201 Mission Street STE 2240
San Francisco, CA 94105
(415) 729-4330
http://abacus.ai

Abacus.AI Data Processing Agreement

This Abacus.AI Data Processing Agreement ("DPA"), that includes the Standard Contractual Clauses and, as applicable, reflects the parties' agreement with respect to the terms governing the Processing of Personal Data under the Abacus.AI Agreement for Services (the "Agreement"). This DPA is an amendment to the Agreement and is effective upon its incorporation into the Agreement, which incorporation may be specified in the Agreement, an Order or an executed amendment to the Agreement.

Upon its incorporation into the Agreement, the DPA will form a part of the Agreement. The term of this DPA shall follow the term of the Agreement. Terms not otherwise defined herein shall have the meaning as set forth in the Agreement.

1. Definitions

"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 Protection Law" means all applicable legislation relating to data protection and privacy including without limitation the EU Data Protection Directive 95/46/EC and all local laws and regulations which amend or replace any of them, including the GDPR, together with any national implementing laws in any Member State of the European Union or, to the extent applicable, in any other country, as amended, repealed, consolidated or replaced from time to time. The terms "process", "processes" and "processed" will be construed accordingly.

"Data Subject" means the individual to whom Personal Data relates.

"GDPR" means the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

"Instruction" means the written, documented instruction, issued by Controller to Processor, and directing the same to perform a specific action with regard to Personal Data (including, but not limited to, depersonalizing, blocking, deletion, making available).

“Personal Data” means any information relating to an identified or identifiable individual where such information is contained within Customer Data and is protected similarly as personal data or personally identifiable information under applicable Data Protection Law.

“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.

“Processing” means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data.

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

“Standard Contractual Clauses” means the clauses attached hereto as Exhibit 1 pursuant to the European Commission’s Standard Contractual Clauses as of 2021 for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

2. Details of the Processing

a. Categories of Data Subjects. Controller may submit Personal Data to Abacus.AI, the extent of which is determined and controlled by Controller in its sole discretion, and which may include, but is not limited to Controller’s Contacts and other end users including Controller’s employees, contractors, collaborators, customers, prospects, suppliers and subcontractors. Data Subjects also include individuals attempting to communicate with or transfer Personal Data to the Controller’s end users.

b. Types of Personal Data. Contact Information, the extent of which is determined and controlled by the Customer in its sole discretion, and other Personal Data such as navigational data (including website usage information), email data, system usage data, application integration data, and other electronic data submitted, stored, sent, or received by the Controller, or the Controller’s end users, via the RealtiyEngines.AI’s Service.

c. Subject-Matter and Nature of the Processing. The subject-matter of Processing of Personal Data by Processor is the provision of the services to the Controller that involves the Processing of Personal Data. Personal Data will be subject to those Processing activities as may be specified in the Agreement and an Order.

d. Purpose of the Processing. Personal Data will be Processed for purposes of providing the services set out, as further instructed by Controller in its use of the Services, and otherwise agreed to in the Agreement and any applicable Order.

e. Duration of the Processing. Personal Data will be Processed for the duration of the Agreement, subject to Section 4 of this DPA.

3. Controller Responsibility

Within the scope of the Agreement and in its use of the services, Controller shall be solely responsible for complying with the statutory requirements relating to data protection and privacy, in particular regarding the disclosure and transfer of Personal Data to the Processor and the Processing of Personal Data. For the avoidance of doubt, Controller's instructions for the Processing of Personal Data shall comply with the Data Protection Law. This DPA is Customer's complete and final instruction to Abacus.AI in relation to Personal Data and that additional instructions outside the scope of DPA would require prior written agreement between the parties. Instructions shall initially be specified in the Agreement and may, from time to time thereafter, be amended, amplified or replaced by Controller in separate written instructions (as individual instructions).

Controller shall inform Processor without undue delay and comprehensively about any errors or irregularities related to statutory provisions on the Processing of Personal Data.

4. Obligations of Processor

a. Compliance with Instructions. The parties acknowledge and agree that Customer is the Controller of Personal Data and Abacus.AI is the Processor of that data. Processor shall collect, process and use Personal Data only within the scope of Controller's Instructions. If the Processor believes that an Instruction of the Controller infringes the Data Protection Law, it shall immediately inform the Controller without delay. If Processor cannot process Personal Data in accordance with the Instructions due to a legal requirement under any applicable European Union or Member State law, Processor will (i) promptly notify the Controller of that legal requirement before the relevant Processing to the extent permitted by the Data Protection Law; and (ii) cease all Processing (other than merely storing and maintaining the security of the affected Personal Data) until such time as the Controller issues new instructions with which Processor is able to comply. If this provision is invoked, Processor will not be liable to the Controller under the Agreement for any failure to perform the applicable services until such time as the Controller issues new instructions in regard to the Processing.

b. Security. Processor shall take the appropriate technical and organizational measures to adequately protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, described under Appendix 2 to the Standard Contractual Clauses. Such measures include, but are not limited to:

i. the prevention of unauthorized persons from gaining access to Personal Data Processing systems,
ii. the prevention of Personal Data Processing systems from being used without authorization,
iii. ensuring that persons entitled to use a Personal Data Processing system gain access only to such Personal Data as they are entitled to accessing in accordance with their access rights, and

that, in the course of Processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorization,
iv. ensuring that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media, and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified,
v. ensuring the establishment of an audit trail to document whether and by whom Personal Data have been entered into, modified in, or removed from Personal Data Processing systems,
vi. ensuring that Personal Data is Processed solely in accordance with the Instructions,
vii. ensuring that Personal Data is protected against accidental destruction or loss.
Processor will facilitate Controller's compliance with the Controller's obligation to implement security measures with respect to Personal Data (including if applicable Controller's obligations pursuant to Articles 32 to 34 (inclusive) of the GDPR), by (i) implementing and maintaining the security measures described under Appendix 2, (ii) complying with the terms of Section 4.d. (Personal Data Breaches); and (iii) providing the Controller with information in relation to the Processing in accordance with Section 6 (Audits).

c. Confidentiality. Processor shall ensure that any personnel whom Processor authorizes to process Personal Data on its behalf is subject to confidentiality obligations with respect to that Personal Data. The undertaking to confidentiality shall continue after the termination of the above-entitled activities.

d. Personal Data Breaches. Processor will notify the Controller without undue delay after it becomes aware of any Personal Data Breach affecting any Personal Data. At the Controller's request, Processor will promptly provide the Controller with all reasonable assistance necessary to enable the Controller to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if Controller is required to do so under the Data Protection Law.

e. Deletion or Retrieval of Personal Data. Other than to the extent required to comply with Data Protection Law, following termination or expiration of the Agreement, Processor will delete or return all Personal Data (including copies thereof) processed pursuant to this DPA. If Processor is unable to delete Personal Data for technical or other reasons, Processor will apply measures to ensure that Personal Data is blocked from any further Processing.

Controller shall, upon termination or expiration of the Agreement and by way of issuing an Instruction, stipulate, within a period of time set by Processor, the reasonable measures to return data or to delete stored data. Any additional cost arising in connection with the return or deletion of Personal Data after the termination or expiration of the Agreement shall be borne by Controller. Processor will enable Controller to delete Personal Data of end users using the functionality of the Abacus.AI Cloud Service.

f. Data Protection Impact Assessments and Consultation with Supervisory Authorities. To the extent that the required information is available to Processor and the Controller does not otherwise have access to the required information, Processor will provide reasonable

assistance to Controller with any data protection impact assessments, and prior consultations with supervisory authorities or other competent data privacy authorities, which Controller reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to the processing of Personal Data.

5. Data Subject Requests
Processor will enable Controller to respond to requests from Data Subjects to exercise their rights under the applicable Data Protection Law in a manner consistent with the functionality of the Abacus.AI Service. To the extent that Controller does not have the ability to address a Data Subject request, then upon Controller's request Processor shall provide reasonable assistance to the Controller to facilitate such Data Subject request to the extent able and only as required by applicable Data Protection Law. Controller shall reimburse Processor for the commercially reasonable costs arising from this assistance.

Processor will provide reasonable assistance, including by appropriate technical and organizational measures and taking into account the nature of the Processing, to enable Controller to respond to any request from Data Subjects seeking to exercise their rights under the Data Protection Law with respect to Personal Data (including access, rectification, restriction, deletion or portability of Personal Data, as applicable), to the extent permitted by the law. If such request is made directly to Processor, Processor will promptly inform Controller and will advise Data Subjects to submit their request to the Controller. Controller shall be solely responsible for responding to any Data Subjects' requests.

6. Audits
Processor shall, in accordance with Data Protection Laws and in response to a reasonable written request by Controller, make available to Controller such information in Processor's possession or control related to Processor's compliance with the obligations of data processors under Data Protection Law in relation to its Processing of Personal Data.
Controller may, upon written request and at least 30 days' notice to Processor, during regular business hours and without interrupting Processor's business operations, conduct an inspection of Processor's business operations or have the same conducted by a qualified third party auditor subject to Processor's approval, which shall not be unreasonably withheld.
Processor shall, upon Controller's written request and on at least 30 days' notice to the Processor, provide Controller with all information necessary for such audit, to the extent that such information is within Processor's control and Processor is not precluded from disclosing it by applicable law, a duty of confidentiality, or any other obligation owed to a third party.

7. Data Transfers
Controller acknowledges and agrees that, in connection with the performance of the services under the Agreement, Personal Data will be transferred to Abacus.AI, Inc. in the United States.

To the extent that Controller or Processor are relying on a specific statutory mechanism to normalize international data transfers and that mechanism is subsequently revoked, or held in a

court of competent jurisdiction to be invalid, Controller and Processor agree to cooperate in good faith to pursue a suitable alternate mechanism that can lawfully support the transfer.

8. Consent to Subprocessor Engagement.
Controller specifically authorizes the engagement of Subprocessors, Amazon Web Services (AWS), Google Cloud Platform (GCP), or Azure from time to time.

AWS in regions - us-east-1, us-west-2, canada-central, eu-west-1
GCP in regions - us-central, asia-southeast2
Azure in regions - EastUS, EastUS2
OpenAI in regions - US, Canada, EU
Anthropic in regions - US, Canada, EU
Notion in regions - US, EU

9. General Provisions
In case of any conflict, this DPA shall take precedence over the regulations of the Agreement. Where individual provisions of this DPA are invalid or unenforceable, the validity and enforceability of the other provisions of this DPA shall not be affected.

10. Parties to this DPA
This DPA is an amendment to and forms part of the Agreement. Upon the incorporation of this DPA into the Agreement, Controller and the Abacus.AI entity that are each a party to the Agreement are also each a party to this DPA. The legal entity agreeing to this DPA as Controller represents that it is authorized to agree to and enter into this DPA for, and is agreeing to this DPA solely on behalf of,the Controller.

11. Technical and Organisational Measures (TOMs)
Access Control
Access to personal data is restricted to authorized personnel only, based on the principle of least privilege.User authentication is enforced via strong passwords and, where possible, multi-factor authentication. Access rights are reviewed regularly and revoked promptly upon role change or termination.

Data Encryption
Personal data is encrypted at rest using industry-standard algorithms (e.g., AES-256). Data in transit is protected using TLS 1.2 or higher. Encryption keys are managed securely and access is restricted.

Physical Security
Data processing facilities are protected by physical access controls (e.g., key cards, security personnel, CCTV). Visitors are registered and supervised at all times.

Data Backup and Recovery
Regular backups of personal data are performed. Backups are encrypted and stored securely. Disaster recovery and business continuity plans are in place and tested periodically.

System Security
Systems are regularly updated with security patches. Firewalls and anti-malware solutions are deployed and maintained. Vulnerability assessments and penetration tests are conducted regularly.

Data Minimization and Retention
Only the minimum necessary personal data is collected and processed. Data retention periods are defined and enforced; data is securely deleted when no longer needed.

Incident Management
Security incidents and data breaches are logged, investigated, and reported in accordance with legal requirements. An incident response plan is in place and staff are trained on its execution.

Employee Training and Awareness
Employees receive regular training on data protection, privacy, and security best practices. Confidentiality agreements are signed by all personnel with access to personal data.

Sub-Processor Management
Sub-processors are vetted for adequate data protection measures. Data processing agreements are in place with all sub-processors.

Audit and Monitoring
Regular audits are conducted to ensure compliance with data protection policies and procedures. Monitoring tools are used to detect unauthorized access or anomalous activities.

By:_____

Name: _____

Title: _____

Abacus.AI

By:_____

Name: _____

Title: _____