SERVICES AGREEMENT
BETWEEN
CONSERVATION INTERNATIONAL FOUNDATION
AND

Service Agreement Number:
Project Title:

This Services Agreement (the 'Agreement') is made and entered into as of xxx (the 'Effective Date') by and between Conservation International Foundation ('CI'), a nonprofit public benefit corporation organized under the laws of the State of California and xxx ('Service Provider'). Building upon a strong foundation of science, partnership and field demonstration, CI uses funds raised by it with the advice and counsel of Service Provider to empower societies to responsibly and sustainably care for nature, our global biodiversity, for the well-being of humanity.

1. Services: Project Description. CI hereby engages Service Provider as an independent contractor, on a non-exclusive basis, to perform the activities and provide the deliverables set forth below (the 'Services'), as may be modified from time to time:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Due date</th>
<th>Deliverable</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

a. During the Period of Performance (as defined in Section 2) of this Agreement, CI shall have the right to request reasonable changes to the scope of the Services. All changes shall be in writing and signed by authorized representatives of the parties. Service Provider shall receive technical direction from xxx or his/her designee, as authorized in writing.

b. To the extent applicable to the Services conducted hereunder, this Agreement is subject to the provisions of statutory law and the implementing regulations applicable to the solicitation of contributions and funds for charitable organizations that are in effect in each of the States of the United States, as amended, from time to time.

c. Service Provider will not at any time solicit funds, assets, or property for charitable purposes, receive or control funds, assets, or property solicited for charitable purposes, or employ, procure, or engage any compensated person to solicit, receive, or control funds, assets or property for charitable purposes. Service Provider will not have custody or control of contributions at any time. CI exercises control and approval over the content, volume and frequency of all solicitations.

2. Period of Performance. The Performance Start Date is xxx. The Performance End Date is xxx unless otherwise modified, or the Agreement is terminated in accordance with Section 5 (also deemed the “term of the Agreement”). Any extension of the Period of Performance or the term of the Agreement requires a written amendment of this Agreement signed by authorized representatives of both Parties.

Last updated 3-2020
3. Compensation.
   a. Fee for Services. In consideration of Service Provider’s performance of the Services during the Period of Performance, CI shall pay Service Provider an amount not to exceed, $xxx for such times as the Service Provider actually performs Services under this Agreement.
   b. Expenses. The Fee for Services set forth above is inclusive of all expenses.
   c. All activities and expenditures must occur during the Period of Performance of this Agreement to be reimbursable.
   d. Payment Terms.
      i. Payment shall be made against invoice(s). Service Provider shall invoice CI on a monthly basis. Service Provider shall provide invoices to CI containing name and address, place of performance, days/period and hours worked according to activities and deliverables (as defined in Section 1), and payment instructions. Invoices for reimbursable expenses shall be accompanied by an itemized account of such expenses, together with original receipts for expenses over $40.00. All amounts will be paid within thirty (30) days after receipt and approval of Service Provider invoice.
      ii. Service Provider shall provide an IRS W-9 form for US entities, or an IRS W-8 form for non-US entities.

4. Acceptance of Deliverables; Time is of the Essence.
   a. Acceptance Criteria. Service Provider is expected to perform the Services and Deliverables in accordance with the following acceptance criteria, which may be revised and supplemented from time to time during the Period of Performance of this Agreement to accommodate for successful performance of the Services.
   b. Acceptance. In the event that a Deliverable meets CI’s acceptance criteria, CI shall notify the Service Provider via email that such Deliverable has been accepted. In the event that a Deliverable does not meet CI’s acceptance criteria, CI shall advise the Service Provider via email as to which aspects of the Deliverable require revision. Service Provider shall implement such revisions in accordance with CI’s instructions and deliver the revised Deliverable to CI for review within 10 business days following receipt by Service Provider of the revision request. CI may request that this process be repeated for as many times as necessary to meet the acceptance criteria. Time spent on necessary revisions to meet acceptance criteria may not be charged to CI, unless authorized in writing by CI.
   c. Time is of the Essence. Service Provider shall perform the Services in strict compliance with the Delivery Schedule set forth in Appendix 1. Time is of the essence with respect to all aspects of this Agreement and the subject matter hereof.

5. Termination. Either party may terminate this Agreement at any time upon ten (10) days prior written notice. In such event, Service Provider shall provide to CI all deliverables (incl. all embodiments thereof) completed or partially completed up to the effective date of termination to CI in a format and medium specified by CI, and CI shall pay a pro-rated fee for all Services provided by the Service Provider in good faith prior to the effective date of termination. Any payment effected by CI in excess of the pro-rated fee due on the effective date of termination shall be returned by the Service Provider immediately upon request by CI. If CI terminates this Agreement due to a material breach by Service Provider or due to the Service Provider’s failure to perform any of the Services to CI’s satisfaction, CI may withhold payment for any such unsatisfactory Services until such Services are performed to CI’s satisfaction.
6. **Indemnification.** Service Provider hereby covenants and agrees to indemnify, defend and hold harmless CI from and against any and all claims, actions, losses, liabilities, damages, costs and expenses (including reasonable attorney’s fees) arising out of or resulting from any claim, action or other proceeding (including any proceeding by any of Service Provider’s employees, agents or contractors (a “Claim”) related to or arising out of Service Provider’s performance of the Services under this Agreement except to the extent a Claim is related to or arises out of (i) content provided by CI for use in connection with the Services; (ii) CI’s breach of the Agreement; or (iii) CI’s negligence or willful misconduct, for which CI will instead indemnify, defend and hold harmless Service Provider.

7. **Relationship of CI and Service Provider.**
   
a. Service Provider is not an employee, agent or assign of CI for any purposes whatsoever. Accordingly, Service Provider shall be solely responsible for all matters relating to the employment of its personnel including, but not limited to, compliance with all applicable workers’ compensation, unemployment compensation and social security laws and with all withholding and all other federal, state and local laws and regulations governing such matters. CI shall not provide Service Provider or its employees with any insurance or other benefits including, but not limited to, unemployment, medical, dental, worker’s compensation and/or disability insurance.

b. Service Provider is performing the Services as an independent contractor of CI and not as an officer, employee, partner or agent of CI. Accordingly, Service Provider has no right or authority to assume or create any obligation of any kind or to make any representation or warranty, whether expressed or implied, on behalf of CI or to bind CI in any respect.

8. **Government Officials and Employees.** Service Provider hereby certifies that no assistance, payments or anything of value (monetary or non-monetary) shall be made, promised, offered to or accepted by any government employee or official (a) in contravention of any U.S. or other applicable law or regulation including, but not limited to, the U.S. Foreign Corrupt Practices Act; (b) without the express consent of the government for which the employee or official works; and (c) that is not reasonable, *bona fide*, and directly related to the activities funded under this Agreement. It is Service Provider’s responsibility to ensure compliance with this clause, and to maintain and provide at CI’s request, documentation demonstrating such compliance. Service Provider hereby certifies that no payments or other form of assistance shall be made to or accepted by any government employee or official (x) to influence any official government act or decision; (y) to induce any government employee or official to do or omit to do any act in violation of his or her lawful duty; or (z) to obtain or retain business for, or direct business to any individual or entity. If Service Provider is a government employee or official, Service Provider shall recuse him/herself from any governmental act or decision affecting CI, and shall not influence any governmental act or decision affecting CI. Under no circumstances shall any payments or anything of value be given, made, promised or offered to any U.S. Federal, State or local employee or official.

9. **Confidential Matters and Proprietary Information.** During the course of this Agreement, either party may acquire confidential information or trade secrets of the other ("Confidential Information"). Each party agrees to keep all such Confidential Information in a secure place, and further agrees not to publish, communicate, divulge, use, or disclose, directly or indirectly, for his own benefit or for the benefit of another, either during or after performance of this Agreement, any of the Confidential Information, except as may be required by law or this Agreement. Upon termination or expiration of this Agreement, each party shall deliver all Confidential Information produced or acquired during the performance of this Agreement and all copies thereof to the other. This obligation of confidence shall not apply with respect to information that is (a) available to the receiving party from third parties on an unrestricted basis; (b) independently developed by the receiving party; or (c) disclosed by the other party to others on an unrestricted basis.

10. **Intellectual Property**
Upon payment in full pursuant to this Agreement, Service Provider hereby transfers and assigns to CI all right, title and interest (including copyright rights) in and to the materials produced by Service Provider for CI as a result of the Services provided pursuant to this Agreement (collectively, the "Work Product"), with the exception of any software or other tools that Service Provider may produce for CI hereunder (collectively, the "Software"). Service Provider shall retain full ownership rights with respect to all Software, but hereby grants CI an unlimited royalty-free right and license to use such Software as CI wishes in perpetuity. Notwithstanding the foregoing, Service Provider retains all rights to the methodology and other know-how used in creating the Work Product and Software and has the right to use such methodology and other know-how in work for other clients. In addition, Service Provider retains all rights to any preexisting materials used by Service Provider in connection with the Work Product and Software. Service Provider hereby grants CI a nonexclusive right and license to use all such preexisting materials in the Work Product and Software. CI understands that Service Provider has the right to use all preexisting materials in work for other clients. Service Provider represents and warrants that the Work Product and Software shall either be original works or, if not original works, that Service Provider will procure the necessary licenses and/or releases from third parties to enable CI to use the Work Product and Software as contemplated by this Agreement. Service Provider agrees to indemnify and hold CI harmless from any and all Claims, arising out of a breach of the foregoing representation and warranty.

11. Security and Safety. Service Provider agrees that s/he has read, understands and shall comply with any applicable security regulations provided by CI, and acknowledges that Service Provider shall be solely responsible for Service Provider’s own safety and physical property or equipment during the performance of this Agreement.

12. Travel. Service Provider shall be solely responsible for any travel arrangements, travel insurance, and all arrangements for visas, passports or immunizations.

13. Choice of Law; Arbitration. This Agreement shall be construed and enforced in accordance with the laws of the District of Columbia, USA, applicable to contracts fully executed and performed therein and without giving effect to its conflict of laws principles. Any controversy or claim arising out of or relating to this Agreement, or the breach thereof, shall be settled by arbitration before a single arbitrator in Washington, DC, under the rules of the American Arbitration Association in effect at the time of commencement of the arbitration, and the parties agree that judgment upon the award rendered by the arbitrator shall be final, binding and may be entered in any court having jurisdiction thereof.

14. Compliance with Law; CI Code of Ethics; Data Processing. Service Provider will perform the Services in compliance with (i) the U.S. Foreign Corrupt Practices Act and Office of Foreign Asset Control regulations, as well as (ii) all laws and regulations of the country and state in which the Services are performed or which otherwise may have jurisdiction over the performance of the Services (including, but not limited to, such relating to bribery, corruption, terrorism financing and equal employment opportunity, as well as all the generally accepted standards applicable to such work), as if such aforementioned laws and regulations directly reached the activities of the Service Provider. Further, Service Provider agrees to (a) perform all Services and to conduct all activities related thereto in accordance with CI’s Code of Ethics, a copy of which is attached hereto as Appendix 2 and incorporated by reference; and (b) comply with the provisions of Appendix 3, Global Data Processing and Data Security Addendum.

15. Service Provider’s Anti-Terrorism Representation and Warranty. Service Provider is hereby notified that U.S. Executive Orders and U.S. law prohibit transactions with, and the provision of resources and support to, individuals and organizations associated with terrorism. Service Provider, therefore, represents and warrants that Service Provider has not provided, and will take all reasonable steps to ensure that Service Provider does 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 is compliant with all other applicable provisions of such U.S. Executive Orders and U.S. law.
State Compliance. In order to comply with various state statutes, the following shall be included as terms of the agreement for the various states:

a. For purposes of the State of California, the following shall apply:

Agreement will commence on xxx, within the State of California and will terminate on xxx. Services will commence with respect to solicitation of contributions in California on xxx.

CI has the right to cancel the Agreement without cost, penalty, or liability for a period of 10 days following the date on which the Agreement is executed. CI may cancel the Agreement by serving a written notice of cancellation on Service Provider. If mailed, service shall be by certified mail sent to Service Provider, return receipt requested, and cancellation shall be deemed effective upon the expiration of five (5) calendar days from the date of mailing. Following the 10-day cancellation period, CI may terminate the Agreement by giving 15 days’ written notice. If mailed, service of the notice shall be by certified mail, return receipt requested, and shall be deemed effective upon the expiration of five calendar days from the date of mailing. In the event of termination after the 10-day cancellation period, CI shall be liable for services provided by Service Provider to the effective date of termination.

b. For purposes of the State of New Jersey only, the Agreement between Service Provider and CI is not a percentage-based agreement, and the following language is provided only for purposes of complying with the contract disclosure requirements of State of New Jersey. Service Provider is to be paid as set forth in the Agreement and said compensation provisions shall be controlling.

For purposes of providing language to comply with the New Jersey Charitable Fundraising Rules, the following shall apply:

Service Provider shall receive [INSERT] percent (____%) of the gross revenue from the campaign. The amount going to Service Provider is an estimated percentage based upon previous experience of similar campaigns conducted by Service Provider. This shall not affect or alter compensation provisions as provided in the Agreement.

c. For purposes of the State of Mississippi, the following shall apply:

Solicitation activity under this Agreement is to commence on xxx, within the State of Mississippi or ten working days after the Agreement is received by the Office of the Secretary of State. Solicitation activity and the Agreement will terminate on xxx, within the State of Mississippi.

d. For purposes of the state of New York only, the Agreement shall be modified to add the following section:

Agreement will commence on xxx within the state of New York.

Agreement will terminate on xxx within the state of New York.

CI’s right to cancel this Agreement. It is understood by both parties that the charitable organization has the right under New York State law to cancel this Agreement and that the charitable organization does not have to give any reason for the cancellation. By law, the parties to this Agreement cannot waive or modify this right by any pre-existing agreement or by any subsequent agreement between the parties. Therefore, the charitable organization may cancel this Agreement without cost, penalty or liability if the charitable organization notifies Service Provider in writing as provided below.

Period under which Agreement may be canceled. If Service Provider is registered with the New York State Office of the Attorney General Charities Bureau the charitable organization may cancel this Agreement at any time up to and including the fifteenth day after this Agreement was
filed by Service Provider with the New York State Office of the Attorney General, Charities Bureau. If, however, the Service Provider is not registered with the New York State Office of the Attorney General, Charities Bureau at the time this Agreement is signed, the charitable organization may cancel at any time after it is signed.

**Procedure for canceling this Agreement.** The charitable organization may cancel this Agreement by giving Service Provider written notice of cancellation. This notice can be in the form of a letter indicating that the charitable organization does not intend to be bound by the Agreement. The notice of cancellation may be hand-delivered or mailed to Service Provider. If mailed, it must be sent to the following address:

1101 Connecticut Ave NW 7th Floor
Washington DC 20036

The charitable organization must mail a duplicate copy of the written notice of cancellation to the Office of the Attorney General at the address listed below:

Charities Bureau
Office of the Attorney General
The Capitol
Albany, NY 12224

**When Cancellation is effective.** If the notice of cancellation is hand-delivered, the cancellation is effective as soon as it is delivered to Service Provider. If the notice of cancellation is mailed, the cancellation is effective as soon as the notice is deposited, properly addressed and postage pre-paid, in a mailbox.

e. For purposes of the State of Pennsylvania, the following shall apply:

Services under the terms of the agreement with respect to solicitation of contributions in the Commonwealth will commence on xxx, or ten working days after the Agreement is received by the Department of State, Bureau of Charitable Organizations and/or is approved by the Department of State Bureau of Charitable Solicitations.

f. Services and the Agreement will terminate on xxx, within the Commonwealth of Pennsylvania. For purposes of the State of South Carolina only, the following shall apply: The South Carolina Registration Number of CI is P4482. The South Carolina Registration Number of Service Provider is ________.

17. **Counterparts and Facsimile Signatures.**

a. Each party agrees that the other party may rely on a facsimile copy of the signature of a duly authorized signatory and that upon the exchange of such facsimile signatures, electronically or otherwise, this Agreement shall be binding between the parties whether or not hard copies of this Agreement are ever exchanged between them.

b. This Agreement may be signed in one or more counterparts, each of which shall be deemed an original but all of which together shall constitute one and the same instrument even though all the parties are not signatories to the original or the same counterpart.

18. **Severability.** In the event that any one or more of the provisions contained herein shall, for any reason, be held to be invalid, illegal or unenforceable in any respect, such invalidity, illegality or unenforceability shall not affect any other provisions of this Agreement, but this Agreement shall be construed as if such invalid, illegal or unenforceable provisions had never been contained herein, unless the deletion of such provision or provisions would result in such a material change so as to cause completion of the transactions contemplated herein to be unreasonable.
19. **No Third-Party Beneficiaries.** Except as expressly set forth herein, neither party intends that this Agreement shall benefit or create any right or cause of action in or on behalf of any person or entity other than the Service Provider and CI.

20. **Non-Assignment.** This Agreement shall not be transferred or assigned by Service Provider without prior written consent of CI.

21. **Waiver.** Either party may specifically waive any rights under this Agreement by the other party, but no such waiver shall be deemed effective unless in writing, signed by the waiving party, and specifically designating the rights waived. No waiver shall constitute a continuing waiver of similar or other rights.

22. **Entire Agreement; Amendments.** This Agreement, including all Appendices, supersedes all prior oral or written agreements between the parties and constitutes the entire Agreement between the parties. Unless indicated otherwise herein, this Agreement may not be amended, supplemented, or modified in any respect except by written agreement signed by both parties.

23. **Notices.** Notice under this Agreement shall be deemed to have been sufficiently given either when served personally or when sent by first-class registered mail addressed to the parties at the addresses set forth below. CI shall not be liable for, nor shall Service Provider be liable to perform, services or expenses incurred after the receipt of notice or termination.

If to Service Provider: 
If to CI:
Attn: Conservation International Foundation
Conservation International Foundation
2011 Crystal Drive, Suite 600
Arlington, VA 22202
Phone: 703-341.2400

The authorized representatives of the parties hereto have caused this Agreement to be executed as of the date first written above.

xxx Conservation International Foundation

__________________________________ ______________________________
Ci signatory

Conservation International Foundation

__________________________________ 
CI signatory

Last updated 3-2020
APPENDIX 1

TERMS OF REFERENCE AND DELIVERY SCHEDULE
APPENDIX 2

ETHICS STANDARDS

Conservation International’s reputation derives from our commitment to our core values: Integrity, Respect, Courage, Optimism, and 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 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.

Integrity:
- Act in good faith, responsibly, with due care, competence and diligence and maintain the highest professional standards at all times.
- Comply with all contractual terms as well as all applicable laws, rules and regulations, domestic and international, in every country where Services are carried out.
- Provide true representation of all Services performed.
- Never engage in any of the following acts: falsification of business document or receipts, theft, embezzlement, diversion of funds, bribery, or fraud.

Transparency:
- Avoid conflicts of interest and not allow independent judgment to be compromised.
- Not accept gifts or favors from sub-contractors, suppliers or other 3rd parties that would negatively impact the provision of Services to CI.

Accountability:
- Disclose to CI, at the earliest opportunity, any information you have or become aware of, that may result in a real or perceived conflict of interest or impropriety.
- Implement activities, provide Services, and manage staff and operations in a professionally sound manner, with knowledge and wisdom with the goal of a successful outcome per the terms of this Agreement.

Confidentiality:
- Not disclose confidential or sensitive information obtained during the course of your work with CI.
- Protect confidential relationships between CI and other 3rd parties.
Mutual Respect and Collaboration:

Engage with indigenous peoples and local communities in which CI works in a positive and constructive manner that respects the culture, laws, and practices of those communities, with due regard for the right of free, prior and informed consent.

I hereby acknowledge receipt of CI's Code of Ethics and certify agreement and compliance therewith.

FOR SERVICE PROVIDER:

By: _________________________

Title: _________________________
Appendix 3
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

---

1 **DRAFTING NOTE:** If Supplier will process credit card data on behalf of CI, add the following definitions; else, delete footnote: “Cardholder Data” means primary account number, cardholder name, expiration date and/or service code, and security-related information (including but limited to card validation codes/values, full track data PINs and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions; “PCI DSS” means the Payment Card Industry Data Security Standard of the PCI Security Standards Council, as may be amended from time to time, which can be found at https://www.pcisecuritystandards.org/; “Personal Data” means any information relating to an identified or identifiable natural person that is governed by any Data Law and/or PCI DSS, including, without limitation, Cardholder Data.

Last updated 10-2020
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.

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

---

2 DRAFTING NOTE: IF SUPPLIER WILL PROCESS CREDIT CARD DATA ON BEHALF OF CI, ADD THE FOLLOWING PROVISION; ELSE, DELETE FOOTNOTE: **PCI ACKNOWLEDGEMENT AND ATTESTATION.** Supplier acknowledges that Supplier is responsible for the security of Cardholder Data that it Processes on behalf of CI. Supplier shall at all times comply with PCI DSS. Supplier represents and warrants to CI that Supplier has successfully completed the PCI DSS self-assessment questionnaire (SAQ). Supplier shall complete the SAQ annually and shall provide CI with an Attestation of Compliance upon request.

Last updated 10-2020
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 represents and warrants that:

8.1 it has certified to the United States Department of Commerce and that it complies with the EU-US Privacy Shield Framework and the Swiss-US Privacy Shield Framework, as applicable, and their associated Principles and Supplemental Principles and any related requirements located at www.privacyshield.gov, as may be amended from time to time, (collectively, the “Principles”) for the Personal Data to be transferred pursuant to the Underlying Agreement, with the exception of the Notice and Choice principles. Supplier will maintain such certifications active for the duration of the Underlying Agreement. Supplier will treat Personal Data from the European Economic Area (“EEA”) Processed pursuant to the Underlying Agreement in compliance with the Principles. If Supplier is authorized by CI to subcontract any of its obligations under this Agreement, Supplier will downstream these obligations by entering into an appropriate onward transfer agreement with any such subcontractor for any such disclosure; or

8.2 if (i) Supplier is not EU-US Privacy Shield certified or is not certified under the Swiss-US Privacy Shield, if applicable; or (ii) either of the certifications do not cover the Personal Data to be transferred pursuant to the Underlying Agreement; or (iii) either of these Frameworks is deemed invalid at any point during the term of the Underlying Agreement; or (iv) Supplier no longer complies with the Principles or fails to renew its certification, then Supplier agrees to promptly execute the European Commission Standard Contractual Clauses (“Standard Clauses”) set forth in Schedule 3 hereto 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.

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: 

______________________________

Print Name: 

______________________________

Title: 

______________________________

Date: 

______________________________

By: 

______________________________

Print Name: 

______________________________

Title: 

______________________________

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.]
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.

Last updated 10-2020
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.
Schedule 3

Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)

Data transfer agreement

between

Conservation International Foundation, with its principal place of business at (hereinafter “data exporter”)

and

(name)

(address and country of establishment)

hereinafter “data importer”

each a “party”; together “the parties”.

Definitions

For the purposes of the clauses:

(a)“personal data”, “special categories of data/sensitive data”, “process/processing”, “controller”, “processor”, “data subject” and “supervisory authority/authority” shall have the same meaning as in Directive 95/46/Ec of 24 October 1995 (whereby “the authority” shall mean the competent data protection authority in the territory in which the data exporter is established);

(b)“the data exporter” shall mean the controller who transfers the personal data;

(c)“the data importer” shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country’s system ensuring adequate protection;

(d)“clauses” shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

I. Obligations of the data exporter

The data exporter warrants and undertakes that:

(a) The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.

(b) It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.

(c) It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.

(d) It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.
(e) It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

II. Obligations of the data importer

The data importer warrants and undertakes that:

(a) It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

(b) It will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data.

(c) It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.

(d) It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfill the undertakings set out in these clauses.

(e) It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).

(f) At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfill its responsibilities under clause III (which may include insurance coverage).

(g) Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion.

(h) It will process the personal data, at its option, in accordance with:

(i) the data protection laws of the country in which the data exporter is established, or

(ii) the relevant provisions of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorisation or decision and is based
in a country to which such an authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data, or

(iii) the data processing principles set forth in Annex A.

Data importer to indicate which option it selects: __________________________________________

______

Initials of data importer: __________________________________________

______;

(i) It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and

(i) the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or

(ii) the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or

(iii) data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or

(iv) with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer

III. Liability and third party rights

(a) Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.

(b) The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter’s country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

IV. Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

V. Resolution of disputes with data subjects or the authority

Last updated 10-2020
(a) In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

(b) The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

(c) Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible.

VI. Termination

(a) In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

(b) In the event that:

(i) the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);

(ii) compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;

(iii) the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;

(iv) a final decision against which no further appeal is possible of a competent court of the data exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or

(v) a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs

then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.

(c) Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.

(d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

VII. Variation of these clauses

Last updated 10-2020
The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

VIII. Description of the Transfer
The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

Dated: ____________________________

__________________________________________________________________________ Conservation International Foundation

FOR DATA IMPORTER FOR DATA EXPORTER

__________________________________________________________________________

__________________________________________________________________________

__________________________________________________________________________

__________________________________________________________________________

Last updated 10-2020
ANNEX A

DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.

2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.

4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.

5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.

6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.

7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to “opt-out” from having his data used for such purposes.

8. Automated decisions: For purposes hereof “automated decision” shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:

   (a)   (i)   such decisions are made by the data importer in entering into or performing a contract with the data subject, and

Last updated 10-2020
(ii) the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.

or

(b) where otherwise provided by the law of the data exporter.
ANNEX B
DESCRIPTION OF THE TRANSFER

*(To be completed by the parties)*

Data subjects
The personal data transferred concern the following categories of data subjects:

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

Purposes of the transfer(s)
The transfer is made for the following purposes:

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

Categories of data
The personal data transferred concern the following categories of data:

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

Recipients
The personal data transferred may be disclosed only to the following recipients or categories of recipients:

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

Sensitive data (if appropriate)
The Personal data transferred concern the following categories of sensitive data:

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

Data protection registration information of data exporter *(where applicable)*

________________________________________________________________________

________________________________________________________________________
Additional useful information

Contact points for data protection enquiries

Data importer

______________________________________________________________

______________________________________________________________

______________________________________________________________

Data exporter

______________________________________________________________

______________________________________________________________

______________________________________________________________