MAKING YOURSELF **CLEAR**

LEGAL · DATA PROCESSING

Data Processing Agreement — Template

> ***DRAFT — requires legal review before use.*** *This template is a starting point only. A qualified data-protection lawyer (in your jurisdiction and the customer's) must review and adapt it before signing. Anthropic / Claude is not a law firm and this scaffold is not legal advice.*

This Data Processing Agreement ("**DPA**") forms part of the agreement (the "**Agreement**") between **[CUSTOMER LEGAL ENTITY]** ("**Customer**" or "**Controller**") and **Executive Sound Board** ("**Making Yourself Clear**" or "**Processor**"), operator of the Making Yourself Clear service (the "**Service**"), under which Making Yourself Clear provides the Service to Customer.

In the event of a conflict between this DPA and the Agreement, this DPA controls with respect to the processing of Personal Data.

1. Definitions

Capitalised terms used but not defined here have the meanings given in the Agreement or in applicable Data Protection Law.

- **"Applicable Data Protection Law"** means all laws and regulations applicable to the processing of Personal Data under the Agreement, including the EU General Data Protection Regulation 2016/679 ("**GDPR**"), the UK GDPR, the California Consumer Privacy Act / California Privacy Rights Act ("**CCPA/CPRA**"), and any successor or analogous laws.
- **"Controller", "Processor", "Sub-processor", "Personal Data", "Data Subject", "Processing"**, and **"Personal Data Breach"** have the meanings given in Applicable Data Protection Law.
- **"Customer Data"** means the data Customer or its authorised users submit to the Service.

2. Roles and scope

- Customer is the Controller of Personal Data contained in Customer Data; Making Yourself Clear is the Processor.
- Making Yourself Clear processes Personal Data **only on Customer's documented instructions**, as set out in the Agreement, this DPA, and any further written instructions

Customer provides. Customer's use of the Service constitutes such instructions.

- This DPA applies to all Personal Data processed by Making Yourself Clear on behalf of Customer under the Agreement.

3. Subject matter, duration, nature and purpose of processing

Field	Value
Subject matter	Provision of the Making Yourself Clear communication-coaching service.
Duration	The term of the Agreement, plus any post-termination period in which Making Yourself Clear retains Customer Data per Section 9.
Nature and purpose	Ingesting meeting transcripts uploaded by Customer's users, applying automated redaction, submitting redacted text to an AI provider for analysis, and returning structured coaching output to the user.
Categories of Personal Data	(i) Account data of Customer's users (name, email, role, authentication identifiers); (ii) meeting transcript content, which may include names of meeting participants, names and identifiers of third parties (redacted prior to AI processing per Section 6), and any further Personal Data Customer's users choose to include in transcripts.
Categories of Data Subjects	(i) Customer's authorised users (coachees, coaches, admins); (ii) other meeting participants and third parties referenced in transcripts.

4. Obligations of Making Yourself Clear as Processor

Making Yourself Clear will:

1. Process Personal Data only on Customer's documented instructions.
2. Ensure that personnel authorised to process Personal Data are bound by appropriate confidentiality obligations.
3. Implement and maintain the technical and organisational measures described in **Annex A** (Security Measures).
4. Engage Sub-processors only in accordance with Section 5.
5. Taking the nature of the processing into account, assist Customer by appropriate technical and organisational measures, insofar as reasonable, in the fulfilment of Customer's obligations to respond to requests by Data Subjects.
6. Assist Customer in ensuring compliance with security, breach notification, data protection impact assessment, and prior consultation obligations (Articles 32–36 GDPR or equivalent),

taking the nature of the processing and information available to Making Yourself Clear into account.

7. At Customer's choice, delete or return all Personal Data to Customer at the end of the provision of services, unless retention is required by applicable law.
8. Make available to Customer all information necessary to demonstrate compliance with this DPA and allow for and contribute to audits as described in Section 10.

5. Sub-processors

- Customer grants Making Yourself Clear **general written authorisation** to engage Sub-processors to process Personal Data under this DPA, subject to the following conditions:
  - The current list of authorised Sub-processors is maintained in the Sub-processors section of the `compliance-one-pager.md` document. A dedicated public URL will be published when available.
  - Making Yourself Clear will notify Customer of any intended addition or replacement of Sub-processors at least **30 days** before the change takes effect.
  - Customer may object to a proposed Sub-processor on reasonable data-protection grounds within **14 days** of notification. The parties will then work in good faith to resolve the objection; failing resolution, Customer may terminate the affected portion of the Service.
- Making Yourself Clear will impose, by contract, data-protection obligations on each Sub-processor that are no less protective than those in this DPA.
- Making Yourself Clear remains fully liable to Customer for the performance of each Sub-processor's obligations.

6. Pre-AI redaction

Making Yourself Clear operates an automated redaction layer that scans each transcript for personally identifiable and sensitive information and replaces it with placeholder tokens before transmitting the transcript to any AI provider. The categories of information redacted, and the categories intentionally preserved, are described in `data-flow.md` and the in-app `/privacy` page. Making Yourself Clear will not materially reduce the scope of redaction without notifying Customer.

7. International transfers

Where Personal Data originating in the European Economic Area, United Kingdom, or Switzerland is transferred by Making Yourself Clear to a country outside those jurisdictions that has not received an adequacy decision, the parties agree that:

- The transfer will be governed by the EU Standard Contractual Clauses for Controller-to-Processor transfers (Module Two of the 2021 SCCs), incorporated into this DPA by reference.
- For UK transfers, the UK International Data Transfer Addendum to the EU SCCs applies in addition.
- For Swiss transfers, the SCCs apply with the modifications required by the Swiss Federal Data Protection Act.

A signed copy of the relevant SCCs / Addendum is available on request.

---

8. Personal Data Breach notification

Making Yourself Clear will notify Customer without undue delay, and in any event within **72 hours** of becoming aware of a confirmed Personal Data Breach affecting Customer's Personal Data. The notification will include, to the extent then known:

- The nature of the Personal Data Breach, including categories and approximate number of Data Subjects and records concerned.
- The likely consequences of the Personal Data Breach.
- The measures taken or proposed to address the Personal Data Breach and mitigate its possible adverse effects.
- Contact details for follow-up.

---

9. Return and deletion of Personal Data

At the end of the provision of services, Making Yourself Clear will, at Customer's choice, return or delete all Personal Data processed on Customer's behalf, and delete any existing copies, unless retention is required by applicable law. Customer Personal Data will be returned in a machine-readable format on request, or otherwise deleted within 90 days of the end of the provision of services. Backups containing Personal Data will be deleted in accordance with Making Yourself Clear's backup-retention policy described in `compliance-one-pager.md`.

---

10. Audits

Making Yourself Clear will make available to Customer, on reasonable request and no more than **once per year** (unless a Personal Data Breach has occurred), information reasonably necessary to demonstrate compliance with this DPA. Customer may, on reasonable prior notice, conduct an audit of Making Yourself Clear's processing of Customer's Personal Data, provided that:

- The audit does not unreasonably interfere with Making Yourself Clear's normal business operations.
- Customer pays Making Yourself Clear's reasonable costs of the audit.
- Customer and its auditor are bound by appropriate confidentiality obligations.
- Where Making Yourself Clear holds a current SOC 2 Type II report or equivalent third-party attestation covering the relevant controls, the report may be provided in lieu of an on-site audit.

---

11. Data Subject requests

Where Customer is unable, in its capacity as Controller, to address a Data Subject's request using the Service's self-service controls, Making Yourself Clear will, on reasonable request, provide commercially reasonable assistance to enable Customer to fulfil the request.

---

12. Term, governing law

This DPA is effective on the date the Agreement comes into force and continues until the Agreement terminates, except that provisions necessary to give effect to surviving obligations (e.g. confidentiality, return/deletion, liability for past breaches) survive termination. This DPA is governed by the laws of the **Province of Ontario, Canada**.

Annex A — Technical and organisational security measures

> *Summary form. The full and current description is maintained in* `compliance-one-pager.md` *and the underlying internal security documentation. Updates to the listed controls are tracked via the questionnaire in this folder; the contents of this annex are derived from that source.*

1. **Encryption.** TLS 1.2+ for data in transit. At rest, customer content and secrets are encrypted at the application layer with **AES-256-GCM** under a **per-organization data-encryption key**; on the vendor-hosted service the root key is held in **AWS KMS** (adding decrypt audit and key revocation). Standard cloud-managed AES-256 volume encryption (Railway-managed Postgres on Google Cloud Platform), including backups, applies beneath.
2. **Access control.** Role-based access at the application layer (coachee, coach, admin). Administrative access to production systems is limited to authorised personnel, and MFA is enforced for all such access (hosting console, data store, source control, LLM provider consoles, email provider, domain registrar).
3. **Authentication of users.** Customer's users authenticate via OAuth (Google or Microsoft) or email + verified password. Users authenticating via OAuth inherit MFA from their identity provider. The coach and admin roles are restricted to OAuth-authenticated accounts (enforced at login, registration, and role-change), so all elevated-role users have MFA. Email + password coachee accounts do not currently have application-level MFA — planned.
4. **Pre-AI redaction.** Automated PII redaction is applied to every transcript before any AI-provider call (see Section 6).
5. **LLM-provider retention controls.** OpenAI requests are sent with `store=False` (disabling OpenAI-side conversation storage). OpenAI does not train on API data, and standard OpenAI API retention of up to 30 days (abuse-monitoring) applies. A Zero-Data-Retention agreement with OpenAI has been applied for and is pending — it is not yet in effect. Anthropic is not routed in production by default. Customer-configured (BYO) endpoints inherit the customer's own provider contract.
6. **Logging and monitoring.** Application logs are forwarded from the hosting provider to Better Stack for centralised storage and querying, and retained for 3 days on the current plan. Errors are tracked via Sentry with privacy-conservative defaults. Uptime monitoring via Better Stack pings the health endpoint from four global regions every three minutes. No dedicated SIEM at present; SIEM is planned alongside the SOC 2 Type II trajectory.
7. **Backup.** All customer data is held in the application's Railway-managed Postgres database. Railway provides daily automated backups with point-in-time recovery; restore procedures are exercised at major releases. Backups inherit the same at-rest encryption as the live database.
8. **Personnel.** Personnel with access to Personal Data are bound by written confidentiality obligations and complete data-protection training annually.
9. **Sub-processor controls.** As set out in Section 5.
10. **Incident response.** Documented incident response plan; breach notification within 72 hours of confirmation per Section 8.
11. **Vulnerability management.** Dependency vulnerabilities are monitored via GitHub Dependabot across all package ecosystems (pip, npm, docker, github-actions) with automatic security-update PRs. Source code is scanned by GitHub Secret Scanning. Patching

SLA: critical-severity vulnerabilities are remediated within 7 days of disclosure; high within 30 days; medium within 90 days.

12. **Physical security.** Production infrastructure is hosted by Railway, which runs on Google Cloud Platform. Customers may reference Google Cloud's SOC 2 / ISO 27001 attestations for the underlying physical and infrastructure controls.

Annex B — Sub-processors

See the current list in the Sub-processors section of `compliance-one-pager.md`. A dedicated public URL will be published when available.

Signatures

For Customer	For Making Yourself Clear
Name:	Name:
Title:	Title:
Signature:	Signature:
Date:	Date: