Trust.

How we keep interviews secure, private and fair, and the companies we work with to run testee.

Updated 17 November 2026

Arcolabs OÜ, registry code 17587452, Sepapaja tn 6, 15551 Tallinn, Estonia · hello@testee.ai

Security.

- **Encryption.** TLS for everything in transit; data encrypted at rest on Google Cloud.
- **Isolation.** Every company's data is checked on every request; each service has its own database and credentials.
- **Sign-in.** Two-factor authentication for every user who turns it on, single sign-on (SAML or OIDC) on Scale and Enterprise, and bot protection on sign-up.
- **Secrets.** Keys live in Google Secret Manager, never in code. Invitation links are stored hashed; the latest link is also kept encrypted (AES-256-GCM) so your team can copy it.
- **Audit log.** Who did what in your company, kept 365 days.
- **Our own team.** Staff use a separate admin zone with two-factor authentication, roles and a staff audit log.

Privacy.

- **You stay in control.** Your company is the controller of candidates' data; we process it only on your instructions.
- **No training.** We don't use your data or candidates' data to train AI models.
- **Minimal data.** The analysis gets the transcript and the work, never emails or names.
- **Erase and export.** Erase a candidate everywhere in one step, export their data as a file, and set retention per company.
- **Consent first.** Candidates see the AI notice and, when you record them, the recording notice, and agree before anything is recorded.

Fair and accountable AI.

- **People decide.** The coverage report supports your team; it's never a hiring decision.
- **Evidence for every point.** Each expectation's status comes with the exact quotes behind it, so reviewers can check it.
- **No judgments about the person.** No emotion, accent, fluency or personality assessment, no face analysis, no biometrics.
- **Signals, not proof.** Integrity signals describe what happened in the browser, for a person to review with the recording.
- **Accessible.** Candidates can answer by text instead of voice; captions are always on.

Where data is stored.

Data is stored and processed on Google Cloud in the European Union.

The voice interviewer, transcription and analysis run on OpenAI's API in the United States. OpenAI doesn't train on this data and keeps it for up to 30 days to detect abuse; see Sub-processors below.

Sign-in accounts (Google Identity Platform) and server logs, which hold ids and never interview content, are on Google's global infrastructure.

Sub-processors.

Company	What for	Data	Where
Google Cloud and Firebase	Hosting, databases, storage, sign-in, messaging	All service data	European Union; sign-in and logs global
Cloudflare Turnstile	Bot protection on workspace creation, verification emails and this site's forms	IP address, browser and connection signals	Global

Company	What for	Data	Where
OpenAI	AI interviewer, transcription, analysis, generation, assistant	Interview audio, transcripts, work, interview content	United States
Anam	Real-time video avatar of the AI interviewer (Enterprise, when the company turns it on)	The AI interviewer's voice, connection data (IP address); no candidate audio or video	United States, European Union
Resend	Sending emails	Email address, name, email content	United States
Stripe	Subscriptions and invoices; reseller of the monthly and yearly plans	Billing contact and payment details	United States, European Union
Web Push services (Google, Apple, Mozilla, Microsoft)	Push notifications to the team's devices that turned them on	The device's push address; the notification itself is end-to-end encrypted and holds generic text and ids, never names	Each vendor's own infrastructure (United States and others)
Plausible Analytics	Visit statistics for testee.ai, the dashboard and the interview pages, without cookies	Page addresses without ids or invitation links, referrer, browser and device type, country; IP address only to count visitors, never stored	European Union (Germany)
Upstash	Rate-limit counters (abuse and spend limits)	Counts under keys hashed with a secret key that stays with us (from IP addresses and account, invitation and session ids); no names, emails or content; gone within two days	European Union (Belgium)

How long data is kept.

Data	Kept
Candidates with no activity	Erased after 365 days (set per company, up to 10 years)
Interview audio and camera or screen recordings	Deleted 180 days after the interview (set per company, up to 10 years)
Dashboard assistant conversations	90 days after the last message
Audit log	365 days
AI system log (ids, models, versions, statuses and times; no names or content)	190 days after its last entry, also after an erasure from 2 December 2027 (EU AI Act Articles 12 and 19)
Server logs	30 days
Deleted companies and organizations	Gone after a 7-day grace period; database backups roll over within 30 days

Legal documents.

- Terms of service
- Privacy policy
- Data processing agreement
- Accessibility

Questions.

Security or privacy question, or found a vulnerability? Write to hello@testee.ai. We answer every report.