Data Processing Agreement

Version 3.2, current. Effective 27 October 2026.

This Data Processing Agreement ("DPA") forms part of the Master SaaS Agreement ("Agreement") between Sona8 Inc., a Delaware corporation ("Sona8"), and Customer. It applies whenever Sona8 processes Customer Personal Data. It covers the EU GDPR, the UK GDPR, Swiss and German data protection law, and US state privacy laws. Capitalized terms not defined here have the meaning given in the Agreement.

This DPA applies without a separate signature. Customer accepts it by signing an Order Form that references the Agreement. On request, Sona8 will countersign a copy.

1. Definitions

- Data Protection Laws: all laws that apply to processing of Customer Personal Data under the Agreement. This includes the EU GDPR, the UK GDPR and Data Protection Act 2018, the Swiss Federal Act on Data Protection, the German Federal Data Protection Act (BDSG), and US state privacy laws such as the California Consumer Privacy Act as amended ("CCPA").
- Customer Personal Data: personal data in Customer Data that Sona8 processes on Customer's behalf.
- Effective Date: the date on which this version of the DPA takes effect, as stated in its heading.
- Optional Feature: a feature of the Service that processes additional personal data and is switched on only as described in Section 2.4. Screen sharing and camera sharing are Optional Features.
- Shared Content: the images and short video segments created when a Participant shares their screen or camera during an interview, and the AI-generated notes describing them.
- Security Incident: a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data.

- SCCs: the standard contractual clauses approved by European Commission Implementing Decision (EU) 2021/914.
- UK Addendum: the International Data Transfer Addendum to the SCCs issued by the UK Information Commissioner.
- Subprocessor: a third party engaged by Sona8 that processes Customer Personal Data.
- "Controller", "processor", "data subject", "personal data", "processing", "service provider" and "business" have the meanings given in Data Protection Laws.

2. Roles and scope

2.1 Customer is the controller, or a processor acting for its Affiliates as controllers. Sona8 is the processor or, where Customer is itself a processor, a subprocessor. Under US state privacy laws, Sona8 is Customer's service provider or processor.

2.2 Annex I sets out the subject matter, nature, purpose and duration of the processing, and the types of personal data and categories of data subjects.

2.3 Customer is responsible for the lawfulness of the processing it instructs. This includes having a legal basis, informing data subjects, and completing any required employee consultation. Under German law, works council co-determination under § 87(1) no. 6 BetrVG may apply.

2.4 Optional Features. Optional Features are off unless the Order Form enables them for Customer. When screen or camera sharing is enabled, the interviewer asks the Participant first, and a share starts only after the Participant agrees and starts it. The Participant can stop sharing at any time. Annex I and Annex II describe the Shared Content and the safeguards that apply. Section 2.3 also applies to Optional Features, including any employee consultation they require.

3. Processing on instructions

3.1 Sona8 processes Customer Personal Data only on Customer's documented instructions, unless required otherwise by law. In that case Sona8 informs Customer before processing, where legally permitted. The Agreement, the Order Form, this DPA and Customer's configuration of the Service are Customer's complete instructions. Additional instructions must be agreed in writing.

3.2 Sona8 will inform Customer promptly if it believes an instruction infringes Data Protection Laws.

3.3 No AI training. Sona8 does not use Customer Personal Data to train, fine-tune or improve AI models. It uses its AI Subprocessors under terms that exclude the use of Customer Personal Data for training. Those providers may retain request data for a limited period for abuse monitoring under their own terms, and for no other purpose. As an exception, TypeSafe may keep request data for as long as needed to provide its service to Sona8, as its data processing terms allow.

3.4 US state law commitments. Sona8 will not: (a) sell or share Customer Personal Data, as those terms are defined in the CCPA; (b) retain, use or disclose it outside the direct business relationship with Customer, or for any purpose other than the business purposes in Annex I; (c) combine it with personal data from other sources, except as permitted by law; or (d) attempt to re-identify de-identified data. Sona8 will notify Customer if it can no longer meet its obligations under the CCPA. Customer may take reasonable steps to stop and remediate unauthorized use. Sona8 certifies that it understands and will comply with these restrictions.

4. Confidentiality and personnel

Sona8 ensures that everyone authorized to process Customer Personal Data is bound by confidentiality obligations. Access is limited to personnel who need it to provide, support or secure the Service.

5. Security

5.1 Sona8 implements the technical and organizational measures in Annex II. They provide a level of security appropriate to the risk, taking into account the nature of the data, including the possibility of sensitive information in interview content and Shared Content.

5.2 Sona8 may update these measures, provided it does not materially reduce the overall level of security.

6. Subprocessors

6.1 Customer gives Sona8 general authorization to engage Subprocessors. The Subprocessors authorized as of the Effective Date are listed in Annex III. Sona8 maintains the current list at trust.sona8.com/subprocessors and updates it under Section 6.2; such updates do not require a new version of this DPA.

6.2 Sona8 will give at least 30 days' notice before adding or replacing a Subprocessor, by email to subscribed contacts and on its Trust Center. Customer may object on reasonable

data protection grounds within that period. The parties will then discuss the objection in good faith. If Sona8 cannot offer a reasonable alternative, Customer may terminate the affected part of the Service and receive a refund of prepaid fees for the remaining term.

6.3 Sona8 imposes data protection obligations on each Subprocessor that are at least as protective as this DPA. It remains liable for its Subprocessors' performance.

7. Assistance

7.1 Data subject requests. Sona8 will forward to Customer any request it receives from a data subject about Customer Personal Data, without responding itself except to redirect the request. The Service lets Customer export results. For access to, correction or deletion of specific personal data, including Shared Content, Sona8 will provide reasonable assistance within the deadlines Customer must meet.

7.2 Impact assessments and consultation. Sona8 will give reasonable assistance with data protection impact assessments, prior consultations with supervisory authorities, and works council information requests. This includes providing documentation of the Service's data flows, anonymity safeguards, Optional Features and security measures.

7.3 Authority requests. If a public authority requests access to Customer Personal Data, Sona8 will redirect the request to Customer where possible. Unless legally prohibited, it will notify Customer promptly, and will challenge requests that are overbroad or unlawful.

8. Security Incidents

8.1 Sona8 will notify Customer without undue delay, and in any event within 48 hours, after becoming aware of a Security Incident.

8.2 The notice will describe, as far as known: the nature of the incident; the categories and approximate number of data subjects and records affected; the likely consequences; and the measures taken or proposed. Sona8 will update Customer as more information becomes available.

8.3 Sona8 will take reasonable steps to contain and remediate the incident. It will cooperate with Customer's notifications to authorities and data subjects. Notification is not an admission of fault.

9. Audits

9.1 On request, Sona8 will provide information needed to demonstrate compliance with this DPA. This includes summaries of its security testing and completed security questionnaires, and, once available, its most recent SOC 2 Type II report.

9.2 If that information is not enough to demonstrate compliance, or a supervisory authority requires it, Customer may audit Sona8 once per year. The audit may be carried out by Customer or an independent auditor bound by confidentiality. Customer must give 30 days' notice. The audit must be conducted during business hours and limited to what is necessary. Customer bears its own costs.

10. International transfers

10.1 Customer Data is hosted in the region stated in the Order Form. Shared Content is stored in the EU (Frankfurt, Germany), whatever the hosting region. Sona8 and some Subprocessors may access or process Customer Personal Data outside the EEA, UK or Switzerland, including in the United States, as listed in Annex III.

10.2 Where a transfer of Customer Personal Data from the EEA to Sona8 is a restricted transfer, the SCCs are incorporated into this DPA as follows:

- Module 2 (controller to processor) applies where Customer is a controller. Module 3 (processor to processor) applies where Customer is a processor.
- Clause 7 (docking clause) applies.
- Clause 9: option 2 (general authorization), with the notice period in Section 6.2.
- Clause 11: the optional redress language does not apply.
- Clauses 17 and 18: the laws and courts of Ireland. Where the Order Form specifies German governing law, the laws and courts of Germany apply instead.
- Annexes I to III of the SCCs are completed by Annexes I to III of this DPA.

10.3 For transfers from the UK, the UK Addendum is incorporated. Its Tables 1 to 3 are completed with the information in this DPA, and either party may end it as allowed by its Section 19. For transfers from Switzerland, the SCCs apply with the adaptations required by the Swiss FDPIC.

10.4 Sona8 has assessed the laws of the destination countries and implements the supplementary measures in Annex II, including encryption in transit and at rest.

11. Return and deletion

When the Agreement ends, Customer may export its results through the Service for 30 days. On request within that period, Sona8 returns transcripts and other raw data in a machine-readable format within 30 days. Sona8 then deletes Customer Personal Data, including Shared Content, within a further 30 days for live systems and 90 days for backups, unless the law requires retention. Sona8 will confirm deletion in writing on request.

12. Liability and precedence

12.1 Each party's liability under this DPA and the SCCs is subject to the limitations and the Increased Claims cap in Section 9 of the Agreement, as far as permitted by Data Protection Laws. Nothing limits either party's liability to data subjects under the SCCs.

12.2 If there is a conflict, the SCCs and UK Addendum prevail over this DPA, and this DPA prevails over the Agreement on data protection matters.

13. Term

This DPA applies for as long as Sona8 processes Customer Personal Data.

14. EU contact point

Sona8's contact point for data protection matters in the EU is: Sona8 Inc., c/o Madeleine Malmsten, Stargarder Straße 55, 10435 Berlin, Germany. Email: privacy@sona8.com.

Annex I: Details of processing

Item	Description
Parties	Data exporter: Customer, as named in the Order Form. Data importer: Sona8 Inc., processor
Subject matter	Providing the Sona8 employee-listening platform: voice-based interviews of Customer's workforce, and analysis of the results for Customer's leadership

Item	Description
Nature of processing	Collection, recording, transcription, translation, redaction of names and contact details, AI-assisted analysis (theme coding, summarization, extraction of de-identified supporting statements), detection of distress indicators in interview text so that support resources can be offered to the Participant, storage, display and deletion. Where an Optional Feature is enabled, also capture and AI analysis of Shared Content
Purpose	Providing, supporting and securing the Service for Customer under the Agreement
Data subjects	(a) Participants: Customer's employees, contractors and other individuals invited to interviews; (b) Authorized Users: Customer staff who administer the Service or view results
Personal data	Participants: voice during the interview, transcripts and translations, interview answers, language, phone number or email where used to invite or remind them, and, if Customer provides them, name, employee ID, department, role, location and similar organizational attributes. Authorized Users: name, email, role, login and usage logs
Optional Features (only if enabled in the Order Form)	Screen and camera sharing: Shared Content, meaning images and short video segments of what a Participant chooses to show on their screen or camera, and AI-generated notes describing them. Shared Content may show other people's personal data or Customer's confidential information. It is kept in a private storage bucket in the EU (Frankfurt, Germany) that only Sona8's backend can read, and it is not shown in any screen, export or report of the Service
Special categories	Not intended. Participants may voluntarily mention or show health, trade union membership, religious beliefs or similar. Safeguards in Annex II apply, including access controls and anonymity thresholds in reporting
Frequency	Continuous for the Subscription Term
Retention	Voice recordings: not stored by Sona8; the voice provider's copy is deleted when the interview closes, within 24 hours. Transcripts and results: for the retention period Customer configures in the Service (indefinite, or a number of months from when the interview closes, minimum 7 days), otherwise for the Subscription Term. Shared Content: deleted together with the transcripts on the same retention period, and with the rest of a Participant's data when that Participant's data is erased. Invitation and reminder emails: 90 days. Deletion after termination per Section 11
Subprocessor transfers	As listed in Annex III, for the same purposes

Item	Description
Competent supervisory authority	The supervisory authority competent for Customer under Clause 13 of the SCCs

Annex II: Technical and organizational measures

- Encryption: TLS 1.2 or higher in transit; AES-256 at rest for databases, file storage and backups.
- Access control: SSO and enforced MFA for all Sona8 staff; role-based access; least privilege; access reviews at least annually; production access logged.
- Customer access: SSO/SAML for Authorized Users; role-based permissions for results.
- Anonymity safeguards: results are shown aggregated by theme; a minimum group size of 5 Participants applies to every view, export and API response, and figures below that threshold are withheld; verbatim statements are not shown to Customer; names, email addresses and phone numbers are redacted before transcripts are processed by AI providers. Sona8 support staff with elevated access may see unaggregated data only to operate and support the Service, under Section 4.
- Optional Features: off by default and enabled only through the Order Form. The interviewer asks before any share, the Participant starts it and can stop it at any time. Shared Content is kept in a private storage bucket in the EU (Frankfurt, Germany) that only Sona8's backend can read, and it is not shown in any screen, export or report. Images are analysed by OpenAI with storage switched off on every request; when the interviewer takes a closer look, that single image is analysed by Anthropic.
- Tenant isolation: logical separation of each customer's data at database level (row-level security); separate development and production environments; no production data in development.
- AI providers: no-training terms with every AI provider; prompts limited to the data needed, with names and contact details redacted; provider retention limited to abuse monitoring under the provider's terms, except as stated for TypeSafe in Section 3.3. No emotion recognition from voice, face or other biometric data.
- Monitoring and testing: continuous scanning of code, dependencies, secrets and cloud configuration and monitoring of the external attack surface (Aikido, osv-scanner);

compliance monitoring (Vanta); error monitoring with personal data scrubbing (Sentry).

- Resilience: daily automated backups; documented backup restoration test, most recently in October 2026.
- Incident response: documented and approved incident response plan; 48-hour customer notification.
- Personnel: confidentiality agreements; security and privacy training at onboarding and annually; managed company devices.
- Vendor management: security review and data processing agreement before onboarding any Subprocessor.
- Compliance: SOC 2 Type II (Security) audit by an independent CPA firm planned, with an observation period starting 1 November 2026; report expected in the first quarter of 2027.

Annex III: Subprocessors as of the Effective Date

Subprocessor	Purpose	Location of processing	Transfer mechanism
Supabase, Inc.	Database and file storage, including Shared Content	Hosting region stated in the Order Form; Shared Content in the EU (Frankfurt, Germany)	DPA with SCCs
Vercel Inc.	Application hosting	Hosting region stated in the Order Form; global edge network for request routing	DPA with SCCs
Anthropic, PBC	Language model analysis, and analysis of single images of Shared Content when the interviewer takes a closer look (direct API)	United States	DPA with SCCs

Subprocessor	Purpose	Location of processing	Transfer mechanism
OpenAI	Language model analysis and embeddings, and analysis of Shared Content with storage switched off (direct API)	United States	DPA with SCCs
ElevenLabs Inc.	Voice interviewer, including the language model that runs the live conversation; speech-to-text and text-to-speech	United States	DPA with SCCs
Twilio Inc.	Telephony and SMS (phone interviews, text invitations and reminders)	United States	EU-US Data Privacy Framework; Twilio Binding Corporate Rules; SCCs as fallback
TypeSafe	Structured coding of interview observations	United States	DPA with SCCs
Functional Software, Inc. (Sentry)	Error monitoring, personal data scrubbed before transmission	EU (Germany)	DPA with SCCs; EU-US Data Privacy Framework
WorkOS, Inc.	Authentication and SSO	United States	DPA with SCCs
Resend	Invitation and reminder emails	United States	DPA with SCCs; EU-US Data Privacy Framework

Integrations that Customer enables itself, such as Google Workspace, Slack or Granola, are not Subprocessors of Sona8. Sona8's internal tools that never process Customer Personal Data are not listed.

Referenced texts

- EU Standard Contractual Clauses, Commission Implementing Decision (EU) 2021/914
- UK International Data Transfer Addendum (ICO)
- Current subprocessor list (Trust Center)