DATA PROTECTION AGREEMENT

This Data Protection Agreement, including its Annexes and the Standard Contractual Clauses ("**DPA**"), is supplemental to and forms part of the Enterprise License Agreement or other written or electronic terms of service or agreement for the provision of the Services (the "**Agreement**") entered into between Instabase, Inc. ("**Instabase**") and the entity identified as "Customer" in the Agreement.

Customer enters into the DPA on behalf of itself and, to the extent required under Applicable Data Protection Law, in the name and on behalf of any Authorized Affiliates (defined below). Any terms not defined in this DPA shall have the meanings set forth in the Agreement. In the event of a conflict between the terms and conditions of this DPA and the Agreement, the terms and conditions of this DPA shall supersede and control.

The parties agree as follows:

1. DEFINITIONS

1.1 "**Affiliate**" means an entity that directly or indirectly controls, is controlled by, or is under common control with a party where "control" means either (a) direct or indirect ownership or control of greater than 50% of the voting securities of such entity; or (b) the ability to control the activities of the entity through contractual rights.

1.2 "**Applicable Data Protection Law**" means data protection and privacy laws and regulations of Europe applicable to Instabase's provision of the Services under the Agreement, including where applicable (a) the General Data Protection Regulation 2016/679 ("**GDPR**"); (b) the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 and the Data Protection Act 2019 (together, "**UK GDPR**"); and (c) the Swiss Federal Data Protection Act and its implementing regulations ("**Swiss Data Protection Act**"); in each case, as amended, superseded or replaced from time to time.

1.3 "**Authorized Affiliate**" means a Customer Affiliate that is authorized to use the Services under the Agreement and has not signed their own separate Agreement with Instabase.

1.4 "**Authorized Person**" means any person authorized by Instabase to process Customer Personal Data, including Instabase employees, officers, contractors and consultants.

1.5 "**Customer Personal Data**" means any personal data contained in the text, image files or other data or content that Instabase processes on behalf of Customer in connection with the Agreement, as further described in Annex 1.

1.6 "**Europe**" means for the purposes of this DPA, the European Economic Area, Switzerland and the United Kingdom.

1.7 "**Restricted Transfer**" means: (i) where the GDPR applies, a transfer of personal data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; (ii) where the UK GDPR applies, a transfer of personal data from the UK to any other country which is not based on adequacy regulations pursuant to Section 17A of the Data Protection Act 2018; and (iii) where the Swiss DPA applies, a transfer of personal data to a country outside of Switzerland which is not included on the list of adequate jurisdictions published by the Swiss Federal Data Protection and Information Commissioner, in each case whether such transfer is a direct or onward transfer.

1.8 "**Personal Data Breach**" means a confirmed breach of security leading to any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data processed in environments controlled by Instabase or its Subprocessors. A "Personal Data Breach" does not include an unsuccessful attempt to access Customer Personal Data or Instabase equipment or facilities storing Customer Personal Data, including without limitation unsuccessful pings and other broadcast attacks of firewalls or edge servers, port scans, log-on attempts, denial of service attacks, packet sniffing or similar incidents.

1.9 "**Services**" means the services provided by Instabase to Customer under the Agreement, as more particularly described in the applicable Order Form or Statement of Work.

1.10 "**Standard Contractual Clauses**" or "**SCCs**" means the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021, as amended, superseded or replaced from time to time.

1.11 "**Subprocessor**" means any third party processor used by Instabase to process Customer Personal Data, including any Instabase Affiliate. A "Subprocessor" does not include any employee, contractor or consultant of Instabase or its Affiliates.

1.12 "**UK Addendum**" means the International Data Transfer Addendum (version B1.0) issued by Information Commissioners Office under S.119(A) of the UK Data Protection Act 2018, as amended, superseded or replaced from time to time.

The lower case terms "**controller**," "**processor**," "**personal data**," "**data subject**," "**process**," and "**processing**" have the meanings given to them by Applicable Data Protection Law.

2. PURPOSE & SCOPE

2.1 Scope and details of processing. This DPA applies solely to the extent that Instabase processes Customer Personal Data subject to Applicable Data Protection Law as a processor on Customer's behalf. The subject matter, nature, purpose, and duration of the processing, as well as the types of personal data processed and categories of data subjects involved, are described in **Annex 1**.

2.2 Role and processing instructions. Instabase shall process Customer Personal Data as a processor on Customer's behalf and solely in accordance with Customer's lawful documented instructions. For these purposes, Customer instructs Instabase to process Customer Personal Data to perform the Services in accordance with the Agreement (including this DPA) and any applicable Statement of Work or Order Form (the "**Permitted Purposes**"). The parties agree that the Agreement (including this DPA) sets out Customer's complete and final instructions to Instabase in relation to the processing of Customer Personal Data and processing outside the scope of these instructions (if any) shall require prior written agreement between the parties.

3. CUSTOMER RESPONSIBILITIES

3.1 Customer's responsibilities. Customer shall be responsible for complying with its obligations under Applicable Data Protection Law in its processing of Customer Personal Data. In particular, Customer agrees that it shall (a) be responsible for determining whether the Services are appropriate for processing Customer Personal Data consistent with Customer's legal and regulatory obligations; (b) comply with its obligations under Applicable Data Protection Law in its use of the Services and any processing instructions it issues to Instabase; and (c) ensure it has the right to transfer Customer Personal Data to Instabase, including providing notice and obtaining all consents necessary under Applicable Data Protection Law for Instabase (and its Subprocessors) to lawfully process Customer Personal Data for the Permitted Purposes. Instabase is not responsible for determining if Customer's instructions are compliant with applicable law, however Instabase shall inform Customer if, in its opinion, Customer's processing instructions infringe Applicable Data Protection Law and Instabase shall not be required to comply with such instruction. Taking into account the nature of the processing, Customer agrees that it is unlikely that Instabase would become aware of Customer Personal Data processed by Instabase is inaccurate or outdated. To the extent Instabase becomes aware of such inaccurate or outdated data, Instabase will inform the Customer.

3.2 Third-party controllers. Where Customer is itself a processor of Customer Personal Data acting on behalf of a third party controller (or other intermediaries), Customer represents and warrants that (a) it is authorized to provide Customer Personal Data to Instabase and that Customer's processing instructions reflect and do not conflict with the instructions of such

third party controller; and (b) it will act as the sole point of contact for Instabase with regard to such third party controller and Instabase need not interact directly with (including seeking authorizations directly from or providing notifications directly to) such third party controller other than through the regular provision of the Services.

4. INSTABASE OBLIGATIONS

4.1 Confidentiality. Instabase shall ensure that any Authorized Person is subject to a duty of confidentiality (whether contractual or statutory) and that they shall only process Customer Personal Data for the Permitted Purposes.

4.2 Security. Instabase shall implement and maintain appropriate technical and organizational measures designed to protect Customer Personal Data from Personal Data Breaches. Additional details regarding the specific security measures that apply to the Services are set out in the relevant security practices for these Services, accessible here [https://instabase.com/trust] (the "**Security Measures**"):

4.3 Security Updates. Instabase may update the Security Measures from time to time, provided that any updates shall not materially diminish the overall security of Customer Personal Data. Notwithstanding anything to the contrary in the Agreement and this DPA, Customer agrees that it (not Instabase) shall be responsible for determining whether the Security Measures are appropriate for the processing of Customer Personal Data consistent with Customer's obligations under Applicable Data Protection Law.

4.4 Personal Data Breaches. Instabase shall inform Customer without undue delay, and in any event within 72 hours, upon becoming aware of a Personal Data Breach and take such measures as Instabase may deem necessary and reasonable to remediate the Personal Data Breach. Instabase shall provide Customer with timely information about the nature of the Personal Data Breach as soon as such information becomes known or available to Instabase, and provide reasonable cooperation and assistance to enable Customer to comply with its obligations under Applicable Data Protection Law with respect to notifying the relevant supervisory authority and/or affected data subjects. The obligations described in this Section 4.4 shall not apply to Personal Data Breaches that result from Customer's actions or omissions, and any obligation for to report or respond to a Personal Data Breach will not be construed as an acknowledgement by Instabase of any fault or liability with respect to the Customer Personal Data concerned.

4.5 Audits. Upon Customer's request, and no more than once per calendar year, Instabase shall (a) make available for Customer's review copies of certifications or reports demonstrating Instabase's compliance with prevailing data security standards with respect to its processing of Customer Personal Data; and (b) only if such reports or certifications are not reasonably sufficient to allow Customer to assess Instabase's compliance with Applicable Data Protection Law or this DPA, allow Customer (at Customer's expense) or its authorized representative to conduct an audit or inspection of Instabase's data security infrastructure and procedures, provided that Customer shall give Instabase reasonable prior notice of any such request and the audit or inspection shall not be unreasonably disruptive to Instabase's business and take place at a mutually agreed date and time. The parties agree that the audit rights granted under the Standard Contractual Clauses shall be exercised in accordance with this Section 4.5.

4.6 Subprocessors. Customer provides a general authorization for Instabase to appoint Subprocessors, including the Subprocessors listed here [https://instabase.com/trust/subprocessors] (or such other successor URL as may be notified to Customer from time to time), provided that:

(a) Subprocessors shall be bound by a written agreement, including data protection and security measures, no less protective of Customer Personal Data than the Agreement and this DPA;

(b) Instabase shall be liable for any breach of this DPA caused by an act, error or omission of its Subprocessors to the extent Instabase would have been liable had such breach been caused by Instabase; and

(c) Instabase shall notify Customer in advance of any intended additions or replacements to its Subprocessors.

Instabase shall notify Customer if it engages a new Subprocessor at least thirty (30) days prior to any such changes if Customer opts-in to receive such notifications here [https://instabase.com/trust/subprocessors/]. Customer may object in writing to Instabase's appointment of a new Subprocessor based on reasonable data protection concerns within ten (10) calendar days of such notice from Instabase and the parties will discuss such concerns in good faith. If the parties are unable to reach a mutually agreeable resolution, Customer may terminate the relevant order form or the Agreement as it relates to the affected Services for convenience and Instabase shall provide Customer with a pro rata reimbursement of any prepaid but unused fees for the terminated portion of the Agreement.

4.7 Cooperation.

(a) Data Subject Rights. Instabase shall, taking into account the nature of the processing, provide Customer with reasonable assistance (including by appropriate technical and organization mean, in so far as this is possible) to enable Customer to (i) respond to any requests from a data subject seeking to exercise any of their rights under Applicable Data Protection Law (including its right of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Personal Data (collectively "**Correspondence**"). In the event the Correspondence is made directly to Instabase, it shall where the Customer is identified or identifiable from the Correspondence, promptly notify Customer and shall not, unless legally compelled to do so, respond directly to the Correspondence except to refer the requestor to Customer to allow Customer to respond as appropriate. Any assistance provided shall be relevant to the Services that support the processing of Customer Personal Data, and shall be commercially reasonable and proportionate to the objective of the exercise with which Instabase is requested to assist.

(b) Law Enforcement Requests. If Instabase receives a subpoena, court order, warrant or other legal demand from law enforcement or public or judicial authorities seeking the disclosure of Customer Personal Data, Instabase shall, where the Customer is identified or identifiable from such disclosure request and to the extent required and permitted by applicable law, promptly notify Customer of such request and reasonably cooperate with Customer to limit, challenge or protect against such disclosure.

(c) Data Protection Impact Assessments. Instabase shall provide Customer with reasonable cooperation and assistance where necessary for Customer to comply with its obligations under Applicable Data Protection Law to conduct a data protection impact assessment and/or to consult with the competent supervisory authorities with respect to Instabase's processing of Customer Personal Data. Instabase shall comply with the foregoing by: (i) complying with Section 4.5 (Audit Rights); (ii) providing the information contained in the Agreement, including this DPA; and (iii) if the foregoing sub-sections (i) and (ii) are insufficient for Customer to comply with such obligations, upon request, providing additional reasonable assistance at Customer's expense.

4.8 Deletion on termination. Upon Customer’s request following termination or expiry of the Agreement, Instabase shall return or delete all Customer Personal Data in its possession or control (except to the extent Instabase is required to retain any Customer Personal Data under applicable law, in which case Instabase shall isolate and protect such data from any further processing until it can be lawfully deleted). Instabase will issue a certificate of deletion upon Customer’s request.

5. INTERNATIONAL TRANSFERS

5.1 Processing locations. Instabase may transfer and Process Customer Personal Data in the United States and anywhere else in the world where Instabase or Subprocessors maintain data processing operations. Instabase shall ensure that Customer Personal Data is adequately protected in accordance with the requirements of Applicable Data Protection Law and this DPA.

5.2 Standard Contractual Clauses. Where the transfer of Customer Personal Data from Customer to Instabase is a Restricted Transfer and Applicable Data Protection Law requires that appropriate safeguards are put in place, such transfer shall be governed by the Standard Contractual Clauses, which shall be deemed incorporated into and form an integral part of this DPA in accordance with **Annex B**.

5.3 Alternative transfer mechanism. To the extent that Instabase adopts an alternative data export mechanism (including any new version of or successor to the Standard Contractual Clauses or Privacy Shield) ("**Alternative Transfer Mechanism**"), such Alternative Transfer Mechanism shall automatically apply instead of the Standard Contractual Clauses described in this DPA, but only to the extent such Alternative Transfer Mechanism complies with Applicable Data Protection Law and extends to territories to which Customer Personal Data is transferred.

6. GENERAL

6.1 Governing law. This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by Applicable Data Protection Law.

6.2 Modifications. This DPA may not be modified except by a subsequent written instrument signed by both parties. If any part of this DPA is held unenforceable, the validity of all remaining parts will not be affected.

6.3 Survival. The obligations placed upon Instabase under this DPA shall survive so long as Instabase and its Subprocessors processes Customer Personal Data on Customer's behalf.

6.4 Limitation of liability**.** The total and combined liability of each of the parties (and their respective employees, directors, officers, affiliates, successors, and assigns), arising out of or related to this DPA (including the Standard Contractual Clauses), whether in contract, tort (including negligence), or any other theory of liability, shall be subject to the exclusions and limitations of liability set forth in the Agreement.

6.5 Third party rights. In no event shall this DPA benefit or create any right or cause of action on behalf of a third party (including a third party controller), but without prejudice to the rights or remedies available to data subjects under Applicable Data Protection Law or the Standard Contractual Clauses.

ANNEX A – DESCRIPTION OF THE PROCESSING

ANNEX 1(A): LIST OF PARTIES		
Data exporter:	*Name of data exporter:*	The entity identified as "Customer" in the Agreement
	Contact person's details:	See the Agreement
	Activities relevant to data transfer:	See Annex 1.B below
	Signature and date:	Execution of the Agreement shall be deemed valid execution of the DPA (including the SCCs)
	Role (controller/processor):	Controller (for Module 2) or processor (for Module 3)
Data importer:	*Name of the data importer:*	Instabase, Inc.
	Contact person's details:	See the Agreement
	Activities relevant to data transfer:	See Annex 1.B below
	Signature and date:	Execution of the Agreement shall be deemed valid execution of the DPA (including the SCCs)
	Role (controller/processor):	Processor
ANNEX 1(B): DESCRIPTION OF THE TRANSFER AND PROCESSING		
Categories of data subjects:	The categories of data subjects included in Customer Personal Data are determined and controlled by Customer in its sole discretion and may include, without limitation: (i) Customer's employees, agents, authorized sub-contractors and advisors; and/or (ii) Customer's prospects, customers, business partners and vendors.	
Categories of personal data:	The categories of personal data included in Customer Personal Data are determined and controlled by Customer in its sole discretion and may include, without limitation: (i) name, address, title, contact details (as found in KYC or other documents); (ii) financial data (as found in bank statements, pay slips and other financial and tax documents); biometric data (as found in drivers' licenses, ID cards, passports, etc.); and/or (iii) health data (as found in health records, lab reports, x-rays, insurance claims, etc.).	
Sensitive data (if applicable):	Customer Personal Data may include 'special categories of personal data' as defined under Applicable Data Protection Laws, subject to any applicable restrictions and/or conditions in the Agreement. The nature of any such data is determined and controlled by Customer in its sole discretion and may include, without limitation: (i) biometric data (processed for unique identification); and/or (ii) health data (as found in health records, lab reports, x-rays, insurance claims, etc.).	
Frequency of the transfer:	Continuous or one-off depending on the nature of the Services being provided by Instabase.	
Nature, subject matter and duration of processing:	The nature of the processing is the provision of the Services as further described in the Agreement, and the subject matter is Customer Personal Data. The processing duration is the period for which Instabase processes Customer Personal Data as determined by the Customer through its processing instructions.	
Purpose of processing:	The nature of the processing is the provision of the Services as further described in the Agreement, and the subject matter is Customer Personal Data. The processing duration is the period for which Instabase processes Customer Personal Data as determined by the Customer through its processing instructions.	
Retention period:	Instabase will retain Customer Personal Data as instructed by Customer and in accordance with the Agreement, including this DPA.	
ANNEX 1(C): COMPETENT SUPERVISORY AUTHORITY		
Competent supervisory authority	The data exporter's competent supervisory authority shall be determined in accordance with the GDPR.	

ANNEX B – STANDARD CONTRACTUAL CLAUSES (MODULES 2 AND 3)

1.1 To the extent the Standard Contractual Clauses are deemed incorporated into and form an integral part of the DPA pursuant to Section 5.2 of the DPA, they shall apply as follows:

(a) In relation to transfers of Customer Personal Data protected by the GDPR, the SCCs shall apply as follows:

(1) the Module Two terms shall apply where Customer is the controller of Customer Personal Data and the Module Three terms shall apply where Customer is a processor of Customer Personal Data;
(2) in Clause 7, the optional docking clause shall apply and Affiliates may accede to the SCCs subject to mutual agreement of the parties;
(3) in Clause 9, option 2 ("general authorization") is selected and the process and time period for prior notice of Subprocessor changes is set out in Section 4.5 of the DPA;
(4) in Clause 11, the optional language shall not apply;
(5) in Clause 17, option 1 shall apply and the SCCs will be governed by Irish law;
(6) in Clause 18(b), disputes shall be resolved before the courts of Ireland;
(7) Annex I shall be deemed completed with the information set out in Annex A of the DPA;
(8) Annex II shall be deemed completed with the applicable Security Measures.

(b) In relation to transfers of Customer Personal Data protected by the UK GDPR, the SCCs as implemented by Section 1.1(a) above shall apply with the following modifications:

(1) the SCCs shall be modified and interpreted in accordance with Part 2 of the UK Addendum, which shall be deemed incorporated into and form an integral part of the DPA;
(2) Tables 1, 2 and 3 in Part 1 of the UK Addendum shall be deemed completed with the information set out in the DPA (including its Annexes) and Table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "importer"; and
(3) any conflict between the terms of the SCCs and the UK Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

(c) In relation to transfers of Customer Personal Data protected by the Swiss Data Protection Act, the SCCs as implemented by Section 1.1(a) above shall apply with the following modifications:

(1) references to "Regulation (EU) 2016/679" and specific articles therein shall be interpreted as references to the Swiss Data Protection Act and the equivalent articles or sections therein;
(2) references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "Switzerland" and "Swiss law" and references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection Information Commissioner" and "competent Swiss courts"; and
(3) the SCCs shall be governed by the laws of Switzerland and disputes shall be resolved before the competent Swiss courts.