SOLARACLOUD AI LLC

DATA PROCESSING AGREEMENT

Effective Date: March 5, 2026

Version 1.1

TABLE OF CONTENTS

1. INTRODUCTION AND SCOPE

1.1. This Data Processing Agreement (**"DPA"**) forms part of and is incorporated by reference into the Terms & Conditions (**"Agreement"**) between SolaraCloud AI LLC, a Florida limited liability company (**"SolaraCloud," "Processor," "we," "us," or "our"**), and the entity executing an Order Form for the SolaraCloud IMPACT platform (**"Client," "Controller," or "you"**).

1.2. This DPA applies to the extent that SolaraCloud processes Personal Data on behalf of the Client in the course of providing the SolaraCloud IMPACT platform and related services (**"Services"**) under the Agreement.

1.3. This DPA reflects the parties' agreement regarding the processing of Personal Data in compliance with applicable Data Protection Laws, including the European Union General Data Protection Regulation (EU 2016/679) (**"GDPR"**), the UK General Data Protection Regulation (**"UK GDPR"**), and the California Consumer Privacy Act, as amended by the California Privacy Rights Act (**"CCPA/CPRA"**).

1.4. In the event of any conflict between this DPA and the Agreement, this DPA shall prevail with respect to the processing of Personal Data.

2. DEFINITIONS

In this DPA, the following terms shall have the meanings set forth below. Capitalized terms not defined herein shall have the meanings given to them in the Agreement.

"Data Protection Laws" means all applicable laws and regulations relating to the processing of Personal Data, including the GDPR, UK GDPR, CCPA/CPRA, and any other applicable data protection or privacy legislation.

"Data Subject" means an identified or identifiable natural person whose Personal Data is processed under this DPA.

“Personal Data” means any information relating to an identified or identifiable natural person that is processed by SolaraCloud on behalf of the Client in connection with the Services. Under the CCPA/CPRA, this includes “Personal Information” as defined therein.

“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.

“Process” or “Processing” means any operation or set of operations performed on Personal Data, whether or not by automated means, including collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment, combination, restriction, erasure, or destruction.

“Standard Contractual Clauses” or “SCCs” means the standard contractual clauses for the transfer of personal data to processors established in third countries, as approved by the European Commission (Commission Implementing Decision (EU) 2021/914).

“Sub-processor” means any third party engaged by SolaraCloud to process Personal Data on behalf of the Client.

3. ROLES AND RESPONSIBILITIES

3.1. Controller and Processor. The parties acknowledge and agree that with respect to the processing of Personal Data under this DPA: (a) the Client is the Controller; and (b) SolaraCloud is the Processor.

3.2. CCPA/CPRA Classification. For purposes of the CCPA/CPRA, SolaraCloud is a “Service Provider” and the Client is a “Business.” SolaraCloud shall not sell, share, or use Personal Information for any purpose other than performing the Services, and shall not combine Personal Information received from or on behalf of the Client with Personal Information received from other sources except as permitted by the CCPA/CPRA.

3.3. Client Obligations. The Client shall: (a) comply with all applicable Data Protection Laws with respect to its use of the Services and any instructions it issues to SolaraCloud; (b) ensure that it has obtained all necessary consents, authorizations, and legal bases for the processing of Personal Data by SolaraCloud; and (c) be responsible for the accuracy, quality, and legality of the Personal Data provided to SolaraCloud.

3.4. SolaraCloud Obligations. SolaraCloud shall process Personal Data only on documented instructions from the Client, unless required to do so by applicable law. SolaraCloud shall immediately inform the Client if, in SolaraCloud’s opinion, an instruction from the Client infringes applicable Data Protection Laws.

4. DETAILS OF PROCESSING

The following details of processing are provided pursuant to Article 28(3) of the GDPR:

Subject Matter	Processing of Personal Data in connection with the provision of the SolaraCloud IMPACT platform and related Services.
Duration	For the duration of the Agreement, plus any post-termination data retention period as specified in Section 7 of the Terms & Conditions (30 days).
Nature and Purpose	AI-powered data analysis, insight generation, automated workflows, data storage and hosting, and customer support, as further described in the Agreement.
Types of Personal Data	Account data (names, email addresses, phone numbers, company information, business addresses, account credentials); project data (project names, client profiles, agency profiles); job inputs (marketing briefs, target audiences, competitor names, campaign goals); job outputs (strategic analyses, recommendations, reports, insights); file uploads (PDFs, documents, spreadsheets uploaded by users for AI analysis); usage metadata (job timestamps, module usage, token consumption); and technical data (IP addresses, browser and device information). Any other Personal Data contained in Client Data uploaded to the platform may also be processed.
Categories of Data Subjects	Client’s employees, contractors, end users, customers, prospects, and business contacts whose data is uploaded to or processed through the platform.

5. SECURITY MEASURES

5.1. Technical and Organizational Measures. SolaraCloud shall implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including the measures described in Annex II to this DPA. SolaraCloud maintains SOC 2 Type II certification, demonstrating its commitment to industry-leading security, availability, and confidentiality controls.

5.2. Ongoing Security. SolaraCloud shall regularly test, assess, and evaluate the effectiveness of its technical and organizational measures for ensuring the security of processing and shall make improvements as necessary.

5.3. Confidentiality. SolaraCloud shall ensure that any personnel authorized to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

5.4. No AI Training. Consistent with the Agreement and the SolaraCloud Privacy Policy, SolaraCloud does not use Client Data or AI-generated outputs to train artificial intelligence models. Personal Data is processed solely to deliver the Services. All third-party AI providers are contractually committed to not using API customer data to train or fine-tune their models. Provider-specific data retention is as follows: (a) Anthropic (Claude): zero retention — prompts and responses are not stored after processing; (b) Google (Gemini): API data stored for up to fifty-five (55) days solely for policy enforcement purposes, not used for training; (c) OpenAI (GPT): API data retained for up to thirty (30) days for abuse monitoring, then deleted (Zero Data Retention option available); (d) xAI (Grok): thirty (30) day retention window (Zero Data Retention option available for enterprise). SolaraCloud will use commercially reasonable efforts to enable zero-data-retention configurations where available from each provider.

6. SUB-PROCESSORS

6.1. General Authorization. The Client hereby provides general written authorization for SolaraCloud to engage Sub-processors to process Personal Data on behalf of the Client, subject to the requirements of this Section 6.

6.2. List of Sub-processors. SolaraCloud shall maintain a current list of Sub-processors, which shall be made available to the Client upon request. The current list of Sub-processors is set forth in Annex III to this DPA.

6.3. Notification of Changes. SolaraCloud shall notify the Client of any intended changes to the list of Sub-processors (additions or replacements) at least thirty (30) days prior to engaging any new Sub-processor, thereby giving the Client the opportunity to object to such changes.

6.4. Right to Object. If the Client reasonably objects to a new Sub-processor on data protection grounds, the parties shall discuss the Client's concerns in good faith. If the parties are unable to reach a resolution within thirty (30) days, the Client may terminate the affected Services without penalty by providing written notice.

6.5. Sub-processor Obligations. SolaraCloud shall impose data protection obligations on each Sub-processor that are no less protective than those set forth in this DPA. SolaraCloud shall remain fully liable to the Client for the performance of each Sub-processor's obligations.

7. DATA SUBJECT RIGHTS

7.1. Assistance with Requests. SolaraCloud shall, taking into account the nature of the processing, assist the Client by appropriate technical and organizational measures, insofar as this is possible, in fulfilling the Client’s obligation to respond to requests from Data Subjects exercising their rights under applicable Data Protection Laws.

7.2. Notification. If SolaraCloud receives a request from a Data Subject directly, SolaraCloud shall promptly notify the Client and shall not respond to the Data Subject directly unless instructed to do so by the Client or required by applicable law.

8. PERSONAL DATA BREACH

8.1. Notification. SolaraCloud shall notify the Client within twenty-four (24) hours of becoming aware of a Personal Data Breach affecting the Client’s Personal Data. Where required by applicable Data Protection Laws (including Article 33 of the GDPR), SolaraCloud shall notify the relevant supervisory authority within seventy-two (72) hours and shall promptly notify affected Data Subjects in accordance with applicable requirements.

8.2. Content of Notification. Such notification shall include, to the extent available: (a) a description of the nature of the Personal Data Breach, including the categories and approximate number of Data Subjects and Personal Data records concerned; (b) the likely consequences of the breach; (c) the measures taken or proposed to be taken to address the breach and mitigate its possible adverse effects; and (d) the name and contact details of SolaraCloud’s designated point of contact.

8.3. Cooperation. SolaraCloud shall cooperate with the Client and take commercially reasonable steps to assist the Client in investigating, mitigating, and remediating the Personal Data Breach.

8.4. Documentation. SolaraCloud shall document all Personal Data Breaches, including the facts surrounding the breach, its effects, and the remedial actions taken.

9. INTERNATIONAL DATA TRANSFERS

9.1. Data Location. Client Data is stored on Microsoft Azure infrastructure located in the United States, as described in the SolaraCloud Privacy Policy.

9.2. Transfer Mechanisms. To the extent that the processing of Personal Data involves the transfer of Personal Data from the European Economic Area (“EEA”), the United Kingdom, or Switzerland to the United States, the parties agree that such transfers shall be governed by the Standard Contractual Clauses (SCCs) as set forth in Annex I to this DPA. SolaraCloud shall also rely on any additional transfer mechanism recognized under applicable Data Protection Laws.

9.3. SCC Module. The parties agree that Module Two (Controller to Processor) of the SCCs shall apply to transfers of Personal Data from the Client (as data exporter) to SolaraCloud (as data importer).

9.4. Supplementary Measures. SolaraCloud shall implement appropriate supplementary measures, including encryption in transit and at rest and access controls, to ensure that the transferred Personal Data is afforded a level of protection that is essentially equivalent to that guaranteed within the EEA.

10. AUDITS AND COMPLIANCE

10.1. Audit Rights. SolaraCloud shall make available to the Client all information necessary to demonstrate compliance with the obligations set forth in this DPA and shall allow for and contribute to audits, including inspections, conducted by the Client or an auditor mandated by the Client.

10.2. SOC 2 Reports. SolaraCloud’s SOC 2 Type II report shall serve as the primary mechanism for demonstrating compliance with its security and organizational obligations under this DPA. SolaraCloud shall provide a copy of its most recent SOC 2 Type II report upon the Client’s written request.

10.3. Audit Procedure. The Client shall provide at least thirty (30) days’ prior written notice of any audit request. Audits shall be conducted during normal business hours, shall not unreasonably interfere with SolaraCloud’s operations, and shall be at the Client’s expense. The Client shall ensure that any third-party auditor is bound by confidentiality obligations.

10.4. Frequency. The Client may exercise its audit rights no more than once per twelve (12) month period, unless required by a supervisory authority or following a Personal Data Breach.

11. DATA RETURN AND DELETION

11.1. Post-Termination. Upon termination or expiration of the Agreement, and consistent with Section 7 of the Terms & Conditions, the Client shall have thirty (30) days to retrieve its data from the SolaraCloud IMPACT platform. SolaraCloud shall provide reasonable assistance to the Client in retrieving its data.

11.2. Deletion. Following the expiration of the thirty (30) day retrieval period, SolaraCloud shall delete or anonymize all Personal Data in its possession or control within thirty (30) days, unless applicable law requires retention. SolaraCloud shall certify in writing that it has complied with this obligation upon the Client's request.

11.3. Time-Based Deletion. Upon the Client's request, SolaraCloud can configure automated time-based deletion policies for job outputs and associated data (e.g., purge after a specified number of days). Such policies will be configured at the organizational level and documented in writing between the parties.

11.4. Sub-processor Data. SolaraCloud shall ensure that all Sub-processors delete or return Personal Data in accordance with the terms of this Section 11.

12. CCPA/CPRA SPECIFIC PROVISIONS

To the extent the CCPA/CPRA applies to the processing of Personal Data under this DPA, the following provisions shall apply in addition to the other terms of this DPA:

12.1. Service Provider Status. SolaraCloud is a "Service Provider" as defined under the CCPA/CPRA and shall process Personal Information solely for the business purposes specified in the Agreement.

12.2. Prohibited Activities. SolaraCloud shall not: (a) sell or share Personal Information; (b) retain, use, or disclose Personal Information for any purpose other than performing the Services, including for a commercial purpose other than providing the Services; (c) retain, use, or disclose Personal Information outside the direct business relationship with the Client; or (d) combine Personal Information received from or on behalf of the Client with Personal Information received from other sources, except as permitted by the CCPA/CPRA.

12.3. Compliance Certification. SolaraCloud certifies that it understands the restrictions set forth in this Section 12 and will comply with them.

12.4. Consumer Rights. SolaraCloud shall assist the Client in responding to verifiable consumer requests under the CCPA/CPRA, including requests to know, delete, correct, and opt out.

13. GENERAL PROVISIONS

13.1. Governing Law. This DPA shall be governed by and construed in accordance with the laws of the State of Florida, United States of America, without regard to conflict of law principles, consistent with Section 14 of the Agreement. However, to the extent required by applicable Data Protection Laws, the mandatory provisions of such laws shall apply.

13.2. Dispute Resolution. Any dispute arising out of or in connection with this DPA shall be resolved in accordance with Section 14 of the Agreement. For the avoidance of doubt, the choice of Irish courts specified in Annex I applies solely to disputes arising under the Standard Contractual Clauses and does not affect the dispute resolution mechanism set forth in Section 14 of the Agreement.

13.3. Severability. If any provision of this DPA is held to be invalid or unenforceable, the remaining provisions shall continue in full force and effect.

13.4. Amendments. SolaraCloud may update this DPA from time to time to reflect changes in applicable Data Protection Laws. Material changes will be communicated to the Client at least thirty (30) days before taking effect.

13.5. Entire DPA. This DPA, together with its Annexes and the Agreement, constitutes the entire agreement between the parties regarding the subject matter hereof and supersedes all prior agreements relating to data processing.

13.6. Contact. For questions or requests regarding this DPA, the Client may contact SolaraCloud at privacy@solaracloud.ai.

SIGNATURES

IN WITNESS WHEREOF, the parties have executed this Data Processing Agreement as of the Effective Date.

SOLARACLOUD AI LLC	**CLIENT**
(Processor / Service Provider)	*(Controller / Business)*
Signature: ______________________________	Signature: ______________________________
Name: Mykhaylo Antonovych	Name: ______________________________
Title: Founder & CEO	Title: ______________________________
Date: ______________________________	Date: ______________________________

ANNEX I: STANDARD CONTRACTUAL CLAUSES

The parties agree that the Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914) are hereby incorporated by reference into this DPA, with the following specifications:

Module Two: Controller to Processor

Clause 7 (Docking Clause): The optional docking clause SHALL apply, allowing additional parties to accede to the SCCs.

Clause 9(a) (Sub-processors): OPTION 2 (General written authorization) shall apply. SolaraCloud shall inform the Client of any intended changes to its Sub-processors with at least thirty (30) days' prior notice.

Clause 11 (Redress): The optional clause shall NOT apply.

Clause 13 (Supervision): Where the data exporter is established in an EU Member State, the supervisory authority of that Member State shall act as the competent supervisory authority. Where the data exporter is not established in an EU Member State, the Irish Data Protection Commission shall act as the competent supervisory authority.

Clause 17 (Governing Law): OPTION 1 shall apply. The SCCs shall be governed by the law of Ireland.

Clause 18 (Choice of Forum): Disputes shall be resolved before the courts of Ireland.

UK International Data Transfer Addendum

For transfers of Personal Data from the United Kingdom, the parties agree that the UK International Data Transfer Addendum to the EU SCCs (as issued by the UK Information Commissioner's Office) shall apply and is hereby incorporated by reference.

Swiss Data Protection

For transfers of Personal Data from Switzerland, the SCCs shall apply with the modifications necessary to comply with the Swiss Federal Act on Data Protection (FADP), and the competent supervisory authority shall be the Swiss Federal Data Protection and Information Commissioner.

ANNEX II: TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

SolaraCloud implements and maintains the following technical and organizational security measures, as evidenced by its SOC 2 Type II certification:

A. Encryption

- Encryption of data in transit using TLS 1.2 or higher
- Encryption of data at rest using AES-256 encryption
- Encryption key management through industry-standard key management services

B. Access Controls

- Role-based access control (RBAC) limiting access to Personal Data to authorized personnel
- Multi-factor authentication (MFA) for administrative access
- Principle of least privilege enforced across all systems
- Regular access reviews and prompt deprovisioning of terminated personnel

C. Infrastructure Security

- Hosting on Microsoft Azure with enterprise-grade physical and network security
- Network segmentation and firewalls
- Intrusion detection and prevention systems
- Regular vulnerability scanning and penetration testing

D. Data Management

- Automated backup and disaster recovery procedures
- Data isolation between Client environments
- Secure data deletion procedures upon termination
- No use of Client Data for AI model training

E. Organizational Measures

- Employee security awareness training
- Confidentiality agreements for all personnel
- Incident response plan and procedures
- Regular security audits and SOC 2 Type II assessments
- Business continuity and disaster recovery planning

F. Monitoring and Logging

- Comprehensive logging of access to Personal Data

- Real-time monitoring and alerting for security events
- Regular log review and audit trail retention

ANNEX III: LIST OF SUB-PROCESSORS

The following Sub-processors are authorized to process Personal Data on behalf of the Client as of the Effective Date:

Sub-processor	Purpose	Location	Transfer Mechanism
Microsoft Azure	Cloud hosting and infrastructure	United States	SCCs / DPF
Anthropic, PBC	AI language model processing (zero-retention API)	United States	SCCs / DPF
OpenAI, LLC	AI language model processing (30-day retention for abuse monitoring; ZDR available)	United States	SCCs / DPF
Google LLC	AI language model processing (55-day retention for policy enforcement only; not used for training)	United States	SCCs / DPF
xAI (Grok)	AI language model processing (30-day retention; ZDR available for enterprise)	United States	SCCs / DPF
Stripe, Inc.	Payment processing	United States	SCCs / DPF
Google LLC (Google Analytics)	Website analytics (solaracloud.ai marketing site only; not used on the SolaraIMPACT platform)	United States	SCCs / DPF

Clerk, Inc.	User authentication and identity management	United States	SCCs / DPF

Note: *Items in brackets [ ] must be completed with specific Sub-processor details prior to execution. SolaraCloud will maintain a current Sub-processor list and notify the Client of changes in accordance with Section 6 of this DPA.*

* * *

Last Updated: March 2026

SolaraCloud AI LLC

A Florida Limited Liability Company