Request for Proposals

Title: Compliance Onboarding Software Solution
RFP No: CI-SS-FY2022
Date of Issuance: November 5, 2021

---

1. **Background**
   Conservation International Foundation (CI) has been fighting to protect nature for people for over 30 years. Conservation International works to spotlight and secure the critical benefits that nature provides to humanity. Since our inception, we've helped to protect more than 6 million square kilometers (2.3 million square miles) of land and sea across more than 70 countries. Currently with offices in 29 countries and 2,000 partners worldwide, our reach is truly global.

   Building upon a strong foundation of science, partnership and field demonstration, CI empowers societies to responsibly and sustainably care for nature, our global biodiversity, for the well-being of humanity. We imagine a healthy, prosperous world in which societies are forever committed to caring for and valuing nature, for the long-term benefit of people and all life on Earth.

   As a US-based 501c(3), CI must comply with US Patriot Act and Executive Order 13224 and demonstrate that all funds are used for charitable purposes and that funds are not used to support sanctioned entities or individuals. In addition, a multitude of CI's donors require representations and warranties related to international sanction compliance (based on additional sanction lists). In order to meet those requirements, a security screening of all grantees must be performed. CI represents to the US Government, multinational and other funders and grantors and our donors that CI follows a rigorous screening process for all funds recipients.

   CI engages contractors, vendors and grant recipients in jurisdictions within and outside of the U.S., across the globe and must comply with a multitude of data protection and data retention requirements.

2. **Project Overview**
   Conservation International is required to conduct due diligence for all CI funding recipients which includes screening those recipients against Anti-Money Laundering ("AML"), Counter-Terrorist Financing ("CTF") legislation, and international or donor-specific sanctions lists. CI is seeking a vendor who can help us meet AML/CTF/Know Your Customer ("KYC") international obligations that meets applicable data protection requirements for a minimum period of two (2) years, with the option for annual renewal.

3. **Timeline for engagement**
   As stated, CI plans to engage selected service provider on a 2-year contract, starting February 1, 2022, with the option for annual renewal.

4. **Submission Details**
   a. Deadline. Proposals must be received no later than November 28, 2021 at 11:59 PM ETD (UTC – 03:59). Late submissions will not be accepted. Proposals must be submitted via email to ciprocurement@conservation.org. All proposals are to be submitted following the guidelines listed in this RFP.

   b. Validity of bid. 120 days from the submission deadline

c. Clarifications. Questions may be submitted to ciprocurement@conservation.org by the specified date and time in the timeline below. The subject of the email must contain the RFP number and title of the RFP. CI will respond in writing to submitted clarifications by the date specified in the timeline below. Responses to questions that may be of common interest to all bidders will be posted to the CI website and/or communicated via email.

d. Amendments. At any time prior to the deadline for submission of proposals, CI may, for any reason, modify the RFP documents by amendment which will be posted to the CI website and/or communicated via email.

5. Minimum Requirements

Mandatory Specifications. The following requirements (a-i) are mandatory specifications:

a. System must provide compliance monitoring access to the following lists:
   - The Australian Department of Foreign Affairs and Trade list
   - The Bureau of Industry and Security (BIS) list
   - The Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 (CISADA) list
   - The Department of State: Defense Trade Controls list (DTC)
   - The Department of State: International Security & Nonproliferation list (ISN)
   - The HM Treasury Department Sanctions list (Formerly known as Bank of England)
   - The SAM Exclusions (EPLS) list
   - The European Union (EU) list
   - The Financial Action Task Force (FATF) Non-Cooperative Countries and Territories list
   - The Federal Bureau of Investigation (FBI) list
   - The Interpol's Most Wanted list
   - The Japan Ministry of Economy, Trade and Industry (METI) End User list
   - The Office of Foreign Assets Control (OFAC) list
   - Politically Exposed Persons – Foreign Officials list
   - Department of State Terrorist Exclusion (TEL) list
   - United Nations (UN) Security Council Sanctions
   - World Bank Listing of Ineligible Firms and Individuals (WBNK) list
   - World Bank Listing of Temporary Suspensions
   - French Sanction Lists
   - Additional screening lists as needed

b. System must be updated on a regular basis

c. System must be able to screen in large batches (a number of listed names/entities) as well as single names/entities

d. System must retain a General Data Protection Regulation (GDPR) and privacy compliant audit trail of each transaction (individual and batch) for a minimum of 7 years

e. System must use 'fuzzy logic' on entity matches and enable CI to change the match rate (e.g. threshold of match 85%-100%)

f. System can assign CI users with different profiles or roles and enable CI to use different screening configurations (e.g., Human Resources settings/configuration, Finance Division settings/configuration)

g. CI is able to assign Vendor with screening responsibilities in lieu of direct screening as an optional process

h. User training and manuals are available

i. Regular user support is provided

Preferred Specifications. The following requirements (j-n) are preferred additional specifications:

j. System integrates with third party databases and enables easy adding and removing of lists
k. Vendor provides usage reports on transactions, including global reports on number of transactions and number of batches by time period
l. System supports and recognizes different languages and characters (e.g., Arabic, Chinese, Russian)
m. Import of individual names/entities into the screening database is automated and simple (i.e., limited steps to upload entity names)
n. Vendor provides sanction training and "how to confirm/clear" training for screening professionals

6. Proposal Documents to Include

a. Signed cover page on bidder's letterhead with the bidder's contact information.
b. Signed Representation of Transparency, Integrity, Environmental and Social Responsibility (Attachment 1)
c. Technical Proposal.
    i. Corporate Capabilities, Experience, Past Performance, and 3 client references. Please include descriptions of similar projects or assignments and at least three client references.
    ii. Technical Approach. The Technical Proposal should describe in detail
        a) how the bidder meets the Minimum Requirements,
        b) to what extent bidder meets preferred specifications, and
        c) a process for transition and training.

d. Financial Proposal. Offerors should submit a pricing model, by transaction. A transaction is defined as the number of individual names or entities that are screened.

   The cost proposal must be all-inclusive of profit, fees or taxes. Additional costs cannot be included after award, and revisions to proposed costs may not be made after submission unless expressly requested by CI should the offerors proposal be accepted. Nevertheless, for the purpose of the proposal, Offerors must provide a detailed budget showing major expense line items. Offers must show unit prices, quantities, and total price. All items, services, etc. must be clearly labeled and included in the total offered price. All cost information must be expressed in USD.

   If selected, Offeror shall use its best efforts to minimize the financing of any taxes on goods and services, or the importation, manufacture, procurement or supply thereof. If Offeror is eligible to apply for refunds on taxes paid, Offeror shall do so. Any tax savings should be reflected in the total cost.

7. Evaluation Criteria In evaluating proposals, CI will seek the best value for money considering the merits of the technical and costs proposals. Proposals will be evaluated using the following criteria:

Stage 1: Minimum Requirements
Eligible vendors who meet all Mandatory Specifications (a-i in the minimum requirements, Section 5) will be selected to provide a live demonstration of the system in December 2021.

Stage 2: Demonstration
The finalists who meet the initial criteria, will conduct live demonstrations of the screening system. The demonstration will be 45 minutes and must show:

- User log in
- Process for entering and screening data/names/entities

- Process for match clearing
- Audit trail
- Different settings/configurations

Stage 3: Full Proposal Evaluation
The award will be made to the offeror whose proposal is determined to be responsive to this solicitation document, meets the minimum requirements stated in this RFP, meets the technical capability requirements, and is determined to represent the most advantageous to CI. Scoring will be based on the following criteria:

Evaluation Criteria	**Score (out of 100)**
Does the proposed system meet the Preferred additional Specifications? (max of 4 points each)	20 Max points
Is the proposed system user friendly with limited manual/human intervention from CI?	10 Max points
Does the bidder's past performance demonstrate recent proven experience doing similar work for similar clients?	20 Max points
Does the bidder and the proposed personnel have the specific technical expertise for the assignment?	20 Max points
Client references	10 Max points
Cost: Costs proposed are reasonable and realistic and demonstrate fair cost to CI.	20 Max points

8. Proposal Timeline

RFP Issued	05 November 2021
Clarifications submitted to CI	12 November 2021
Clarifications provided to known bidders	17 November 2021
Complete proposals due to CI	28 November 2021
Demonstration	06 - 10 December 2021
Final selection	December 31, 2021

9. **Resulting Award** CI anticipates entering into an agreement with the selected bidder with services to start by 1 February 2022. Any resulting agreement will be subject to the terms and conditions of CI's Services Agreement. A model form of agreement can be provided upon request.

   This RFP does not obligate CI to execute a contract, nor does it commit CI to pay any costs incurred in the preparation or submission of the proposals. Furthermore, CI reserves the right to reject any and all offers, if such action is considered to be in the best interest of CI. CI will, in its sole discretion, select the winning proposal and is not obligated to share individual evaluation results.

10. **Confidentiality** All proprietary information provided by the bidder shall be treated as confidential and will not be shared with potential or actual applicants during the solicitation process. This includes but is not limited to price quotations, cost proposals and technical proposals. CI may, but

is not obliged to, post procurement awards on its public website after the solicitation process has concluded, and the contract has been awarded. CI's evaluation results are confidential and applicant scoring will not be shared among bidders.

11. **Code of Ethics** All Offerors are expected to exercise the highest standards of conduct in preparing, submitting and if selected, eventually carrying out the specified work in accordance with CI's Code of Ethics. Conservation International's reputation derives from our commitment to our values: Integrity, Respect, Courage, Optimism, Passion and Teamwork. CI's Code of Ethics (the "Code") provides guidance to CI employees, service providers, experts, interns, and volunteers in living CI's core values, and outlines minimum standards for ethical conduct which all parties must adhere to. Any violation of the Code of Ethics, as well as concerns regarding the integrity of the procurement process and documents should be reported to CI via its Ethics Hotline at www.ci.ethicspoint.com.

    Vendors will be expected to agree to CI's Global Data Security and Processing Addendum to the extent that the vendor is processing protected information (personal information or CI confidential information); See Attachment 2.

12. **Attachments**:

    Attachment 1: Representation of Transparency, Integrity, Environmental and Social Responsibility
    Attachment 2: Global Data Processing and Data Security Addendum

Attachment 1: Representation of Transparency, Integrity, Environmental and Social Responsibility

RFP No. CI-SS-FY2022

All Offerors are expected to exercise the highest standards of conduct in preparing, submitting and if selected, eventually carrying out the specified work in accordance with CI's Code of Ethics. CI's Code of Ethics provides guidance to CI employees, service providers, experts, interns, and volunteers in living CI's core values, and outlines minimum standards for ethical conduct which all parties must adhere to. Any violations of the Code of Ethics should be reported to CI via its Ethics Hotline at www.ci.ethicspoint.com.

CI relies on the personal integrity, good judgment and common sense of all third parties acting on behalf, or providing services to the organization, to deal with issues not expressly addressed by the Code or as noted below.

I. With respect to CI's Code of Ethics, we certify:

- **a.** We understand and accept that CI, its contractual partners, grantees and other parties with whom we work are expected to commit to the highest standards of Transparency, Fairness, and Integrity in procurement.

II. With respect to social and environmental standards, we certify:

- **a.** We are committed to high standards of ethics and integrity and compliance with all applicable laws across our operations, including prohibition of actions that facilitate trafficking in persons, child labor, forced labor, sexual abuse, exploitation or harassment. We respect internationally proclaimed human rights and take no action that contributes to the infringement of human rights. We protect those who are most vulnerable to infringements of their rights and the ecosystems that sustain them.

- **b.** We fully respect and enforce the environmental and social standards recognized by the international community, including the fundamental conventions of International Labour Organization (ILO) and international conventions for the protection of the environment, in line with the laws and regulations applicable to the country where the contract is to be performed.

III. With respect to our eligibility and professional conduct, we certify:

- **a.** We are not and none of our affiliates [members, employees, contractors, subcontractors, and consultants] are in a state of bankruptcy, liquidation, legal settlement, termination of activity, or guilty of grave professional misconduct as determined by a regulatory body responsible for licensing and/or regulating the offeror's business
- **b.** We have not and will not engage in criminal or fraudulent acts. By a final judgment, we were not convicted in the last five years for offenses such as fraud or corruption, money laundering or professional misconduct.
- **c.** We are/were not involved in writing or recommending the terms of reference for this solicitation document.
- **d.** We have not engaged in any collusion or price fixing with other offerors.
- **e.** We have not made promises, offers, or grants, directly or indirectly to any CI employees involved in this procurement, or to any government official in relation to the contract to be performed, with the intention of unduly influencing a decision or receiving an improper advantage.

f. We have taken no action nor will we take any action to limit or restrict access of other companies, organizations or individuals to participate in the competitive bidding process launched by CI.

g. We have fulfilled our obligations relating to the payment of social security contributions or taxes in accordance with the legal provisions of the country where the contract is to be performed.

h. We have not provided, and will take all reasonable steps to ensure that we do not and will not knowingly provide, material support or resources to any individual or entity that commits, attempts to commit, advocates, facilitates, or participates in terrorist acts, or has committed, attempted to commit, facilitate, or participated in terrorist acts, and we are compliant with all applicable Counter-Terrorist Financing and Anti-Money Laundering laws (including USA Patriot Act and U.S. Executive Order 13224).

i. We certify that neither we nor our directors, officers, key employees or beneficial owners are included in any list of financial or economic sanctions, debarment or suspension adopted by the United States, United Nations, the European Union, the World Bank, or General Services Administration's List of Parties Excluded from Federal Procurement or Non-procurement programs in accordance with E.O.s 12549 and 12689, "Debarment and Suspension".

Name: _____

Signature: _____

Title: _____

Date: _____

Attachment 2: Global Data Processing and Data Security Addendum

This Data Processing Addendum (the "**Addendum**") is made as of _____, 20___ (the "**Effective Date**"), by and between Conservation International Foundation ("CI"), having a principal place of business at 2011 Crystal Drive, Arlington, VA 22202, and _____, whose principal place of business is located at _____ ("**Supplier**"). This Addendum is attached to and forms a part of the agreements set forth on Schedule 1 attached hereto, and any other agreement, statement of work, or service order under which Supplier Processes Personal Data for or on behalf of CI (each, an "Underlying Agreement"). This Addendum supersedes each Underlying Agreement by adding to and modifying such Underlying Agreement as set forth herein. To the extent any such addition or modification results in any conflict or inconsistency between an Underlying Agreement and this Addendum, this Addendum shall govern and the terms of the Underlying Agreement that conflict with this Addendum or are inconsistent with this Addendum shall be of no force or effect. Other than as set forth in this Addendum, all other terms and provisions of each Underlying Agreement shall remain in full force and effect in accordance with their terms and nothing contained herein shall be deemed to be a waiver, amendment, modification or other change of any term, condition or provision of the Underlying Agreement (or a consent to any such waiver, amendment, modification or other change).

For good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties, intending to be legally bound, agree as follows:

1. DEFINITIONS. "Data Law" means any applicable data privacy or security law worldwide, including laws in the United States, Canada, the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom (including, without limitation, the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR")); "Personal Data" means any information relating to an identified or identifiable natural person that is governed by Data Laws; "Data Subject," "Controller," and "Processor" shall have the meaning as defined under GDPR; "Processing" shall mean access to, and use, storage, disclosure, handling, consultation, retrieval, deletion, modification, or other processing of Protected Information; "Protected Information" is CI Personal Data and Proprietary Information; "Proprietary Information" means CI's confidential information, whether disclosed verbally or in writing or on any kind of media, including project and operational information in relation to collaborating organizations and grantees, donor information, business plans and methods, marketing information, research data, financial information and budgets, licensing, grant and other legal agreements, and other information designated by CI as confidential; "Security Breach" means any unauthorized access, acquisition, use, alteration disclosure, loss or destruction of, or damage to, Protected Information, and/or any compromise of or unauthorized access to a Supplier system, network, or infrastructure that may result in harm or damage to Protected Information or a CI system, network, or infrastructure, and/or any breach of applicable privacy or data protection law or of this Agreement with respect to the Processing of Protected Information by Supplier; "Supervisory Authority" means a public agency or authority of any country, state, territory, or political subdivision of a country, state or territory, or a person or entity acting under a grant of authority from or under contract with such public agency or authority, that is authorized by law to enforce individual rights with respect to Personal Data, or to oversee, enforce, or monitor compliance with any Data Law.[1]

2. COMPLIANCE. The parties agree that, with respect to the Processing of Personal Data as detailed in Schedule 1 hereto, CI is the Controller under GDPR, and Supplier is the Processor under GDPR. Supplier will ensure that all access, use, disclosure, and other Processing of Personal Data by Supplier is in accordance with this Addendum and any Underlying Agreement and complies with all applicable Data Laws. Supplier shall notify CI if it determines that any instruction by CI with respect to Supplier's Processing of Personal Data does not comply with applicable Data Laws. Without prejudice to CI's rights and remedies, if Supplier is unable (or reasonably believes it will become unable) to comply with this Addendum or any Underlying Agreement, Supplier will promptly notify CI of such circumstances. [2]

3. **LIMITATIONS ON PROCESSING AND DISCLOSURE.**

3.1 Permissible Processing.

(a) Supplier may not Process Personal Data for any purpose other than as set forth in Schedule 1 or in any manner that would be a violation of any Data Law. The initial nature and purpose of the Processing, duration of the Processing, categories of Data Subjects, and types of Personal Data are set forth on Schedule 1.

(b) Supplier may not disclose Personal Data to any third party unless: (1) the disclosure is expressly permitted pursuant to the terms of this Addendum, or (2) CI authorizes in writing the transfer of such Personal Data to such third party.

(c) Supplier shall not transfer Personal Data outside the country specified on Schedule 1 without CI's prior approval.

3.2 Onward Transfers. Schedule 1 hereto sets forth each subcontractor of Supplier (including any affiliate) that Processes Personal Data that was received or created by Supplier pursuant to an Underlying Agreement with CI. Supplier shall notify CI of any changes to the listed subcontractors during the term of the Underlying Agreement(s), and CI shall approve any such changes before any such subcontractor is permitted to process any such Personal Data. Supplier may only subcontract or outsource the processing of Personal Data if Supplier has imposed on the subcontractor legally binding contractual terms that require the subcontractor to provide at least the same level of protection for the Personal Data as set forth in this Addendum. Supplier will perform reasonable ongoing reviews of all such subcontractors on not less than an annual basis to ensure such subcontractors maintain capabilities adequate to perform all such requirements and obligations and have not failed to comply with all such requirements and obligations. Upon request by CI, Supplier will provide CI or any of its subcontractors with the results of any such review and confirm compliance with this Section. Any Processing or other act or omission by any person that obtains access to or possession of Personal Data through Supplier that would be a breach of this Addendum if committed by Supplier is deemed a breach of this Addendum by Supplier for which Supplier shall be responsible. Supplier agrees, upon CI's request, to provide CI with details of any subcontractors who process Personal Data, including the subcontracting activities they fulfill, their locations, and a copy of the data protection and privacy terms within Supplier's written agreement with such subcontractors.

3.3 **Cooperation**. Supplier agrees to cooperate with and assist CI in responding without undue delay to any requests, complaints, or inquiries from a Data Subject, including from Data Subjects exercising their rights of access, correction, data portability, and/or deletion under GDPR. In the event that a Data Subject contacts Supplier directly, Supplier agrees to direct the Data Subject to contact CI and to notify CI promptly (and in any event within five days of receipt) that a request, complaint, or inquiry from a Data Subject has been made.

3.4 Legal Obligation. If Supplier is required by law or receives any order, demand, warrant or any other document requesting or purporting to compel the production of Personal Data (such as oral questions, interrogatories, requests for information or documents in legal proceedings, subpoenas, civil investigative demands or other similar processes), Supplier shall, except to the extent prohibited by law, immediately notify CI and shall not produce the Protected Information for at least forty-eight (48) hours following such notice to CI so that CI may, at its own expense, exercise such rights as it may have under law to prevent or limit such disclosure. In addition to the foregoing, Supplier shall exercise commercially reasonable efforts to prevent and limit any such disclosure, to otherwise preserve the confidentiality of the Personal Data and shall cooperate with CI with respect to any action taken with respect to such request, complaint, order or other document, including to obtain an appropriate protective order or other reliable assurance that confidential treatment will be accorded to the Personal Data.

3.5 Records. Supplier shall maintain records sufficient to demonstrate its compliance with its obligations under this Addendum, and retain such records for a period of three (3) years after the termination of the Underlying Agreement. CI shall, with reasonable notice to Supplier, have the right to review, audit and copy such records at Supplier's offices during regular business hours.

4. DATA SECURITY. Supplier represents and warrants that it (i) has implemented and maintains appropriate and reasonable physical, technical, and organizational measures to protect Protected Information against: (1) accidental or unlawful destruction, (2) accidental loss, (3) alteration, and (4) unauthorized disclosure or access, (ii) its technical and organizational measures are such that its processing of Protected Information complies with all Data Laws, and (iii) has an information security program in place to safeguard Protected Information and such information security program is commensurate with and complies with applicable industry standards and any applicable Data Law. Supplier shall meet or exceed the information security standards set forth in Schedule 2 hereto with respect to all Protected Information processed in performing under the Underlying Agreement.

In cases where CI allows Supplier to connect its network or systems to CI's network, Supplier shall only use such access for the purpose of performing its obligations under the Underlying Agreement and for no other purpose. Supplier shall follow all instructions and policies of CI with respect to such access and use that are provided to Supplier in writing. Supplier shall ensure that no employee or individual who is permitted access to CI's network or computing resources through Supplier (i) shares his or her password or account access with any other party, (ii) introduces unauthorized files onto CI's system, or (iii) attempts to access CI information or applications other than those expressly authorized by CI. CI shall be permitted to disconnect or terminate Supplier's access immediately, without notice, upon CI learning of any violation of this Addendum or other misuse of the system by Supplier or its employees or representatives. Supplier shall immediately notify CI if an employee or representative of Supplier with access to CI networking or computing resources no longer requires such access, including as a result of a change of assignment or employment status.

5. Audit. Upon CI's request, Supplier shall provide CI with a copy of Supplier's most recent audit report regarding Supplier's data security program. Supplier will respond within a reasonable time period to any inquiries from CI relating to Supplier's data security program. Supplier will, upon CI's request, provide CI or CI's representatives access to Supplier's systems and records that involve or are related to any processing of Protected Information so that an audit may be conducted. CI will not exercise such audit right more frequently than once per twelve (12) month period and CI will bear the full cost and expense of any such audit, unless such audit discloses a security incident or a breach of this Agreement, in which case Supplier will bear the full cost and expense of such audit and a further audit may be conducted by CI or CI's representatives within the then-current twelve (12) month period.

6. INCIDENT RESPONSE. Supplier shall notify CI immediately upon (and in no event more than 24 hours after) learning of any actual or suspected Security Breach. Such notice shall include detailed information regarding the nature and scope of the Security Breach, any reports to law enforcement related to the Security Breach, the actual or suspected cause of the Security Breach, the measures being taken by Supplier to investigate the Security Breach, correct or mitigate the Security Breach, and prevent future Security Breaches. Supplier shall provide reasonable assistance to, and shall cooperate with all reasonable requests of, CI to investigate and mitigate any Security Breach. Supplier agrees that any decision to notify data subjects or any Supervisory Authority of the Security Breach shall be in CI's sole discretion and any notice shall be approved in advance by CI. Supplier shall reimburse CI for all costs and expenses incurred by CI related to providing any notice to individuals or third parties, including any Supervisory Authority, of a Security Breach and offering an identity monitoring service if supplied to impacted data subjects. Without limiting any other rights of CI under this Agreement, CI may at its discretion immediately terminate the Underlying Agreement and this Addendum as a result of a Security Breach.

7. IMPACT ASSESSMENTS. Supplier will assist CI in ensuring compliance with any obligations of CI with respect to data protection impact assessments and prior consultation, including CI's obligations pursuant to Article 35 and 36 of GDPR.

8. CROSS-Border Transfers. If Supplier processes Personal Data regarding residents of the European Economic Area ("EEA") in providing services to CI under the Underlying Agreement, Supplier and CI agree that any cross-border transfer will be governed by the European Commission Standard Contractual Clauses (Controller to Processor) ("Standard Clauses") as annexed to EU Commission Decision 2010/87/EU or subsequently adopted SCC by EU Commission Decision with CI or comply with another cross-border data transfer mechanism deemed compliant by the European Commission, to allow Personal Data to be transferred to Supplier and any affiliate or subcontractor of Supplier by CI. In the event of a conflict between the Standard Clauses and this Addendum or the Underlying Agreement, the Standard Clauses shall prevail as to Personal Data subject to protection under the GDPR.

9. MISCELLANEOUS.

9.1 Liability and Indemnification. Supplier shall defend, indemnify, and hold harmless CI, and CI's subsidiaries, affiliates, and their respective officers, directors, employees, agents, successors, and assigns (each, a "**CI Indemnitee**") from and against all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs or expenses of whatever kind, including reasonable attorneys' fees, arising out of or resulting from any claim against any CI Indemnitee arising out of or resulting from Supplier's failure to comply with its obligations (ii) under this Addendum, including without limitation any failure to comply with its obligations under the Standard Clauses if entered into by the Parties, or (ii) under any applicable Data Law. No limitation of liability provision in any Underlying Agreement shall apply to this Addendum.

9.2 Insurance. Through the term of this Addendum and for at least three (3) years thereafter for any insurance written on a claims-made basis, Supplier shall obtain and maintain privacy and cyber security insurance coverage providing standard comprehensive first-party and third-party (liability) coverages, with third-party coverage limits of not less than $1,000,000 for each claim and $3,000,000 in the aggregate. Supplier shall provide CI with a certificate of insurance evidencing the required insurance naming CI as an additional insured with respect to any claims that arise from Suppliers acts or omissions in connection with the processing of personal data for or on behalf of CI.

9.3 Term and Termination. The term of this Addendum shall run concurrently with the term of the Underlying Agreement, unless this Addendum is sooner terminated in accordance with this Section 9.3. In the event that Supplier breaches any of its obligations under this Addendum, CI may terminate this Addendum if such breach is not cured by Supplier within thirty (30) days after receipt of written notice of such breach from CI, provided that CI may terminate this Addendum immediately upon written notice to Supplier if CI determines in its discretion that the breach is not capable of cure. Upon the expiration or termination of this Addendum, Supplier shall return, or, at CI's request, delete (with written certification of deletion), all Protected Information in Supplier's control or possession and all Protected Information in the possession of Supplier's affiliates and subcontractors.

9.4 Governing Law and Venue. This Addendum shall be governed by the laws of the District of Columbia, without regard to the principles of conflicts of laws. The Parties agree that any claims relating directly or indirectly to this Addendum shall be brought before court of competent jurisdiction in the District of Columbia. The Parties hereby consent to and waive any objection to personal jurisdiction in those courts.

9.5 Survival. Paragraphs 1, 3.5, 6, and 9 shall survive the termination of this Addendum.

9.6 **MISCELLANEOUS**. This Addendum may not be amended or modified, in whole or part, except by a writing signed by duly authorized representative of both parties. No provision or part of this Addendum or remedy hereunder may be waived except by a writing signed by a duly authorized representative of the Party making the waiver. Failure or delay by either party to enforce any provision of this Addendum will not be deemed a waiver of future enforcement of that or any other provision. Nothing in this Addendum shall be construed to place the parties in an agency, employment, franchise, joint venture, or partnership relationship. Neither party will have the authority to obligate or bind the other in any manner, and nothing herein contained shall give rise or is intended to give rise to any rights of any kind to any third parties. In the event that any provision of this Addendum is found to be unenforceable, such provision will be reformed only to the extent necessary to make it enforceable, and such provision as so reformed will continue in effect, to the extent consistent with the intent of the parties as of the Effective Date.

[Signatures on next page]

IN WITNESS WHEREOF, the parties hereto have executed this Addendum effective as of the Effective Date. Each party acknowledges that it has read this Addendum, understands it, and will be bound by its terms.

Conservation International Foundation	[_____]
By:	By:
_____	_____
Print Name:	Print Name:
_____	_____
Title:	Title:
_____	_____
Date:	Date:
_____	_____

Schedule 1
Processing Details

Underlying Agreement(s)
[To be filled in.]
Nature and Purpose of Processing
[To be filled in.]
Duration of Processing and Retention of Data
Supplier will Process Personal Data for the duration of the Underlying Agreement, unless otherwise agreed upon in writing. Supplier will retain Personal Data as long as required under applicable law, unless otherwise agreed to in writing.
Categories of Data Subjects
[To be filled in.]
Type of Personal Data
[To be filled in.]
Country
[To be filled in.]

Schedule 2
Information Security Standards

Supplier will implement security requirements for staff and all subcontractors, vendors, or agents who have access to Protected Information. These are designed to:

- Prevent unauthorized persons from gaining access to Protected Information processing systems (physical access control);
- Prevent Protected Information processing systems being used without authorization (logical access control);
- Ensure that persons entitled to use a Protected Information processing system gain access only to such Protected Information as they are entitled to access in accordance with their access rights and that, in the course of Processing or use and after storage, Protected Information cannot be read, copied, modified or deleted without authorization (data access control);
- Ensure that Protected Information cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage, and that the target entities for any transfer of Protected Information by means of data transmission facilities can be established and verified (data transfer control);
- Ensure the establishment of an audit trail to document whether and by whom Protected Information have been entered into, modified in, or removed from Protected Information Processing (entry control);
- Ensure that Protected Information are Processed solely in accordance with the instructions (control of instructions);
- Ensure that Protected Information are protected against accidental destruction or loss (availability control);
- Ensure that only the minimum amount of Protected Information necessary to accomplish the specified purpose is processed; and
- Ensure that Protected Information collected for different purposes can be processed separately (separation control).

These rules are kept up to date, and revised whenever relevant changes are made to the information system that uses or houses Protected Information, or to how that system is organized.

2. Physical Security

The Supplier will maintain commercially reasonable security systems at all Supplier sites at which an information system that uses or houses Protected Information is located. The Supplier reasonably restricts access to such Protected Information appropriately.

Physical access control has been implemented for all data centers. Unauthorized access is prohibited through 24x7 onsite staff, biometric scanning, and /or security camera monitoring.

Surveillance camera on entry door is installed and security monitoring by building management is implemented.

3. Organizational Security

When media are to be disposed of or reused, procedures have been implemented to prevent any subsequent retrieval of any Protected Information stored on them before they are withdrawn from the inventory.

Supplier implemented security policies and procedures to classify sensitive information assets, clarify security responsibilities and promote awareness for employees.

All Protected Information security incidents are managed in accordance with appropriate incident response procedures.

All sensitive Personal Data processed by Supplier are encrypted while in transit and when on portable devices or media. Sensitive Personal Data include Personal Data that include social security number, drivers' license number, financial account information, username and password or PIN that allow access to an online account, data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning sex life and sexual orientation; data about health or medical treatment; and genetic data or biometric data.

4. Network Security

The Supplier maintains network security using commercially available equipment and industry standard techniques, including firewalls, intrusion detection systems, access control lists and routing protocols.

5. Access Control

Only authorized staff can grant, modify or revoke access to an information system that uses or houses Protected Information.

User administration procedures define user roles and their privileges, how access is granted, changed and terminated; addresses appropriate segregation of duties; and defines the logging/monitoring requirements and mechanisms.

All employees of the Supplier are assigned unique User-IDs.

Access rights are implemented adhering to the "least privilege" approach.

The Supplier implements commercially reasonable physical and electronic security to create and protect passwords.

6. Virus and Malware Controls

The Supplier installs and maintains anti-virus and malware protection software on the system.

7. Personnel

The Supplier implements a security awareness program to train personnel about their security obligations. This program includes training about data classification obligations; physical security controls; security practices and security incident reporting.

Supplier has clearly defined roles and responsibilities for the employees. Screening is implemented before employment with terms and conditions of employment applied appropriately.

Supplier employees follow established security policies and procedures. Discipline will be applied if employees commit a security breach.

8. Business Continuity

The Supplier implements appropriate disaster recovery and business resumption plans. Supplier reviews both business continuity plan and risk assessment regularly. Business continuity plans are being tested and updated regularly to ensure that they are up to date and effective.