FUNDRAISING SERVICES CONTRACT

BY AND BETWEEN

Sandra Carrera Bonet, with ID number 38149005D, acting on behalf of Xarxa per a la Conservació de la Natura (hereinafter the "NGO"), with business address at C/Sagrada Família, 7 , Vic 08500 and Tax ID number G63122402

AND

Aureli Bou i Balust, with Spanish ID number 47871408-J, acting in his capacity as joint and several administrator of WORLDCOO S.L (hereinafter "Worldcoo") with business address at Via Augusta 13-15, Planta 6, oficina 603, 08006 - Barcelona, and Tax ID number B65855611

DECLARE

I. That the NGO is officially recognised in all its activities, for which it receives collaboration from individuals, public administrations, institutions, entities and enterprises.

II. That Worldcoo is a company devoted to:

1. Fundraising for cooperation and social-development projects.
2. Selecting projects, partners, collaborating organisations and sponsor companies.
3. Activities related with sustainable development, the environment, human development, education, human rights and other solidary causes.
4. Activities related with Corporate Social Responsibility in sponsor companies and managing their social funds.

III. That the NGO needs the help and collaboration of third parties to meet its financial goals.

IV. That Worldcoo has created the worldcoo.com domain as an online tool to raise funds that go to social projects, alongside other fundraising channels.

CLAUSES

ONE.- PURPOSE

1.1. The purpose of these conditions is to establish the terms of collaboration between the NGO and Worldcoo for promoting projects and raising funds.

1.2. Worldcoo shall raise funds for the NGO's projects that are introduced via Worldcoo (hereinafter the "Projects") through its fundraising channels. The conditions herein shall apply to all of them expressly.

1.3. After being presented and approved by Worldcoo, each of the Projects shall be subject to funding by a company collaborating with Worldcoo (hereinafter "Partner"). The Projects will be made visible on all Worldcoo channels.

1.4. When a Project is selected by one or several Partners, a funding process for the Project (hereinafter "Campaign") will begin.

1.5. To carry out each of the Projects, a budget will be set (hereinafter "Funding Goal"), which the NGO will receive as donations from third parties to the NGO.

TWO.- TYPES OF CAMPAIGNS

There are three types of campaign, depending on the number of Partners collaborating to fund the project and the timeline:

Public campaigns. In these campaigns, the funds for the Project come from several Partners that work together on fundraising for the Project. The campaign is fully funded once the Funding Goal is reached.

Private campaigns. In these campaigns, the funds for the Project come from just one Partner. The campaign is fully funded once the Funding Goal is reached.

Emergency campaigns. In these campaigns, the funds for the Project come from several Partners that work together on fundraising for the Project for a specific period of time. The campaign is fully funded once the deadline is reached and the amount raised at that time is the Funding Goal for the project.

THREE.- FUNDRAISING CHANNELS

There are different fundraising channels, depending on where donations are made. The most noteworthy are:

Websites other than Worldcoo. E-commerce sites put a donation widget on their site to allow customers to make donations to the campaign when checking out.

Online banking platforms. Banks connect to the Worldcoo systems with an API and allow their clients to make donations to the campaign at several points in the online banking process.

Point-of-sale terminals. Physical point-of-sale terminals are modified to accept donations to the campaign when customers go to pay by card.

Worldcoo websites. Worldcoo designs and implements employee sites for large corporations to give their clients and employees a website where they can donate to a campaign on a one-off or recurring basis.

FOUR.- COMPENSATION AND LIQUIDATION OF DONATIONS RECEIVED

4.1. Compensation: For providing the services listed in section one, Worldcoo shall be compensated with 8% of the funds received as donations from third parties to the NGO.

If the NGO brings in a Partner to work with Worldcoo, this compensation shall be 4% for campaigns executed with that Partner.

This compensation for services rendered shall be subject to the legally required VAT at any given time.

4.2. Accounting: Worldcoo shall automatically handle the accounting for all donations received.

4.3. Invoicing: Worldcoo shall issue an invoice for the fees due for the provision of services. The amount invoiced shall be calculated based on the amount received in donations from third parties to the NGO for the Project funded.

Given their specific nature, the funds received and deposited by Worldcoo in donations to the NGO belong to the NGO, although the donations shall not be made effective until Worldcoo transfers them to the NGO. Worldcoo is obliged to deliver the funds according to the calendar agreed upon in section 4.4 below.

4.4. Calendar: Once the Funding Goal for the Project has been reached and the amount received, Worldcoo shall issue an invoice for the services provided in association with the Project funded and deposit the amount in the bank account provided by the NGO:

IBAN: ES80 1491 0001 2720 3932 4625

According to the following calendar:

First instalment and invoice: once the Funding Goal for the Project has been reached, 50% of the full amount will be transferred and an invoice issued for the services provided. A list of any donors who requested a tax deduction certificate shall also be sent.

Second (and final) instalment: once the invoice for the services provided by Worldcoo has been paid and the Project Report (see section 6.1) approved, the final 50% shall be transferred.

The NGO must provide Worldcoo with a receipt for the amounts transferred.

4.5. Specific conditions: Any fees or commissions charged for exchanging currency or making international bank transfers shall be covered by the NGO.

Likewise, donations made through point-of-sale terminals shall be subject to a surcharge of no more than €0.03 to cover bank charges.

The legally required VAT at any given time shall be applied to said commissions.

If the Funding goal is not met, the amount raised shall be transferred to the NGO after the deadline set by the two parties.

FIVE.- USE OF THE BRAND AND LOGO

The NGO hereby authorises Worldcoo and its partners to use its name and logo to disseminate the Project.

SIX.- OTHER OBLIGATIONS

6.1. Final campaign report: the NGO must provide Worldcoo with a report containing at least the following information:

- Achievements
- Beneficiaries
- Photographs and/or testimonials and other audiovisual materials
- Detailed financial justification of use of the funds

The report must be submitted within 12 months of the end of the campaign.

6.2. Commitment to remain: The NGO hereby undertakes to activate each Worldcoo campaign and not remove it over the course of the fundraising period.

6.3. On-site visits: Worldcoo may visit and follow up on any of the Projects in any way it deems appropriate, coordinating these visits with the NGO whenever possible. Any travel expenses arising from the visit from representatives of Worldcoo, will be covered exclusively by Worldcoo.

SEVEN.- EXCLUSION OF LIABILITY

Worldcoo has no responsibility for the execution of the Projects and, thus, may not be held liable in any way for any accidents or errors in the construction and/or repair and/or maintenance of said Projects and the associated works.

EIGHT.- TAX DEDUCTIONS ON CONTRIBUTIONS

When the fundraising for the Project is finished, Worldcoo shall provide the NGO with a list of the donors who requested a tax deduction certificate (as per the calendar established in point 4.4) and anyone who donated more than €100 with their corresponding fiscal details as per section nine of this document.

As the donations are in Worldcoo's possession for safekeeping, they are not made effective for tax or accounting purposes until Worldcoo transfers them to the NGO. As such, the certificates shall be issued at the end of the fiscal year in which the NGO receives the funds from Worldcoo. Donors are duly informed of this when donating.

When the NGO can issue donation certificates, the NGO must provide each donor a certificate for the donation made.

When the NGO cannot issue donation certificates, the NGO must provide each donor a receipt for the donation made.

NINE.- DONOR DATA CONTROLLER AND OBLIGATIONS OF THE DATA PROCESSOR

The NGO is the data controller for the personal details pertaining to this contract and must comply with EU Regulation 2016/679 of the European Parliament and Council dated 27 April on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter, GDPR), and any other applicable data protection regulations.

Worldcoo shall act as the NGO Data Processor in channelling donations and collecting donors' details, in compliance with the provisions of article 28.3 of the GDPR.

The handling operations shall consist in collecting, registering, organising, saving, querying and communicating via transfer.

9.1. Identification of the information affected

Types of data: Personal and contact details.

Category of subjects: Donors.

9.2. Obligations of the Data Processor

The data processor and its entire staff undertake to:

a. Use the personal data processed, or collected to be processed, only for the purposes of this commission. Under no circumstances shall the data be used for internal purposes.

b. Process the data according to instructions from the handling controller.

   If the data processor believes any of these instructions infringe on the GDPR or any other ruling on data protection in the Union or the Member States, they shall notify the controller immediately.

c. Keep a written registry of all categories of processing activities carried out for the controller containing:

   1. The name and contact details of the processor or processors and each controller for which they are acting and, when applicable, the representative of the controller or processor and the data protection delegate.
   2. The processing categories carried out for each controller.
   3. When applicable, the transfer of personal data to a third country or international organisation, including identification of said third country or international organisation and, for transfers indicated in article 49 section 1 paragraph 2 of the GDPR, proof of adequate guarantees.
   4. A general description of the technical and organisational security measures for:
      a. Pseudonymisation and encryption of personal data.
      b. Guaranteeing confidentiality, integrity, availability and resilience of the data handling systems and services at all times.
      c. Restoring availability and access to personal data quickly in the case of physical or technical incident.
      d. Regularly verifying, evaluating and assessing the efficacy of the technical and organisational measures implemented to ensure handling security.

d. Not share data with third parties, except with the express authorisation of the handling controller in legally admissible situations.

   The processor may communicate data to other processors of data from the same controller, according to the controller's instructions. In this case, the controller shall identify in writing prior to any transfer the organisation to which the data must be communicated and the security measures to apply in said communication.

   If the processor needs to transfer personal data to a third country or international organisation, based on applicable EU law or of the Member States, the controller must be notified beforehand, except when prohibited for significant reasons of public interest.

e. Outsourcing

The data processor may not outsource any of the services to which this contract pertains that entail the processing of personal data, except for the necessary auxiliary services required for normal operations of the processor's services.

If it were necessary to outsource any handling, the controller must be notified in writing 15 days prior, indicating the handling to be outsourced and clearly, unequivocally identifying the subprocessor and its contact details. Said subprocessing may be carried out if the controller does not communicate its opposition within the established period.

The subprocessor, who shall also be considered a processor, is equally obliged to comply with the obligations established in this document for the data processor, as well as any instructions given by the controller. The processor shall be responsible for the new relationship so that the new subprocessor is subject to the same conditions (instructions, obligations, security measures, etc.) and with the same formal requirements as the original processor, with regard to proper processing of personal data and ensuring the rights of the data subjects. The original processor shall be fully responsible to the controller for compliance with all obligations, even if it is the subprocessor who fails to comply.

f. Maintain the duty of secrecy regarding data of a personal nature to which access has been gained through this commission, including after its purpose has concluded.

g. Ensure individuals authorised to handle personal data expressly undertake in writing to respect confidentiality and comply with corresponding security measures, of which they must be duly informed.

h. Make available to the controller documentation accrediting compliance with the obligations established in the previous section.

i. Ensure individuals authorised to handle personal data receive the training necessary on the protection of personal data.

j. Assist the controller in responding to data subjects exercising their rights to:

   1. Access, correct, eliminate and oppose to handling
   2. Limit handling
   3. Data portability
   4. Not be subject to automated individual decision-making (including profiling)

When the data subjects exercise their rights to access, correct, delete or oppose to the handling of their data, limit handling, data portability or to not be subject to automated individual decision-making, notification must be given through the standard channels of communication. Notification must be made immediately and under no circumstances more than one business day after receiving the request, along with any other information that may be relevant to resolve the situation.

k. Right to be informed

Worldcoo shall notify donors of their right to be informed when collecting the data, providing basic information on data protection, also known as the first layer, which will include a link to additional data protection information, also known as the second layer.

Donors will be duly informed and shown the following content:

> **Controller:** Xarxa per a la Conservació de la Natura; **Purpose:** To raise funds for the NGO's projects, keep you up to date on the NGO and the progress of the project you donated to and issue tax seduction certificates; **Lawfulness:** The legal basis for handling your data is your consent; **Recipients:** No data shall be transferred to third parties; **Rights:** You have the right to access, correct and delete your data, as well as other rights, as explained in the additional information; **Additional information:** For more details and additional information on data protection, please go to our website: http://www.xct.cat/ca/politicaprivadesa

The NGO will provide Worldcoo with the address for the link where it informs users regarding basic data protection information. The NGO is responsible for the information in the second layer being accessible to data subjects via the link provided.

l. Notification of any breach of the data security

The data processor shall notify the controller of any breach of security affecting the personal data it holds when it becomes aware of them, without undue delay and in any case within 48 hours, via the standard channels of communication, and pass along any relevant information to document and notify the incident.

It shall not be necessary to send when it is improbable that the breach in question poses a risk to the rights and freedoms of individuals.

If available, the following, at least, shall be provided:

a. Description of the nature of the security breach affecting personal data including, when possible, the categories and approximate number of subjects affected, and the category and approximate number of files of personal data affected.
b. The number and contact details of the data protection delegate or other contacts hat may have more information.
c. Description of the possible consequences of the security breach affecting personal data.
d. Description of the measures taken or proposed to remedy the security breach affecting personal data, including, if necessary, the measures adopted to mitigate any possible negative effects.

If it is not possible to provide this information all at once, and to the extent to which it is not possible, the information shall be provided gradually with no undue delay.

m. Support the controller in carrying out impact evaluations regarding the protection of data, when necessary.
n. Support the controller in carrying out preliminary queries with the supervisory authority, when necessary.
o. Provide the controller with any information necessary to demonstrate compliance with its obligations, as well as to conduct any audits or inspections carried out by the controller or other authorised auditor on their behalf.

p. Implement the following security measures:

GENERAL MEASURES

- Document the policy regarding the handling of personal data
- Implement and promote a proactive culture of compliance with data protection obligations within the organisation
- Establish procedures to regularly verify, evaluate and assess the efficacy of the technical and organisational measures implemented to ensure handling security

STAFF

- The duties and obligations of each user or user profile regarding the handling of personal data shall be clearly defined
- The organisation shall ensure that all employees understand their responsibilities and obligations regarding the handling of personal data
- Any employees involved with the handling of personal data will be duly informed of the applicable data protection requirements and legal obligations, through awareness-raising campaigns
- Providing written rules for employees to follow regarding data protection, according to their functions
- The responsibilities and obligations shall be communicated to employees clearly and duly documented
- All employees with access to personal data will sign a non-disclosure agreement

ICT RESOURCES AND INFORMATION SYSTEMS

- Establish rules for use of ICT resources
- Keep a registry of computer resources used for the handling of personal data (hardware, software and network)
- Review and update ICT resources regularly, monitoring expiry of guarantees and maintenance contracts
- Install critical security updates from the manufacturer of the operating system
- Users should not be able to deactivate or get around the security settings
- The systems must have antivirus software, updated with reasonable frequency
- Establish a policy for using mobile and portable devices
- Mobile devices accessing computer systems must be authorised and registered previously
- Mobile devices will be subject to the same security levels monitoring access as any other workplace
- Have a firewall, if the Internet is used frequently, in order to stop any attempts at intrusion or improper use by the users themselves
- The systems must require a password when a terminal has been inactive for a certain amount of time

ACCESS CONTROL

- Implement an access control system that applies to all users accessing the information systems. The system must allow for the creation, approval, review and elimination of user accounts
- Have a mechanism to guarantee correct user identification and authentication when accessing the ICT system. At the very least, a username and password must be used
- Keep a current list of users and user profiles, the type of access authorised for each one and the related access permissions
- Ensure the access granted to each user is in line with and limited to their assigned duties

- Only authorised staff may grant, change or revoke access authorisation
- Revocation of rights and responsibilities must be clearly defined in internal reorganisation processes, firings or change of employment
- Implement measures to prevent unauthorised access to data or resources
- Limit reiterated attempts at unauthorised access
- Establish a minimum complexity required for passwords
- The access-control system must be able to detect and not allow passwords that do not meet the minimum level of complexity required
- Adopt a procedure to assign, distribute and store passwords that ensures they are confidential and not accessible
- Store the passwords in an unintelligible format
- Establish how often passwords must be changed
- Prevent the use of generic accounts. When it is necessary to use generic accounts, the users of said accounts must have the same functions and responsibilities
- The physical perimeter of the facilities housing the systems that contain personal data must not be accessible to unauthorised staff
- Paper documents must be filed according to criteria that allow for proper storage, querying and locating of documents to ensure the rights afforded data subjects in the GDPR can be properly attended
- Fit storage devices with mechanisms to prevent them from being opened

MEDIA AND DOCUMENT MANAGEMENT

- Keep an inventory of all media and documents in the organisation
- Adopt an authorisation procedure for the creation of media not laid out in the security policy
- Adopt an authorisation procedure for physical media leaving the physical environment of the organisation and monitoring and controlling it until it is returned or destroyed
- Establish rules to ensure due diligence and safeguarding of paper documents by the staff in charge of them while they are being processed, reviewed or handled to prevent any unauthorised access
- Implement measures for the use or moving and sending of physical media and mobile devices outside the company facilities

BACK-UP COPIES

- Procedures must be established to back up and restore personal data
- Periodically check the effectiveness of the back-up procedures
- Make back-up copies at least once a week
- The media on which back-up copies are stored must have proper physical and environmental protection, as per regulations applicable to the original data
- Back-up copies must be monitored to ensure their integrity
- As a good practice, complete back-up copies must be made regularly

INCIDENTS

- Adopt the necessary controls and procedures to ensure information systems used in handling personal data continue to be available in the case of a physical or technical incident
- Adopt a procedure to identify, track and manage incidents

ERASING DATA AND DESTROYING MEDIA

- Personal data shall be erased by overwriting (secure delete) or, if this is not possible, by physically destroying the media or resources
- Any paper copies containing personal data must be destroyed securely (shredded) or sent to service providers that specialise in secure destruction of certified documents, with the proper guarantees

En todo caso, deberá implantar mecanismos para:

a. Ensure the confidentiality, integrity, availability and resilience of the handling systems and services
b. Restore availability and access to personal details quickly if any physical or technical incidents were to occur
c. Verify, evaluate and assess the efficacy of the technical and organisational measures in place to ensure security of data handled on a regular basis
d. Anonymise and encrypt personal details, when necessary

q. Designate a data protection delegate when necessary and inform the controller, even when done voluntarily, of the delegate's identity and contact details.

r. Intended use of data

Return any personal data to the controller and, if applicable, the media on which it was stored, after the commission has been completed.

The return of said data must entail it is fully erased from the computer systems used by the processor.

Nevertheless, the processor may save a copy, with the data duly blocked, for as long as they may be held responsible for the execution of the services provided.

TEN.- OBLIGATIONS OF THE RESPONSIBLE OF THE TREATMENT

It corresponds to the person responsible for the treatment:

a. Deliver or facilitate the access to the manager the data referred to in point 9.2 of this document, if applicable.
b. Perform an analysis and evaluation of risks, and in cases that are legally required, perform an evaluation of the impact on the protection of personal data of the treatment operations to be performed by the person in charge.
c. If applicable, carry out the corresponding prior consultations.
d. Ensure, prior to and throughout the treatment, compliance with the GDPR by the person in charge.
e. Supervise the treatment, including the carrying out of inspections and audits.

ELEVEN.- DURATION

This contract shall be valid for one year, automatically extended for the same term unless one of the parties opposes more than 15 days from the date of expiry.

TWELVE.- PROTECTION OF PERSONAL DETAILS

The personal data included in this contract will be included in the treatments for which each of the contracting parties is responsible, as part of a regulatory contract for a business and / or administrative relationship, and be necessary for the maintenance and compliance with it. The data provided will be kept during the term of the contract and, where appropriate, until the statutory limitations that may arise from it, will not be subject to automated decisions, including the creation of profiles and will not be transferred to third parties, except legal obligation. It is also informed that they may exercise their rights of access, rectification, deletion, opposition, limitation to processing, portability of data and opposition to be the subject of automated individual decisions, writing to **rgpd@worldcoo.com** and that they have the right to submit a complaint to the competent control authority in the event that they understand that their right to data protection has been violated.

And, in witness whereof, both parties have signed these conditions:

Signed:

WORLDCOO S.L.
Aureli Bou i Balust
47871408-J

Barcelona

July 10, 2019

Signed:

Xarxa per a la Conservació de la Natura
Sandra Carrera Bonet
38149005D