Embry Privacy Policy

Effective: April 28th, 2026 **Last updated:** April 28th, 2026

> **Plain-English summary.** Embry is a fertility and cycle-tracking app built with privacy as a core feature, not an afterthought. Your cycle and health data is encrypted with a key unique to you — even our database operators cannot read it. We never sell your data, never share it with advertisers, and never use it to train AI models. This document explains in detail what we collect, why, how we protect it, and what rights you have. If anything is unclear, email privacy@embry.ca.
>
> **This is a draft.** This document is in draft form pending review by qualified privacy counsel. It will be finalised before Embry is opened to the general public.

---

1. Who we are

Embry ("Embry," "we," "us," "our") is operated by [Legal entity TBD], based in Ontario, Canada. Embry is the data controller for the personal data described in this policy.

- **Privacy contact:** privacy@embry.ca
- **Data Protection Officer:** We have not appointed a DPO. Our internal DPO assessment concluded that a designated DPO is not required at our current scale and processing scope. We will reassess if our processing changes materially.
- **EU representative (Article 27 GDPR):** To be appointed prior to any launch in the European Economic Area.

---

2. Where Embry is available

Embry's availability varies by region for legal and product-readiness reasons. The current status is:

Region	**Status**
Canada	Open
United Kingdom	Gated waitlist

Region	Status
Australia	Gated waitlist
United States (excluding Washington State)	Gated waitlist
Washington State	Closed
European Economic Area	Closed (waitlist only)

If Embry is not yet available in your jurisdiction, you may join the waitlist; we do not begin processing your health data until you are admitted.

A note on US health-privacy law. Embry is a consumer wellness app, not a healthcare provider. **The US Health Insurance Portability and Accountability Act (HIPAA) does not apply to Embry.** References elsewhere in this policy to consumer health-privacy laws (such as Washington State's My Health My Data Act) reflect those specific frameworks, not HIPAA.

---

3. What data we collect

3.1 Account and identity

- Email address
- Password (stored only as a hash by Supabase Auth; we cannot read or recover your password)
- Session tokens (delivered as httpOnly, SameSite=Strict cookies)
- IP address (used for security, abuse prevention, and region detection)
- Consent records (timestamps and versions of agreements you have accepted)
- Multi-factor authentication credentials, if you enable MFA

3.2 Health data (special-category data under GDPR Article 9)

The data you log in Embry to track your cycle and conception journey, which may include:

- Cycle and period dates
- Basal body temperature (BBT) readings
- Luteinizing hormone (LH) test results
- Cervical mucus observations
- Intercourse logs
- Pregnancy test results
- Symptoms, mood, and free-text notes

- Predictions and insights derived from your data
- Profile information: name, date of birth, last period date, cycle regularity

3.3 AI conversational data

- The text of your messages to Embry's AI assistant
- Classifier outputs (e.g., whether a message was identified as a medical-advice request)
- Records of your acknowledgements of medical-advice gates

3.4 Operational data

- Audit log entries (who did what, when — used for security and Article 30 records)
- Feedback you submit (a hash is stored on Supabase; the free-text body is sent to a private operator GitHub repository)
- Error telemetry (limited to non-content technical signals, e.g., stack traces with personal data redacted)

3.5 Product analytics — and what we will *never* send to analytics

We use a privacy-respecting analytics provider (PostHog EU) to understand how the app is used, but we apply a strict **forbidden-fields list**. The following data is never sent to product analytics under any circumstances:

- Intercourse logs
- Pregnancy test results
- LH test values
- BBT values
- Raw cycle or period dates
- Symptoms, mood, or cervical mucus observations
- The content of your AI chat messages

Analytics events we *do* collect are limited to anonymous interaction signals (screen visits, feature usage, performance metrics) and only when you have opted in. Autocapture and session replay are turned off.

---

4. Lawful bases for processing (GDPR / UK GDPR)

Where GDPR or UK GDPR applies, we rely on the following lawful bases:

Processing	**Lawful basis**
Account creation, login, core cycle-tracking features	Article 6(1)(b) — performance of contract
Processing of health data (special-category)	Article 9(2)(a) — your **explicit consent**, collected separately from acceptance of these Terms
Maintaining audit logs	Article 6(1)(c) — legal obligation; and Article 6(1)(f) — legitimate interest in security
Product analytics	Article 6(1)(a) — consent only; analytics is off until you opt in
Error monitoring	Article 6(1)(f) — legitimate interest in service reliability

Your consent to health-data processing is collected **separately** from your acceptance of the Terms of Use. This separation is intentional: consent under MHMDA and GDPR Article 9 must be specific and unbundled from contractual acceptance.

---

5. How we use your data

We use your data to:

- Provide cycle tracking and predictions
- Generate AI insights grounded in your own data
- Authenticate you and protect your account
- Respond to your support requests
- Detect, prevent, and respond to security incidents and abuse
- Comply with legal obligations
- Understand product usage (only with your consent)

What we will never do

These commitments are unconditional:

- **We will never sell your data.**
- **We will never share your data with advertisers or third-party ad networks.**
- **We will never use your data to train AI models.** Our AI provider, Anthropic, operates under zero-retention terms — your inputs and the AI's outputs are not retained or used for training.
- **We do not embed third-party advertising trackers in the app.**

---

6. Sub-processors

We use a small number of carefully selected sub-processors to deliver the service. The current list is:

Sub-processor	**Purpose**	**Region**
Supabase	Database, authentication, storage	EU (migration in progress)
Vercel	Application hosting	Global edge
Anthropic	AI assistant (Claude), zero-retention	US
AWS KMS	Cryptographic key management for envelope encryption	Region-specific
Sentry	Error monitoring	EU
Resend	Email	EU
Cloudflare Turnstile	Bot protection	Global edge
Upstash	Rate limiting	EU
PostHog EU	Product analytics (consented only)	EU
GitHub	Operator-facing feedback storage	US
Stripe	Payment processing (post-launch)	Global

We will publish updates to this list whenever it changes. Where a sub-processor accesses personal data on our behalf, we have a Data Processing Agreement in place.

---

7. International transfers

Some sub-processors are located outside Canada, the EEA, or the UK. Where personal data is transferred internationally we rely on:

- **EU/UK to US transfers:** Standard Contractual Clauses (SCCs); UK International Data Transfer Addendum (IDTA) where applicable.
- **Anthropic:** Zero-retention configuration so your AI inputs and outputs are not stored.
- **Supabase:** Migration to EU-region infrastructure is a pre-launch commitment.

If you would like a copy of the safeguards in place for a specific transfer, contact privacy@embry.ca.

---

8. How we protect your data (Article 32 summary)

Embry's security architecture is designed around the assumption that the database itself should not be a single point of compromise.

- **Per-user envelope encryption.** Sensitive fields are encrypted with AES-256-GCM. Each user has their own data encryption key (DEK), wrapped by a master key in AWS KMS. The encryption uses Additional Authenticated Data (AAD) bound to `{userId, table, column}` to prevent cross-record substitution.
- **Row-Level Security (RLS).** Every user-data table in our database enforces RLS, so a query can only return rows belonging to the authenticated user.
- **Service-role isolation.** The privileged Supabase service-role key is fenced to two specific server files and never exposed to the browser or wider codebase.
- **Append-only audit logging.** Security-relevant actions are written to an append-only audit log retained for 7 years.
- **Transport security.** TLS 1.2 or higher; HTTP Strict Transport Security (HSTS).
- **Authentication.** Multi-factor authentication is available; sessions use httpOnly, SameSite=Strict cookies.
- **Abuse prevention.** Cloudflare Turnstile and per-route rate limiting (default 30 requests per hour for sensitive endpoints).

No security architecture is perfect, but ours is designed to limit the blast radius of any single failure.

---

9. How long we keep your data

Data category	**Retention**
Account and cycle data	Lifetime of your account; on deletion, cryptographically shredded (see Section 10)
Audit logs	7 years
Sentry error data	30 days
PostHog analytics — events	1 year
PostHog analytics — feature flags / cohort data	7 years
Rate-limit counters	Hours
Consent records	Lifetime of account + 7 years (evidentiary)

---

10. Your rights

Depending on where you live, you have some or all of the rights below. You can exercise most of them in-app; for anything not available in-app, email privacy@embry.ca.

- **Access (GDPR Article 15):** Request a copy of your data via the in-app export feature (`GET /api/export`).
- **Rectification (Article 16):** Edit or correct your data directly in the app.
- **Erasure / "right to be forgotten" (Article 17):** Delete your account, which triggers **cryptographic shredding** — we destroy your unique data encryption key in constant time, rendering your encrypted data permanently unrecoverable. We then issue you a signed deletion receipt.
- **Data portability (Article 20):** Request a portable, integrity-signed JSON export of your data via the in-app export feature.
- **Object to processing (Article 21):** Toggle your privacy status to object to specific processing.

- **Withdraw consent:** You can withdraw consent at any time. Withdrawal does not affect processing carried out before withdrawal.
- **Lodge a complaint:** See Section 15 below for jurisdiction-specific complaint paths.

---

11. Cookies and similar technologies

We use cookies sparingly and only for functional purposes:

- **Authentication cookies.** httpOnly, SameSite=Strict. Required to keep you logged in.
- **No advertising cookies.** We do not use cookies for advertising or cross-site tracking.
- **PostHog autocapture and session replay are turned off.** We do not record your sessions or capture interactions automatically.

---

12. Children

Embry is not intended for users under the age of 18, or older where local law sets a higher minimum. We collect date of birth at signup and decline to create accounts that fall below the threshold.

---

13. Breach notification

In the event of a personal data breach, we follow the procedures documented in our internal breach-notification runbook:

- Notification to the lead supervisory authority within 72 hours of becoming aware of a notifiable breach (GDPR Article 33).
- Direct notification to affected users when the breach is likely to result in a high risk to their rights and freedoms (Article 34).

---

14. Changes to this policy

We will update this policy when our practices change. For material changes — particularly any change that would expand how your health data is processed — we will re-prompt you for consent before the change takes effect. We will provide reasonable notice of all changes by email or in-app notification.

15. Per-jurisdiction supplements

15.1 Canada (PIPEDA, plus provincial laws including Quebec's Law 25)

- Privacy contact: privacy@embry.ca
- You have the right to access and correct your personal information.
- You may file a complaint with the Office of the Privacy Commissioner of Canada (OPC) or your provincial regulator.

15.2 United Kingdom (UK GDPR, Data Protection Act 2018)

- Lead supervisory authority: Information Commissioner's Office (ICO).
- All GDPR rights described above apply.

15.3 European Economic Area (GDPR)

- Once Embry is available in the EEA, you may lodge a complaint with your local data protection authority.
- Article 27 representative: To be appointed.

15.4 Washington State (My Health My Data Act)

- Embry is currently **not available** in Washington State.
- When we launch in Washington, MHMDA's specific rights apply, including the right to bring a private action under the Washington Consumer Protection Act for violations.
- Consumer health data processing is gated behind explicit consent collected separately from these Terms.

15.5 California (CPRA / CCPA)

- We do not "sell" or "share" your personal information as those terms are defined under the CPRA.
- You have the right to know, correct, delete, and limit use of sensitive personal information.
- Categories of sensitive personal information collected: account credentials, health data, region-level geolocation.

15.6 Australia (Privacy Act / Australian Privacy Principles)

- The APPs apply. You may complain to the Office of the Australian Information Commissioner (OAIC).

16. How to contact us

- **Privacy questions and rights requests:** privacy@embry.ca
- **General support:** support@embry.ca