Data Processing Agreement

This Data Processing Agreement ("**Agreement**") forms part of the Contract for Services ("**Principal Agreement**") between

_____

_____

_____

(the "**Company**")

and

Collectif AI OÜ
Sepapaja tn 6
15551 Tallinn
Estonia
(the "Data Processor")
(together as the "**Parties**")

WHEREAS

(A) The Company acts as a Data Controller.

(B) The Company wishes to subcontract certain Services, which imply the processing of personal data, to the Data Processor.

(C) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

(D) The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1.1.1 “Agreement” means this Data Processing Agreement and all Schedules;

1.1.2 “Company Personal Data” means any Personal Data Processed by a Contracted Processor on behalf of Company pursuant to or in connection with the Principal Agreement;

1.1.3 “Contracted Processor” means a Subprocessor;

1.1.4 “Data Protection Laws” means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.5 “EEA” means the European Economic Area;

1.1.6 “EU Data Protection Laws” means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.7 “GDPR” means EU General Data Protection Regulation 2016/679;

1.1.8 “Data Transfer” means:

1.1.8.1 a transfer of Company Personal Data from the Company to a Contracted Processor; or

1.1.8.2 an onward transfer of Company Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor, in each case, where such transfer would be prohibited by

Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.1.10 **"**Services**"** means online secure services provided by the Data Processor, such as video transcription, qualitative data analysis using artificial intelligence, file storage, and other services as developed by the Data Processor. The details and pricing of the Services can be found on the Data Processor's website.

1.1.11 **"**Subprocessor**"** means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Company in connection with the Agreement.

1.2 The terms, "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Processing of Company Personal Data

2.1 Processor shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

2.1.2 not Process Company Personal Data other than on the relevant Company's documented instructions.

2.2 The Company instructs the Processor to process the Company Personal Data pertaining to the following categories of data subjects and for the following purposes:

2.2.1 Categories of Data Subjects:

- Company Representatives: Individuals employed by or associated with the Company, whose personal data may be processed as part of providing the services. This can include employees, agents, or contractors of the Company who interact with the Processor's services.
- Company Customers: Individuals whose data (such as support tickets or sales calls) is processed by the Company using the Processor's services. This refers to the customers or clients of the Company.

2.2.2 Purposes and Nature of Processing:

2.2.2.1 Collection**:** Company Personal Data may be collected when Company inputs, uploads, or imports their data (including but not limited to support tickets, sales calls, and related metadata) into the Processor's platform through, e.g., API or web forms. This may also include data related to the Company Representatives, such as names, email addresses, transaction details, or job titles, as necessary for the provision of the Services.

2.2.2.2 Storage**:** Company Personal Data shall be stored on secure servers. The Processor ensures that adequate security measures are in place to protect the data against unauthorized or unlawful processing and against accidental loss, destruction, or damage.

2.2.2.3 Access**:** Access to Company Personal Data is strictly limited to authorized Processor personnel who require the data to perform their job functions, and to approved Subprocessors, as necessary for the provision of the Services. All individuals with access to the data are subject to strict confidentiality obligations.

2.2.2.4 Analysis**:** The Processor shall perform data analysis services as per the Principal Agreement. This may include, but is not limited to, analyzing content using OpenAI language models, transcribing recordings using Deepgram, data anonymization using Google Cloud, and other data analytics services as instructed by the Company.

2.2.2.5 Transfer**:** Company Personal Data may be transferred to Subprocessors for the purposes of providing the Services. Any such transfer is subject to:

- The Company’s prior consent, which may be granted either specifically or in a general manner as part of this Agreement.
- Compliance with the applicable Data Protection Laws, including the implementation of appropriate safeguards for data transfers to countries not recognized as providing an adequate level of data protection, such as the execution of Standard Contractual Clauses (SCCs) approved by the European Commission, or any other mechanism deemed adequate under GDPR.

2.2.2.6 Retention: Company Personal Data shall be retained only for as long as is necessary for the provision of the Services, or as required to comply with legal obligations, resolve disputes, and enforce agreements.

2.2.2.7 Deletion: Upon the termination of the Services or at the Company’s request, the Processor shall, in accordance with the Company’s instructions, delete or return all the Company Personal Data to the Company, and delete existing copies unless EU law or the law of an EU Member State requires storage of the data.

2.3 Record of Processing Activities: The Processor shall maintain a comprehensive record of all processing activities conducted on behalf of the Company, as mandated by Article 30 of the GDPR. This record will encompass all necessary details as specified in Article 30(1) and (2) of the GDPR, such as the purposes of processing, categories of data subjects, types of personal data processed, and specifics regarding data transfers to non-EU countries. Upon the Company's request, the Processor commits to providing this record within 10 business days, ensuring it is consistently updated and accurately reflects all processing activities.

2.4 The Company acknowledges that the Processor is reliant on the Company for direction as to the extent the Processor is entitled to use and process the Company Personal Data. Consequently, the Processor will not be liable for any claim brought by a Data Subject arising from any action or omission by the Processor, to the extent that such action or omission resulted directly from the Company’s instructions.

3. Processor Personnel

Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security and organizational measures

4.1 The Processor is committed to maintaining the integrity, confidentiality, and security of Company Personal Data in line with the principles of proper data processing as stipulated by Art. 32 in conjunction with Art. 5 para. 1 GDPR. Recognizing its role in the broader data processing ecosystem, the Processor undertakes the following specific technical and organizational measures:

4.1.1 Technical Measures:

- Data Encryption: Leveraging the robust security infrastructure of Bubble.io, the Processor ensures the use of strong encryption algorithms for data at rest and in transit, safeguarding personal data from unauthorized access.
- Access Controls: The Processor implements role-based access controls to ensure that access to personal data is strictly limited to authorized personnel, adhering to the principle of least privilege. This includes the use of multi-factor authentication (MFA) mechanisms for accessing systems that process personal data, aligning with industry best practices.
- Network Security: Relying on Bubble.io's advanced security measures, the Processor benefits from comprehensive network security solutions to protect data from malicious attacks and unauthorized access.
- Data Backup: Through Bubble.io's secure infrastructure, the Processor ensures regular backups of personal data, guaranteeing the availability

and resilience of systems and the ability to restore data in the event of physical or technical incidents.

- Data Anonymization and Pseudonymization: The Processor employs Google Cloud Platform services for the de-identification of personal data upon upload. This proactive approach to data anonymization and pseudonymization minimizes the risks to data subjects by replacing original data with de-identified copies, thereby enhancing privacy protection.

4.1.2 Organizational Measures:

- Data Protection Policies: The Processor establishes, maintains, and regularly updates comprehensive data protection policies and procedures. These policies are effectively communicated to and mandatorily followed by all staff, ensuring a consistent approach to data protection across the organization.
- Staff Training: Recognizing the critical role of human factors in data security, the Processor conducts regular training programs for all employees. These programs are designed to raise awareness about data protection principles, security protocols, and incident response procedures, fostering a culture of data privacy and security.
- Data Processing Records: In accordance with GDPR requirements, the Processor meticulously maintains records of all data processing activities. These records detail the purposes of processing, categories of data subjects, types of personal data processed, and specifics regarding data transfers, ensuring transparency and accountability in data handling practices.
- Data Breach Response Plan: The Processor has in place a data breach response plan, ensuring the ability to promptly detect, report, and investigate personal data breaches. This plan outlines the procedures for managing data breaches effectively, minimizing potential harm to data subjects.
- Vendor Risk Management: The Processor conducts thorough assessments of the data protection measures of all third-party service providers (subprocessors). Data protection terms are explicitly included in contracts

with subprocessors, ensuring an unbroken chain of data protection compliance across all data processing activities.

The Processor is dedicated to continuously evaluating and updating these measures to address evolving threats and to ensure compliance with the latest data protection standards and practices.

4.2 In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. Subprocessing

5.1 The Processor shall not appoint (or disclose any Company Personal Data to) any Subprocessor without obtaining the consent of the Company, which is to be granted implicitly during the account creation process through the checking of a designated checkbox by the Company. This consent mechanism shall be clearly described and made available to the Company during account setup. The Company can refer to the Privacy Policy, Section 4, for a current list of authorized Subprocessors.

5.2 The Processor shall inform the Company of any intended changes concerning the addition or replacement of other Subprocessors, thereby giving the Company the opportunity to object to such changes prior to the engagement of the prospective Subprocessor(s). Such notice shall be provided at least 10 business days before the engagement of the prospective Subprocessor and shall include relevant details necessary for the Company to make an informed decision, including but not limited to the processing activities to be undertaken and the measures taken to ensure the protection of the Company Personal Data.

5.3 For each Subprocessor, Processor shall carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Company Personal Data required by the GDPR. Processor shall ensure that the arrangement between the Processor and the Subprocessor is governed by a

written Data Processing Agreement (DPA) that offers at least the same level of protection for Company Personal Data as those set out in this Agreement. The DPA shall include, where necessary, Standard Contractual Clauses (SCCs) or other legal mechanisms to ensure the lawful transfer of personal data in accordance with Article 46 of the GDPR.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, Processor shall assist the Company by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Processor shall:

6.2.1 promptly notify Company if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

6.2.2 ensure that it does not respond to that request except on the documented instructions of Company or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform Company of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

7.1 Processor shall notify Company without undue delay upon Processor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow the Company to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Processor shall co-operate with the Company and take reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

8.1 Processor shall provide reasonable assistance to the Company with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company 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 Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. Deletion or Return of Company Personal Data

9.1 Processor shall, within 90 days of the date of cessation of any Services involving the Processing of Company Personal Data (the “Cessation Date”), delete all copies of those Company Personal Data, unless EU or national law requires storage of the data. Upon Company's request, Processor shall expedite this process and complete deletion within 14 days.

10. Audit rights

10.1 Subject to this section 10, Processor shall make available to the Company on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Company or an auditor mandated by the Company in relation to the Processing of the Company Personal Data by the Contracted Processors.

10.2 Information and audit rights of the Company only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

10.3 The Controller shall bear all costs associated with the audits conducted under this agreement. The Controller is required to provide a minimum of 15 business days' notice prior to initiating any audit. This notice period is intended to ensure that the Processor can adequately prepare and allocate the necessary resources to facilitate the audit without undue disruption to its operations.

11. Data Transfer

11.1 By agreeing to this DPA and indicating consent through the designated checkbox during the account creation process, the Company provides explicit consent for the transfer of Data to countries outside the EU and/or the European Economic Area (EEA), including the USA where the Processor's product is hosted. The Processor ensures that all such data transfers are conducted in compliance with the GDPR and are protected by implementing appropriate safeguards. To achieve this, the Parties shall:

- Rely on the EU approved Standard Contractual Clauses for controller-processor transfers (SCC Module 2) as a safeguard for protecting personal data when it is transferred outside the EEA, unless agreed otherwise.
- Ensure that the transfer and further processing of personal data adhere to the requirements set forth in SCC Module 2, including but not limited to the obligations of the data importer and data exporter as specified therein.
- Take all necessary measures to ensure that the processing of transferred data under SCC Module 2 remains consistent with the data protection and security standards required by the GDPR.

The Processor agrees to enter into and execute SCC Module 2 with the Company, or any relevant Subprocessors, as applicable, to ensure the lawful and secure transfer of personal data to countries outside the EEA, subject to the terms and conditions outlined in this Agreement.

12. Liability

The Processor shall be liable to the Controller for damages arising from breaches of this DPA or the applicable data protection provisions, attributable to the Processor's negligence or willful misconduct. The Processor's liability for damages resulting from non-compliant data processing activities shall be determined in accordance with Article 82 of the GDPR. The Processor commits to maintaining adequate data protection and breach response measures, as required under the GDPR and this DPA, to mitigate potential damages. The Processor agrees to indemnify the Controller against all claims for damages asserted by Data Subjects or other third parties, to the extent that such claims result from the Processor's breach of this DPA or non-compliance with the GDPR.

13. General Terms

13.1 Confidentiality. Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:
(a) disclosure is required by law;
(b) the relevant information is already in the public domain.

13.2 Notices. All notices and communications given under this Agreement must be in writing and sent by email to the email address security@collectif.ai, or to such other email address as may be designated in writing by the Party receiving the communication.

14. Governing Law and Jurisdiction

14.1 This Agreement is governed by the **Estonian laws**.

14.2 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of **Tallinn**, subject to possible appeal to **Estonian Supreme Court in Tallinn**.

IN WITNESS WHEREOF, this Agreement is entered into with effect from the date first set out below.

Your Company
Signature _____
Name: _____
Title: _____
Date Signed: _____

Processor Company
Signature: Andrzej Pacholik
Name: Andrzej Pacholik
Title: CEO
Date Signed 29/01/2024