DATA PROCESSING ADDENDUM

Last Updated: **19 March 2026**

THIS DATA PROCESSING ADDENDUM ("DPA") is entered into, as of the date that the Agreement (as defined below) is entered into, between Runa and the Buyer, whom are Parties to the Agreement, into which this DPA is incorporated and forms a part. Any undefined terms shall have the meaning ascribed to them in the Agreement.

1. **Applicability**

General Applicability: Where Buyer is not subject to the GDPR, CCPA, or similar DP Laws in its delegation of Processing to Company under the Agreement, this DPA shall apply only to the extent necessary for Company to comply with its obligations under the GDPR, CCPA or similar DP Law.

CCPA Applicability: Annex 3 (California Terms) shall apply only if and to the extent that Company's Processing of Buyer Personal Data is subject to the CCPA and Buyer is a "business" or "service provider" as defined in the CCPA.

2. **Runa Obligations When Acting as a Data Processor**

Obligations: When Runa is acting as a Data Processor for Buyer, Runa will, to the extent required by applicable DP Law:

Processing Activities - Runa shall not Process Buyer Personal Data other than on Buyer's instructions or as required by applicable laws. Buyer instructs Company to Process Buyer Personal Data as necessary to provide the Services to Buyer under and in accordance with the Agreement. Where Company receives an instruction from Buyer that, in its reasonable opinion, infringes the GDPR, Company shall inform Buyer. The Parties acknowledge and agree that the details of Runa's Processing of Personal Data under this DPA and the Agreement (including the respective roles of the Parties relating to such Processing) are as set out in Annex 1 (Data Processing Details) to the DPA.

Runa Personnel Confidentiality - Runa shall take commercially reasonable steps to ascertain the reliability of any Runa Personnel (employees, agents, consultants or contractors) who Process Buyer Personal Data, and shall enter into written confidentiality agreements with all such persons who Process Buyer Personal Data that are not subject to professional or statutory obligations of confidentiality.

Data Subject Request - Runa shall inform Buyer of each request it receives from Data Subjects (including "verifiable consumer requests) exercising their rights under DP Law to (i) access (e.g, right to know) their Personal Data; (ii) have their Personal Data corrected or erased; (iii) restrict or object to Runa's Processing; or (iv) data portability (collectively, "Data Subject Request"). Other than to request further information, identify the Data Subject, and, if applicable, direct the Data Subject to Buyer as Data Controller, Runa will not respond to these requests unless Buyer so instructs in writing.

Reasonable Assistance - Runa will provide Buyer will reasonable assistance, following Buyer's written request, to help Buyer comply with its obligations under DP Law and, taking into account the nature of the Processing and the information available to Runa, Runa shall provide reasonable assistance to Buyer with any data protection impact assessments and prior consultations with Supervisory Authorities which Buyer reasonably considers to be required of it by Article 35 or Article 36 of the GDPR, in each case solely in relation to Processing of Buyer Personal Data by Company. Unless prohibited by law, Runa may charge Buyer a reasonable fee at Runa's then-applicable professional services rates.

Personal Data Breach Assistance - Runa shall notify Buyer without undue delay upon Company's discovering a Personal Data Breach affecting Buyer Personal Data; provide Buyer with information (insofar as such information is within Runa's possession and knowledge and does not otherwise compromise the security of any Personal Data Processed by Runa) to allow Buyer to meet its obligations under the Applicable Data Protection Laws to report the Personal Data Breach; and reasonably co-operate with Buyer and take such commercially reasonable steps as may be directed by Buyer to assist in the investigation of any such Personal Data Breach.

Data Security - Runa shall implement and maintain technical and organisational measures in relation to Buyer Personal Data designed to protect Buyer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access as described in Annex 2 (Security Measures) (the "Security Measures"). Runa may update the Security Measures from time to time, provided the updated measures do not materially decrease the overall protection of Buyer Personal Data.

Return or Deletion - (a) Subject to sub-paragraphs b, c and d, upon the date of cessation of any Services involving the Processing of Buyer Personal Data (the "Cessation Date"), Runa shall promptly cease all Processing of Buyer Personal Data for any purpose other than for storage or as otherwise permitted or required under this DPA. (b) Subject to sub-paragraph d, to the extent technically possible in the circumstances (as determined in Runa's sole discretion), on written request to Runa (to be made no later than fourteen (14) days after the Cessation Date ("Post-cessation Storage Period")), Runa shall within thirty (30) days of such request: (i) return a complete copy of all Buyer Personal Data within Company's possession to Buyer by secure file transfer, promptly following which Company shall delete or irreversibly anonymise all other copies of such Buyer Personal Data; or (ii) either (at its option) delete or irreversibly anonymise all Buyer Personal Data within Company's possession. (c) In the event that during the Post-cessation Storage Period, Buyer does not instruct Runa in writing to either delete or return Buyer Personal Data pursuant to sub-paragraph b, Runa shall promptly after the expiry of the Post-cessation Storage Period either (at its option) delete; or irreversibly render anonymous, all Buyer Personal Data then within Runa's possession to the fullest extent technically possible in the circumstances. (d) Runa may retain Buyer Personal Data where permitted or required by applicable law, or compliance requirements, for such period as may be required by such applicable law, provided that Runa shall: (i) maintain the confidentiality of all such Buyer Personal Data; and (ii) Process the Buyer Personal Data only as necessary for the purpose(s) specified in the applicable law permitting or requiring such retention.

Sub-Processors: Buyer generally authorises Runa to appoint Sub-Processors in accordance with this Section.

Runa may continue to use those Sub-Processors already engaged by Runa as of the date this DPA is entered into by the Parties (as those Sub-Processors are shown at https://runa.io/subprocessors (the "Sub-Processor List")).

Company shall update the Sub-Processor List. Buyer can register for notifications of any updates to the Sub-Processing List by submitting their details at the distribution list here - https://runa.io/subprocessors. Notices will be sent out 30 days before a new Sub-Processor is to be appointed. If, within fourteen (14) days of receipt of that notice, Buyer notifies Company in writing of any objections (on reasonable grounds) to the proposed appointment: (a) Company shall use reasonable efforts to make available a commercially reasonable change in the provision of the Services, which avoids the use of that proposed Sub-Processor; and (b) where: (i) such a change cannot be made within thirty (30) days from Company's receipt of Buyer's notice; (ii) no commercially reasonable change is available; and/or (iii) Buyer declines to bear the cost of the proposed change, then either Party may by written notice to the other Party with immediate effect terminate the Agreement, either in whole or to the extent that it relates to the Services which require the use of the proposed Sub-Processor, as its sole and exclusive remedy.

If Buyer does not object to Company's appointment of a Sub-Processor during the objection as provided above, Buyer shall be deemed to have approved the engagement and ongoing use of that Sub-Processor.

Runa shall maintain a written contract between Runa and each Sub-Processor that includes terms which offer at least an equivalent level of protection for Buyer Personal Data as those set out in this DPA (including the Security Measures). Runa shall remain liable for any breach of this DPA caused by a Sub-Processor.

DISCLAIMER OF LIABILITY: Notwithstanding anything to the contrary in the Agreement, including this DPA, Runa and its Affiliates will not be liable for any claim made by a Data Subject

arising from or related to Runa or any of its Affiliates' acts or omissions, to the extent that Runa was acting in accordance with User's Instructions.

3. Buyer Obligations When Runa Acting as a Data Controller

Obligations: When Runa is acting as a Data Processor for Buyer, and Buyer is acting as a Data Controller, Buyer will do the following:

Instructions: Buyer must only provide instructions to Runa that are lawful.

Compliance with DP Law: Buyer acknowledges and agrees that any instructions issued by Buyer with regards to the Processing of Buyer Personal Data by or on behalf of Company pursuant to or in connection with the Agreement shall be in strict compliance with the GDPR and all other applicable laws.

Disclosures: Buyer must provide all necessary notices (including by making available a Privacy Policy) to, and obtain all necessary rights, permissions and consents from, Data Subjects (including Digital Asset Recipients), to enable Runa to lawfully Process any Personal Data provided by User as described in the Agreement, including this DPA. User is solely responsible for the content of notices it provides to its Customers.

Personal Data Breach: If Buyer determines that a Personal Data Breach must be notified to any Supervisory Authority, any Data Subject(s), the public or others under Applicable Data Protection Laws, to the extent such notice directly or indirectly refers to or identifies Company, where permitted by applicable laws, Buyer agrees to: (a) notify Company in advance; and (b) in good faith, consult with Runa and consider any clarifications or corrections Runa may reasonably recommend or request to any such notification, which: (i) relate to Runa's involvement in or relevance to such Personal Data Breach; and (ii) are consistent with applicable laws.

Security Obligations: Buyer shall (a) make appropriate use of the Services to maintain a level of security appropriate to the risk in respect of the Buyer Personal Data; (b) secure the account authentication credentials, systems and devices (including the Buyer Platform) Buyer uses to access the Services; (c) secure Buyer's systems and devices that Company uses to provide the Services; and (d) back up Buyer Personal Data.

Provision of Data: Unless specifically requested by Runa, Buyer shall not provide or otherwise make available to Runa any Buyer Personal Data that contains any (a) Social Security numbers or other government-issued identification numbers; (b) protected health information subject to the Health Insurance Portability and Accountability Act (HIPAA) or other information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; (c) health insurance information; (d) biometric information; (e) passwords to any online accounts; (f) credentials to any financial accounts; (g) tax return data; (h) any payment card information subject to the Payment Card Industry Data Security Standard; (i) Personal Data of children under 13 years of age; or (j) any other information that falls within any special categories of personal data (as defined in GDPR) and/or data relating to criminal convictions and offences or related security measures.

4. Runa's Obligations When Runa Acting as a Data Controller

Runa must comply with and perform its obligations under DP Law when Processing Personal Data, including making available a Privacy Policy that explains how and for what purposes Runa collects, uses, retains, discloses and safeguards Personal Data.

5. Restricted Transfers

a. Buyer acknowledges and agrees that Company may effect Restricted Transfers to third parties under or in connection with this DPA, subject to the rest of this Section (including where Runa's use of a Sub-Processor involving a Restricted Transfer is approved in accordance with the Sub-Processor Section above).

b. Runa agrees that it shall not make any Restricted Transfer in connection with Runa's Processing of Buyer Personal Data as Buyer's Processor otherwise than in reliance on a 'transfer mechanism' under Chapter V of the GDPR for that Restricted Transfer, for which purpose Buyer agrees that Runa's entry into a UK Transfer Tool with the relevant 'importer' shall be sufficient in relation to any Restricted Transfer.

6. Audit Rights

a. Runa shall make available to Buyer on request, such information as Company (acting reasonably) considers appropriate in the circumstances to demonstrate its compliance with this DPA.

b. Subject to Sections 6(c) to 6(h), in the event that Buyer (acting reasonably) is able to provide documentary evidence that the information made available by Company pursuant to Section 6(a) is not sufficient in the circumstances to demonstrate Company's compliance with this DPA, Company shall allow for and contribute to audits, including on-premise inspections, by Buyer or an auditor mandated by Buyer in relation to the Processing of Buyer Personal Data by Company.

c. Buyer shall give Company reasonable notice of any audit or inspection to be conducted under Section 6(b) (which shall in no event be less than fourteen (14) days' notice) and shall use its best efforts (and ensure that each of its mandated auditors uses its best efforts) to avoid causing any destruction, damage, injury or disruption to Company's premises, equipment, Personnel, data, and business (including any interference with the confidentiality or security of the data of Company's other Buyers or the availability of Company's services to such other Buyers).

d. Prior to conducting any audit, Buyer must submit a detailed proposed audit plan providing for the confidential treatment of all information exchanged in connection with the audit and any reports regarding the results or findings thereof. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Company will review the proposed audit plan and provide Buyer with any concerns or questions (for example, any request for information that could compromise Company security, privacy, employment or other relevant policies). Company will work cooperatively with Buyer to agree on a final audit plan.

e. If the controls or measures to be assessed in the requested audit are addressed in a SOC 2 Type 2, ISO, NIST or similar audit report performed by a qualified third-party auditor within twelve (12) months of Buyer's audit request ("Audit Report") and Company has confirmed in writing that there are no known material changes in the controls audited and covered by such Audit Report(s), Buyer agrees to accept provision of such Audit Report(s) in lieu of requesting an audit of such controls or measures.

f. Company need not give access to its premises for the purposes of such an audit or inspection:
   i. where an Audit Report is accepted in lieu of such controls or measures in accordance with Section 6(e);
   ii. to any individual unless they produce reasonable evidence of their identity;
   iii. to any auditor whom Company has not approved in advance (acting reasonably);
   iv. to any individual who has not entered into a non-disclosure agreement with Company on terms acceptable to Company;
   v. outside normal business hours at those premises; or
   vi. on more than one occasion in any calendar year during the term of the Agreement, except for any audits or inspections which Buyer is required to carry out under the GDPR or by a Supervisory Authority.

g. Nothing in this DPA shall require Company to furnish more information about its Sub-Processors in connection with such audits than such Sub-Processors make generally available to their Buyers.

h. Except to the extent prohibited by applicable law, Buyer shall be fully responsible for all time spent by Company (at Company's then-current professional services rates) in Company's provision of any cooperation and assistance provided to Buyer under this Section (excluding any costs incurred in the procurement, preparation or delivery of Audit Reports to Buyer pursuant to Section 6(e)), and shall on demand reimburse Company any such costs incurred by Company.

7. Conflict

To the extent of any conflict between the provisions of this DPA and any provision of the:

(a) Agreement regarding Personal Data Processing, the provisions of this DPA will prevail; and
(b) Data Transfers Addendum, the provisions of the Data Transfers Addendum will prevail.

8. Liability

The total aggregate liability of either Party towards the other Party, howsoever arising, under or in connection with this DPA will under no circumstances exceed any limitations or caps on, and shall be subject to any exclusions of, liability and loss agreed by the Parties in the Agreement.

9. Change In Laws

Runa may on notice vary this DPA to the extent that (acting reasonably) it considers necessary to address the requirements of Applicable Data Protection Laws from time to time.

10. Definitions

In this DPA, the following terms shall have the meanings set out below:

"Addendum Effective Date" means the Commencement Date.

"Agreement" means the Digital Assets Supply Agreement entered into by and between the Parties.

"Authorized Services" means services that a Supervisory Authority licences, authorizes, or regulates.

"**DP Laws**" means any applicable privacy, data protection and data security laws and regulations of any jurisdiction applicable to the Processing of Buyer Personal Data under the Agreement, including, without limitation, the GDPR and CCPA.

"Buyer Personal Data" means any Personal Data Processed by Company or its Sub-Processors on behalf of Buyer to perform the Services under the Agreement (including, for the avoidance of doubt, any such Personal Data comprised within Buyer Data).

"CCPA" means the California Consumer Privacy Act of 2018, and any regulations promulgated thereunder, in each case, as amended from time to time.

"Data Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

"Data Subject Request" means the exercise by a Data Subject of its rights in accordance with DP Laws in respect of Buyer Personal Data and the Processing thereof.

"Data Subject" means the identified or identifiable natural person to whom Buyer Personal Data relates.

"GDPR" means, as and where applicable to Processing concerned: (i) the General Data Protection Regulation (Regulation (EU) 2016/679) ("EU GDPR"); and/or (ii) the EU GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018 (as amended, including by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019) ("UK GDPR"), including, in each case (i) and (ii) any applicable national implementing or supplementary legislation (e.g., the UK Data Protection Act 2018), and any successor, amendment or

re-enactment, to or of the foregoing. References to "Articles" and "Chapters" of, and other relevant defined terms in, the GDPR shall be construed accordingly.

"Personal Data" means "personal data," "personal information," "personally identifiable information" or similar term defined in DP Laws.

"Personal Data Breach" means a breach of Company's security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Buyer Personal Data in Company's possession, custody or control. For clarity, Personal Data Breach does not include unsuccessful attempts or activities that do not compromise the security of Buyer Personal Data (such as unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems).

"Process" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. **"Processed"** and **"Processing"** have corresponding meanings.

"Data Processor" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

"Restricted Transfer" means the disclosure, grant of access or other transfer of Buyer Personal Data by Company to a Sub-processor located in any country or territory outside the UK, which does not benefit from an adequacy decision from the UK Government.

"Services" means those services and activities to be supplied to or carried out by or on behalf of Company for Buyer pursuant to the Agreement.

"Sub-Processor" means any third party appointed by or on behalf of Company to Process Buyer Personal Data.

"Supervisory Authority" means (i) in the context of theEuropean Economic Area and the EU GDPR, the meaning given to that term in the EU GDPR; and (ii) in the context of the UK and the UK GDPR, the UK Information Commissioner's Office.

"UK Transfer Tool" means either (i) the template International Data Transfer Agreement version A.1.0; or (ii) the template International Data Transfer Addendum version B.1.0, in each case as issued by the UK Information Commissioner's Office and laid before the UK Parliament in accordance with s119A of the UK Data Protection Act 2018 on 2 February 2022 and in each case as revised under the relevant Mandatory Clauses thereof set out in Part 4 or Part 2 (respectively).

[REMAINDER OF PAGE INTENTIONALLY BLANK]

Annex 1
Data Processing Details

<table>
<tr><td>Categories of Data Subjects:</td><td colspan="2">Digital Asset Recipients.

Buyer’s Staff, such as: (a) Employees; (b) Non-Employee workers; (c) Directors; (d) Officers; (e) Advisers; and (f) Consultants

Each category includes current, past and prospective Data Subjects.</td></tr>
<tr><td>Categories of Personal Data:</td><td>Digital Asset Recipients:
Name,
surname,
email address,
phone number; and</td><td>Buyer’s Staff:
Name,
surname,
email address,
social security number (or similar number), and
date of birth.</td></tr>
<tr><td>Nature of the Processing:</td><td><u>Runa as a Data Processor:</u>

When Runa Processes Personal Data, it is acting as a Data Processors on behalf of Buyer, the Data Controller.</td><td><u>Runa as a Data Controller:</u>

When Runa Processes Personal Data as a Data Controller, Runa: (a) has the sole and exclusive authority to determine the purposes and means of Processing Personal Data it receives from or through Buyer; and (b) may engage a Runa Affiliate to act as a Data Processor to provide services other than Authorized Services.</td></tr>
<tr><td>Purpose of the Processing:</td><td><u>Runa as Data Processor:</u>

To (a) service the Runa Platform; and (b) provide, and provide access to, Runa’s products and services.</td><td><u>Runa as Data Controller:</u>
When providing Runa products and services, to (a) determine and utilize third parties (banks and payment method providers); (b) monitor, prevent and detect fraudulent transactions and other fraudulent activity on the Runa platform; (c) monitor, prevent and mitigate financial loss, security risks, and other harm; (d) implement, maintain and perform internal processes that enable Runa to provide its products and services, including relationship management, billing and invoicing; (e) comply with Law, including applicable anti-money laundering screening, and know-your-customer obligations, and Supervisory Authority requests; and (f) analyze, improve and develop Runa’s products and services.</td></tr>
<tr><td>Duration of Processing / Retention Period:</td><td colspan="2">For the Term and any period required to perform a party’s post-termination obligations, except as required to comply with legal/regulatory obligations.</td></tr>
<tr><td>Transfers to (sub-)processors:</td><td colspan="2">Transfers to Sub-Processors are as, and for the purposes, described from time to time in the Sub-Processor List (as may be updated from time to time in accordance with Section 2(b)).</td></tr>
</table>

Annex 2
Security Measures

As from the Addendum Effective Date, Company will implement and maintain the Security Measures as set out in this Annex 2.

1. Organisational management and dedicated staff responsible for the development, implementation and maintenance of Company's information security program.

2. Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Company's organisation, monitoring and maintaining compliance with Company's policies and procedures, and reporting the condition of its information security and compliance to internal senior management.

3. Data security controls which include at a minimum logical segregation of data, restricted (e.g. role-based) access and monitoring, and utilisation of commercially available and industry standard encryption technologies for Buyer Personal Data.

4. Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions.

5. Password controls designed to manage and control password strength, expiration and usage.

6. System audit or event logging and related monitoring procedures to proactively record user access and system activity.

7. Physical and environmental security of data centres, server room facilities and other areas containing Buyer Personal Data designed to protect information assets from unauthorised physical access or damage.

8. Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from Company's possession.

9. Change management procedures and tracking mechanisms designed to test, approve and monitor all material changes to Company's technology and information assets.

10. Incident management procedures designed to allow Company to investigate, respond to, mitigate and notify of events related to Company's technology and information assets.

11. Network security controls that provide for the use of enterprise firewalls and intrusion detection systems designed to protect systems from intrusion and limit the scope of any successful attack.

12. Vulnerability assessment and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.

13. Business resiliency/continuity and disaster recovery procedures designed and tested to maintain service and/or recovery from foreseeable emergency situations or disasters.

Annex 3
California Terms

1. For purposes of this Annex 3, the terms “business,” “commercial purpose,” “sell” and “service provider” shall have the respective meanings given thereto in the CCPA, and “personal information” shall mean Buyer Personal Data that constitutes personal information governed by the CCPA.

2. Company shall not (a) sell any personal information; (b) retain, use or disclose any personal information for any purpose other than for the specific purpose of providing the Services, including retaining, using, or disclosing the personal information for a commercial purpose other than provision of the Services; or (c) retain, use or disclose the personal information outside of the direct business relationship between Company and Buyer. Company hereby certifies that it understands its obligations under this Section 2 of Annex 3 to the DPA and will comply with them.

3. It is the Parties’ intent that with respect to any personal information, Company is a service provider.

4. Provision of the Services encompasses the Processing authorized by Buyer’s instructions under Section 2 of the DPA. The Parties acknowledge that Company’s retention, use and disclosure of personal information authorized by Buyer’s instructions are integral to Company’s provision of the Services and the business relationship between the Parties.

5. Notwithstanding anything in the Agreement or DPA or any order form entered in connection therewith to the contrary, the Parties acknowledge and agree that Company’s access to personal information does not constitute part of the consideration exchanged by the Parties in respect of the Agreement.