

Privacy Policy

Effective 16 September 2026

Who this notice covers

This Privacy Policy covers Adversarial AI's hosted website, chat, API and billing services. The provider is Adversarial AI LLC, a New Jersey limited liability company, at 1078 Summit Ave #605, Jersey City, NJ 07307, USA. Contact contact@adversarial.ai for privacy questions. We serve adults worldwide, subject to applicable legal restrictions.

Account and authentication data

We process account identifiers, name and email, authentication information and, where used, Google sign-in information. Account and activity timestamps support access and account administration. Authentication data is separate from prompts and model responses.

Billing and account-linked usage

We retain wallet balances and ledger entries, membership and payment references, and usage records associated with accounts or API credentials. Usage includes model, request identifier, input tokens, cached input tokens and output tokens. These records support charging, subscription caps, reconciliation and disputes; they are not anonymous. Stripe processes card payments. Do not send payment credentials in prompts or support messages.

Prompts, responses and temporary processing

Hosted inference processes your input and generated output. Temporary chat is configured not to save conversations to chat history. This does not mean immediate erasure from every processing layer: runtime buffers and GPU prefix/KV caches can remain until eviction, overwrite or process termination. Uploaded files, saved notes or other saved features, support correspondence and customer-connected integrations have separate lifecycles. Closing a browser window does not guarantee erasure from all systems. Do not submit sensitive workloads that require a specific retention or hosting guarantee without an appropriate written agreement.

Model training

We do not use customer prompts or outputs to train or fine-tune our models unless you separately and expressly opt in. General Terms acceptance is not training consent. We do not grant ourselves a license to sell customer content. Customer-authorized third-party integrations have their own data practices.

Operational telemetry

We collect service demand and reliability metrics, including running and waiting requests, queued input-token counts and infrastructure memory usage. The dashboard collector exports counts, not prompt text. Operational samples have a 30-day database cleanup rule. Security and service providers may separately process connection details, IP addresses, timestamps and error diagnostics. These records are distinct from billing usage.

Service providers and integrations

Our service uses Heroku for application infrastructure, RunPod for GPU hosting, Stripe for card payments, and Google when you select Google sign-in. Providers process information needed for their respective services. Crypto payments create transaction and reconciliation records; paying with crypto does not make your platform account anonymous. Customer-selected integrations can receive data under their own terms. We may disclose information for a valid legal obligation, to protect rights or service security, or in a business transfer subject to applicable safeguards.

Cookies and browser storage

We use cookies and browser storage for authentication, account sessions and interface functionality. The billing account cookie has a configured lifetime of 30 days. Session and browser storage can persist until expiry, logout or removal, depending on the feature. Removing required storage can sign you out or interrupt access. Optional processing requiring consent must be presented separately; agreeing to the Terms is not consent to unrelated advertising or tracking.

Retention and deletion

Operational metric samples are deleted under a 30-day cleanup rule. Account, usage and payment records do not share that expiry and are not automatically erased when a chat closes. Retention depends on account operation, payment reconciliation, tax and accounting duties, security investigations, disputes and legal obligations. Contact us to request account closure and deletion; we assess and delete information that is no longer needed, subject to lawful exceptions. Some records and backups can remain after removal from an active interface. We do not promise one universal deletion deadline or zero retention across all providers.

Privacy requests

Contact contact@adversarial.ai to request access, correction, deletion, an export, or to object to or restrict processing where applicable. We may request proportionate identity verification. Depending on your location, you may withdraw consent for consent-based processing and complain to your local data-protection authority. We respond under applicable legal deadlines and explain applicable exceptions. Do not email passwords, API keys or unnecessary sensitive information.

Security and legal disclosures

We use access controls and safeguards appropriate to the service; no system is perfectly secure. Access and disclosures must be limited to authorized purposes and legal obligations. If a breach triggers notification duties, we will provide the notices required by applicable law. This policy is not a promise of a security certification, air-gapping, private tenancy or mutual TLS on every connection.

International users and children

We are based in the United States and use infrastructure that can process information in the United States and other countries. Processing location depends on the service and provider. Where applicable data-protection law requires a lawful basis, we rely on performance of our contract for requested services, legitimate interests for proportionate security and operations, legal obligations for required records, and consent where required. We do not claim that worldwide availability itself establishes a lawful transfer mechanism. Contact us before transferring regulated or third-party personal data that requires a DPA, specified region or particular international-transfer safeguards; those arrangements must be established for the applicable service. The service is for adults aged 18 or over; report suspected child accounts to our contact address.

Changes and acceptance

This policy is effective 16 September 2026. We will publish dated revisions and give notice of material changes as required. We record Terms acceptance using an account identifier, timestamp, document version/hash and affirmative action; we retain that evidence to administer and establish the agreement and address disputes. Acknowledging this notice is not blanket consent to other processing. Recurring payment consent is disclosed separately at checkout.