DATA PROCESSING AGREEMENT

Sonacove Meets — Controller to Processor

Version 1.1 · 5 November 2026

This Data Processing Agreement (the "DPA") forms part of the agreement between the parties for the use of the Sonacove Meets service (the "Agreement") and is entered into between:

(1) The Customer identified in the Agreement or applicable order form (the "Customer" or "Controller"); and

(2) Alfaz Studio LLC, an Oregon limited liability company (Oregon registry number 264949398), registered at 5441 S Macadam Ave, Ste N, Portland, OR 97239, USA ("Sonacove" or "Processor").

By using the Service or signing an order form that references this DPA, the Customer accepts this DPA. Capitalised terms not defined here have the meaning given in the Agreement.

1. Definitions

"Applicable Data Protection Law" means the EU General Data Protection Regulation (EU) 2016/679 ("GDPR"), the UK GDPR and Data Protection Act 2018, the Turkish Personal Data Protection Law (KVKK) where applicable, and any other data protection law applicable to the Processing.

"Controller", "Processor", "Data Subject", "Personal Data", "Processing", "Supervisory Authority" and **"Personal Data Breach"** have the meanings given in the GDPR.

"Customer Personal Data" means Personal Data that Sonacove Processes on behalf of the Customer in connection with the Service.

"Service" means the Sonacove Meets video-conferencing and collaboration service and related applications.

"Subprocessor" means a third party engaged by Sonacove to Process Customer Personal Data.

2. Roles and Scope

2.1 The Customer is the Controller of Customer Personal Data. Sonacove Processes Customer Personal Data as a Processor on the Customer's behalf.

2.2 Sonacove acts as an independent Controller for account, billing, security and product-analytics data relating to the Customer's administrators and registered users, as described in the Privacy Policy. This DPA does not cover that Processing.

2.3 The subject matter, duration, nature and purpose of the Processing, the types of Personal Data and the categories of Data Subjects are set out in **Annex 1**.

2.4 Sonacove will Process Customer Personal Data only on the documented instructions of the Customer, including for international transfers, unless required to do otherwise by law. Where Sonacove is required by law to Process otherwise, it will inform the Customer unless the law prohibits it.

2.5 **Guest participants.** Where the Customer invites or permits participants who do not hold a Sonacove account ("Guests"), Sonacove Processes the Guests' Personal Data as a Processor on the Customer's behalf. The Customer is responsible for giving Guests an appropriate notice and for having a lawful basis for the Processing.

3. Processor Obligations

3.1 Sonacove will:

- Process Customer Personal Data only as necessary to provide the Service and in accordance with the Customer's documented instructions;

- implement the technical and organisational measures in **Annex 2**;
- ensure that personnel authorised to Process Customer Personal Data are bound by appropriate confidentiality obligations;
- assist the Customer in responding to Data Subject requests and in ensuring compliance with Articles 32–36 GDPR, taking into account the nature of the Processing;
- notify the Customer of a Personal Data Breach in accordance with clause 10;
- make available all information reasonably necessary to demonstrate compliance and allow for audits in accordance with clause 12;
- not sell Customer Personal Data and not use it for advertising or to train artificial-intelligence models; and
- delete or return Customer Personal Data in accordance with clause 11.

4. Customer Obligations

4.1 The Customer warrants that it has a lawful basis for the Processing and has provided all required notices and obtained all required consents.

4.2 The Customer will not use the Service to Process special-category data or criminal-offence data unless it has put appropriate additional safeguards in place and instructed Sonacove in writing.

4.3 The Customer is responsible for the acts and omissions of its administrators and users, including configuring meeting settings such as recording, transcription, waiting rooms and guest access.

5. Confidentiality

Each party will keep the other’s confidential information confidential and use it only for the purposes of the Agreement.

6. Security

Sonacove will implement appropriate technical and organisational measures to protect Customer Personal Data, including those in Annex 2, and may update them provided the overall level of protection is not reduced.

7. Subprocessors

7.1 The Customer provides a general authorisation for Sonacove to engage Subprocessors. The current Subprocessors are listed in **Annex 3**.

7.2 Sonacove will (a) impose data-protection obligations on each Subprocessor no less protective than this DPA, and (b) remain liable for the Subprocessor’s performance.

7.3 Sonacove will notify the Customer of changes to Subprocessors and give the Customer a reasonable opportunity to object. If the Customer objects on reasonable data-protection grounds and the parties cannot resolve the matter, the Customer may terminate the affected part of the Service.

8. International Transfers

8.1 Sonacove’s primary infrastructure and analytics are located in the EU/EEA. Sonacove is established in the United States, and its personnel may remotely access Customer Personal Data from Türkiye to provide support and maintain the Service; Türkiye has not received an EU adequacy decision. Some Subprocessors are also established outside the EEA or operate global networks.

8.2 Where Sonacove or a Subprocessor transfers Customer Personal Data outside the EEA or the UK, Sonacove will ensure appropriate safeguards are in place. For transfers to Sonacove in the United States, including access by its personnel from Türkiye, the parties agree that the European Commission's Standard Contractual Clauses (Module 2, controller-to-processor, Commission Implementing Decision (EU) 2021/914) apply, with Sonacove as the data importer, together with the UK International Data Transfer Addendum for UK data. For Subprocessors, Sonacove ensures equivalent safeguards (the SCCs, the UK Addendum, or an adequacy decision including the EU-U.S. Data Privacy Framework where the recipient is certified).

8.3 A copy of the relevant safeguards can be requested at privacy@sonacove.com. The completed SCC Module 2 annexes are published at https://sonacove.com/legal/sonacove-sccs.pdf.

9. Data Subject Rights

Sonacove will, to the extent legally permitted, promptly notify the Customer if it receives a request from a Data Subject relating to Customer Personal Data, and will not respond except on the Customer's instructions or as required by law. Sonacove will provide reasonable assistance to the Customer in fulfilling such requests.

10. Personal Data Breach

Sonacove will notify the Customer without undue delay, and in any event within 72 hours, after becoming aware of a Personal Data Breach affecting Customer Personal Data. The notification will describe the nature of the breach, its likely consequences, and the measures taken or proposed. Sonacove will take reasonable steps to mitigate and remediate the breach.

11. Deletion and Return

11.1 On termination or expiry of the Agreement, or on the Customer's written request, Sonacove will delete or return Customer Personal Data and delete existing copies within 30 days, unless Applicable Data Protection Law requires retention.

11.2 Customer Personal Data in routine backups is overwritten or deleted in the ordinary course (currently within 30 days).

11.3 Where a Data Subject deletes their own account but meeting records are shared with, or controlled by, an organisation, retention and deletion are the Customer's responsibility as Controller. The Customer or the Data Subject may request erasure at privacy@sonacove.com.

12. Audit

12.1 Sonacove will make available information reasonably necessary to demonstrate compliance with this DPA.

12.2 No more than once per year (or more often following a Personal Data Breach or a Supervisory Authority request), Sonacove will allow the Customer or its auditor to conduct an audit, subject to confidentiality and reasonable notice, and at the Customer's cost. Audits must not compromise the security or confidentiality of other customers' data.

13. Liability

Each party's liability under this DPA is subject to the limitations and exclusions of liability in the Agreement.

14. Term

This DPA takes effect on the effective date of the Agreement and continues until Sonacove has deleted or returned all Customer Personal Data.

15. Governing Law

This DPA is governed by the law of the Republic of Türkiye, without prejudice to any mandatory data-protection law applicable to the Customer, including the GDPR where the Customer is established in the EEA or the Processing is otherwise subject to Article 3 GDPR.

Annex 1 — Details of Processing

Subject matter: provision of the Sonacove Meets video-conferencing and collaboration service.

Duration: the term of the Agreement, plus the retention period in clause 11.

Nature and purpose: hosting, transmitting and storing meeting content; providing accounts, meetings, chat, polls, file sharing, whiteboards, attendance records and support.

Categories of Data Subjects: the Customer's administrators, hosts, teachers and users; and participants and guests of the Customer's meetings.

Categories of Personal Data:

- **Identification and contact data:** name or display name, email address (where provided), user identifier.
- **Connection data:** IP address, browser and operating-system type, device type, app version.
- **Meeting data:** meeting/room name, join and leave times, attendance records, chat messages, poll questions and votes, reactions, hand raises, shared-file names and content, whiteboard content, and meeting settings.
- **Support data:** correspondence with Sonacove support.

Sensitive data: none intended. The Customer must not use the Service for special-category data without a written instruction and appropriate safeguards.

Annex 2 — Technical and Organisational Measures

- Encryption of data in transit (TLS) and at rest (volume and object-storage encryption, e.g. SSE-AES-256).
- Access control: least privilege, unique credentials, role-based access, and audited administrative access.
- Pseudonymisation and minimisation: analytics use stable pseudonymous identifiers; guests need no account.
- Tenant and role separation within and between organisations.
- Availability and resilience: regular backups (daily) and tested restore procedures.
- Incident response: monitored alerting, defined severity levels and a documented breach-notification process.
- Personnel: confidentiality obligations and security awareness.
- Vendors: due diligence and contractual data-protection obligations, including EU Standard Contractual Clauses where required.
- Retention and deletion: documented retention periods and deletion on request or termination.
- Optional recording is off by default and automatic cloud recording is disabled. Session replay is disabled across the Service, including in meetings; we do not record screens.
- Live transcription and AI features are optional and per-meeting; they use EU inference and transcript segments are not stored.

Annex 3 — Authorised Subprocessors

The table below lists the Subprocessors engaged as at the version date of this DPA, with the data each Processes and the applicable location and transfer safeguard.

Subprocessor	Purpose and data	Location and safeguard
Amazon Web Services EMEA SARL	Cloud hosting for the API and database, and encrypted object storage for files, avatars and logos.	EU (Frankfurt, eu-central-1). Intra-EEA.
LiveKit, Inc.	Managed real-time audio, video and data infrastructure. Media is relayed in real time and is not recorded by LiveKit.	LiveKit Cloud (project pinned to the EU region). EU.
PostHog, Inc.	Product analytics, error and diagnostic tracking, and the support inbox; pseudonymous identifiers, usage and diagnostic data.	EU cloud (eu.i.posthog.com). Intra-EEA.
Svix	Delivery of outbound webhooks to endpoints the Customer configures; event payloads.	EU cluster (api.eu.svix.com). Intra-EEA.
Paddle.com Market Ltd	Payment processing and Merchant of Record; billing name, email, address and tax details.	United Kingdom; adequacy / SCCs.
Google LLC (Firebase Cloud Messaging)	Delivery of mobile push notifications; device token and notification payload.	United States; SCCs and EU-U.S. Data Privacy Framework.
Cloudflare, Inc.	DNS, TLS, transactional email delivery and Turnstile bot protection; email addresses, IP addresses and message content.	Global network; SCCs and EU-U.S. Data Privacy Framework.
Polar Software, Inc.	Usage-based billing for organisations where enabled; organisation billing data.	United States; SCCs / DPF.
Zoom Video Communications, Inc.	Only where a Zoom account is connected; Zoom account tokens and meeting/attendance data.	United States; SCCs / DPF.
Meta Platforms, Inc. (WhatsApp Cloud API)	Only where WhatsApp reminders are enabled; phone number and message content.	United States / global; SCCs.
Automattic Inc. (Gravatar)	Optional avatar images; a hash of the user's email address.	United States; SCCs / DPF.
LiveKit Inference	Optional live transcription and the teaching copilot; real-time audio. Transcript segments are not stored.	EU endpoint.

Distribution platforms (Apple App Store, Google Play Store and Microsoft Store) publish the mobile and desktop applications. They do not receive Customer Personal Data from Sonacove, but the Customer's use of those stores is governed by their own terms.

Signatures

This DPA may be executed electronically. Signing below incorporates this DPA into the Agreement.

For the Customer (Controller)

Name: _____

Title: _____

Signature: _____

Date: _____

For Sonacove (Processor)

Name: Mohammed Ibrahim Ali

Title: Member, Alfaz Studio LLC

Signature: _____

Date: _____

Questions about this DPA, or requests for the transfer safeguards referred to in clause 8, can be sent to privacy@sonacove.com.