LIMELEDGER

DATA PROCESSING AGREEMENT

Rev. June 2026

This Data Processing Agreement (the "DPA") is made by and between _____ ("Client") and the LimeLedger entity identified on the applicable Order Schedule or Statement of Work - being LimeLedger Pty Ltd (ABN 96 696 961 565) for engagements in Australia, LimeLedger Ltd for engagements in Kenya, or such other related entity of the LimeLedger group as identified on the applicable Order Schedule or SOW (in each case referred to as "LimeLedger") - and entered into on [INSERT DATE].

This DPA forms part of the written agreement(s) between Client and LimeLedger in connection with and in consideration of the provision of Services by LimeLedger to Client (collectively, the "Agreement"). This DPA is governed by the terms of the Agreement. In the event of a direct conflict between this DPA and the Agreement, the provisions of this DPA shall prevail with respect to the subject matter herein. Each LimeLedger entity that issues an Order Schedule or SOW pursuant to this Agreement does so as a separate and independent legal entity, and no other LimeLedger entity shall have any liability for the acts or omissions of another LimeLedger entity. Client and LimeLedger may be referred to individually as a "Party" and collectively as the "Parties."

By signing below, Client enters into this DPA on behalf of itself and, to the extent required under Data Protection Laws, in the name and on behalf of its Authorised Affiliates, if and to the extent LimeLedger processes Personal Data for which such Authorised Affiliates qualify as the Controller. For the purposes of this DPA only, and except where indicated otherwise, the term "Client" shall include Client and Authorised Affiliates. All capitalised terms not defined herein shall have the meaning set forth in the Agreement.

1. Definitions

1.1 "Affiliate" means any legal entity that directly or indirectly Controls, is Controlled by, or is under common Control with the subject entity.

1.2 "Authorised Affiliate" means Client's Affiliate which (a) is subject to Data Protection Laws, and (b) is permitted to use the Services pursuant to the Agreement between Client and LimeLedger.

1.3 "Control" means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity (and "Controls" and "Controlled by" shall be construed accordingly).

1.4 "Controller" has the same meaning as set forth in the applicable Data Protection Laws, being an entity that determines the purposes and means of processing Personal Data (or equivalent concept under applicable law).

1.5 "Data Protection Laws" means any local, state, or international laws and regulations, as amended from time to time, applicable to the Processing of Personal Data in the provision of Services. This includes, without limitation: (a) the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs) for engagements involving personal information of individuals located in Australia; (b) the Kenya Data

Protection Act 2019 for engagements involving personal data of individuals located in Kenya; (c) the General Data Protection Regulation (EU) 2016/679 and the UK GDPR, together with applicable EEA Member State or UK implementing legislation, to the extent applicable to transfers or processing of personal data of individuals located in the EU or UK (collectively, GDPR); and (d) any other applicable data protection or privacy legislation of the jurisdiction in which the relevant LimeLedger entity operates or in which Client's data subjects are located. Client acknowledges and agrees it is responsible for informing LimeLedger of any specific Data Protection Laws applicable to the Processing of Personal Data hereunder.

1.6 "Data Subject" has the same meaning as set forth in Data Protection Laws, being the identified or identifiable natural person to whom the Personal Data relates (or equivalent concept, such as "individual" under the Privacy Act 1988 (Cth)).

1.7 "Personal Data" has the same meaning as set forth in the applicable Data Protection Laws, limited to data LimeLedger is Processing on behalf of the Client as part of the Services. This includes "personal information" as defined in the Privacy Act 1988 (Cth) and equivalent terms under other applicable Data Protection Laws.

1.8 "Processor," "Process," "Processed," or "Processing" have the same meaning as set forth in the applicable Data Protection Laws (or equivalent concepts such as "handling personal information" under the Privacy Act 1988 (Cth)).

1.9 "Security Incident" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to Personal Data in LimeLedger's custody or control, and includes an "eligible data breach" as defined in the Privacy Act 1988 (Cth) and a "personal data breach" as defined in the GDPR.

1.10 "Services" means the services provided by LimeLedger that are described in the Agreement.

2. Applicability; Processing of Personal Data

2.1 This DPA shall apply to the extent LimeLedger processes Personal Data in relation to LimeLedger's performance of Services pursuant to the Agreement, and where such Processing is regulated under Data Protection Laws.

2.2 Client, as Controller, appoints LimeLedger as a Processor to Process the Personal Data on Client's behalf; provided, however, that where Client acts as a Processor of the Personal Data, LimeLedger is a subprocessor. LimeLedger and its related entities are service providers processing personal information on behalf of Client.

2.3 Each Party will comply with the obligations that apply to it under Data Protection Laws and will notify the other Party if it determines it can no longer meet these obligations.

3. Services

3.1 As part of its Services for Client, LimeLedger shall Process Personal Data in relation to the categories of Data Subjects outlined in Annex I.

3.2 Client's ordering of specific Services with respect to any entities and individuals shall be based on this DPA and the then-current description of such Services, which, together, shall constitute Client's documented instructions to LimeLedger regarding the Processing of any Personal Data associated with such order. Client may supplement such instructions with other documented instructions.

4. Obligations of LimeLedger as Processor

4.1 LimeLedger agrees that, to the extent LimeLedger Processes Personal Data:

4.1.1 it shall Process the Personal Data in accordance with the lawful, documented instructions of Client and for the specific purposes detailed in the applicable Agreement and as set forth in Annex I of this DPA;

4.1.2 it shall not, unless otherwise permitted under Data Protection Laws: (i) use Personal Data for any purpose other than for the specific purpose as specified in the Agreement; (ii) retain, use, or disclose the Personal Data outside the direct business relationship between the Parties; or (iii) combine the Personal Data with personal information LimeLedger receives from, or on behalf of, another person, or that LimeLedger collects from its own interaction with the Data Subject, except as required to perform the Services;

4.1.3 it shall hold the Personal Data in confidence and shall require any person it authorises to Process the Personal Data to be subject to a strict duty of confidentiality;

4.1.4 it shall implement and maintain appropriate technical and organisational measures designed to protect the Personal Data from a Security Incident, including the measures described in Annex II to this DPA;

4.1.5 it shall provide Client with reasonable and timely cooperation and assistance, at Client's expense, to allow Client to respond to: (i) any request from a Data Subject to exercise any of its rights under Data Protection Laws (including rights of access, correction, deletion, and data portability); and (ii) any other correspondence, inquiry or complaint received from a Data Subject or regulator in connection with LimeLedger's Processing of Client Personal Data. In the event any such request, correspondence, inquiry or complaint is made directly to LimeLedger, LimeLedger shall, to the extent legally permitted and without undue delay, inform Client. LimeLedger shall not be obligated to respond directly to a Data Subject regarding a Data Subject request except as required by applicable laws;

4.1.6 it shall assist Client in its compliance with applicable obligations to the extent required under Data Protection Laws;

4.1.7 it shall, at Client's written request: (i) return to Client, or securely destroy or permanently erase (and upon request certify in writing such secure destruction or erasure) all Personal Data in its possession or control. This requirement shall not apply to the extent LimeLedger is required by applicable law or recordkeeping policy to retain some or all of the Personal Data, in which event LimeLedger shall protect the Personal Data from any further Processing except to the extent required by such applicable law or recordkeeping policy. LimeLedger will not be obligated to erase Personal Data contained in an archived computer system backup made in accordance with LimeLedger's security or disaster recovery procedures, provided such archived copy will: (a) eventually be erased or destroyed

in the ordinary course of LimeLedger's data processing procedures; and (b) remain fully subject to the obligations of confidentiality stated herein, until the erasure or destruction of such copy;

4.1.8 it shall, if and to the extent required under Data Protection Laws, upon written request by Client and execution of LimeLedger's confidentiality agreement, make available to Client: (i) information necessary to demonstrate compliance with LimeLedger's obligations in this DPA; and (ii) allow for and assist with annual audits, including inspections, conducted by Client or another auditor retained by it (bound by a duty of confidentiality and reasonably approved by LimeLedger); provided however that in lieu of such audit, Client shall accept completion of a due diligence questionnaire on an annual basis which is related to technical and operational testing of the systems used to provide the Services. Any audit will be: (a) conducted during LimeLedger's regular business hours; (b) with thirty (30) days' advance notice to LimeLedger; (c) conducted not more than once every twelve (12) months; (d) carried out in a manner that prevents unnecessary disruption to LimeLedger's operations; and (e) subject to reasonable confidentiality procedures. The Parties will agree on the scope of the audit in advance, and Client will pay LimeLedger's reasonable out-of-pocket costs to assist Client in the audit;

4.1.9 it shall inform Client, without undue delay if, in its opinion, it receives an instruction from Client which infringes Data Protection Laws;

4.1.10 it shall grant Client the right, upon notice, to take reasonable and appropriate steps to stop and remediate LimeLedger's unauthorised use of Personal Data;

4.1.11 it shall notify Client without undue delay upon becoming aware of a Security Incident and provide Client with information, cooperation and assistance as Client may commercially reasonably request to comply with its data breach reporting obligations under Data Protection Laws. LimeLedger shall further take commercially reasonable steps in LimeLedger's discretion to remedy or mitigate the effects of the Security Incident;

4.1.12 upon Client's written request and to the extent Data Protection Laws require Client to perform a data impact assessment or prior consultation with a data regulator, LimeLedger will provide Client with commercially reasonable information as is generally available with respect to the Services.

4.2 Client hereby grants a general written authorisation for LimeLedger to engage another processor (a "Subprocessor") without Client's prior specific authorisation, including but not limited to LimeLedger's related entities and LimeLedger's applicable third-party IT providers.

4.3 LimeLedger may continue to use Subprocessors engaged as of the effective date of this DPA, subject to compliance with LimeLedger's obligations under the Agreement and Data Protection Laws.

4.4 Subprocessors shall be bound by a written agreement requiring the Subprocessor to adhere to applicable Data Protection Laws. All transfers of Personal Data from LimeLedger to a Subprocessor shall be done in accordance with an approved transfer mechanism, including where required the Standard Contractual Clauses or other safeguards as described in Appendix II.

5. Notification Obligations of LimeLedger

5.1 LimeLedger shall notify Client promptly if at any point LimeLedger determines it cannot meet or has not met its obligations to Client within this DPA.

6. Obligations of Client as Controller

6.1 Client will ensure it has obtained or will obtain all necessary Data Subject consents, and has provided or will provide the necessary notifications, to the extent required by Data Protection Laws.

6.2 Client shall be responsible for ensuring that, in connection with Client's Personal Data and the Services: (a) it has complied, and will continue to comply, with all applicable laws, rules and regulations, including but not limited to all Data Protection Laws; and (b) it has, and will continue to have, the right to disclose, transfer, or provide access to, the Personal Data to LimeLedger for Processing in accordance with the terms of the Agreement and this DPA.

7. Recordkeeping

7.1 Both Parties agree that this DPA, together with Annex I, constitutes a record of the processing activities that LimeLedger is required to maintain under applicable Data Protection Laws with regard to processing activities carried out on behalf of Client.

8. General Terms

8.1 LimeLedger may share Personal Data with affiliated entities and subcontractors which may require cross-border transfer. Any such transfer will be conducted in accordance with Data Protection Laws, including the overseas disclosure requirements of the Privacy Act 1988 (Cth) (APP 8) where applicable, and under compliant methods of transfer as further described in Appendix II.

8.2 This DPA is governed and interpreted pursuant to the laws of the jurisdiction set forth in the Agreement, and any claim arising out of this DPA will be resolved pursuant to the dispute resolution provisions set forth in the Agreement.

8.3 If any part of the DPA is found to be unlawful, void, or unenforceable, that part will be deemed severable and will not affect the validity and enforceability of the remaining provisions.

8.4 Upon written agreement by both Parties, this DPA may be amended as required to comply with updates to Data Protection Laws.

IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Agreement with effect from the date first set out above.

CLIENT

Company Name: _____
ABN / ACN: _____
Signature: _____
Print Name: _____
Title: _____
Date: _____

LIMELEDGER

(Insert contracting entity name and registration number as identified on the applicable Order Schedule or SOW)

Entity: _____
Signature: _____
Print Name: _____
Title: _____
Date: _____

APPENDIX I

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer Controller to Processor

Data exporter (Client):

Name: The entity identified as "Client" in the DPA and Agreement

Address: The address for Client as specified in the DPA or the Agreement

Contact: The contact details associated with Client's account or engagement, or as otherwise specified in the DPA or the Agreement

Activities: The Services specified in the Agreement and any applicable Statement of Work

Signature and date: _____

Role: Controller

Data importer (LimeLedger):

Name: The LimeLedger entity identified on the applicable Order Schedule or SOW

Address: As identified on the applicable Order Schedule or SOW

Contact: info@limeledger.com.au

Activities: The Services specified in the Agreement

Signature and date: [INSERT SIGNATURE OF ENGAGEMENT LEAD]

Role: Processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer Controller to Processor

Categories of Data Subjects:

The Data Subjects could include Client's or Client's clients' employees, representatives, customers, clients, and vendor representatives.

Categories of Personal Data transferred:

The personal data could include personal details and financial information of Client's employees, customers, and suppliers, including name, address, contact information, employment data, income/salary, and other information associated with HR records (including various personally identifiable information of Client employees).

Sensitive data transferred (if applicable):

N/A. Client will not transfer sensitive information (as defined under the Privacy Act 1988 (Cth)) without a separate written agreement specifying the applicable safeguards.

Frequency of transfer:

Personal data is transferred in accordance with Client's instructions as described in the DPA.

Nature of the Processing:

The Services specified in the Agreement.

Purpose(s) of the data transfer and further Processing:

To provide the Services.

Retention period:

Personal data will be retained in accordance with LimeLedger's records retention policies and in accordance with any applicable Agreement with Client.

For transfers to Subprocessors:

The subject matter and nature of the processing are described in the Agreement and the DPA. As between LimeLedger, any subprocessors and the Client, the duration of the data processing is determined by Client.

C. COMPETENT SUPERVISORY AUTHORITY

Where Data Protection Laws require notification of, or engagement with, a supervisory authority or regulator, the relevant authority will be determined by the applicable Data Protection Laws and the jurisdiction of the data exporter. For Australian personal information, this is the Office of the Australian Information Commissioner (OAIC). For EU/EEA personal data, this is the data exporter's competent supervisory authority under the GDPR. For Kenyan personal data, this is the Office of the Data Protection Commissioner (ODPC).

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES

LimeLedger is responsible for and will comply with the following technical and organisational measures for the security of personal data:

Data Centres and Architecture Availability

LimeLedger utilises third-party cloud infrastructure and hosting services. Those providers restrict physical access to facilities and protected information assets to authorised personnel and have controls in place to ensure capacity and redundancy.

Business Process Continuity

LimeLedger has designed its technology environment to support continuity needs by reducing the impact of events resulting in unavailable locations or systems. Technology continuity controls include:

- Laptops issued to all team members to enable remote work from any location with internet connectivity
- VPN technology for secure remote access

- Cloud-based systems to reduce recovery time and facilitate security patch management

Security - Administrative Controls

- Background checks prior to hire where required by applicable law
- Comprehensive, documented IT security policy reviewed annually
- Security awareness program including new hire training and periodic security awareness communications
- Signed confidentiality and security agreements by all employees
- Independent contractors and subcontractors are required to sign contracts that include IT security standards and requirements prior to their start date
- Centralised change and patch management
- Business continuity plans evaluated and updated as needed
- Documented incident response plan with annual training for relevant personnel

Security - Network and Endpoint Security

- Industry standard firewalls
- Multi-layered intrusion prevention tools
- Anti-virus and endpoint protection software
- Network and host-based web-filtering tools
- Mobile device management (MDM) to enforce complex passwords and allow remote wiping of corporate data if a device is lost or stolen
- Internal and external vulnerability management programs

Security - Physical and Logical Access Security

- Access control for LimeLedger premises and network infrastructure
- Privileged account management for end user computers
- Secure authentication for all remote access using multi-factor authentication (MFA)
- Two-step authentication for all employees accessing cloud services

Security - Information Security

- Encryption for all laptops and portable storage devices carrying personal information
- 128-bit SSL (or higher) required for all remote access
- Policy-based and manual email encryption available to all employees
- Data deletion/destruction processes for Personal Data stored in electronic media, including remote laptop wiping capability
- Access to personal data limited to employees and subcontractors who need it to perform the Services

Appendix II - International Data Transfer Mechanisms

The following provisions apply to the extent the Services require a cross-border transfer of Personal Data.

1. Definitions

For this Appendix:

"Restricted Transfer" means a transfer of Personal Data to a country or recipient that requires a transfer safeguard under applicable Data Protection Laws.

"EU SCCs" means the standard contractual clauses in Commission Implementing Decision (EU) 2021/914, as amended or replaced.

"UK Addendum" means the International Data Transfer Addendum to the EU SCCs issued by the UK Information Commissioner under section 119A of the Data Protection Act 2018, as amended or replaced.

"UK IDTA" means the UK International Data Transfer Agreement issued by the UK Information Commissioner under section 119A of the Data Protection Act 2018, as amended or replaced.

"FADP" means the Swiss Federal Act on Data Protection.

2. Australian Cross-Border Transfers

For personal information subject to the Privacy Act 1988 (Cth), any transfer of personal information overseas by LimeLedger shall be conducted in accordance with APP 8. Before transferring personal information to an overseas recipient, LimeLedger will take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to that information, including by: (a) entering into a contractual arrangement with the overseas recipient requiring it to handle the personal information in accordance with the APPs; or (b) relying on another applicable exception under APP 8. Where LimeLedger relies on Client's consent under APP 8.2(b), LimeLedger will inform Client of the relevant overseas jurisdictions in advance.

3. EU/EEA Transfers

For Restricted Transfers subject to the EU GDPR, the EU SCCs are incorporated by reference and deemed executed at transfer commencement. They are completed as follows: (a) Modules 2 and 3 apply as the Parties' roles require (controller-to-processor and processor-to-processor or processor-to-subprocessor, respectively); (b) Clause 7 applies; (c) Clause 9(a), Option 2, applies, subject to this DPA's Subprocessor provisions; (d) the optional wording in Clause 11(a) does not apply; (e) the competent supervisory authority under Clause 13 and Annex I.C is determined in accordance with the EU SCCs and, if no authority is otherwise identified, is the Irish Data Protection Commission; (f) Clause 17, Option 1, and Clause 18 select Irish law and the courts of Ireland; and (g) Annexes I, II, and III are completed by this DPA, the Agreement, and their applicable schedules or appendices.

4. UK Transfers

For Restricted Transfers subject to UK Data Protection Laws, the UK Addendum is incorporated by reference and deemed executed at transfer commencement. For Part 1: Table 1 is completed by the Parties' details, signatures, and key contacts in this DPA, Appendix I, and the Agreement; Table 2 selects the EU SCCs above; Table 3 is completed by this DPA, Appendix I, and the Agreement; and Table 4 permits either Party to end the UK Addendum under Section 19. The UK Addendum's Mandatory Clauses amend the EU SCCs as required for UK law. If the UK Addendum is unavailable or insufficient for a UK Restricted Transfer, the UK IDTA applies instead, with its tables completed by the same information and its Mandatory Clauses incorporated by reference.

5. Swiss Transfers

For Restricted Transfers subject to the FADP, the EU SCCs apply with Swiss-law modifications: (a) GDPR references include the FADP; (b) EU, Union, EU Member State, and Member State references include Switzerland and do not limit enforcement rights in Switzerland; (c) the Swiss Federal Data Protection and

Information Commissioner is the competent supervisory authority; and (d) for transfers governed solely by the FADP, Clauses 17 and 18 select Swiss law and Swiss courts. For transfers subject to both the FADP and the EU GDPR, these modifications apply only to FADP-governed aspects and Section 3 above otherwise applies.

6. Kenyan Transfers

For transfers of personal data subject to the Kenya Data Protection Act 2019, LimeLedger will ensure that any transfer to a jurisdiction not recognised as providing adequate protection is conducted under an appropriate transfer safeguard, such as binding contractual provisions that impose equivalent obligations to those under the Kenya Data Protection Act 2019.

7. Conflicts; Replacement Mechanisms

If this DPA conflicts with the EU SCCs, UK Addendum, UK IDTA, or mandatory Data Protection Laws, those terms or laws prevail for the relevant Restricted Transfer and only to the extent of the conflict. If a transfer mechanism is invalidated, replaced, or becomes insufficient, the Parties will cooperate to implement a lawful alternative and will suspend the affected transfer if required by Data Protection Laws.