

DATA PROCESSING AGREEMENT

Swell (San Gregorio Labs Inc.)

This Data Processing Agreement (“DPA”) is entered into as of the date of last signature below (“DPA Effective Date”) between *[Customer Legal Name]*, a company with a principal place of business at *[Customer Address]* (“Customer”, “Controller”), and San Gregorio Labs Inc., d/b/a Swell, with a principal place of business at 185 Wythe Ave f2, Brooklyn, NY 11249 (“Swell”, “Processor”). This DPA supplements and forms part of the Master Subscription Agreement, Order Form, Pilot Agreement, or other written agreement governing Customer's use of the Swell service between the parties (the “Agreement”).

This DPA reflects Swell's standard, proactively-available data processing terms and is written to match Swell's actual architecture as documented at security.tryswell.co. It is designed to be signed as-is by most prospects; if a customer's legal or security team requires deal-specific redlines, route those to hello@tryswell.co rather than renegotiating from a blank document.

1. Definitions

- 1.1 **“Personal Data”** means any information relating to an identified or identifiable natural person that Swell Processes on Customer's behalf in connection with the Agreement, including without limitation voice audio processed transiently for transcription, the resulting call transcripts, and derived coaching notes and metadata (“Call Data”). Swell does not retain raw audio recordings; Call Data is limited to transcript text and coaching metadata as described in Annex 1.
- 1.2 **“Processing”** means any operation performed on Personal Data, including collection, transient receipt of audio, transcription, storage, analysis, and deletion.
- 1.3 **“Data Protection Laws”** means all laws and regulations applicable to the Processing of Personal Data under this DPA, including, as applicable, the EU General Data Protection Regulation (2016/679) (“GDPR”), the UK GDPR and Data Protection Act 2018, the California Consumer Privacy Act as amended by the California Privacy Rights Act (“CCPA”), and applicable U.S. state wiretapping / call-recording consent laws.
- 1.4 **“Sub-processor”** means any third party engaged by Swell to Process Personal Data on Customer's behalf, including infrastructure, authentication, observability, and AI/speech-to-text providers listed in Annex 3.
- 1.5 **“Data Subject”, “Controller”, “Processor”, and “Personal Data Breach”** have the meanings given in the GDPR and shall be interpreted accordingly where CCPA or another Data Protection Law uses different terms (e.g., “Business”/“Service Provider”/“Consumer”).
- 1.6 **“Call Participant”** means any individual whose voice is captured during a coaching session other than the Customer user operating the Service, including prospects, customers, or other third parties on the call.

2. Scope and Roles

- 2.1 This DPA applies to Swell's Processing of Personal Data on behalf of Customer in the course of providing the Swell real-time sales-call transcription and coaching service (the “Service”), as further described in Annex 1.
- 2.2 The parties agree that, with respect to the Processing of Personal Data under this DPA: Customer is the Controller (or “Business” under CCPA) and Swell is the Processor (or “Service Provider” under CCPA).
- 2.3 Swell shall Process Personal Data only on documented instructions from Customer, including with regard to transfers, unless required to do so by law, in which case Swell shall inform Customer of that legal requirement before Processing, unless prohibited from doing so.

- 2.4** The subject matter, duration, nature and purpose of Processing, types of Personal Data, and categories of Data Subjects are described in Annex 1.

3. Customer Obligations

- 3.1** Customer represents and warrants that it has, and will maintain, a valid legal basis under applicable Data Protection Laws for all Personal Data it submits to or generates through the Service, including the voices and communications of Call Participants.
- 3.2** As between the parties, Customer (and its users conducting coaching sessions) is solely responsible for providing any notice to, and obtaining any consent required from, Call Participants for the recording, transcription, and analysis of their voice and communications, including compliance with one-party and two-party consent recording laws in the relevant jurisdictions. This allocation mirrors Section 5 of Swell's Terms of Service.
- 3.3** Customer's instructions for the Processing of Personal Data shall comply with applicable Data Protection Laws. Customer shall not, and shall ensure its users do not, submit special categories of Personal Data (e.g., health, biometric-for-identification, or similarly sensitive data) to the Service.

4. Swell's Obligations as Processor

- 4.1** Swell shall ensure that persons authorized to Process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- 4.2** Swell shall implement and maintain appropriate technical and organizational measures to protect Personal Data against unauthorized or unlawful Processing and against accidental loss, destruction, or damage, as described in Annex 2.
- 4.3** Swell shall not engage a Sub-processor without prior general or specific written authorization of Customer. Swell's currently authorized Sub-processors are listed in Annex 3. Swell shall provide at least 14 days' notice before adding a new Sub-processor that will Process Personal Data or Call Data, during which Customer may object on reasonable data-protection grounds.
- 4.4** Taking into account the nature of the Processing, Swell shall assist Customer, insofar as reasonably possible, by appropriate technical and organizational measures, in fulfilling Customer's obligation to respond to requests for exercising Data Subjects' rights (e.g., access, deletion, correction, portability).
- 4.5** Swell shall assist Customer in ensuring compliance with obligations related to the security of Processing, Personal Data Breach notification, and data protection impact assessments, taking into account the information available to Swell.
- 4.6** At Customer's choice, Swell shall delete or return Personal Data still held by Swell after the end of the provision of the Service, and delete existing copies, unless applicable law requires storage. Given Swell's standard 24-hour transcript retention (Annex 1), most Call Data will already have been automatically purged prior to termination in the ordinary course.
- 4.7** Swell shall make available to Customer all information reasonably necessary to demonstrate compliance with this DPA and shall allow for and contribute to audits, including inspections, conducted by Customer or an auditor mandated by Customer, subject to reasonable notice, confidentiality, and no more than once per 12-month period absent a Personal Data Breach or legal requirement.

5. Personal Data Breach Notification

- 5.1** Swell shall notify Customer without undue delay, and in any event within 72 hours of confirming, a Personal Data Breach affecting Customer's Personal Data, consistent with the incident notification commitment in Swell's Privacy Policy.
- 5.2** Such notification shall include, to the extent known: the nature of the breach, categories and approximate number of Data Subjects and records affected, likely consequences, and measures taken or proposed to address the breach and mitigate its effects.
- 5.3** Swell shall cooperate with Customer and take reasonable steps to assist in the investigation, mitigation, and remediation of any Personal Data Breach.

6. International Data Transfers

- 6.1** Where Swell Processes Personal Data originating in the European Economic Area, the United Kingdom, or Switzerland in a country not recognized as providing an adequate level of data protection, the transfer shall be governed by the Standard Contractual Clauses (Module Two: Controller to Processor), incorporated into this DPA by reference and available at Annex 4.
- 6.2** For UK transfers, the UK International Data Transfer Addendum to the EU Standard Contractual Clauses applies in place of, or in addition to, the SCCs as required.

7. CCPA / U.S. State Privacy Law Terms

- 7.1** Swell shall Process Personal Data solely for the business purposes specified in the Agreement and this DPA, and shall not sell or share Personal Data, or retain, use, or disclose Personal Data for any purpose other than performing the Service, including any commercial purpose other than the business purposes specified, or outside the direct business relationship between Swell and Customer.
- 7.2** Swell certifies that it understands the restrictions in Section 7.1 and will comply with them.

8. AI Processing and Model Training

- 8.1** Swell does not use Customer's Call Data to train Swell's own models. Sub-processors performing AI or speech-to-text Processing (Deepgram, OpenAI, and Anthropic via Vercel AI Gateway) are contractually or technically prevented from using Call Data to train their public models under their standard commercial/API terms, as detailed in Annex 3.
- 8.2** Suggestion-generation requests (Anthropic, via Vercel AI Gateway) are made with zero data retention enforced in Swell's application code. Moment-detection requests (OpenAI Realtime API) connect directly and are not routed through a zero-data-retention configuration; Customer acknowledges that OpenAI may retain transcript snapshots in abuse-monitoring logs for up to 30 days under Swell's standard account, as disclosed in Annex 3.

9. Liability and Indemnification

- 9.1** Each party's liability arising out of or related to this DPA shall be subject to the exclusions and limitations of liability set forth in the Agreement.
- 9.2** Nothing in this DPA shall relieve either party of any liability it may have to Data Subjects or to regulators under applicable Data Protection Laws.

10. Term and Termination

10.1 This DPA shall remain in effect for as long as Swell Processes Personal Data on behalf of Customer under the Agreement.

10.2 Termination or expiry of the Agreement shall automatically terminate this DPA.

11. Order of Precedence

In the event of a conflict between this DPA and the Agreement with respect to the Processing of Personal Data, this DPA shall prevail. In the event of a conflict between this DPA and the Standard Contractual Clauses (where applicable), the Standard Contractual Clauses shall prevail.

12. Governing Law

This DPA is governed by the laws of the State of New York, without regard to conflict-of-laws principles, consistent with the governing law and forum provisions in Swell's Terms of Service, except that Section 6 (International Data Transfers) shall be governed by the law specified in the applicable Standard Contractual Clauses. Except where prohibited, exclusive jurisdiction for disputes arising from this DPA is in the courts located in New York, New York.

Signatures

This DPA is executed by the duly authorized representatives of the parties as of the DPA Effective Date.

SAN GREGORIO LABS INC. (d/b/a SWELL)	<i>[CUSTOMER LEGAL NAME]</i>
Signature: _____	Signature: _____
Name:	Name:
Title:	Title:
Date:	Date:

Annex 1 — Details of Processing

Field	Description
Subject Matter	Real-time transcription and AI-assisted coaching analysis of Customer's sales calls, delivered via Swell's macOS app and coaching relay.
Duration	For the term of the Agreement, plus any post-termination period required for deletion/return of data under Section 4.6.
Nature & Purpose	Providing the Service: streaming call audio server-side for real-time transcription, generating short coaching prompts and detailed instruction cards, and surfacing them to Customer's sales team during and after the call.
Categories of Personal Data	Audio (processed transiently in transit; not stored as recordings); call transcript text and coaching metadata (retained 24 hours by default, then automatically purged); account information (name, email, user ID); optional sales-framework preferences; diagnostic/crash data (Sentry, PII collection disabled by default); rate-limiting metadata (Upstash).
Special Categories of Data	None anticipated. Customer shall not knowingly submit special categories of Personal Data (e.g., health, biometric-for-identification, or similar sensitive data) to the Service.
Categories of Data Subjects	Customer's employees and contractors using the Service (e.g., account executives); and Call Participants such as prospects, customers, and other third parties whose voices are captured on coached calls.
Frequency of Transfer	Continuous, for as long as the Service is in use.

Annex 2 — Technical and Organizational Security Measures

This Annex reflects Swell's published Security Overview (security.tryswell.co) as of July 24, 2026.

- Encryption in transit: TLS 1.2+ on all client and server connections.
- Encryption at rest: Convex and cloud-provider-managed encryption; local auth tokens stored in macOS Keychain.
- Authentication: WorkOS AuthKit (Google OAuth, PKCE); WorkOS JWT required on all protected API and coaching-WebSocket endpoints.
- Access control: user-scoped Convex database reads bound to the authenticated JWT; server-only Convex writes gated by per-service sync secrets. The Mac app never holds Deepgram or LLM API keys.
- Rate limiting: Upstash-backed limits on authentication and LLM-cost paths; deployed environments fail closed if Upstash is unavailable.
- Automatic data minimization: raw audio is never persisted; transcripts and coaching metadata are purged via an hourly cron job (24-hour default retention).
- API hardening: HSTS, X-Frame-Options: DENY, X-Content-Type-Options: nosniff, and related headers on api.tryswell.co.
- Diagnostics: Sentry crash/error reporting with default PII collection disabled and sensitive fields scrubbed before upload; production logs avoid transcript text, tokens, and full user identifiers.
- Internal access: production systems are accessible only to San Gregorio Labs' founding engineering team; Swell does not yet operate a separate least-privilege/production-support role (early-stage company disclosure, consistent with security.tryswell.co).

- Certifications: San Gregorio Labs Inc. does not currently hold SOC 2 Type II or ISO 27001. Key sub-processors (e.g., Deepgram, WorkOS) publish their own certifications — see Annex 3. Full compensating-controls detail (access model, retention, LLM data handling) is published at security.tryswell.co/soc2.

Annex 3 — Authorized Sub-processors

Sub-processor	Purpose	Data Processed	Location
Vercel	REST API hosting, auth proxy, transcript purge cron	Account tokens (transit), API metadata	United States
Railway	WebSocket coaching relay (audio ingress, STT, AI coaching)	Audio streams (transit), transcript text, session metadata	United States
Convex	Database — profiles and session storage	Email, user ID, transcripts, coaching data (temporary)	United States
Upstash	Distributed rate limiting	User IDs, rate-limit counters (metadata)	US or EU (region-dependent)
WorkOS	Authentication (Google OAuth via AuthKit)	Email, user identifier, auth tokens	United States
Deepgram	Speech-to-text	Audio stream (transit); transcript text. Not opted into model-improvement programs.	United States
OpenAI	Moment detection (Realtime API, direct connection)	Transcript snapshots (transit). Not used for model training; standard account (no ZDR) — abuse-monitoring logs retained up to 30 days.	United States
Vercel AI Gateway	LLM request routing for suggestion generation	Transcript text, coaching context (transit). Zero data retention enforced on every request.	United States
Anthropic	Suggestion generation (invoked only via Vercel AI Gateway)	Transcript text, coaching context (transit). Commercial terms prohibit training on customer content.	United States
Sentry	Crash and error reporting (Mac app, API, coaching relay)	Stack traces, app version, error context; PII disabled by default	United States

Full detail and live updates: security.tryswell.co/subprocessors.

Annex 4 — Standard Contractual Clauses

Where Section 6 applies, the EU Standard Contractual Clauses (Module Two: Controller to Processor, Commission Implementing Decision (EU) 2021/914, published at eur-lex.europa.eu/eli/dec_impl/2021/914) are incorporated into this DPA by reference, with *[Customer]* as “data exporter” and San Gregorio Labs Inc. (d/b/a Swell) as “data importer.” Annexes I–III of the SCCs are populated using the tables in Annexes 1–3 of this DPA.