

Security and Privacy Overview

For institutional review (IT security, privacy, research compliance). The sections follow the structure of the HECVAT.

Product	Airtape Studio (airtape.co), browser-based remote recording
Document date	October 22, 2026
Vendor	Montazeri Ventures GmbH, Dresdner Straße 12, 69181 Leimen, Germany. Commercial register Mannheim. VAT ID DE346412503.
Security and privacy contact	Hamed Montazeri, Managing Director, hamed@airtape.co
Applicable law	EU General Data Protection Regulation (GDPR), German Federal Data Protection Act (BDSG)

1. Company and assessments

- Airtape is developed and operated by a small team in Germany. The managing director is responsible for security and data protection.
- Third-party certifications: Airtape does not currently hold SOC 2 or ISO 27001 certification, and no external penetration test has been performed. Our infrastructure providers hold their own certifications (see section 9).
- We will complete an institution's own questionnaire, such as the HECVAT Lite or Full, on request.

2. How the service works

- A host (for example, a researcher) creates an account and a session, and sends the session link to participants.
- Participants join in a current web browser. They do not create an account or install software. They enter a display name and grant camera and microphone access in their browser.
- Hosts can turn on a waiting room. Participants then wait until the host admits them, and this is enforced on the server.
- Each participant's audio and video is recorded locally in their own browser, in short segments, and uploaded to cloud storage during the session. After the session, the server assembles one file per participant.
- Only the host who owns the session can access, download, share or delete its recordings. Share links are opt-in, per recording, and can be revoked.
- Transcription is optional and only runs when the host requests it for a recording.

3. Data collected

WHO	DATA	PURPOSE
Hosts	Name, email address, password hash or Google account ID, plan and billing status, sessions, recordings, transcripts	Providing the account and service, billing
Participants	Display name they enter, audio and video recording, chat messages, IP address and connection data during the session	Recording the conversation for the host, establishing the live connection
All users	Pseudonymous product telemetry (for example, connection and upload diagnostics), without names, emails or recording content	Reliability and troubleshooting

Airtape does not sell personal data, does not use it for advertising, and does not use customer recordings or transcripts to train AI models. The website uses no advertising or tracking cookies. Website analytics are self-hosted, cookieless and anonymous.

4. Data location and hosting

- Application servers and database:** Hetzner Online GmbH, data centers in Germany.
- Recording storage:** Cloudflare R2 object storage, primarily processed in the EU.
- Transcription:** Airtape's own transcription software (an open-source speech recognition model) running on hardware that Airtape operates itself in Germany, administered by the managing director, with full-disk encryption. The worker fetches the audio over TLS, deletes it as soon as the transcript is finished, and only

sends the text back. Audio is never sent to third-party AI providers.

- **Live audio and video during the session:** relayed through Cloudflare's real-time media network (SFU/TURN). Cloudflare connects each participant to a nearby location, which can be outside the EU for participants outside the EU. Live media passes through only to deliver the conversation and is not stored.
- Where a provider processes data outside the EU/EEA, transfers rely on the EU Standard Contractual Clauses or the EU-U.S. Data Privacy Framework.

5. Encryption

- **In transit:** all connections use HTTPS/TLS. The edge to origin connection uses TLS with strict certificate validation. Live media is encrypted with DTLS-SRTP, the WebRTC standard.
- **Browser security headers:** every response carries HTTP Strict Transport Security (one year, including subdomains), X-Content-Type-Options: nosniff, a strict-origin-when-cross-origin referrer policy, clickjacking protection (X-Frame-Options and CSP frame-ancestors) and a Permissions-Policy that limits browser features to those the recording studio needs (camera, microphone, screen capture). Cross-origin access is enabled only for the API, which authenticates with bearer tokens rather than cookies.
- **Uploads:** recording segments are sent over TLS directly to storage with short-lived, signed upload URLs.
- **At rest:** Cloudflare R2 encrypts all stored objects with AES-256. Two-factor secrets are sealed with AES-256-GCM. Passwords are stored as bcrypt hashes. Recovery codes, email login codes and API tokens are stored only as keyed hashes.

6. Authentication and access control

- Host sign-in by password, a one-time email code or Google sign-in. Optional two-factor authentication with an authenticator app (TOTP) and recovery codes.
- Sign-in endpoints are rate-limited. Sessions use signed tokens that expire after 24 hours.
- Session links contain random, unguessable tokens. Every request for session data, recordings and uploads checks on the server that the caller owns the session or has a valid participant link.
- Personal access tokens for the optional API are scoped, can expire, can be revoked, and are stored only as hashes.
- Production access is restricted to the managing director. Secrets are kept in the hosting platform's encrypted settings, not in source code.

7. Retention and deletion

- **Recordings:** kept for 7, 30 or 90 days depending on the host's plan, then deleted automatically. Hosts receive a reminder before deletion and can delete any recording or session earlier.
- **Upload segments:** deleted from storage and from the participant's browser once the final file is assembled.
- **Accounts:** hosts can export their data and permanently delete their account in the settings. This removes their sessions, recordings and transcripts from storage.
- **Unconfirmed sign-ups:** deleted after 72 hours.
- **Telemetry:** pseudonymous events are deleted after 24 months. Recording diagnostics are deleted after 14 days.

8. Operations and resilience

- **Deployment:** container images are built in CI from version-controlled source. Production releases go through a deploy guard that waits until no recording is in progress.
- **Backups:** daily consistent database backups with an integrity check, kept for 14 days, with an offsite copy.
- **Recording safety:** recording segments are kept in the participant's browser until the server confirms receipt. Interrupted uploads resume automatically, including after a page reload.
- **Edge protection:** traffic is served through Cloudflare's network, with rate limiting in the application.
- **Development:** automated test suites run on every change. Changes are test-driven.

9. Subprocessorsors

PROVIDER	PURPOSE	LOCATION
Hetzner Online GmbH	Application servers and database	Germany
Cloudflare, Inc.	Recording storage (R2), content delivery, live media relay	EU (storage); global edge (relay)
Resend	Transactional email (sign-in codes, invitations, notices)	USA (SCC/DPF)
Stripe	Payment processing for paid plans	EU/USA (SCC/DPF)
Google	Optional "Sign in with Google" for hosts	EU/USA (SCC/DPF)

10. Incident response

- Production errors and recording failures are monitored with automated alerts.

- In the event of a personal data breach, we inform affected customers without undue delay and notify the competent supervisory authority within 72 hours, as required by GDPR Article 33.
- Report security issues to hamed@airtape.co.

11. Use in research

- Participants need no account, and no participant data is shared with anyone other than the host.
- The host decides what to record, when to delete it, and whether to transcribe it. Recordings can be downloaded and stored under the institution's own data management plan, then deleted from Airtape.
- A data processing agreement under GDPR Article 28 is available on request. We are happy to review institutional data use or research agreements.
- For consent procedures: participants see the host's name and the session before joining, and a recording indicator is visible to everyone while a recording runs.

This document describes the service as of the date above and is provided for vendor assessment. It is not a contract. The privacy policy at airtape.co/privacy and any signed agreement take precedence.