Data Processing Addendum

This Data Processing Addendum (the "**DPA**") is an addendum to the [Volunteer Operator Agreement] (the "Agreement") effective [AGREEMENT EFFECTIVE DATE] between Ruby Central, Inc. ("**Controller**") and [Contractor's details] (the "**Processor**").

This DPA serves to provide sufficient safeguards regarding the protection of Personal Data. Terms used in the DPA have the same meaning as those used in the Agreement, unless explicitly provided otherwise. Any terms used in this DPA, which are defined in the EU General Data Protection Regulation (2016/679) ("**GDPR**") and not otherwise defined in this DPA or the Agreement, shall have the meaning as set out in the GDPR.

If there are any conflicts or inconsistencies between the DPA and the Agreement, the provisions in the DPA prevail.

1 Instructions

1.1 Controller, hereby instructs Processor to carry out the Processing services as specified in the Agreement.

1.2 When carrying out the Processing services mentioned in the Agreement, Processor shall: (i) act on the documented instructions from Controller (and from Controller only) and (ii) act only for the purposes authorised by Controller. This processing activity is further specified in Appendix C to this DPA.

2 Applicable law

2.1 When carrying out the obligations under the Agreement, Processor shall comply with this DPA, Applicable Data Protection Law and with Applicable Data Processor Law and shall make all the information available necessary to demonstrate compliance with this legislation and this DPA.

2.2 Processor shall deal promptly and appropriately with requests for assistance of Controller to ensure compliance of the Processing with Applicable Data Protection Law.

3 Security

3.1 Processor shall implement appropriate technical, physical and organizational security measures to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized Disclosure or access, and against all other forms of unlawful Processing including, but not limited to, unnecessary collection or further Processing. These measures shall, taking into account the state of the art and the costs of the implementation and execution of the measures, ensure an adequate level of protection appropriate to the risk, taking into account the risks involved in the Processing and the nature of the Personal Data to be secured as defined in Applicable Data Protection Law. The measures that Processor shall take must be based on a risk assessment and shall reflect industry standards.

4 Non-disclosure and confidentiality

4.1 Processor shall keep Personal Data confidential and shall not Disclose Personal Data in any way to any Employee or Third Party without the prior written approval of Controller, except where, (i) subject to Clause **4.2** to **5.2** of the DPA, the Disclosure is required for the performance of the Services under the Agreement, or (ii) subject to Clause **7.1** of the DPA, where Personal Data need to be Disclosed to a competent public authority to comply with a legal obligation or as required for audit purposes.

4.2 Processor shall provide its employees access to Personal Data only to the extent strictly necessary to perform the Processing. Processor shall ensure that any Employee it authorizes to have access to Personal Data Processed on behalf of Processor respects and maintains the confidentiality and security of the Personal Data.

5 Sub-processors

5.1 Processor shall not permit Sub-Processors to Process Personal Data unless the appointment of the Sub-Processor is duly notified to Controller and Controller does not oppose to the appointment within 15 business days. Any authorization by Controller to use a Sub-Processor is subject to the condition that Processor remains fully liable to Controller for the Sub-Processor's performance of the contract, as well as for any acts or omissions of the Sub-Processor in regard to its Processing. A list with pre-approved Sub-processors is recorded in Appendix B, which is attached to this DPA.

5.2 Processor shall ensure that Sub-Processors are contractually bound to the same obligations with respect to the Processing as those which Processor is bound to under the Agreement, including the DPA. Controller has the right to monitor compliance with these obligations of the Sub-Processors, in particular compliance with the agreed technical and organizational measures, before data processing by Sub-Processor begins and periodically.

6 Audit and compliance

6.1 Processor shall make the processed Personal Data under this Agreement and the Processing systems, facilities and supporting documentation relevant to the Processing of Personal Data available for an audit by Controller or a qualified independent assessor selected by Controller and provide all assistance Controller may reasonably require for the audit. If the audit demonstrates that Processor has breached any obligation under the DPA, Processor shall immediately cure that breach and pay or reimburse Controller for all reasonable costs of the audit. Otherwise Controller shall bear its own costs of the audit.

6.2 Controller shall:

(a) give Processor reasonable notice of the intention to perform an audit;
(b) procure that its representatives and nominees conducting the audit comply with Processor's reasonable confidentiality and health and safety regulations, as notified by Processor to Controller; and
(c) procure that its representatives and nominees conducting the audit use reasonable efforts to minimize any disruption to Processor's business caused by the performance of the audit.

7 Inspection or audits by public authorities

7.1 Processor shall submit its relevant Processing systems, facilities and supporting documentation to an inspection or audit relating to the Processing by a competent public authority if this is necessary to comply with a legal obligation. In the event of any inspection or audit, each Party shall provide all reasonable assistance to the other Party in responding to that inspection or audit. If a competent public authority deems the Processing in relation to the Agreement unlawful, the Parties shall take immediate action to ensure future compliance with Applicable Data Protection Law and Applicable Data Processor Law.

8 Notifications to Controller

8.1 Processor shall promptly, and in any case within two business days (unless a data breach is discovered, the shorter term thereby applies), inform Controller if it:

(a) has a reason to believe that it is unable to comply with any of its obligations under the Agreement due to legal requirements;
(b) has reason to believe that that any instructions of Controller regarding the Processing of personal data would violate EU or Member State law;
(c) receives an inquiry, a subpoena or a request for inspection or audit from a competent public authority relating to the Processing, except where Processor is otherwise prohibited by law from making such disclosure;
(d) intends to Disclose Personal Data to any competent public authority, unless it is expressly forbidden to reveal such information; or
(e) within 12 hours from when it has acquired sufficient knowledge of such an incident, detects or reasonably suspects that a security incident or Personal Data Breach has occurred.

8.2 In the event of a Personal Data Breach, Processor shall promptly take adequate remedial measures. Furthermore, Processor shall promptly provide Controller with all relevant information regarding the Personal Data Breach and all information as reasonably requested by Controller regarding the Personal Data Breach. Processor shall inform Controller regarding the nature of the breach, the categories of data subjects and Personal Data concerned, the likely consequences of the data breach and the measures taken or proposed to be taken to address the data breach. Processor shall fully cooperate with Controller to develop and execute a *response plan* to address the Personal Data Breach. Processor shall at the request of Controller cooperate in adequately informing the Individuals involved.

9 Cooperation complaints, requests and enquiries

9.1 Processor shall deal promptly and appropriately with inquiries of Controller related to the Processing under the Agreement.

9.2 Processor shall promptly inform Controller of any complaints, requests or enquiries received from Individuals, including but not limited to requests to correct, delete or block Personal Data. Processor shall not respond to the Individual directly except where specifically instructed by Controller, in which case Processor shall respond within the timeframes prescribed in Applicable Data Protection Law. Processor will in all other cases respond within a reasonable period of time, and in any case within three (3) weeks after receipt of the respective complaint, request or enquiry. Processor shall in any event cooperate with Controller to address and resolve any complaints, requests or enquiries from Individuals. Processor shall establish and maintain procedures to enable compliance with those complaints, requests or enquiries from Individuals.

10 Notification of non-compliance and right to suspend or terminate

10.1 Processor shall promptly notify Controller if Processor:

(i) cannot for any reason comply with its obligations under the DPA; or
(ii) becomes aware of any circumstance or change in Applicable Data Processor Law that is likely to have a substantial adverse effect on Processor's ability to meet its obligations under the DPA.

10.2 Without prejudice of the termination rights included in the Agreement, Controller is entitled to temporarily suspend the Processing in whole or in part if Processor is unable to meet its obligations under the DPA until such time that the non-compliance is remedied. To the extent such remedy is not available, Controller is entitled to terminate the relevant part of the Processing with immediate effect. Controller is also entitled to terminate the Agreement with immediate effect if suspension of the Processing by Controller pursuant to this provision exceeds a period of six (6) calendar months.

11 Return and destruction of Personal Data

11.1 All Personal Data shall be immediately returned to Controller upon Controller’s first request. Processor shall not retain Personal Data any longer than necessary for the purposes of performing its obligations under the Agreement.

11.2 Upon termination of the Agreement, Processor shall, at the option of Controller, return the Personal Data and copies and back-ups thereof to Controller and/or shall securely destroy such Personal Data, except to the extent the Agreement or Applicable Processor Law provides otherwise. In that case, Processor shall no longer Process the Personal Data, except to the extent required by the Agreement or Applicable Data Processor Law. Controller may require Processor to promptly, in any case within two (2) business days, confirm and warrant that Processor has returned, deleted and/or destroyed all copies of Personal Data. Processor shall, at the request of Controller, allow its Processing facilities to be audited to verify that Processor has complied with its obligations under this Clause **11.2**.

12 Insurance

12.1 It is agreed that Controller shall maintain sufficient insurance coverage, at its own cost, to the benefit of the Processor, so that Processor's obligation to reimburse audit costs under Section 6.1 shall be properly insured.

13 International Data Transfer

13.1 Personal Data shall not be Transferred to Supplier or a Sub-Processor in a Non-Adequate Country without the prior written approval of Controller.

13.2 If a Transfer of Personal Data to Supplier or a Sub-Processor in a Non-Adequate Country is approved by Controller, such Transfer shall only be permitted if the Transfer is subject to the EC Standard Contractual Clauses (SCC).

14 Transfers from the United Kingdom.

14.1 Where the transfer of personal data is subject to the UK Data Protection Laws as defined in the UK 2021 SCCs Addendum, the parties agree:

(a) The provisions of the UK 2021 SCCs Addendum, including Part 2 'Mandatory Clauses', shall apply in full;
(b) For the purposes of Table 1 of the UK 2021 SCCs Addendum, the names of the parties, their roles and their details shall be as set out in Section 5.e above;
(c) For the purposes of Tables 2 and 3 of the UK 2021 SCCs Addendum, Module 2 of the 2021 SCCs, including the information as set out in the Annex to the SCCs below, shall apply; and
(d) For the purposes of Table 4 of the UK 2021 SCCs Addendum, neither party may end the UK 2021 SCCs Addendum.
(e) Notwithstanding the foregoing, the UK 2021 SCCs Addendum will not apply to a transfer to a country that is outside the United Kingdom and is subject to the UK's adequacy regulations.

15 Obligation to renegotiate arrangements

15.1 Periodically the Parties shall evaluate the Processing by Processor. Processor shall promptly inform Controller of any relevant circumstances, including, but not limited to:

(a) material changes in the Processing services of Processor or any of its Sub-Processors;
(b) lessons learned from any Personal Data Breaches.

16 Notices

16.1 All notices, confirmations and other statements made by the Parties in connection with this DPA shall be in writing and via e-mail to:

Controller: [redacted]

Processor: [name, address, email]

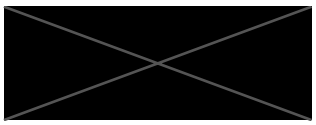
Personal Data Breaches as described in article **8.1c** need also to be notified to [redacted] with subject line: ''POTENTIAL DATA BREACH''.

17 Governing law

17.1 This Agreement is subject to the same laws and jurisdiction as the Agreement

18 Signing

18.1 As agreed by Controller and Processor:

Date:	……..	
	Controller	Processor
Organisation	Ruby Central, Inc.	……
Name:		……
Function:		……
Signature:	……	……

Appendix A: Definitions

"**Applicable Data Processor Law**"	means the Data Protection Laws that are applicable to Processor as a processor of Personal Data.
"**Applicable Data Protection Law**"	means the Data Protection Laws applicable to Controller as the Controller.
"**Data Protection Law**"	means the GDPR and all laws and regulations and sectoral recommendations containing rules for the protection of individuals with regard to the Processing, including without limitation security requirements for and the free movement of Personal Data.
"**Personal Data Breach**"	means the unauthorized acquisition, access, use or Disclosure of Personal Data as specified in Applicable Data Protection Law.
Disclosure"	means any form of disclosure of Personal Data to (including remote access by) any Employee or any Third Party. "**Disclose**" and "**Disclosed**" are to be construed accordingly.
"**EEA**"	means all member states of the European Union, Norway, Iceland, Liechtenstein and, for the purposes of the Annex, Switzerland.
"**Employee**"	means any employee, agent, contractor, work-for-hire or any other person working under the direct authority of Processor.
"**GDPR**"	means Regulation 2016/679/EU on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
"**Individual**"	means any individual whose Personal Data are Processed by Processor in the course of the performance of the Agreement.
"**International Data Transfer**"	means transfer of Personal Data that is subject to transfer restrictions under the Data Protection Laws from the Controller contracting entity (the "**Data Exporter**") to the vendor (the "**Data Importer**") which is located in a Non-Adequate Country
"**Non-Adequate Country**"	means a country that is deemed not to provide an adequate level of protection of Personal Data as defined in Applicable Data Protection Law.
"**Personal Data**"	means any information relating to an identified or identifiable individual as specified in Applicable Data Protection Law.
"**Processing**"	means any operation that is performed on Personal Data, whether or not by automated means, such as collection, recording, storage, organization, alteration, use, disclosure (including the granting of remote access), transmission or deletion of Personal Data as specified in Applicable Data Protection Law. "**Process**" and "**Processed**" are to be construed accordingly.
"SCCs"	means the Standard Contractual Clauses (2021/914/EU) as approved in July 2021 by the European Commission
"**Sub-Processor**"	means any Third Party that Processes Personal Data under the instruction or supervision of Processor but that does not fall under the direct authority of Processor.
"**Third Party**"	means any party other than the Parties to the Agreement;

"**UK 2021 SCCs Addendum**"	means UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, Version B1.0, in force from March 21, 2022.

Appendix B: List of approved Sub-Processors

Sub-Processor (Name, legal entity, place of business)	Location of Processing	Description of Processing
None		

Appendix C: Description of Processing

Service	Description
Type of data	The categories of Personal Data Processed by the Processor are: - Registration information - Web traffic information - Gem data and metadata
Group of data subjects	The categories Individuals whose Personal Data are being Processed by the Processor are: - Website users
Nature, type and purpose of the Processing	- Collection of personal data - Recording of web traffic