

DATA PROCESSING AGREEMENT

This Data Processing Agreement (“**DPA**”) is entered into by and between Tabnam, Inc. d/b/a Greptile (“**Company**”) and the legal entity (“**Customer**”) that enters into an Agreement with Company incorporating this DPA by reference, including by hyperlink on the webpage on which it is posted. Customer and Company are referred to herein individually as a “**Party**” and collectively as the “**Parties**.” This DPA is incorporated into any master services agreement, subscription agreement, terms of service, order form, statement of work, or other binding written or electronic agreement between Customer and Company that expressly references or links to this DPA (an “**Agreement**”) between the Parties and reflects the Parties’ agreement regarding the Processing of Personal Data in accordance with Applicable Data Protection Law.

Except as modified in this DPA, the terms of the applicable Agreement shall remain in full force and effect. In the event of any conflict or inconsistency between this DPA and any other part of an applicable Agreement, this DPA shall control. In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses (defined below), the Standard Contractual Clauses shall control.

1. **Definitions.** Capitalized words and phrases used in this DPA shall have the meanings set forth in this DPA unless Applicable Data Protection Law provides a different definition or meaning for the specific circumstance at issue. Capitalized words and phrases not defined in this DPA or by Applicable Data Protection Law shall have the meaning given to them in the Agreement.

The following definitions apply to this DPA:

- (a) “**Applicable Data Protection Law**” means applicable data privacy, data protection, and cybersecurity laws, rules, and regulations, each as amended from time to time, including but not limited to:
 - (i) the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act, and any binding regulations issued under either Act (“**CCPA**”);
 - (ii) the EU General Data Protection Regulation 2016/679, including the applicable implementing legislation of each Member State (“**EU GDPR**”);
 - (iii) the UK Data Protection Act 2018 and the UK General Data Protection Regulation as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018, as amended (including by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019) (“**UK GDPR**” and together with the EU GDPR, the “**GDPR**”);
 - (iv) the Swiss Federal Act on Data Protection of 25 September 2020;
 - (v) any applicable U.S. state privacy laws; and
 - (vi) any other applicable data protection law and any guidance or statutory codes of practice issued by any relevant regulatory authority.
- (b) “**Customer Personal Data**” means all Personal Data that is Processed by Company on behalf of Customer under the applicable Agreement.
- (c) “**Data Subject**” (i) means the natural person or household to whom Personal Data pertains; and (ii) encompasses the terms “consumer” and “Data Subject” as defined under Applicable Data Protection Law.
- (d) “**Data Subject Request**” means any request made by a Data Subject to exercise rights granted under Applicable Data Protection Law, including but not limited to, a Data Subject’s request to access, correct, delete, opt out of certain Processing, or object to certain Processing.

- (e) “**Personal Data**” (i) means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular Data Subject; and (ii) encompasses the terms “Personal Data” and “personal information” as defined under Applicable Data Protection Law.
- (f) “**Process**,” “**Processing**,” or “**Processed**” means any operation or set of operations performed upon Personal Data. This includes but is not limited to collecting, recording, organizing, storing, adapting, altering, retrieving, consulting, using, disclosing, making available, aligning, combining, blocking, erasing, and destroying Personal Data.
- (g) “**Sell**” means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a Data Subject’s Personal Data to a third party for monetary or other valuable consideration.
- (h) “**Sensitive Personal Data**” shall have the meaning ascribed to “special category data,” “sensitive data,” “sensitive personal data,” or “sensitive personal information” under Applicable Data Protection Law.
- (i) “**Services**” shall mean the services as described in the applicable Agreement, including any related order form or statement of work.
- (j) “**Standard Contractual Clauses**” or “**SCCs**” means:
 - (i) with respect to “restricted transfers” (as that phrase is defined under Applicable Data Protection Law) that are subject to the EU GDPR, or subject to other Applicable Data Protection Law pursuant to which the EU standard contractual clauses have been adopted, the Controller-to-Processor standard contractual clauses, as set out in Annex 1 to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as may be amended or replaced by the European Commission from time to time (the “**EU SCCs**”); and
 - (ii) with respect to restricted transfers subject to the UK GDPR, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses of 21 March 2022, as may be amended or replaced by the UK Information Commissioner’s Office from time to time (the “**UK SCCs**”).
- (k) “**Subprocessor**” shall mean any subcontractor (including any third party and/or Company affiliate) engaged by Company to Process Personal Data on behalf of Company or Customer.

2. **Roles of the Parties for Processing of Customer Personal Data.** The Parties acknowledge and agree that with regard to the Processing of Customer Personal Data under this DPA, Customer is the “Business” or “Controller,” and Company is the “Service Provider” or “Processor,” as defined by Applicable Data Protection Law, unless expressly agreed otherwise. If Customer’s customer is the “Business” or “Controller,” then Customer may be the Processor and Company will be a Subprocessor under Applicable Data Protection Law. In either case, each Party will be subject to the relevant obligations as defined by Applicable Data Protection Law based on its role as described above.
3. **Details of Processing of Customer Personal Data.** The subject matter, nature, purpose and duration of the Processing of Customer Personal Data, as well as the types of Customer Personal Data collected and categories of Data Subjects, are described in Exhibit A to this DPA, as may be supplemented by the Services ordered under the applicable Agreement and information provided by Customer in connection with the Services.
4. **Processing of Customer Personal Data.** Company is prohibited from Processing Customer Personal Data for any purpose other than the specific purpose of performing the Services and in accordance with Customer’s

instructions, including those set out in the applicable Agreement, Customer's configuration and use of the Services, and instructions otherwise documented in writing. With respect to Customer Personal Data Processed under the applicable Agreement, Company:

- (a) shall at all times comply with Applicable Data Protection Law;
- (b) agrees that Customer has the right to take reasonable and appropriate steps to help to ensure that Company's use of Customer Personal Data is consistent with Customer's rights and obligations under Applicable Data Protection Law and the applicable Agreement;
- (c) shall notify Customer in writing of any determination by Company that (i) Customer's instructions regarding the Processing of Customer Personal Data would breach Applicable Data Protection Law or the applicable Agreement; or (ii) it can no longer meet its obligations under Applicable Data Protection Law or the applicable Agreement;
- (d) agrees that Customer has the right to take reasonable and appropriate steps to stop and remediate unauthorized use of Customer Personal Data;
- (e) shall not Sell Customer Personal Data or disclose Customer Personal Data to third parties for the purposes of targeted or cross-context behavioral advertising;
- (f) shall not retain, use, or disclose Customer Personal Data for any purpose, commercial or otherwise, other than for the specific purpose of performing the Services;
- (g) shall not retain, use, or disclose Customer Personal Data outside of the direct business relationship between the Customer and Company;
- (h) shall not combine Customer Personal Data with Personal Data that Company receives from or on behalf of another business or person, or that it collects from its own interactions with Data Subjects.

To the extent Company receives deidentified data from Customer or the Services allow for the deidentification of Customer Personal Data, Company represents and warrants that it shall not reidentify, attempt to reidentify, or direct any other party to reidentify any Customer Personal Data that has been deidentified.

Company certifies that it understands the restrictions set forth in this Section 4 and will comply with them.

5. Cross-Border Data Transfers.

- (a) **EEA Transfers.** To the extent that the Services or Processing involve the transfer of Customer Personal Data from a member state of the European Union or European Economic Area to or within any country that does not ensure an adequate level of protection according to the European Commission, the EU SCCs will apply, as follows:
 - (i) Module 2 (Controller-to-Processor) will apply where Customer is the data exporter and Company is the data importer;
 - (ii) Clause 7: The optional docking clause will not apply;
 - (iii) Clause 9: Option 2 will apply as per the terms set out in Section 8 of this DPA (Subprocessors);
 - (iv) Clause 11: The optional language will not apply;
 - (v) Clause 17: Option 1 will apply, and the EU SCCs will be governed by the laws of Ireland;

- (vi) Clause 18(b): Disputes shall be resolved by the courts of Ireland;
 - (vii) Annex I of the EU SCCs shall be deemed completed with the information set out in Exhibit A to this DPA, together with the Customer's legal name, address and contact information in the applicable Agreement and Customer's account records maintained in connection with the Services;
 - (viii) Annex II of the EU SCCs shall be deemed completed with the information set out in Exhibit B to this DPA; and
 - (ix) Annex III of the EU SCCs shall be deemed completed with the information set out in Exhibit C to this DPA, as maintained in accordance with Section 8.
- (b) **UK Transfers.** To the extent that the Services or Processing involve the transfer of Customer Personal Data from the United Kingdom to or within any country that does not ensure an adequate level of protection according to the UK Information Commissioner's Office, the UK SCCs will apply, as follows:
- (i) in Table 1, the parties' contact information shall be satisfied by the information in Exhibit A and the applicable Agreement and Customer account records;
 - (ii) in Table 2, the Approved EU SCCs shall be the EU SCCs, Module 2 (Controller-to-Processor);
 - (iii) references to Table 3 shall be satisfied by the applicable information in Exhibits A, B, and C, as supplemented by the applicable Agreement and Customer account records; and
 - (iv) in Table 4, the Importer shall have the rights outlined in Section 19 of the UK SCCs.
- (c) **Swiss Transfers.** To the extent that the Services or Processing involve the transfer of Customer Personal Data from Switzerland to or within any country that does not ensure an adequate level of protection according to the Federal Data Protection and Information Commissioner, the following terms will apply:
- (i) The term "Member State" as used in EU SCCs shall be interpreted as including Switzerland and Data Subjects in Switzerland; and
 - (ii) Data Subjects with their regular place of residence in Switzerland are allowed to bring a lawsuit in Switzerland against either the data exporter or the data importer in accordance with Clause 18(c) of EU SCCs.
- (d) **Transfers From Other Jurisdictions.** To the extent that the Services or Processing involve the transfer of Customer Personal Data from countries, nations, or jurisdictions not accounted for in Sections 5(a) through (c) to other countries, nations, or jurisdictions, Company shall cooperate with Customer to ensure that such transfers comply with Applicable Data Protection Law including, when the Parties Agree, by amending this DPA or entering into model agreements authorized under Applicable Data Protection Law .

6. **Company Obligations.**

- (a) **Assistance.** Company shall provide Customer reasonable assistance in conducting any privacy impact assessments, responding to requests from regulatory authorities, and performing prior consultations with regulatory authorities, each only to the extent required by Applicable Data Protection Law. Company shall also assist Customer in responding to and fulfilling any Data Subject Requests that Customer receives from Data Subjects.
- (b) **Deletion of Customer Personal Data.** At the termination or expiration of the applicable Agreement or

at the request of Customer, Company shall promptly either return or delete all Customer Personal Data (whichever is requested by Customer). However, if Company is required by Applicable Data Protection Law or any other applicable law to retain any Customer Personal Data, Company may retain the minimal amount of Customer Personal Data required by law. If Company is required by law to retain any Customer Personal Data after termination or expiration of the applicable Agreement, Company will continue to safeguard Customer Personal Data in accordance with Applicable Data Protection Law and the terms of this DPA.

- (c) **Confidentiality.** Company shall ensure that all persons Processing Customer Personal Data on its behalf, including Company's and its Subprocessors' employees, agents, and contractors, are subject to a contractual duty of confidentiality or are under an appropriate statutory obligation of confidentiality.
 - (d) **Personal Data Security.** Company shall implement and maintain appropriate technical and organizational measures designed to ensure the security of the Customer Personal Data it Processes as set forth in Exhibit B.
 - (e) **Records and Audits.** Company shall maintain complete and accurate records regarding the Processing it performs under the applicable Agreement and this DPA, including as necessary to demonstrate its compliance with the obligations under this DPA and Applicable Data Protection Law. Company shall make available to Customer all information requested by Customer to demonstrate Company's compliance with the obligations set out in this DPA. To the extent Customer determines that the provided information does not adequately address Customer's needs, then, upon at least sixty (60) days' prior written notice, at a time that minimizes business interruptions to Company, and no more than once per year, Company shall allow for and contribute to audits and inspections by Customer or its designated agents as required for Customer to establish both Customer's and Company's compliance with this DPA and Applicable Data Protection Law.
 - (f) **Third-Party Disclosure Requests.** Unless prohibited by applicable law, Company shall notify Customer of any inquiry, communication, request or complaint, to the extent relating to Company's Processing of Customer Personal Data, from: (i) any government or private entity, organization, or authority, including but not limited to a data protection authority or the U.S. Federal Trade Commission; and/or (ii) any individual. Company shall, taking into account the nature of the Processing, provide reasonable assistance to enable Customer to respond to such inquiries, communications, requests, or complaints, and to meet applicable legal deadlines. Company shall not disclose Customer Personal Data to any of the persons or entities above unless it is legally required to do so and has otherwise complied with the obligations in this DPA.
7. **Customer Obligations.** Customer shall: (1) comply with Applicable Data Protection Law in its use of the Services; (2) ensure that it has established a legal basis for Company's Processing of the Customer Personal Data; (3) be solely responsible for ensuring that it has obtained all necessary consents and rights from Data Subjects for the Processing activities performed by Company; and (4) not disclose or make available to Company, request that Company Process, or use the Services to Process, Sensitive Personal Data.
8. **Subprocessors.** Customer authorizes Company to engage Subprocessors to Process Customer Personal Data under the applicable Agreement as set forth in Exhibit C. Company shall remain liable for any Processing of Customer Personal Data by each such Subprocessor as if it had undertaken such Processing itself. Company will contractually impose obligations on its Subprocessors that are substantially similar to, and no less onerous than, those imposed on Company under this DPA.
9. **Security Incident.** Company shall notify Customer without undue delay after becoming aware of any accidental, unauthorized, or unlawful destruction, loss, alteration, or disclosure of, or access to, Customer Personal Data ("**Security Incident**"). Company shall send notices to Customer's designated account contact in accordance with Section 10. Such notifications shall include information Customer may reasonably request to meet its obligations under Applicable Data Protection Law. Company shall make commercially reasonable efforts to investigate and mitigate the effects of any Security Incident. Company shall provide Customer with reasonable assistance to satisfy Customer's legal obligations in relation to the Security Incident.

10. **Notices and Contact Information.** Notices from Company to Customer under this DPA shall be sent to the current administrative or privacy contact email address designated by Customer in the applicable Agreement or its Services account, unless a different method is required by Applicable Data Protection Law. Customer shall keep its contact information current. Customer may send notices, Subprocessor objections and privacy inquiries under this DPA to security@greptile.com, unless the applicable Agreement provides another designated legal-notice address.

Exhibit A

DETAILS OF PROCESSING OF PERSONAL DATA

A. List of Parties

Data Exporter Details	Name: The legal entity identified as Customer in the applicable Agreement (as reflected in the Agreement and Customer's account records). Role: Controller. Address: Customer's business address in the applicable Agreement or Customer's account records. Activities Relevant to the data transferred: Receipt of the Services, as agreed to between the Parties in the Agreement. Contact person's name, position and contact details: Customer's designated privacy or administrative contact identified in the applicable Agreement or Customer's account records. Customer shall keep this information current. Signature and date: By entering into an Agreement that incorporates this DPA by reference, including through electronic acceptance, each Party agrees to be bound by the EU SCCs and UK SCCs (as applicable); the date of such incorporation is the date of acceptance for the relevant Agreement. No separate signature on this DPA is required.
Data Importer Details	Name: Tabnam, Inc. d/b/a Greptile Role: Processor Address: 50 Francisco St, Suite 130, San Francisco, CA 94133 Activities Relevant to the data transferred: Provision of the Services, as agreed to between the Parties in the applicable Agreement. Contact details: security@greptile.com Signature and date: Company's execution or other legally binding acceptance of the applicable Agreement constitutes Company's agreement to the EU SCCs and UK SCCs (as applicable), effective on the date this DPA is incorporated into that Agreement.

B. Description of Transfer

Categories of Data Subjects	Persons identified in code, content, or information submitted to the Services by Exporter.
Categories of Personal Data	All identifiers and related Personal Data entered by Exporter into the Services.
Sensitive/Special Category Personal Data	None
Frequency of Processing/Transfers	Continuous for the duration of the applicable Agreement.
Nature and Purpose of Processing	As described in the applicable Agreement and any accompanying statements of work or order forms.
Period for which Personal Data will be Retained	Company will Process Personal Data for the duration of the applicable Agreement and the DPA or until notified in writing by Customer to discontinue Processing Personal Data (unless otherwise required by Applicable Data Protection Law).
For Transfers to Subprocessors, Please Specify the Subject Matter, Nature, and Duration of the Processing	The subject matter, nature and duration of the Processing shall be as specified in the applicable Agreement.

C. Competent Supervisory Authority

The competent supervisory authority shall be the Irish Data Protection Commission.

Exhibit B

TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF CUSTOMER PERSONAL DATA

Company applies industry-standard security measures, including:

- Encryption of data in transit and at rest
- Role-based access controls
- Regular vulnerability scans and audits
- Secure authentication practices
- Data minimization and retention policies

Exhibit C

LIST OF SUBPROCESSORS

The Subprocessors authorized by Customer are those identified in the current Subprocessor List maintained at <https://trust.greptile.com/>, subject to Section 8 of this DPA. The Subprocessor List, identifying each Subprocessor and its relevant service and Processing location, is incorporated by reference into this Exhibit C and constitutes Annex III of the EU SCCs for the applicable Agreement. Company will maintain records of prior versions and make relevant historical information available on Customer's reasonable request.

Customer may subscribe to Subprocessor List updates at <https://trust.greptile.com/>. Subscription is optional and does not replace the notice obligation in Section 8.