

HoneyBeeDialer — Privacy Policy

Version 1.1 · Effective 31 July 2026 · Permanent URL: <https://honeybeedialer.com/legal/privacy>

This Policy explains what personal data HoneyBeeDialer ("HoneyBee", "we") collects, why, who we share it with, how long we keep it, and what rights you have. It covers our website, the application, and our support channels.

1. Two very different roles

Read this section first — it determines which rules apply and who you contact.

We are the controller of data about our own customers: the account you create, your admin and user records, billing details, support correspondence, and how you use the product. This Policy governs that data.

We are a processor of the calling data our customers put into the platform — the consumers they call, their phone numbers, call recordings, transcripts, and outcomes. For that data the **customer agency is the controller**. They decide who is called and why; we only process on their documented instructions under our agreement with them.

If you were called by an agency using HoneyBee and want your data corrected or deleted, the agency holds it and decides. Contact them. If you cannot identify them, write to us at the address below with the number that called you and the date, and we will route your request to the responsible customer and tell you we have done so. We cannot delete a customer's records on our own initiative, but see section 7 on do-not-call.

2. What we collect

Account and identity. Name, email, phone, hashed password, organization, role, and multi-factor authentication settings. We never store passwords in readable form.

Billing. Plan, subscription status, billing email, and payment history. Payments run through Whop; **we do not receive or store full card numbers.**

Usage and product telemetry. Pages visited, features used, call volumes, credit consumption, timestamps, and device/browser metadata.

Security and audit logs. IP address, user agent, sign-in events, and a record of privileged actions — role changes, credential changes, tenant suspensions, exports, and purges — kept as tamper-evident evidence.

Support. Anything you send us in a ticket or email.

Customer Data (processed for our customers). Lead names and contact details, call audio and recordings, transcripts, AI-generated summaries and coaching notes, dispositions, pipeline and underwriting records, and consent and do-not-call records. **We do not decide what goes in here.** Our customer does.

We do not knowingly collect data from anyone under 18, and the Service is not directed at children.

3. Why we process it, and on what basis

Purpose	Basis (GDPR Art. 6)
Providing and operating the Service	Contract
Billing and collecting fees	Contract
Security, fraud prevention, abuse detection, audit evidence	Legitimate interests; legal obligation
Support and service communications	Contract; legitimate interests

Purpose	Basis (GDPR Art. 6)
Product improvement and aggregate analytics	Legitimate interests
Legal and regulatory compliance, including TCPA record-keeping	Legal obligation
Marketing email to prospects	Consent, withdrawable at any time

We do not sell personal data. We do not share it for cross-context behavioural advertising. We do not use Customer Data to train AI models, and we require the same of our AI subprocessors.

4. Automated processing and AI

The Service transcribes calls and generates summaries, sentiment signals, coaching suggestions, and underwriting assistance. Call audio and content are sent to the AI subprocessors in section 5.

This assists humans; it does not decide anything about a consumer on its own. No legally or similarly significant decision about a person is made solely by automated means within the Service. Agencies remain responsible for their own decisions, and AI output can be wrong — it must be independently verified.

5. Who we share it with

We use these subprocessors. All are bound by written terms restricting them to our instructions.

Subprocessor	Purpose	What it receives
Amazon Web Services	System of record, file storage, queues	Account and lead data, call recordings
Twilio	Telephony, call bridging, recording capture	Phone numbers, call audio, call identifiers
Deepgram	Speech-to-text on live call audio	Call audio, transcripts
Google (Gemini)	AI call and lead analysis	Call and lead content in prompts
Anthropic	AI analysis	Call and lead content in prompts
Cartesia	Speech synthesis	Generated speech text
Whop	Billing and subscriptions	Billing email, plan, membership status
SendGrid	Transactional email	Email addresses
GoHighLevel	Optional CRM sync — only if the customer enables it	Lead and outcome data
Railway	Backend hosting	Traffic in transit and in memory
Vercel	Frontend hosting	Traffic in transit

Each customer connects **their own Twilio account**; telephony credentials are never shared between organizations.

We also disclose personal data when the law compels it, to enforce our Terms, to protect rights and safety, and to a successor in a merger or asset sale (with notice, and this Policy continues to apply until replaced).

The current list lives at <https://honeybeedialer.com/legal/privacy>. We notify customers before adding a new subprocessor that handles personal data, so they can object.

6. Where data is stored

Primary storage is **Amazon Web Services in the US East (Ohio) region**, in a dedicated AWS account. Some subprocessors process data elsewhere. Where personal data protected by UK or EU law is transferred outside those areas, we rely on the European Commission's Standard Contractual Clauses together with appropriate technical and organisational transfer measures.

7. How long we keep it

Data	Retention
Security audit log	400 days
Webhook idempotency keys	30 days
Dialer session state	4 hours
Queue messages	4 days
Call records	7 years (billing and TCPA defence)
Call recordings and transcripts	2 years by default
Lead contacts	Until the customer deletes them, or 90 days after the customer closes their account
User accounts	Life of the account plus 30 days
Outcomes and pipeline records	7 years
Do-not-call and recording-consent records	5 years — see below

Expiry is applied automatically on write, not by a manual sweep.

Do-not-call records are deliberately hard to erase. TCPA 47 CFR § 64.1200 requires them to be kept for five years, and they survive even a full customer account purge. That obligation exists to protect the person who asked not to be called — erasing it would let the same number be dialled again. If you ask us to delete a do-not-call entry, we will normally refuse and explain why.

Backups. Point-in-time recovery retains 35 days. When an organization is purged we write a permanent tombstone, and any restore must consult it, so a restore cannot resurrect deleted data. This check fails closed.

8. Your rights

Depending on where you live, you may have the right to access, correct, delete, port, restrict, or object to processing, to withdraw consent, and to be free from discrimination for exercising these rights.

Under GDPR/UK GDPR you may also complain to your supervisory authority. **Under the CCPA/CPRA** you have rights to know, delete, correct, and opt out of sale or sharing — and again, **we do not sell or share personal data** for those purposes.

To exercise a right, email **support@honeybeedialer.com**. We will verify your identity, respond within **30 days** (extendable where the law allows, with notice), and will not charge unless the request is manifestly unfounded or excessive.

Customers can act directly in-product: export everything via account export, and run an erasure with a dry run first at Organization Settings. Erasure deletes personal records and anonymises call rows so billing and regulatory evidence survive without personal data.

Restores. A purged organization carries a permanent record that a backup restore cannot override, so deleted data is not resurrected. Where a restore could affect an individual erasure, we re-apply that erasure and notify you.

9. Security

We encrypt data in transit (TLS) and at rest (AWS KMS). Tenant isolation is enforced on the server for every request; a client cannot select another organization's data by changing a value in a request. Passwords are hashed. Integration secrets, including Twilio credentials, are encrypted and never returned to the browser after saving. Privileged actions are written to an audit log. Access follows least privilege, and multi-factor authentication is available and recommended.

No system is perfectly secure. If a breach affects your personal data we will notify you and the relevant regulator as the law requires — for GDPR, without undue delay and within 72 hours of becoming aware where feasible.

Report a vulnerability using the contact address below. We will not pursue good-faith researchers who follow responsible disclosure.

10. Cookies

We use cookies strictly necessary for signing in, keeping your session, and security. We do not use advertising cookies and we do not sell data to advertisers. If we add analytics cookies we will ask for consent first where required.

11. Call recording

The platform records calls when a customer enables it. **Recording law varies by state**, and several require every party's consent. Our customers are responsible for obtaining consent and for the announcements they make. The platform can capture and store consent evidence, and retains it for the life of the recording.

If you were recorded and want a copy or its deletion, contact the agency that called you, or write to us and we will route it.

12. Changes

We will post any change here with a new version number and effective date. Material changes are notified to account admins at least 30 days in advance. Superseded versions are available on request.

Contact

HoneyBeeDialer

All enquiries — privacy and data-subject requests, security reports, support and legal notices — go to support@honeybeedialer.com. Mark a privacy or security matter in the subject line so it is routed promptly.

Related documents: [Terms of Service](#)

Document version 1.1 · Effective 31 July 2026 · Supersedes: 1.0

Generated 01 August 2026. The authoritative version is published at <https://honeybeedialer.com/legal/> — if this copy and the published page differ, the published page governs.