Data Processing Addendum

Version 1.0 — Effective April 1, 2026

This Data Processing Addendum ("**DPA**") forms part of the Master Services Agreement (the "**Agreement**") between **Aclymate, Inc.** ("**Aclymate**," "**Processor**," or "**we**") and the entity identified on the applicable Order Form ("**Customer**," "**Controller**," or "**you**"). Capitalized terms not defined in this DPA have the meanings given in the Agreement.

This DPA governs Aclymate's processing of Personal Data on Customer's behalf in connection with the Services. By executing an Order Form that incorporates the Agreement, or by accessing or using any Aclymate Service, Customer agrees to the terms of this DPA.

1. DEFINITIONS

"Applicable Privacy Law" means all laws and regulations applicable to the processing of Personal Data under this DPA, including, without limitation, the Colorado Privacy Act ("CPA") and any other applicable U.S. federal, state, or international data protection legislation.

"Controller" means the Party that determines the purposes and means of the Processing of Personal Data. For purposes of this DPA, Customer is the Controller with respect to Customer Personal Data.

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

"Personal Data" means any information processed on behalf of Customer that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with an identified or identifiable natural person. Personal Data includes, without limitation, names, email addresses, phone numbers, postal addresses, employment information, financial account data, transaction data, and any other information processed on behalf of Customer that constitutes "personal information" or "personal data" under Applicable Privacy Law.

"Processing" or "Process" means any operation or set of operations performed on Personal Data, including collecting, recording, organizing, structuring, storing, adapting, altering, retrieving, consulting, using, disclosing, disseminating, making available, aligning, combining, restricting, erasing, or destroying.

"Processor" means the Party that Processes Personal Data on behalf of the Controller. For purposes of this DPA, Aclymate is the Processor with respect to Customer Personal Data.

"Security Incident" means any confirmed accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to Personal Data Processed by Aclymate in connection with the Services.

"Sub-Processor" means any third party engaged by Aclymate to Process Personal Data on behalf of Customer.

---

2. SCOPE AND ROLES

2.1 Roles of the Parties

Customer is the Controller. Aclymate is the Processor. Aclymate Processes Customer Personal Data solely on behalf of, and under the documented instructions of, Customer.

2.2 Categories of Personal Data

Depending on Customer's use of the Services and the data Customer provides or makes available through Third-Party Integrations, Aclymate may Process the following categories of Personal Data:

- Contact information: Names, email addresses, phone numbers, mailing addresses of Customer employees and authorized contacts.
- Employment information: Job titles, departments, and employer identity.
- Utility and operational data: Utility account information, energy consumption data, and operational data relevant to emissions calculations.
- Travel and fleet data: Flight records, vehicle types, mileage logs, and corporate rideshare account data.
- Communications data: Personal Data and other information shared by Customer with Aclymate personnel via email or other communication

channels in connection with the Services (including the Turn Key Service).

2.3 Purposes of Processing

Aclymate Processes Personal Data solely for the following purposes in connection with the Services:

(a) Providing the Services described in the Agreement and the applicable Order Form, including carbon footprint calculation, emissions tracking, reporting, and carbon credit procurement;

(b) Performing Turn Key Service tasks on Customer's behalf, where applicable;

(c) Communicating with Customer regarding the Services;

(d) Maintaining, improving, and securing the Platform;

(e) Generating aggregated and anonymized data as permitted under Section 5.3 of the Agreement; and

(f) Complying with applicable legal obligations.

2.4 Duration of Processing

Aclymate will process Personal Data for the duration of the Agreement.

2.5 Customer Data Access Obligations

Customer acknowledges that the accuracy, completeness, and quality of the Services — including carbon footprint calculations, emissions reports, Scope 1, 2, and 3 analyses, and regulatory compliance deliverables — depend directly on the completeness of the data Customer provides or makes available through Third-Party Integrations. In particular:

(a) Certain Services (including Scope 3 emissions calculations) require

access to detailed financial transaction data, vendor spend data, and related operational records. If Customer restricts or withholds access to data categories necessary for the Services, Aclymate will notify Customer of the impact on deliverable accuracy and completeness, and Aclymate shall not be responsible for inaccuracies, gaps, or deficiencies in Deliverables that result from incomplete or restricted data access.

(b) Customer is responsible for ensuring that any data provided to Aclymate (whether through the Platform, Third-Party Integrations, or other channels) is lawfully collected and that Customer has the necessary rights and authorizations to share such data with Aclymate for the purposes described in this DPA.

(c) Aclymate will work with Customer in good faith to identify the minimum data necessary to deliver the contracted Services and will not request access to data beyond what is reasonably required.

---

3. DATA PROCESSING OBLIGATIONS

3.1 Processing Limitations

Aclymate will:

(a) Process Personal Data only for the purposes described in this DPA and the Agreement, and not for any other purpose without Customer's prior written consent;

(b) Process Personal Data in compliance with all Applicable Privacy Law;

(c) Not sell, rent, or otherwise transfer Personal Data to any third party for monetary or other valuable consideration;

(d) Not use Personal Data for profiling, targeted advertising, or any purpose

unrelated to the delivery of the Services; and

(e) Promptly notify Customer if Aclymate becomes aware that any processing instruction from Customer would violate Applicable Privacy Law.

3.2 AI and Machine Learning Processing

Where the Services utilize artificial intelligence or machine learning capabilities (including services provided by Anthropic/Claude), Aclymate will:

(a) Use such technologies solely to deliver and improve the Services on Customer's behalf;

(b) Not use Customer Personal Data to train general-purpose AI models that are not specific to Customer's account or the Services;

(c) Ensure that AI Sub-Processors are subject to the same data protection obligations as other Sub-Processors under Section 5 of this DPA; and

(d) Maintain transparency with Customer regarding which AI technologies are used in connection with the Services, as reflected in the Sub-Processor list.

3.3 Personnel Obligations

Aclymate will ensure that all personnel authorized to Process Personal Data:

(a) Are subject to obligations of confidentiality (whether by contract or statutory duty) with respect to such data;

(b) Have received appropriate training on data protection and handling procedures relevant to their role; and

(c) Access Personal Data only on a need-to-know basis to perform their assigned tasks.

3.4 Turn Key Service Personnel

In addition to the obligations in Section 3.3, Aclymate personnel providing the Turn Key Service:

(a) Will access Customer Personal Data solely through the Aclymate Platform and only as necessary to perform the Turn Key Service tasks described in the applicable Order Form;

(b) Will not download, copy, or transfer Customer Personal Data to personal devices, personal accounts, or unsecured systems;

(c) Will process any Customer Personal Data received via email or other communication channels outside the Platform with the same protections and limitations applicable to data accessed through the Platform; and

(d) Will be subject to periodic review by Aclymate management to confirm compliance with these obligations.

---

4. DATA SUBJECT OBLIGATIONS

4.1 Cooperation

Aclymate will provide reasonable assistance to Customer in fulfilling Customer's obligations to respond to Data Subject requests under Applicable Privacy Law, including requests to access, correct, delete, port, or restrict Processing of Personal Data, and requests to opt out of the sale or sharing of Personal Data.

4.2 Forwarding Requests

If Aclymate receives a Data Subject request directly that relates to Customer's Personal Data, Aclymate will promptly (and in any event within five (5) business days) forward such request to Customer and will not respond to the request directly without Customer's prior written authorization, except as

required by law.

4.3 Costs

Where Aclymate's assistance with Data Subject requests requires effort beyond what is routine and reasonable, Aclymate may charge Customer for such assistance at Aclymate's then-current professional services rates, provided Aclymate notifies Customer of estimated costs in advance.

---

5. SUB-PROCESSORS

5.1 General Authorization

Customer hereby provides general written authorization for Aclymate to engage Sub-Processors to Process Personal Data in connection with the Services, subject to the requirements of this Section 5.

5.2 Current Sub-Processors

As of the Effective Date, Aclymate uses the following Sub-Processors to process Personal Data:

Sub-Processsor	Purpose	Data Accessed	Location
Google Cloud / Firebase	Data storage, hosting, and platform infrastructure	All Customer Data stored on the Platform	United States

Stripe, Inc.	Payment processing	Transaction records and invoice data (Aclymate does not receive or store credit card or bank account numbers)	United States
Plaid, Inc.	Financial account connectivity	Financial transaction data accessed in read-only mode	United States
Intuit / QuickBooks	Accounting platform integration	Accounting and financial records accessed in read-only mode from Customer's connected QuickBooks account	United States
Twilio / SendGrid	Transactional email delivery	Customer contact information (name, email address) and email content	United States

Anthropic (Claude)	AI-powered data analysis, emissions calculations, integration development, and internal operational support	Customer Personal Data as necessary to deliver AI-assisted features of the Services; data is not used to train Anthropic's general models	United States
CNaught	Carbon offset procurement and retirement through integrated marketplace	Customer identity, offset purchase details, and emissions data necessary to facilitate offset transactions and retirement certificates	United States

Mixpanel	Data Analytics Services	Customer Personal Data as needed to deliver Data Analytics Services, including personal information such as geolocation, device ID, and internet activity.	The United States, the European Economic Area, and other countries and territories as identified in the Mixpanel DPA https://mixpanel.com/legal/dpa/

5.3 New Sub-Processors and Integration Partners

(a) Notification. Aclymate will maintain a current list of Sub-Processors at aclymate.com/sub-processors and will update this list at least fifteen (15) days prior to engaging any new Sub-Processor that will Process Customer Personal Data. Aclymate will provide notice of updates by email to Customer's designated contact or through the Platform.

(b) Customer Integrations. Where Customer connects new Third-Party Integrations through the Platform (e.g., additional financial, utility, or operational data sources), the third-party providers of such integrations will be treated as Sub-Processors to the extent they Process Personal Data on Customer's behalf through the Platform. Aclymate will ensure that all integration partners meet the requirements of Section 5.4 before making them available on the Platform. Customer's act of connecting a new integration constitutes consent to the addition of that provider as a

Sub-Processor.

(c) Objection Right. If Customer reasonably objects to a new Sub-Processor on legitimate data protection grounds, Customer will notify Aclymate in writing within fifteen (15) days of receiving notice. The Parties will discuss the concern in good faith. If the Parties cannot resolve the objection within thirty (30) days, Customer may terminate the affected Services (or the Agreement, if the Sub-Processor is integral to all Services) without early termination fee, and Aclymate will provide a pro-rata refund of prepaid Fees for the unused portion of the Term.

5.4 Sub-Processor Requirements

Aclymate will:

(a) Enter into a written agreement with each Sub-Processor imposing data protection obligations no less protective than those in this DPA;

(b) Conduct reasonable due diligence on each Sub-Processor's data protection practices before engagement; and

(c) Remain fully liable to Customer for the acts and omissions of its Sub-Processors to the same extent as if Aclymate had performed the processing itself.

5.5 Customer-Authorized Third-Party Consultants

From time to time, the Services may involve or benefit from the engagement of third-party consultants to support specialized work on Customer's behalf, such as regulatory compliance filings (e.g., SB 253, SBTi submissions), technical assessments, or advisory services (collectively, "Authorized Consultants"). Where Customer engages an Authorized Consultant directly (under a separate agreement between Customer and the Authorized Consultant), and such consultant requires access to Customer Data

processed through the Platform in order to perform their engagement:

(a) Customer will notify Aclymate in writing of the Authorized Consultant and the scope of data access required;

(b) Aclymate will provide the Authorized Consultant with access to Customer Data only as directed by Customer and limited to the scope identified by Customer;

(c) Customer is responsible for ensuring that the Authorized Consultant is bound by data protection obligations at least as protective as those in this DPA, whether through Customer's own agreement with the Authorized Consultant or otherwise; and

(d) Aclymate is not liable for the acts or omissions of Customer's Authorized Consultants with respect to Customer Data, except to the extent that a data incident is caused by Aclymate's own failure to limit access as directed by Customer.

For clarity, Authorized Consultants engaged directly by Customer are not Aclymate Sub-Processors. If Aclymate (rather than Customer) engages a consultant to perform work on Customer's behalf, such consultant will be treated as a Sub-Processor under Section 5.4.

---

6. SECURITY MEASURES

6.1 Technical and Organizational Measures

Aclymate will implement and maintain appropriate technical and organizational measures to protect Personal Data against unauthorized or unlawful Processing and against accidental loss, destruction, damage, alteration, or disclosure of Personal Data.

7. SECURITY INCIDENT RESPONSE

7.1 Incident Response Plan

Aclymate maintains a documented incident response plan and will promptly investigate any actual or suspected Security Incident.

7.2 Notification

In the event Aclymate becomes aware of a confirmed Security Incident, Aclymate will subject to applicable law notify Customer without undue delay, and in any event within forty-eight (48) hours of confirmation, providing at a minimum:

(a) A general description of the nature of the Security Incident, including, where known, the categories and approximate number of Data Subjects affected and the categories and approximate volume of Personal Data records affected;

(b) The name and contact information of a designated point of contact from whom additional information can be obtained;

(c) A description of the measures taken or proposed to address the Security Incident, including measures to mitigate its potential adverse effects.

7.3 Cooperation

Aclymate will cooperate with Customer in good faith in responding to any Security Incident, including with respect to any required regulatory notifications or communications to affected Data Subjects. Aclymate will provide timely updates as additional information becomes available.

7.4 Limitations

Aclymate's notification of a Security Incident does not constitute an acknowledgment of fault or liability. Aclymate is not responsible for Security Incidents caused by Customer's own systems, Authorized Users' actions or omissions, or Third-Party Integration providers' acts or omissions.

8. DATA RETENTION AND DELETION

8.1 Retention During the Term

Aclymate will retain Personal Data for the duration of the Agreement as necessary to provide the Services.

8.2 Post-Termination

Upon termination or expiration of the Agreement:

(a) Data Export. Customer will have sixty (60) days to export Customer Data including Personal Data from the Platform in standard formats (CSV, Excel, PDF, JSON), as set forth in Section 11.5 of the Agreement.

(b) Deletion from Production Systems. Following the data export period, Aclymate will delete Customer Data including Personal Data from production systems within sixty (60) days.

(c) Deletion from Backup Systems. Aclymate will use reasonable efforts to remove Customer Data including Personal Data from backup systems within one hundred eighty (180) days following termination.

(d) Certification. Upon Customer's written request, Aclymate will certify in writing that deletion has been completed.

8.3 Retention Exceptions

Notwithstanding Section 8.2, Aclymate may retain Personal Data to the extent:

(a) Required by Applicable Privacy Law, regulation, or legal obligation;

(b) Necessary to maintain legal documents, correspondence, and records needed to verify compliance with this DPA or the Agreement; or

(c) The data has been aggregated and anonymized in accordance with Section 5.3 of the Agreement, in which case it may be retained and used indefinitely.

All retained Personal Data (other than anonymized data) remains subject to the protections of this DPA.

---

9. CROSS-BORDER DATA TRANSFERS

9.1 Data Location

Aclymate stores and processes Customer Personal Data in the United States. As of the Effective Date, Aclymate does not transfer Personal Data outside the United States.

9.2 Future Transfers

Aclymate will not transfer Personal Data to a jurisdiction outside the United States without: (a) prior written notice to Customer; and (b) implementation of appropriate safeguards as required by Applicable Privacy Law, such as standard contractual clauses or other legally recognized transfer mechanisms.

---

10. AUDITS AND ASSESSMENTS

10.1 Information Requests

Upon Customer's reasonable written request (not more than once per calendar year, unless a Security Incident has occurred), Aclymate will provide Customer with:

(a) Relevant certifications, attestations, or completed security questionnaires demonstrating Aclymate's compliance with this DPA;

(b) A summary of Aclymate's most recent security assessment or penetration test results (with commercially sensitive details redacted); and

(c) Confirmation of current Sub-Processor compliance.

10.2 Audits

If the information provided under Section 10.1 is not reasonably sufficient to confirm Aclymate's compliance with this DPA, Customer may, upon at least fifteen (15) business days' prior written notice, conduct or commission a reasonable audit of Aclymate's data protection practices relevant to the Processing of Personal Data under this DPA, subject to the following:

(a) The audit will be conducted during normal business hours and will not unreasonably interfere with Aclymate's business operations;

(b) The audit will be at Customer's expense;

(c) The auditor will be subject to reasonable confidentiality obligations; and

(d) Audit scope will be limited to Aclymate's Processing of Customer Personal Data under this DPA.

10.3 Regulatory Inquiries

Aclymate will provide reasonable cooperation with Customer in responding to inquiries from data protection authorities regarding the Processing of

Personal Data under this DPA.

---

11. REPRESENTATIONS AND WARRANTIES

Each Party represents and warrants that:

(a) It has the legal authority to enter into this DPA and to Process Personal Data as contemplated herein;

(b) All Personal Data shared with the other Party has been collected in compliance with Applicable Privacy Law, including with valid notice to and, where required, consent of the relevant Data Subjects;

(c) It will promptly notify the other Party of any change in Applicable Privacy Law or regulatory guidance that materially affects either Party's obligations under this DPA; and

(d) It will Process Personal Data in compliance with all Applicable Privacy Law and in accordance with the terms of this DPA.

---

12. LIMITATION OF LIABILITY

12.1 Incorporation

The limitation of liability provisions in Section 10 of the Agreement apply to this DPA.

12.2 Indemnification

The indemnification provisions in Section 12 of the Agreement apply to this DPA. Aclymate's indemnification obligations cover claims arising from Aclymate's breach of this DPA, including claims arising from a Security

Incident directly caused by Aclymate's acts.

---

13. GENERAL

13.1 Conflict

In the event of any conflict between this DPA and the Agreement with respect to the Processing of Personal Data, this DPA controls.

13.2 Amendments

Aclymate may update this DPA from time to time to reflect changes in Applicable Privacy Law, regulatory guidance, or Aclymate's data processing practices. Material changes will be communicated to Customer with at least thirty (30) days' prior written notice, in accordance with Section 14.9 of the Agreement.

13.3 Governing Law

This DPA is governed by the same governing law and dispute resolution provisions as the Agreement (Section 14.1 and 14.2 of the Agreement — Colorado law, Denver courts).

13.4 Survival

The obligations of the Parties under Sections 3, 4, 6, 7, 8, and 13 of this DPA will survive termination or expiration of the Agreement for a period of two (2) years, or for the period required by Applicable Privacy Law, whichever is shorter.

ANNEX A: DETAILS OF PROCESSING

Element	Description
Subject Matter	Processing of Personal Data in connection with Aclymate's carbon accounting, emissions tracking, reporting, and Turn Key climate bookkeeping Services
Duration	For the Term of the Agreement, plus applicable retention periods
Nature and Purpose	Collection, storage, analysis, and reporting of business financial, operational, and utility data for carbon footprint calculation, emissions tracking, sustainability reporting, and carbon credit procurement
Categories of Data Subjects	Customer employees, authorized contacts, vendors, and third parties whose data is included in Customer's financial, operational, or utility records
Categories of Personal Data	Contact information, employment information, financial and transaction data, utility and operational data, travel and fleet data, and communications data (as detailed in Section 2.2)

Sensitive Data	Financial account data accessed through Third-Party Integrations (Plaid, QuickBooks/Intuit); processed in read-only mode with encryption and access controls
Controller	Customer
Processor	Aclymate, Inc.
Sub-Processors	As listed in Section 5.2 and at aclymate.com/sub-processors

---

This Data Processing Addendum is effective as of the Effective Date of the first Order Form executed by Customer, or the date Customer first accesses or uses any Aclymate Service, whichever occurs first.

[END OF DATA PROCESSING ADDENDUM]