS) shall be purchased during the term of the Arrangement and is not bound to purchase any minimum amount of services. UNICEF reserves the right to utilize other sources at its discretion. List of countries that are currently or in the next 7 years will be conducting telemarketing activities can be seen under the Technical Response Grid – Payment Gateway/PSP and Telephony System Compatibility document (ANNEX C of the RFPS document).

3. Scope of Works

The proposed vendor/s' telemarketing solution is expected to be able to provide the below capabilities. UNICEF will use the telemarketing solution to receive calls as well as to contact potential donors, inviting them to become UNICEF recurring monthly donors, through automatic charges on their credit card, debit card, bank account or other payment mechanism as agreed with UNICEF staff in each country. In addition, it could also involve activities of contacting current UNICEF pledge donors and inviting them to increase their existing donation and/or to be able to call donors who present donations pending charge due to problem in payment method.

Capabilities required from the telemarketing solution:

User management

- The UNICEF administrator must be able to set up Agent users (UNICEF staff and appointed consultants and Telemarketing Agency staff) with their own unique and secure login.
- The SaaS solution shall follow the principle of least privilege, guaranteeing that users, group, role, and device identifiers will be unique. The vendor shall integrate their solution with UNICEF's authentication and identity framework; implementation/ adoption of Single Sign-On which uses UNICEF's own federated identities for integrating third-party systems. The support must support Single Sign-On (Azure Identity Management) capabilities for internal staff members as well as authenticated sign-in for staff from third party service providers. UNICEF will provide all the required information to the vendor.
- Online monitoring for coaching & supervision. Desirable: Ability to populate a questionnaire with the evaluation of the listening.
- System must enforce PCI level access controls, e.g. Agents users must have a separate login, and a complex password. Agent users must be logged out after 15 minutes inactivity and must be required to change their password every 3 months.
- System must support Multi Factor Authentication.
- Ability to create teams and assign Agent users to the teams. Agent users or teams must not be able to view call lists, reports and data belonging to another Agent users or teams.
- Scalable from 5 Agent users to 100+ Agent users per Country.
- Ability to control the number of Admin Operations roles through a controlled process.
- Having audit capabilities available.

Ability to Handle Outbound and Inbound Calls

- Automatic / Predictive dialing highly desirable
- Inbound ACD functions for multiple and simultaneous queues and trunks
- Screen popping for inbound calls (e.g. the ability for Native integration to display the correct contact record based on the incoming call number)
- Call timer
- Display the correct script
- Ability to automatically create case records in the CRM based on call outcome
- Ability to record notes / next actions based on call
- Ability to assign follow up actions to users in the CRM based on call outcomes
- Blending mode for in/out agents

Lead Management

- Ability to import leads as a file and run filters on this file and clarity on the list of formats that can be used to import data into the vendor's product.
- Ability to manually create leads.
- Ability to filter leads based on location, number of call back attempts, and other parameters.
- Ability to create several different call lists from a single leads file and save each list with a unique name and assign them to different teams of Agent users.
- Ability to create and manage a "Do-not-call" list.
- Automatic callback feature for abandoned calls (for example for DRTV campaign, detect missed calls and set an outbound list to make outbound calls)
- Ability to reschedule calls on certain date and time or according to priorities
- Manage click to call opportunities.
- Ability to report performance against segments and Agent users and teams.

Call Lists

- Ability to set up call lists and assign lists to teams or Agent users.
- Ability to import call lists and create new call lists manually. Clarity on the list of formats that can be used to import data into the vendor's product.
- Have admin operations dashboard to view call lists across teams and Agent users.
- Assigned user must be able to see all the leads as well as search for specific donors or Agent users.

Pledge Creation and Updates

- Once payment card data is successfully entered, according to the voice prompts, the lead must automatically be saved and converted to a pledge.
- Ability to accept other payment types relevant in the country and the ability to manually convert the lead to a pledge.
- Ability to change payment details in a PCI Compliant way.

Payment Card Handling

- Neither the Agent users nor the device that the Agent user is using must come into any contact with the payment card details.
- The solution must request and process payment card details according to PCI-DSS Standards.
- The call recording must not record the card number.
- The card details must be exchanged with the Payment Service provider or a Tokenisation Service Provider, upon which a token will be received and returned to UNICEF systems.
- The token must be recorded in the solution.

- When payment card details are changed, the solution must manage the tokenization process.

Ability to Manage Costs

- Ability to monitor usage of and spending on the product.

Links with other Systems

- Integration via APIs and other flexible and secure (PCI compliant) ways of integrating to multiple services.
- Integration with Payment Gateway/ Payment Service Provider for Tokenisation and Payment processing.
- Ability to integrate with BI tools such as Power Bi or Tableau.
- The IVR must be integrated with the Payment Service Provider (PSP) and the response (successful / rejected transaction) from the PSP must be captured and displayed to the agent in the CRM.
- Run on windows or Linux
- Standard integration connectors to the following CRM systems in addition to the one built in-house will be beneficial:
 - ✓ DPO
 - ✓ MS Dynamics
 - ✓ Salesforce NPSP
- Ability to keep a reference number to maintain links between UNICEF's internal systems and other systems such as Payment Service Providers. This reference number must be usable in reconciliation of records.
- Ability to link data in the system with UNICEF campaigns.
- Ability to export data to other systems and clarity on the list of formats that can be used to export data from the vendor's product.
- Access to the database with read/write permissions for specific users.
- Ability to retrieve certain fields of information from DPO and be able to update it, for example email, donation amount, etc.
- Clarity if the integration to other applications provided out of the box or paid add on. And having a list of applications to which vendor's product integrates out of the box.

Call Recordings

- Call recordings must use Dual Tone Multi_Frequency (DTMF) technology or its equivalent and when replaying a message, the Payment Card details must not be present.
- Call recordings must keep all metadata associated with a call, e.g. date, time, phone number, campaign, segment, length of call, outcome of call, Agent users details.
- Ability to locate and listen recordings by the metadata included on the files.
- Ability to update call recordings with the outcome of the calls and the status of the call.
- Ability to listen to all call recordings for a lead.
- Ability for UNICEF to supply pre-recorded voice prompts to help the donor update their credit card details over the phone.
- Ability to offer voice prompts in the local language and English.
- Ability to add a Voicemail recording to a Campaign.
- When calls are made to the specific campaign, the specific voice recording must be played.
- Ability to add a phone number to a Campaign.
- The donor must have the ability to leave a message.
- Ability to record all actions on call recordings and associate a status the call recording and should be made available to UNICEF when required.
- Ability to switch to DTMF (Dual Tone Multi Frequency) mode or its equivalent when callers capture credit card details (i.e. switches to the caller and asks the caller to enter their credit card details, after which the caller returns to the Agent users on the call).
- The media archives will be preserved for the duration of the LTA before transporting them to UNICEF upon termination of the agreement.
- Ability to initiate calls to donors and follow the same workflows as for incoming calls.
- Ability to receive calls from donors when they react to fund raising campaigns or when they have a query of an update to their donation details such as card number, amount, etc.
- System must support Predictive/ Automated dialing – (i.e. the ability for the system to initiate calls to donors / prospective donors automatically, and only connecting agents when the call is answered – thereby increasing productivity).

Use Verified Phone Numbers

- Ability to use our own local phone numbers or ability to hire local phone carriers to optimize telephony costs and improve contact rates.

Social Media and Communication Channel Integration

- Ability for restricted users to connect campaigns to UNICEF's Facebook page and Messenger.
- Ability to integrate with WhatsApp.
- Ability to send customized emails with the goals: 1) provide information to the donor or 2) input payment details (donor should be able to load input its CHD, when pressing submit this information should automatically impact on the system as a Positive Donation).
- Ability of email admin module to receive and reply messages.
- Ability to manage web chat

- Email integration with email platforms. The integration to include but not limited to:
 - ✓ The agent should be able to send emails in plain text and/or HTML (the agent should be able to select which HTML should be sent according to a preloaded set of HTMLs assigned to the campaign that the agent has been assigned).
 - ✓ Automatic email sending once the agent selects the final call result (ie: positive/negative). This as well depends on the campaign the agent is working on as there is a specific HTML per type of campaign.
 - ✓ The emails should be customizable in certain parameters, for example Name and Surname should be captured in the mail.
 - ✓ In order to do this configuration a specific module would be needed in order to customize which HTMLs should apply to each campaign and which mails should be sent automatically and which ones should be chosen manually.
 - ✓ Final note: these interactions should be recorded in the CRM as well as in the main system (DPO and Salesforce).

Training

- Solution must offer out of the box training to users and administrators including the training material on use of the system.

Dashboards and Reports

- Admin operations dashboard to view activity across the system.
- Provide the capability to define Key Performance Indicators (KPIs) and measure performance against defined KPIs both online and with scheduled/ad-hoc reports with following reports at the minimum:
 - ✓ Detailed reports that contain the data of the donations and the donors
 - ✓ Agent Performance Analysis
 - ✓ Call Traffic Analysis
- Ability to export data to UNICEF Datawarehouse or any other system as well as clarity on the list of formats that can be used to export data from the vendor's product.
- Ability to visualize and configure only the campaign assigned to each one. UNICEF should be able to see the performance and configure of all of them.
- Each form/campaign have different fields and validations to accomplish its goal. Must be customizable.
- Ability to customize call results/ "dispositions" according to each type of campaign. (For example, Upgrade, Upgrade + AAC, Negative + AAC).
- Ability to customize, edit and validate different fields on each record.
- Provide customizable online reports (contactability, conversion, average amounts, log on, talking time, occupancy and availability reports, etc.)

Non-Functional/ Administration

- 98% availability of the time per month to be guaranteed through a Service Level Agreement (SLA) and remedies to be provided should the vendor does not meet the SLA parameters. Planned maintenance windows to be communicated to UNICEF at least a week before downtime occurs and have clear mechanism for monitoring SLA compliance. UNICEF expects frequency of SLA compliance reported on a monthly basis.
- It is expected that the application will include back-up, archiving, automated error handling, high availability, and performance monitoring services associated with reliable SAAS solutions.
- Adhere to national and international standard on a) security of CHD of donors (i.e. ISO 27001 and must have the relevant PCI DSS Certification of Attestation related to the specific services) and b) data protection.
- This project/requirement has been classified by Information Security Classification Tool as a Class I – Confidential information and therefore, vendors shall confirm that they currently comply with Class I System UNICEF Security Requirements as detailed in Appendix 2.
- Ability to create different accounts directly with different offices in different countries while consolidating the volume of purchase from those different offices.
- Must run on Desktop PC or laptop running either Microsoft Edge or Chrome.
- Must be available for use on mobile devices and must be optimized for small screens.
- Must be compatible with mobile device or tablet to on iOS and Safari or Android and Chrome.
- Ability to transport UNICEF's full data set from the solution upon termination of the agreement.
- Technical Support:
 - ✓ Operational service from Monday to Friday based on "follow-the-sun" support model through online and phone to enable offices from any region to get service in their own time zone from 9 to 21 hours and if required, operational service 7 days for 24 hours.
 - ✓ Ability to speak local language.
 - ✓ Availability of issue tracking system and escalation process.
- Guarantee full system reliability, including:
 - ✓ Establish simplicity and speed of processes.
 - ✓ A robust capacity to process high volume transactions.
 - ✓ A strong service provision in relation to downtimes/response times.
 - ✓ A full and robust disaster recovery process and procedure (documented).

Maintenance, Support & Upgrades

After implementation, UNICEF requires ongoing support and maintenance from the vendor. This shall include support and maintenance of the basic software tool and of the configuration and customization (if any) implemented for UNICEF.

The vendor shall describe in detail all the annual support and maintenance schemes that they provide. This will include the internal procedures and processes for resolution of problems and strategies for service improvements etc.

The Vendor shall also specify the annual support scheme that will fit the requirements of UNICEF including the specific maintenance entitlements, i.e. software fixes, releases and updates, toll-free telephone support, round-the-clock telephone support, access to bulletin boards, newsletters or general information, account management services, etc.

The vendor shall also provide changes to system and/or application post baseline will be documented, along with description via a formal change management process. The vendor shall report the following information about patches, at a minimum: type, version, reason, post test results after implementation. Patches that fail testing will also be recorded and documented. The vendor should clearly define the procedure to handle escalation issues, bugs, and service packs.

The vendor must guarantee that UNICEF will be available to renew the service and purchase incremental services with original features, functionalities, metrics, and pricing as established in the price proposal. Once the LTA is signed, if the vendor releases additional features, capabilities, add-ons or other changes to the solutions ("the Incremental Features"), the vendor shall ensure that UNICEF is able to maintain the solution in accordance with its original features, functionalities and pricing as described in the LTA. If the vendor is not able to provide the full range of features and functionalities of the solution, without the subscription of the Incremental Features, then UNICEF expects such Incremental Features shall be provided to UNICEF free of cost as part of the price of the original service.

Confidentiality of Information

- The LTA vendor must adhere to UNICEF's policies governing the handling of data:
 - ✓ [UNICEF's Policy on Personal Data Protection](#)
 - ✓ [UNICEF Procedure on Personal Data Breach](#)
- Ensure confidentiality of donors' details and that these are not to be used or disclosed for purposes unauthorized by UNICEF in accordance with data protection regulation.
- Ensures that it has a data protection policy in place that meets all applicable data protection standards and legal requirements and that it will apply such policy in the collection, storage, use, processing, retention and destruction of UNICEF Data.
- The LTA vendor will impose the same requirements relating to data protection and non-disclosure of UNICEF Data, as are imposed upon themselves by UNICEF, on its service providers, subcontractors, and other third parties and will remain responsible for compliance with such requirements by its service providers, subcontractors, and other third parties.
- Any information received or generated during the performance of the service is confidential and reserved, so it cannot be disclosed to third parties.

Note: The use of subcontractors must be clearly explained in the Proposal, and they must be identified by name. The primary LTA vendor shall be wholly responsible for the entire performance, whether or not subcontractors are used.

Exit strategy

Having a clear exit strategy including related step-by-step plan, and description of Post-Termination Transition Assistance, in case any of the parties decided to discontinue the service.

The exit strategy must address, at the minimum the following points:

1. Data Retrieval and Transfer:

- The vendor should outline the process and timeline for retrieving and transferring UNICEF data upon termination.
- Specify the format in which the data should be provided to ensure compatibility with UNICEF's systems.
- Ensure that the provider assists with data extraction, conversion, and migration to UNICEF's preferred platform or alternative solution.
- Provide data dump if UNICEF decides to exit the tool in the future and a clear information on how will the dump will be provided.

2. Data Deletion:

- Define the requirements and procedures for the secure deletion of UNICEF data from the vendor's systems after termination.
- Specify the timeframe within which data should be permanently deleted.
- Include provisions for verifying and documenting the completion of data deletion.

3. Data Backup and Archiving:

- Address the responsibilities of the vendor in terms of regularly backing up UNICEF data during the service period.
- Specify the availability and format of backups that will be provided to UNICEF upon termination.
- Outline the duration and conditions for which the vendor retains archived data, if applicable.

4. Deliverables

- Successful integration/ deployment of the telemarketing solution.
- Successful training of the users and administrators.
- Access to data leads, call lists and call recordings, as well as to the dashboard and reports.

- 98% availability to be guaranteed through a Service Level Agreement (SLA). Planned maintenance windows to be communicated to UNICEF at least a week before downtime occurs.
- Annually (and at any time requested by UNICEF) provides an up-to-date certificate of Attestation of Compliance (AoC) or PCI DSS compliance document as specified by the PCI DSS council in electronic and/or paper format.

5. Payment Terms

Invoices may be issued to UNICEF after the services (or components of the services) have been provided and the deliverables (or installments of the deliverables) have been delivered. The standard terms of payment are net 30 days after satisfactory and UNICEF acceptance and approval of delivery of service.

6. UNICEF Standards on Travel

If any travel is required by UNICEF, the UNICEF's Travel Policy shall apply. Travel will be administered in line with UNICEF travel policies, upon proof of travel costs. Vendor will be responsible in arranging their own travel and will be reimbursed accordingly upon presentation of receipts and based on UN standards of travel:

- Travel paid for by UNICEF shall be based on economy class travel
- Prior to undertaking any travel, approval of fare should be requested from UNICEF. Airfare will be reimbursed upon submission of proof of travel and up to fare entitlement provided or actual cost, whichever is lower. Terminal fees will be reimbursed upon submission of proof of travel and up to the UNICEF terminal fees prices, or actual cost, whichever is lower.
- Combination cost of the accommodation, meals, and incidentals shall not exceed applicable United Nations Daily Subsistence Allowance (DSA) rates, as promulgated by the International Civil Service Commission (ICSC): <http://icsc.un.org/> (information on all countries and destinations can be found by navigating on the map).

7. Data Processing Agreement and PCI SCC Provisions attachment

The **Appendix 3** attached to this Terms of Reference contain Data Processing Agreement and PCI SCC Provisions and shall be incorporated in the LTA and each Institutional Contract issued under this LTA.

8. Duration

The Long Term Arrangements (LTAs) shall be valid for an initial period of up to 3 years, with potential extension for two (2) additional periods of two (2) years each (3+2+2 years) at the discretion of UNICEF and subject to satisfactory performance and UNICEF's needs. The LTA is expected to be finalized approximately by February 2024.

9. Project Management

The vendor shall provide experienced Project Manager to act as focal point between UNICEF offices and the company for all communication and coordination.

10. Qualifications or Specialized Knowledge/Experience Required

- The qualified vendor shall operate in accordance with the UNICEF Policy on Personal Data, which is available at <https://www.unicef.org/supply/documents/unicef-policy-personal-data-protection>.
- Has minimum of 5 years of experience in providing similar SaaS or cloud based solution.
- Have proven capacity to deliver volume required and surge potential.
- Have proven capacity in terms of staff and technical infrastructure, as well as experiences in providing the required services.
- Demonstrate the feasibility of the proposed solution to perform the assignment with an acceptable level of effectiveness.
- Must have the legal permission to operate or have a license to perform the necessary work assignments in each state/territory of service. They have presence in the country and/or availability of their networks. *The vendor needs to submit their Certificate of Incorporation along with information of their networks.*
- The proposed solution should be compliant with regulatory requirements, such as but not limited to:
 - Adherence to the international standard on ISO 27001 and has a data protection policy in place that meets all applicable data protection standards and legal. *The vendor needs to submit their ISO 27001 certificate as well as information on their data protection policy.*
 - Ability to present to UNICEF with a valid PCI DSS Attestation of Compliance (AoC) or PCI DSS compliance document as specified by the latest PCI DSS.
- The qualified vendor is financially stable. *Vendor needs to submit their last 2 years Financial Statement, i.e. Income Statement, Balance Sheet, and Cash Flow Statement together with their technical proposal submission.*

11. Evaluation Process and Methods

EVALUATION OF THE PROPOSAL

The evaluation criteria will be split between technical and financial proposal with a weight of 70% for the technical and 30% for the financial proposals. The evaluation is carried out by, and in accordance with UNICEF's regulations, rules, and practices. All

determinations are made in UNICEF's sole discretion. The Evaluation Team first reviews the technical aspect of the proposal for each LOT followed by the review of the financial proposal of those service providers who pass the technical evaluation for the respective LOT.

Proposal for each LOT must be submitted separately as the evaluation for each LOT would be completed separately against the requirements. Following the submission of the proposals, UNICEF will carry out the evaluation in the following order:

11.1. TECHNICAL EVALUATION (70% weight)

The technical evaluation consists of mandatory, technical proposal and demo/ technical presentation evaluations and be evaluated against the following criteria:

| Mandatory Evaluation | | Points |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|---------------------|
| MANDATORY REQUIREMENT | | (PASS/FAIL) |
| <ul style="list-style-type: none"> <i>the required solution will be a SaaS offering or similar cloud based solution.</i> <i>Certificate of Incorporation and other relevant licenses need to be submitted along the with the technical proposal, i.e. ISO 27001 and valid PCI DSS AOC or PCI DSS compliance document as specified by the latest PCI DSS.</i> | | |
| The Vendor has to meet the mandatory requirements to be considered further for Technical Proposal Evaluation | | |
| Technical Proposal Evaluation Criteria | | Points |
| 1. | Company Profile and Experience | Sub-Total 20 |
| <p>Having presence in the country and/or availability of its networks. Demonstrated experience with a proven record in providing similar service.</p> <p><i>The vendor needs to provide:</i></p> <ul style="list-style-type: none"> <i>The vendor or Lead vendor is the owner of the SaaS Product being proposed and NOT a reseller.</i> <i>Vendor information on their global presence and market share globally as well as vendor information on their geographical presence and market share locally as well as example of successful implementation of the Telemarketing solution in the relevant region as per the submitted LOT (for LOT 1: in Asia; LOT 2: in Europe; LOT 3: in South America; LOT 4: in Africa).</i> <i>Vendor profile such as vendor information, technical and business visions, system audits and certifications, as well as description of the proposed solution and its current use. Relevant certificate, e.g. certificate of Attestation of Compliance (AoC) to PCI DSS or PCI DSS compliance document for the specific services as specified by the latest PCI DSS, ISO 27001 certificate, and data protection policy document.</i> <i>Vendor information on experiences with non-profit organizations like UNICEF as well as client list in the different countries along with the size of the projects, and period of Contract and include at least five (5) client references, along with the contact detail, i.e. name and email address.</i> <i>List of third-party partners and subcontractors involved, if any, and their respective roles in providing the proposed solution. Describe if they have access to CHD.</i> <i>The vendor provides experienced Project Manager to act as focal point between UNICEF offices and the company for all communication and coordination.</i> | | |
| 2. | System/ Technical Overview | Sub-Total 30 |
| <p>Understanding of and responsiveness to UNICEF's system/ technical requirements and complies with the related capabilities under point 3 of this Terms of Reference.</p> <p>The vendor needs to elaborate in their proposal that will showcase their capability in meeting the technical related work assignment under point 3. Provide a summary of the proposed solution and describe in detail the vendor's a SaaS offering or similar cloud based solution. Include an overview of the software, architecture and design, processes, management, implementation, and support of the proposed solution to meet the requirements as described in this TOR. Include any additional functionality offered by the Vendor that is not a requirement of this RFP.</p> <p><i>The vendor needs to provide:</i></p> <ul style="list-style-type: none"> <i>Description of proposed solution including roadmap for the next 3-5 years showing upcoming releases and further innovative features.</i> | | |

| | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| <p><i>This should also include description and illustration of the implementation models and deployment options; separately discuss the proposed model for UNICEF requirements and in ensuring that UNICEF will be self-sufficient in using the proposed solution.</i></p> <p><i>This should include the vendor's policy regarding support of previous releases of software and Product End of Life.</i></p> <ul style="list-style-type: none"> • <i>Description of the proposed Telemarketing SaaS offering or similar cloud based solution with detailed information regarding hardware and software requirements that would be essential for a successful implementation of managed solution, including information on the software technologies used and diagrams showing the main components, workflows, and overall scope of the proposed solution as well as technical diagram demonstrating compliance to PCI-DSS standards and their API'S and connectors for integration and their data import and export capabilities.</i> • <i>Ability to link the proposed solution with UNICEF and other systems. The proposal should include a detailed explanation on how the proposed solution will integrate with UNICEF's authentication and identity framework and other systems, including but not limited to the social media, communication channel, and Payment Gateway/PSP and Telephony System in the relevant region as per the submitted LOT (for LOT 1: in Asia; LOT 2: in Europe; LOT 3: in South America; LOT 4: in Africa).</i> • <i>UNICEF should have full access to the database for future migration to another platform/ tool. Preferably, the solution will provide migration capabilities and highly configurable data model that will make it possible for almost any data to be mapped to new data model.</i> • <i>Information needs to be provided regarding the format and fields required for incoming lead information.</i> • <i>Information on how the vendor's system accepts incoming and process outgoing calls.</i> • <i>Description on what is the requirements for using local phone numbers.</i> • <i>Information on ability to offer voice prompts in the local language and English.</i> • <i>Description on the ability for UNICEF to record calls, store those recordings, and listen to the conversation at a later time. Where these recording will be stored and for how long.</i> • <i>Description on the vendor's method for assuring quality of the service provided and the risk mitigation measures.</i> • <i>Information on any donor data encryption used in the proposed solution (during transmission, at rest etc).</i> • <i>Description on how many users can reasonably use the system at one time without any call experiencing quality degradation.</i> • <i>Ability to meet the service required under the User Management, Lead Management, Call Lists, and Payment Card Handling sections of point 3 of this Terms of Reference.</i> | |
| <p>Proposed approach to overall management of service and account management systems and methodology, work plan, and approach of implementation and integration.</p> <ul style="list-style-type: none"> • <i>Outline of project management procedures.</i> • <i>Project implementation and workplan showing the detailed sequence and timeline for each activity and milestone. Should cover, but not limited to, customization, integration, and implementation of the full scope of the project.</i> • <i>Detailed proposal that will demonstrate the feasibility of the proposed methodology to perform the assignment with an acceptable level of effectiveness (including the level of flexibility in integrating to multiple services) how the proposed SaaS offering or similar cloud-based solution will be hosted, and how the proposed solution will securely handle high volume transactions and possible traffic peaks.</i> | |
| <p>3. Training, Reporting, and Non – Functional/ Administration Capabilities</p> | <p>Sub-Total 30</p> |
| <p>Understanding of and responsiveness to UNICEF's training, reporting, and non-functional/administration capabilities requirements and complies with the related capabilities under point 3 of this Terms of Reference.</p> <p>The Vendor needs to elaborate in their proposal that will show case their approach (e.g. train the trainer or directly to the staff) and capability in meeting/delivering the training, reporting and non-functional related capabilities under point 3.</p> <p><i>The vendor needs to provide:</i></p> <ul style="list-style-type: none"> • <i>Vendor confirmation that they currently comply with Class I System UNICEF Security Requirements.</i> • <i>Detail description of the vendor's training approach for the administrators and end users as well as a copy of the vendor's training material including the training plan.</i> • <i>Description of all reporting capabilities of system to generate scheduled reports, customizable reports, and real time reports as well as information if the reports can be exported in different file formats. A sample of standard reports to be provided.</i> • <i>The process to update or modify forms, fields and reports. Who will update them? What is the estimated time of resolution?</i> • <i>Description on any analytics used to evaluate historical trends and make forecasts.</i> | |

| | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <ul style="list-style-type: none"> • Description on vendor's support processes and service level guarantees that Vendor is willing to put into an SLA; include specific commitments or statements and if Vendor can provide a solution which is available 98% of the time per month and the remedies that shall apply should the vendor does not meet the SLA parameters. • Information on ability to create different accounts directly with different offices in different countries while consolidating the volume of purchase from those different offices. • Information on capability to provide technical/customer support services, i.e. post implementation support, and estimated response times. • Description in detail all the annual support and maintenance as well as support and upgrades schemes that they provide. This will include the internal procedures and processes for resolution of problems and strategies for service improvements etc. • Description on the vendor's overall Business Continuity and Disaster Recovery process. Detailed description of their emergency incident process as well as the role of the UNICEF administrator. • Archiving rules as well as a detailed exit strategy, related step-by-step plan, and description of Post-Termination Transition Assistance, in case any of the parties decided to discontinue the service and archiving rules | |
| TOTAL Obtainable Technical Proposal Evaluation Score <i>The Vendor has to meet minimum passing score of 60 points for Technical Proposal Evaluation to be considered further for Demo/ Technical Presentation Evaluation</i> | 80 |
| Demo/ Technical Presentation evaluation | 20 |
| <i>The Vendor has to meet minimum passing score of 10 points for Demo/ Technical Presentation Evaluation to be considered further for Financial Proposal Evaluation</i> | |
| TOTAL Obtainable Technical Evaluation Score (weight 70%) | 100 |

11.2. FINANCIAL EVALUATION (30% weight)

The price proposal should be separate from the technical proposal. The Proposer is required to submit separate pricing for each LOT. The format shown on **Annex C (Price Proposal Format)** is suggested for use as a guide in preparing the Price Proposal.

The total weight allocated for the price component is 30%. The maximum number of points will be allotted to the lowest price proposal that is opened and compared among those price proposals received which obtain the threshold points in the evaluation of the technical component.

All other price proposals will receive points in inverse proportion to the lowest price; e.g.:

$$\text{Score for price proposal X} = \frac{\text{Max. Score for price proposal} * \text{Price of lowest priced proposal}}{\text{Price of proposal X}}$$

11.3. AWARD RECOMMENDATION

The scores attained by the interested vendors in the technical and financial evaluations for each LOT will be combined to attain the overall score, and the Proposals will be ranked accordingly. The overall combined (Technical + Financial) maximum points that could be allocated to a Proposal is 100 points. Off the maximum combined points, the technical proposal score will account for 70 points and the financial proposal score for 30 points.

The recommendation for award(s) will be made per LOT basis based on best combination of technical and price score and based on the results of the reference checks and financial stability of the vendor(s) for respective LOT.

12. IMPORTANT: Additional Submission Instruction

Technical Proposal

Interested Vendors can propose to provide services for all (separately) or one of the LOT, clearly indicating as per below the service they are interested in. **Each proposal must be submitted separately, as the evaluations would be completed separately against specific region. The LTA/s will be awarded on a LOT by LOT basis. The proposal must clearly identify the related region that the vendors are interested as indicated below:**

| | |
|-------|---------------|
| LOT 1 | Asia Region |
| LOT 2 | Europe Region |

| | |
|-------|----------------------|
| LOT 3 | South America Region |
| LOT 4 | Africa Region |

Financial Proposal

The price and technical proposal must be submitted separately. The price proposal for each LOT must be submitted separately, as the evaluation for each LOT would be completed separately against. **The file name of each price proposal file must clearly identify the related LOT as indicated below.**

| | |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LOT 1 | Asia Region (proposed currency: can be USD or other currency) |
| LOT 2 | Europe Region (proposed currency: can be USD or other currency) |
| LOT 3 | South America Region, except price for Argentina and Venezuela to be quoted in the local currency Of Argentine Peso and Venezuelan Bolívar respectively, proposal for other countries can be in USD or other currency |
| LOT 4 | Africa Region (proposed currency: can be USD or other currency) |

Note:

As part of the UN Harmonization efforts, other United Nations (UN) Agencies and National Committees (Natcoms) may place contracts under the prices of the LTA. Contracts placed by other UN and Natcom entities constitute a contractual agreement between the vendor and the ordering UN or Natcom entities (different general terms and conditions of Contract may apply). UNICEF will not be a contractual party to these contracts and has therefore no obligations or liabilities for contracts not issued by UNICEF. The estimated number of transaction volume stated in the price proposal format, however, applies across orders (including from other UN and Natcom entities) during the life of LTA.

13. Appendix to the TOR

Appendix 1 – Detail on the Acquisition Rates for Telemarketing Channel

Acquisition Period: January - December 2022 (Telemarketing Channel)

| Regions | Sum of Total Active Pledge Donors | Sum of Existing Pledge Donors | Sum of New Pledge Donors |
|---------------------------|--------------------------------------|----------------------------------|-----------------------------|
| LOT 1: Asia | 325,950 | 276,112 | 49,838 |
| China | 70,286 | 59,348 | 10,938 |
| India | 29,345 | 24,325 | 5,020 |
| Indonesia | 1,520 | 1,259 | 261 |
| Korea | 25,601 | 23,442 | 2,159 |
| Malaysia | 188,590 | 158,961 | 29,629 |
| Philippine | 1,013 | 878 | 135 |
| Thailand | 9,595 | 7,899 | 1,696 |
| LOT 2: Europe | 38,327 | 29,868 | 8,459 |
| Belgium | 11,973 | 9,843 | 2,130 |
| Croatia | 1,256 | 1,090 | 166 |
| Czechia | 2,557 | 2,165 | 392 |
| Romania | 22,303 | 16,532 | 5,771 |
| Serbia | 238 | 238 | - |
| LOT 3: Latin Ameri | 345,651 | 282,799 | 62,852 |
| Argentina | 27,983 | 23,950 | 4,033 |
| Brazil | 7,169 | 5,798 | 1,371 |
| Chile | 43,210 | 35,610 | 7,600 |
| Colombia | 150,629 | 120,853 | 29,776 |
| Ecuador | 32,419 | 27,492 | 4,927 |
| Mexico | 21,086 | 17,258 | 3,828 |
| Peru | 31,069 | 25,807 | 5,262 |
| Uruguay | 32,086 | 26,031 | 6,055 |
| Grand Total | 709,928 | 588,779 | 121,149 |

NOTES

a. Retention Campaign Outbound Calls of Existing Pledge Donors (on average):

55% Contacted Rate & 36% Conversion/Success Rate

b. Leads Generation Acquisition Calls that resulted into New Pledge Donors (on average):

30% Contacted Rate & 4% Success Rate with average donation USD 15/month

c. Number of Pledge Donors resulted from Inbound Calls is approx. 3% from the total new pledge donors.

d. Total number of Agents that manage the Telemarketing approx. 800 Agents.

Appendix 2 – Class I System UNICEF Security Requirements

1. Categorization

This document describes UNICEF's security requirements for systems classified as Class I. UNICEF recognizes 4 classes of information: Class I - Confidential, Class II - Internal, Class III - Restricted and Class VI - Public. All classes are based on the business value of the information. As such it is the business that drives the data classification.

Class I systems carry the highest classification throughout the organization. This classification is designated for highly sensitive and critical UNICEF ICT assets.

| System Classification | Description | Asset Rating | | |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|-----------|--------------|
| | | Confidentiality | Integrity | Availability |
| Class I | A system which stores and/ or processes confidential information critical to UNICEF operations, individual's safety and/ or is directly linked to critical business processes. Unauthorized access may severely impact UNICEF operations/ business processes, individual's personal safety and or their identity. | High | High | High |

It shall be noted that the system classification and resulting security requirements are based on input provided by the system owner/ sponsor or their delegated authority. That said, if the value - and hence the classification - of the information changes at any point during its life cycle it is the responsibility of the owner or their delegate to reinitiate the information / system classification process. This requirement is an obligatory responsibility of the system owner to ensure proper protection of the system and the underlying information assets.

2. Applicability / Scope

The security requirements outlined in this document are mandatory and apply to any internal or external party who is providing a solution, a system or a service to UNICEF which processes, stores or transmits information that meets the classification criteria reflected in this document.

2.1. Class I System Properties

A defining property of a Class I system is as follows: a system / service(s) which processes and or stores **personal data** or **confidential UNICEF data** or is **linked to a critical business process(es), as defined in this section**.

Personal data

UNICEF defines personal data similar to article 9 of the EU general data protection regulation 2016/679 (GDPR):

"Data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."

Profiling data when there is any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements."

Any system that processes and or stores personal data is a Class I system.

Confidential UNICEF data

Information such as, but not limited to, sensitive Program Division Reports, HR Records, investigative documents, etc. Any system that processes and or stores confidential UNICEF data is a Class I system.

Linked to a critical business process

The input received during this phase, shall be viewed as "initial", and will require follow-up consultation with the office of Business Continuity prior to the system / solution becoming an operational asset (placed into production). Any system that is linked to a critical business process shall be classified as a Class I system.

3. Security Requirements

All the requirements covered in this area reflect controls that shall be included in any Request for Proposal (RFP), Work Orders/ Package, Term of Reference (ToR) or any document that may be used by a service provider or professional services entity which are providing UNICEF a "Product" or "Service".

Both business owner (data controller) and the service provider (data processor) share the obligations for ensuring proper implementation of the requirements.

It shall be noted that the requirements outlined in this section be viewed as an additional layer to complement vendors existing security eco system and not a replacement. In cases where a service provider's controls are more restrictive the service provider's controls shall prevail and be formally captured by both parties.

3.1. General Security Requirements

- a) UNICEF shall reserve the right to assess the quality and accurateness of outsourced software development and operational maintenance of the system/ application; whether it be through security assurance testing or through external security assessment.
- b) Solution / Service shall be protected from unwanted network traffic by network filtering or separating measures that lay outside of the system; such as externally controlled routers and firewalls.
- c) The system shall have proper end-point protection, with the following minimum requirements:
 - malicious code protection measures
 - host firewall configured utilizing, at a minimum, least privileged access controls (services, user, communication access).

3.2. Validation of Security Controls

- a) UNICEF shall reserve the right to periodically validate the implementation of the security requirements outlined in this document via:
 - Security Assurance Testing
 - Vulnerability Testing
 - Penetration Testing
 - Audits
 - On-site checks

3.3. Compliance & Certifications

- a) Any vendor that provides hosting of any class I system, shall carry, at a minimum ISO2700K, certification and provide the following documents for view: ISO Certification, SoA, SOC 2, and SOC3 audit findings.

3.4. Identification, Authentication and Authorization

- a) The service provider shall follow the principle of least privilege, guaranteeing that users, group, role, and device identifiers will be unique, assigned to each entity (user or process). Each application user role shall have a correspondent database connection according to its privileges.
- b) The service provider shall centrally manage the user account using federated identities and whenever possible integrate their solution with the UNICEF Identity Management System.
In case authentication is password based; the password shall forcefully adhere to the common best practice quality requirements and will be forcefully renewed frequently. The allocation of authenticators will be controlled and management through a formal process.
- c) Multi-factor authentication will be used for:
 - privileged accounts and
 - user access outside of UNICEF trusted network.
- d) All the user and system accounts shall be disabled after a defined period of inactivity, in accordance with organizational standards. All default accounts and or passwords shall be removed or changed. Approvals will be required for creation, deletion or modification of any account.
- e) All access from external networks will traverse specific entry and exit points where external communication is terminated and re-established into a UNICEF controlled ICT ecosystem.
- f) Account lockout features will be used for invalid authentication attempts.
- g) Application code shall never contain any credentials.

3.5. Availability and Deletion

- a) Systems availability shall be set according to Service Level Agreements, to meet the Confidentiality, Integrity and Availability requirements commensurate with its classification, as noted above
- b) Any deletion of confidential / personal data must be done so that it cannot be reconstructed.

3.6. Cryptography

- a) The system shall have cryptographic controls in place to secure sensitive data while in transit, while at rest and while in use. At a minimum, UNICEF cryptographic standards shall be used. In cases where vendor cryptographic standards exceed published organizational standards, vendor technical controls shall prevail.
- b) Personal data shall be masked, pseudonymized or otherwise protected from unauthorized access.
- c) The service provider shall use best practice or industry standard secure data exchange protocols and keep them up to date, as per defined UNICEF standards. Outdated and/ or compromised protocols shall never be used.
- d) All passwords shall be encrypted with best current practices or strong industry standards cryptographic algorithms and secure keys. The keys will be generated using strong cryptographic algorithms.
- e) Key files must be protected from unauthorized modification using an application that enforces automatic reconciliation from an authoritative source.
- f) Encryption keys shall be securely stored outside of the systems on which they are used.

3.7. Secure Development

- a) The system shall be engineered following the '*security by design*' principles.¹
- b) The system shall be developed following the '*data protection by design and by default*' principle.²
Hence appropriate technical and organizational measures shall be in place to implement the data protection principles and safeguard individual rights. Data protection shall be integrated in processing activities and operational practices, from the design stage throughout the solutions lifecycle.
- c) Development and tests of the system will be done with fictitious or pseudonymized information.
- d) Any source code developed specifically for the system shall undergo a security assurance testing, and business impact analysis to bring operational business to acceptable level. Risk tolerance level, shall be established by the system / solution owner.
- e) Access to program source code and associated items - such as designs, specifications, testing and validation plans - shall be strictly controlled; to prevent the introduction of unauthorized functionality.
- f) The system shall display generic error messages that do not disclose detailed information such as process logs, account or system information.
- g) Executable code will not be implemented on an operational system until evidence of conforming to the testing criteria (user approval, QA, or the equivalent) is acquired and the associated program source libraries have been updated.

3.8. Updating assets' inventory

- a) The assets' inventory related to UNICEF applications shall be updated, as part of the operational process, capturing all system elements, describing their business function, location/ identifiers and business owner.

3.9. Security Operations

- a) The system shall be hardened, which means that:
 - only the services and network ports necessary for efficient operation are up and running
 - all application code is patched and kept up to date and
 - limiting the accounts and removing, changing or disabling default accounts and passwords**Note:** To ensure proper risk driven methodology is followed, patches shall fall into one of the following categories, which are classified by the application / system vendor.; critical, noncritical. The patching window SLA shall be formally documented by both the vendor and UNICEF's Designated Authority (D.A.).
- b) Servers and applications shall be configured to run with the minimum system authorizations necessary. The service provider shall ensure the implementation of the appropriate technical and organizational measures.
- c) The system must be configured to display generic error messages that do not disclose detailed information such as process logs, account or system information.
- d) The production environment shall be separated from the test and development environments; preferably on logically and physically different systems.
- e) Development and test environment shall have the same patch level as the production environment.
- f) The production environment shall not have any development tools.
- g) Configuration/Application source code/customized work shall be protected from unauthorized access / modification and reside in non-production environment with proper back-up/ resiliency policy.
- h) The system shall have malicious code protection measures. Logs generated by malicious code protection measures shall be monitored.

¹ As described by OWASP in https://www.owasp.org/index.php/Security_by_Design_Principles

² As described in article 25 of the EU general data protection regulation 2016/679 (GDPR)

3.10. Vulnerability Management

- a) The service provider is required to run security tests. Test will run prior to the launch of the system and periodically afterwards; with a minimum frequency of once a year.
- b) The service provider is required to report on the results of the security scans and the remediations taken. These reports will be sent to UNICEF's Chief of IT Security or the relevant focal point(s).
- c) Critical security patches shall be applied within 3 days, following established testing/ change management processes.

3.11. Change Management

- a) Any changes to UNICEF system(s) or software shall be agreed upon between ICT and the business division / office owner of the affected system and third party.
- b) Changes to system and/or application post baseline will be documented (version / build number), along with description via a formal change management process. The service provider shall report the following information about patches, at a minimum: type, version, reason, post test results after implementation. Patches that fail testing will also be recorded and documented.
- c) The updating of the operational software, applications and program libraries will only be performed by trained and qualified administrators upon appropriate management authorization.

3.12. Log Management and Monitoring

- a) The system shall generate and process auditing tracks covering all actions taken on personal data, including data access only.
- b) Authentication validation activities and all changes in authorization shall be logged and securely stored, with limited access.
- c) Access to content, key information and or any modifications to operational program libraries shall be logged and restricted.
- d) Logs and events will be generated in a format that can be easily parsed and used as an input for logging process management.
- e) Integrity log checking shall be performed to ensure consistency.
- f) The system, application, as well as underlying services and or networks, shall be monitored and activities logged.

3.13. Security Incident Management

A security breach, shall be viewed as:

- a failure in security controls which leads to the accidental, unlawful or unauthorized access, destruction, loss or alteration of data / information that processed / stored on system
- a failure in security controls which leads to the accidental, unlawful or unauthorized access to ICT resources, such as - but not limited to - computing resources (processing and or storage/ services) and communication resources (infrastructure).

- a) Security breaches, shall immediately be communicated to UNICEF's Point of Contact.
- b) A security incident notification and escalation procedure shall be formally documented and contractually enforced between the service provider, and UNICEF's Security Operations Centre.

Appendix 3 - Data Processing Agreement and PCI SCC Provisions

PART I: GENERAL

- A. The provision of the Services to UNICEF by the Contractor under the contract identified above (the “Contract”), require the processing of Personal Data belonging to Data Subjects that interact with UNICEF. This Annex is a data processing agreement (“DPA”) that complies with the requirements of the UNICEF Policy on Personal Data Protection (the “UNICEF Data Protection Policy”), which is available at <https://www.unicef.org/supply/documents/unicef-policy-personal-data-protection> (or such other URL as UNICEF may from time to time decide).
- B. The data processing terms pursuant to which the Contractor will process Personal Data under the Contract are set out below in this Annex and will apply to, and be incorporated into, the Contract. In addition, if the Services include the processing of Card Data (as defined below), the additional terms relating to PCI-DSS and other information security standards will also apply to, and be incorporated into, the Contract.
- C. The terms of this DPA are in addition to, and not in replacement of, the terms of the Contract. This DPA and the Contract will be construed and interpreted as complementary of one another.
- D. The terms set out in this Annex will survive provision of the Services and the expiry or earlier termination of the Contract.

PART II: DPA TERMS

1. Definitions

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this Annex attached hereto, will have the following meaning:

- (a) “Applicable Data Protection Law” means any data protection legislation regulating the Contractor;
- (b) “Data Subject” means the individuals whose Personal Data is subject to Processing under the Contract, regardless of who provided the Personal Data or how it was found. The term data subject includes, but it is not limited to past, potential or current beneficiaries, individual donors, supporters, suppliers, individuals in other UNICEF associate organizations and personnel, unless otherwise identified in the Annex hereto;
- (c) “Personal Data” means any personal information including identifying information such as the name, identification or passport number, biometric data such as fingerprints, mobile telephone number, email address, cash transaction details, of whatever nature, format or media that by whatever means, is provided to the Contractor by UNICEF, is accessed or collected by the Contractor on the authority of the UNICEF or is otherwise received by the Contractor on UNICEF's behalf and includes transactional or other information associated with the Data Subject generated by the Contractor in the course of providing the Services to UNICEF;
- 1.2 The Capitalized terms “Data Controller”, “Data Processor”, “Personal Data Transfer”, “Personal Data Breach” and “Process or Processing” used in this DPA have the same meaning as defined in the UNICEF Data Protection Policy.

1.3 All other Capitalized terms used, but not defined, in this Annex have the meaning given to them in the Contract.

2. Roles

2.1 UNICEF is the Data Controller and the Contractor is the Data Processor with respect to Personal Data Processed under the Contract.

3. Processing of UNICEF Personal Data

3.1 Status. The Contractor acknowledges and understands that all Personal Data Processed by the Contractor in the provision of the Services is subject to the privileges and immunities accorded to the United Nations, including UNICEF, pursuant to the General Convention and as such (a) will be deemed part of UNICEF's archives which are inviolable wherever located and by whomsoever held and (b) will, in accordance with the General Convention, be immune from search, requisition, confiscation, expropriation and any form of interference, whether by executive, administrative, judicial or legislative action, unless such immunity is expressly waived in writing by UNICEF.

3.2 Applicable Law and Purpose. The Contractor will:

- (a) Process Personal Data in accordance with any Applicable Data Protection Law and where the standards imposed by the Applicable Data Protection Law are higher than those prescribed under the Contract or pursuant to the UNICEF Data Protection Policy, then in accordance with such Applicable Data Protection Law; and
- (b) Process the Personal Data strictly for the purposes necessary to provide the Services in the manner specified in the Contract; and for no other purpose or in any other manner except with the express prior written consent or instructions of UNICEF.

3.3 Contractor Personnel. The Contractor will ensure that, prior to being granted access to the Personal Data, all Contractor Personnel who will perform Services under the Contract: (a) have successfully completed training of a nature sufficient to enable them to effectively comply with all data protection provisions applicable to the provision of the Services, and (b) possess all qualifications necessary to the nature of their duties and the sensitivity of the Personal Data.

3.4 Confidential Information. The Contractor will treat all Personal Data as Confidential Information of UNICEF as this term is defined in the Contract, and the confidentiality and non-disclosure obligations of the Contract will apply to all such Personal Data.

4. Security

4.1 The Contractor will implement appropriate organizational, administrative, physical and technical safeguards and procedures to protect the security of Personal Data, including against or from accidental or unauthorized destruction, loss, alteration, disclosure, access, or unplanned loss of availability. Such measures may include logging access, changes to or deletion of Personal Data as further specified in the Scope of Work.

4.2 In assessing the appropriate level of security, the Contractor will consider the risks that are presented by Processing for purposes of providing the Services under the Contract, in particular from a Personal Data Breach.

4.3 The Contractor will comply with UNICEF 's standard on managing data and any request from UNICEF to amend, transfer or delete Personal Data; provide a copy of all or specified Personal Data held by it in a format and or a media reasonably specified by UNICEF within reasonable timeframes as agreed between the Parties.

5. Sub-contracting

5.1 The Contractor may appoint (or disclose any Personal Data to) a Subcontractor to process Personal Data subject to the following conditions:

- (a) The appointment of the Sub-contractor is necessary to provide the Services under the Contract;
- (b) The appointment of the Sub-contractor does not violate the Contractor's obligations under the Contract, including the provisions relating to the engagement of Sub-contractors by the Contractor, and
- (c) UNICEF has provided its prior express written consent with respect to the engagement of the named Sub-contractor.

5.2 The Contractor will promptly notify UNICEF of any breach of a Sub-Contractor's obligation vis-à-vis the Contractor in connection with the provision of the Services and will use all commercially reasonable efforts to enforce the relevant obligations of the Sub-Contractor. At UNICEF's request, the Contractor will provide reasonable assistance to UNICEF to support enforcement by UNICEF, as third-party beneficiary, of any of the obligations of the Sub-Contractor in connection with the provision of the Services.

6. Data Subject Rights; Complaints

6.1 The Contractor will, in the event of the exercise by a Data Subject of any rights in relation to their Personal Data, inform UNICEF as soon as possible and provide all commercially reasonable assistance to UNICEF to address all Data Subject information requests or complaints which may be received from any Data Subject in relation to any Personal Data.

6.2 The Contractor will not use the Personal Data of Data Subjects to contact, communicate or otherwise engage with the Data Subjects, including transmission of any marketing or other commercial communications to the Data Subjects, except as strictly necessary to provide the Services, unless it has obtained the express prior written consent of UNICEF.

7. Personal Data Breach; Lost, destroyed, damaged, corrupted or unstable Personal Data

7.1 The Contractor will notify UNICEF immediately upon the Contractor becoming aware of a Personal Data Breach affecting Personal Data, providing UNICEF with sufficient information to allow UNICEF to meet any obligations to report or inform Data Subjects of the Personal Data Breach.

7.2 The Contractor will cooperate with UNICEF and take reasonable steps as are directed by UNICEF to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

7.3 The Contractor will promptly inform UNICEF if any Personal Data is lost or destroyed or becomes damaged, corrupted or unstable and, at the request of UNICEF, restore such Personal Data at its own expense.

8. Deletion or return of Personal Data; Survival

8.1 After expiration or termination of the Contract, the Contractor will return or (at the Contractor's election and upon prior written notice to UNICEF) destroy all Personal Data, except and for so long as required by applicable law.

8.2 In the event that the Contractor elects to destroy Personal Data, such destruction will be effected promptly after written notice of such election is given to UNICEF and will be evidenced by a written attestation issued to UNICEF and signed by an authorized representative of the Contractor.

8.3 The Contractor will give written notice to UNICEF of any Personal Data it is required to retain under applicable law. The Contractor will promptly return or destroy such retained Personal Data as soon as permitted under applicable law, and its obligations under the Contract will survive until such retained Personal Data is returned or destroyed in accordance with this paragraph.

9. Compliance

9.1 If the Contractor receives any request, complaint, notice or communication, that relates directly or indirectly (a) to the Processing of the Personal Data under the Contract or (b) to either Party's compliance with applicable data protection standards, the Contractor will immediately notify UNICEF and provide UNICEF with full co-operation and assistance in addressing any such complaints, notices or communications.

9.2 In accordance with the Contract, at UNICEF's request, the Contractor will provide UNICEF or its authorized representatives access and information necessary for UNICEF to audit or otherwise ascertain compliance with the Contract.

10. Data Transfer

10.1 UNICEF will have the exclusive right to determine the geographical boundaries and location of the facilities where the Personal Data may be transferred to, stored and processed. The Contractor will not transfer or otherwise process Personal Data or change the location of the facilities at which the Personal Data is stored without UNICEF's prior written approval. In particular, the Contractor will not process or transfer the Personal Data outside the country of its registered office, except with the express prior written consent of UNICEF pursuant to a request in writing from the Contractor to UNICEF.

PART III: CARD DATA PROCESSING TERMS

1. Definitions

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this letter and the Annex attached hereto, will have the following meaning:

(a) "Card": a credit, debit, charge, purchase or other card payment method issued by an organisation that issues cards under a Card Scheme and "Cardholder" means the holder of any such Card.

(b) "Card Scheme": Card payment methods, including Visa Europe, Visa Inc, Mastercard Worldwide, UK Maestro, International Maestro, or as may be approved and notified by UNICEF in writing from time to time.

(c) "PCI DSS": those standards issued by the PCI Security Standards Council (or its replacement body or successor), including, but not limited to, the Payment Card Industry Data Security Standard, Payment Application Data Security Standard, the PIN Transaction Security Standard, and the Tokenization Product Security Guidelines as updated from time to time.

(d) "Transaction": any transaction between UNICEF and a Cardholder for the making of a payment to UNICEF.

(e) "Transaction Data": Personal Data relating to a specific Transaction that is required to be processed in connection with the provision of the Services and any other data relating to a specific Transaction.

2. PCI-DSS

2.1 The Contractor will comply with all PCI DSS applicable to the provision of the Services during the term of the Contract. And the Contractor will only use service providers or Sub-contractors that are PCI DSS compliant.

2.2 The Contractor confirms that it has, and will maintain throughout the term of the Contract, all relevant certifications as stipulated in the Scope of Work of the Contract or otherwise required to demonstrate compliance with the PCI DSS and, at UNICEF's request, will promptly provide a copy of such certifications to UNICEF. In the event the Contractor is no longer PCI DSS compliant, the Contractor will immediately notify UNICEF.

2.3 The Contractor will notify UNICEF immediately if it becomes aware of, or suspects, any security breach relating to Transaction Data and will also (and without prejudice to any other remedy available to UNICEF) immediately investigate and take action, at the Contractor's cost, to remedy such breach in accordance with the Contract.

2.4 UNICEF may terminate the Contract with immediate effect by written notice to the Contractor if, at any time, the Contractor ceases to be in compliance with its PCI DSS obligations.

2.5 The Contractor will indemnify UNICEF on demand and defend and hold UNICEF harmless against any losses UNICEF suffers or incurs resulting from a third party claim directly caused by the Contractor's failure to comply with the PCI DSS.