Privacy Policy

Version 1.2.0 · Effective 15 November 2026 · EPIC AI Solutions Pty Ltd

These documents are being finalised and will be reviewed before payments open.

This policy explains what personal information EPIC AI Solutions Pty Ltd (ABN 92 700 539 635) collects when you visit epic-ai.solutions or use our service, why we collect it, who we share it with, how long we keep it, and the choices and rights you have.

Your projects and personal data are yours. We will never sell your information, and we only use it where we need to, to run your account and deliver our services.

1. Who is responsible for your information

EPIC AI Solutions Pty Ltd, an Australian company registered in Queensland, is responsible for your personal information. Under the European Union and United Kingdom General Data Protection Regulation (GDPR) we are the “controller”.

For any privacy question or request, email privacy@epic-ai.solutions. One of the owners of EPIC reads it and will reply within one month.

2. The laws we follow

We write this policy to the Australian Privacy Principles in the Privacy Act 1988 (Cth). Because people from other countries can join EPIC, it also covers the EU and UK GDPR, and the privacy laws of US states such as California. The sections near the end add what those laws require.

3. What we collect

When you create and use an account

- your email address and whether you have confirmed it;
- your display name, your first, middle and last name, and, if you add them, a profile picture and contact details such as a phone number, company name, ABN and postal address;
- your password, which we store only as a one-way hash, and, if you turn on two-step login, its encrypted secret and hashed recovery codes;
- your confirmation that you are 18 or older and the versions of this policy and the Acceptable Use Policy you accepted;
- your sessions: when they started and were last used, the IP address and a description of the browser or device;
- your API keys: their label, the first and last few characters, when they were last used and the internet address they were last used from. Your pages do not show that address; it is in your data export, and our operators use it to look into misuse of a key. We never store a full key, only a hash of it;
- your preferences, such as your colour scheme, layouts, your time zone and which optional emails you want, among them maintenance schedule emails: the confirmed time of a maintenance on a server you hold slots on, sent only if you turn them on;
- a record of the optional emails and service notices we sent you, and when.

When you secure a slot

- the country you declare, which we check against sanctions lists;
- your slot purchases: amounts, refunds, the payment provider’s references, and the name and email on your slot certificate. Your card details go to the payment provider, never to us.

When you use the models

- usage records for each request: when it happened, which account, API key and model were used, how many tokens were sent and generated, how long it took and whether it succeeded. Usage records contain no prompt or answer and no IP address.

Other things you send us

- if you join the waitlist: your email address and an optional message, and a record of the waitlist emails we sent you;
- if you register interest in slots: the kind of interest, how many slots and how likely you are to buy, and whether you asked us to email you when slots open;
- if you join the affiliation programme: your codes, your leaderboard choice, a promotional profile if you publish one, and who joined through your code;
- if you ask the community a question: the question and our answer;
- if you report abuse: your email address, your IP address and what you tell us;
- if you email us: your message and address.

Collected automatically

- your IP address and the country and region your connection comes from, used to protect the service from abuse and, when you create an account, to check that you are not connecting from a sanctioned country;
- a record in our audit log of security-relevant actions, such as logins, changes to two-step login, data exports and deletion requests;
- short-lived technical logs that help us run and fix the service.

4. Your prompts and the answers you receive

We do not store your prompts or the answers the models give you. They pass through our servers to the model and back to you. We do not train AI models on them. There are only two exceptions, and both are encrypted with a key that belongs to your account alone:

- Diagnostic capture: if your account owner turns it on to help us debug a problem, we keep the exact requests while it is on, and delete each one after 7 days, or straight away when it is turned off.
- Elevated-risk review: if your account has an approved opt-out from automated screening, we keep 5% of its prompts so a person on our team can check the opt-out is used as described. Each sample is deleted after 90 days.

To comply with the law and keep the community safe, we may screen requests automatically for a small number of clearly illegal or harmful categories, described in our Acceptable Use Policy. When a request is refused, we record only the category, never the prompt. If a report shows child sexual abuse material, we preserve the evidence and report it to the authorities as the law requires.

5. Why we use your information

We only use your information for the purposes below. Under the GDPR, each has a legal basis:

- to provide your account, your slots, the models, the affiliation programme and the community features you use (performance of our contract with you);
- to keep the service secure, prevent abuse and fraud, share capacity fairly, keep an audit trail, and understand and improve how the service is used (our legitimate interests, which we balance against your rights);
- to run diagnostic capture, send optional emails and keep your waitlist entry (your consent, which you can withdraw at any time);
- to screen for sanctions, keep tax records and report child sexual abuse material (legal obligations).

We do not use your information for advertising, we do not build profiles of you for marketing, and we do not sell it to anyone.

6. The emails we send

Some emails are needed to run your account and are always sent: confirming your address, resetting your password, security alerts, notices about your account and your slots, and service notices to every member about the service itself, such as planned maintenance or an outage.

Others are optional, and you choose them in your Profile:

- Product updates: news about EPIC’s features and plans;
- New model votes: when a model vote opens, its title, its due date and a link to the voting box;
- Monthly usage summary: on the 1st of each month, how many requests and tokens you used with each model in the month before, compared with the month before that. It is not sent for a month without usage.

If you register interest in slots and tick “Email me when slots open”, we email you when slots can be ordered. If you join the waitlist, we may email you about EPIC’s launch and availability. Every optional email and every waitlist email has a link that stops it: it turns that email off, or removes your address from the waitlist. We send them through our email delivery provider.

7. Who can see your information

Within EPIC, only the people who run the service can see your information, and only when they need to. Every time an operator opens encrypted content, it is recorded in our audit log.

If you are a member of a pool, the pool’s manager can see your usage, such as how many requests and tokens you used, but never the content of your prompts or answers. You are told this when you join a pool.

If you join through someone’s referral code, each slot you buy raises that person’s points, which can appear on our public leaderboard. Your name is never shown, but on a small leaderboard a change in their points can reveal that someone they referred made a purchase.

If you take part in the leaderboard, your points and accounts created are shown publicly, under your profile name or as “Anonymous”. An anonymous line shows the same figures, so people who follow the leaderboard closely may be able to link it to you.

A question you ask the community anonymously is published without your name, but our team can see

who asked it and may email you about it.

8. Service providers we share it with

We use a small number of service providers to run EPIC. They may only use your information to provide their service to us:

- a network, security and hosting provider, which protects our website, checks forms for bots and stores our encrypted off-site backups;
- an email delivery provider, which sends the emails you receive from us;
- a mailbox provider, which receives the emails you send us;
- a payment provider, once payments open, which processes your payment.

You can ask privacy@epic-ai.solutions for the current list of providers. We run our AI models, monitoring and logging ourselves, on our own systems.

We may also disclose information when the law requires it, to protect people from harm, or to establish or defend legal claims.

9. Where your information is kept

We store your personal information in Australia, and our encrypted off-site backups are kept in the Oceania region. Some of our service providers process information in other countries, including the United States and countries in the European Union, for example to deliver email or to serve our website from a location near you. When information leaves Australia, we take reasonable steps to make sure it is handled to the standard of the Australian Privacy Principles. For people in the EU and UK, such transfers rely on adequacy decisions or the standard contractual clauses our providers offer.

10. How long we keep it

- Your account and what belongs to it: while your account exists. When you delete your account it is disabled straight away and permanently deleted 30 days later.
- Sessions: deleted one day after they end. A session ends when you log out, after 7 days without use, or 30 days after you logged in, whichever comes first.
- The record of the optional emails and service notices we sent you: kept for the service term, or until you delete your account.
- Email links for confirming an address or resetting a password: deleted one day after they expire.
- Diagnostic captures: 7 days. Elevated-risk review samples: 90 days.
- Purchase records, which include your name, email, company, ABN and address as they stood when you paid: five years from the end of the Australian financial year of the purchase (the 30 June after it), as tax law requires, also after you delete your account. When that period has ended and your account is deleted, your details are removed from them automatically, and we destroy any other copies we keep. Slot certificates lose your name and address when your account is deleted.
- Accounts we block or close for abuse: a restricted record (the account’s ids and email, its last login, its API keys and the reports and decisions about it) is kept for one year from the decision, or longer only under a legal hold. Only our operators can see it, and every look is logged.
- Blocked email addresses: after that year, we keep only a one-way keyed hash of the address, for as long as the block stands, so that it can be refused again.

Other information, such as usage records, abuse reports and our audit log, is kept for as long as we need it for the purpose we collected it for, or for as long as the law requires. Data you delete can remain in our encrypted backups until those backups are deleted in turn.

11. How we protect your information

- Every connection to EPIC is encrypted. Our own servers accept TLS 1.3 only. Our website is reached through Cloudflare, which also accepts TLS 1.2 from older browsers and answers an unencrypted address only with a redirect to its encrypted one, so nothing of yours is sent unencrypted.
- Each account's data is kept apart by row-level security in our database, so one account cannot read another's data even if a query goes wrong.
- Passwords are hashed with Argon2id. API keys are shown to you once, when they are created, and stored only as a hash: we cannot recover a lost key, only replace it.
- Our secrets and encryption keys are held in a dedicated secrets vault, and stored content is encrypted with a key for each account.
- Security-relevant actions are written to a tamper-evident audit log.

12. Your choices and rights

You can, at any time:

- see and download the personal information in your account, from your account page;
- correct your names, display name and contact details on your account page, and change your email address through its confirmation step;
- delete your account from your account page;
- turn optional emails on or off, and leave the leaderboard or the affiliation programme;
- ask us to stop using your information for a purpose, restrict how we use it, or explain how we have used it, by emailing privacy@epic-ai.solutions.

We will reply within one month. We may need to confirm your identity first, and some information we must keep by law, as described above.

If a decision about your account is made automatically, such as an API key being disabled after repeated refused requests, you can ask a person on our team to review it.

If you are unhappy with how we handled your information, please tell us first. You can also complain to the Office of the Australian Information Commissioner (OAIC), or, in the EU or UK, to your local data protection authority.

13. People in the European Union and the United Kingdom

You have the rights of access, correction, erasure, restriction, objection and data portability, and the right to withdraw consent at any time. Your data export is in a common machine-readable format (JSON). The legal bases we rely on are listed above. You can exercise any of these rights by emailing privacy@epic-ai.solutions.

14. People in the United States

We do not sell your personal information, and we do not share it for cross-context behavioural

advertising. Depending on the state you live in, you may have the right to know what we collect, to correct and delete it, and to not be treated differently for using your rights. Email privacy@epic-ai.solutions to use them.

15. Children

EPIC is for adults only. We do not knowingly collect information from anyone under 18. If we learn that an account belongs to someone under 18, we will close it and delete its information.

16. Changes to this policy

When we change this policy, we publish the new version here with a new version number, and tell members before the change takes effect. We may ask you to accept the new version when you next log in. Emails about changes to this policy or our terms are service messages, so they are sent even if you have turned optional emails off.

17. Contact

EPIC AI Solutions Pty Ltd, Queensland, Australia. Privacy questions and requests: privacy@epic-ai.solutions.