

Privacy Policy

Effective date: 26 September 2026

This Privacy Policy explains how Hearttec Software AS collects, uses, shares and protects personal data when you use Repetio: the website at repetio.ai, the Repetio mobile apps and related services (the "Service"). It also explains your rights and how to use them.

1. Who is responsible

The data controller is **Hearttec Software AS**, a company registered in Norway ("we", "us" or "our"). Norway is part of the European Economic Area (EEA), so the EU General Data Protection Regulation (GDPR), as implemented in the Norwegian Personal Data Act (personopplysningsloven), applies to how we handle your data.

For any privacy question or request, contact us at info@repetio.ai.

2. The data we collect

Account data. Your email address and password (or sign-in through a provider we support), display name, username, profile picture, time zone, and the dates your account and subscription started.

Study content. The notes, decks, cards, tags and images you create; files you upload for AI card generation (such as PDFs, slides and documents); exam plans; deck settings; and the decks you import or share with collaborators.

Study activity. Your review history (which cards you studied, when, how you rated them and how long you took), scheduling data, streaks and progress statistics.

AI interactions. Questions you ask the AI study assistant and the support chat, the answers you get back, and records of how many AI generations and questions you have used, which we need to apply plan limits.

Community activity. Decks you publish to Explore, likes, favourites, comments, imports and reports you submit or receive.

Feedback. Messages you send through the in-app feedback tool and whether you allow us to contact you about them. With each submission we record the page you were on, the deck involved, your plan, your screen size and your browser type, so we can understand the problem.

Billing data. Your plan, subscription status, trial dates, payment history and the customer and subscription identifiers from Stripe, Apple, Google or RevenueCat. Card details are handled entirely by the payment provider. We never see or store your full card number.

Communication data. Your email and notification preferences, the emails we have sent you, and

delivery events such as delivered, bounced, complained or unsubscribed. If you turn on push notifications, we store the push subscription your browser gives us, which is an endpoint address plus keys, together with your browser or device type.

Usage and device data. Pages you visit, features you use, clicks and other interactions, referring page, browser and device type, operating system, approximate location derived from your IP address, and performance measurements. See section 8 for the tools we use.

Data from support. Anything you tell us when you email us.

We do not ask for sensitive ("special category") data. Please do not upload patient records or other people's health or sensitive data into the Service. If you study using real clinical material, remove anything that identifies a person first.

3. Why we use your data and our legal bases

- **Providing the Service** (performance of our contract with you, GDPR Art. 6(1)(b)). We use your data to create and run your account, store and sync your content across devices, schedule reviews, generate cards and answers with AI, run Explore and community features, process subscriptions, and send service messages such as sign-in links, security notices, receipts and payment problems.
- **Study reminders and product emails** (legitimate interest, Art. 6(1)(f), or consent, Art. 6(1)(a), where the law requires it). We send reminders when cards are due or a streak is at risk, a weekly digest, onboarding tips and product updates. Every email has an unsubscribe link, and you can change each type in your settings. We send push notifications only when you have granted permission in your browser or device.
- **Improving and securing the Service** (legitimate interest). We use analytics and performance data, feedback and error information to fix bugs, understand which features help students, protect against abuse and fraud, enforce plan limits and keep the Service secure.
- **Moderation** (legitimate interest and legal obligation). We review reports and remove content that breaks our Terms or the law.
- **Legal obligations** (Art. 6(1)(c)). We keep accounting records, respond to lawful requests from authorities, and keep records of suppressed email addresses and account deletions so we honour opt-outs and deletion.

Where we rely on legitimate interest, we have weighed our interest against your rights, and you can object at any time (see section 10).

4. AI processing

When you use an AI feature, we send the relevant input to our AI provider, **OpenAI**, to produce the result. For card generation that is the text of the material you uploaded or pasted; for the assistant it is your question and the cards or notes it concerns. OpenAI processes this data as our processor under a data processing agreement. Under OpenAI's API terms it may keep inputs for a limited period to detect abuse, and it does not use them to train its models. We do not use your content to train AI models ourselves.

AI features do not make decisions that have legal or similarly significant effects on you.

5. Who we share data with

We do not sell your personal data and we do not share it for advertising. We share it only with:

- **Service providers (processors)** that run parts of the Service for us, under data processing agreements:
 - Supabase: authentication, database and file storage
 - Vercel: website hosting, Vercel Analytics and Speed Insights
 - Railway: application server hosting
 - OpenAI: AI card generation, the study assistant and the support chat
 - Stripe: web payments and invoices
 - RevenueCat: management of in-app purchases on mobile
 - Resend: sending emails and managing our email contact list
 - PostHog, EU cloud: product analytics
- **Apple and Google**, when you subscribe through their app stores. They act as independent controllers under their own privacy policies.
- **Browser push services**, such as Google Firebase Cloud Messaging, Mozilla Push Service and Apple Push Notification service, which deliver notifications you have enabled. The notification content we send is limited to a short study reminder.
- **Other users**, for what you choose to make public: published decks, your display name, username and profile picture, comments and likes on Explore, and decks you share with collaborators.
- **Authorities, advisers or others**, where the law requires it or where needed to establish, exercise or defend legal claims, or to protect the rights and safety of our users or others.
- **A buyer or successor**, if our business is merged, acquired or sold. You will be told, and this policy will continue to protect your data.

6. International transfers

Some of our providers are based in, or access data from, countries outside the EEA, particularly the United States. When personal data is transferred outside the EEA, we rely on an adequacy decision, such as the EU–US Data Privacy Framework for certified companies, or on the European Commission's Standard Contractual Clauses with additional safeguards where needed. You can ask us for more information about these safeguards.

7. How long we keep data

- **Account and study data** are kept for as long as you have an account. When you delete your account, your profile, notes, decks, cards, study history, uploaded files, feedback, comments and other account data are deleted from our live systems, and your contact is removed from our email list. Copies of public decks that other users already imported remain in their accounts.
- **Backups** managed by our hosting providers are overwritten on a rolling basis, normally within 30 days.
- **Billing records**, meaning invoices and payment data held by us, Stripe and the app stores, are kept for as long as Norwegian bookkeeping law requires, currently up to five years after the end of the financial year.
- **Deletion and suppression records.** We keep a minimal record of a deleted account (account ID, email address and deletion date) so a deleted account is not recreated by mistake and your deletion is honoured. We keep email addresses that bounced, complained or unsubscribed so we do not email them again.
- **Analytics data** is kept in PostHog for a limited period, and data linked to your account is deleted on request.
- **Security logs** are kept for a short period, normally no more than 90 days.

8. Cookies, local storage and analytics

We use a small number of cookies and similar technologies:

- **Strictly necessary.** Authentication cookies from Supabase keep you signed in. A preference cookie remembers whether the sidebar is open.
- **Local storage and IndexedDB.** These keep reviews you made offline until they sync, unsaved drafts, and small interface preferences on your device. This data stays in your browser.
- **Analytics.** We use PostHog, hosted in the EU and routed through our own domain, to understand how the Service is used, including page views and interactions. When you are signed in, analytics events are linked to your account and email address so we can understand the experience of individual accounts and help with support. We also use Vercel Analytics and Speed Insights, which measure page views and performance without cookies.

You can block or delete cookies in your browser settings, but the Service will not work if you block the authentication cookies. You can object to analytics tracking by emailing info@repetio.ai.

9. Security

We protect your data with encryption in transit (HTTPS), encrypted storage by our providers, access controls, signed webhooks and least-privilege access to production systems. No system is perfectly secure. If a personal data breach is likely to put you at risk, we will notify you and the Norwegian Data Protection Authority as the law requires.

10. Your rights

Under the GDPR you have the right to:

- **Access** the personal data we hold about you and get a copy of it;
- **Rectify** inaccurate data. You can edit most of it yourself in your profile and settings;
- **Erase** your data. You can delete your account at any time in your account settings, or ask us to do it;
- **Restrict** our processing in certain circumstances;
- **Data portability**: receive the data you gave us in a structured, machine-readable format. You can export your decks yourself, and email us for a full copy;
- **Object** to processing based on legitimate interest, including analytics, and to direct marketing at any time;
- **Withdraw consent** at any time where we rely on consent, for example by turning off push notifications or unsubscribing from emails. This does not affect processing that happened before.

To use any of these rights, email info@repetio.ai from the address linked to your account. We will reply within one month, and may ask you to confirm your identity first.

You also have the right to complain to the Norwegian Data Protection Authority (Datatilsynet, www.datatilsynet.no) or to the data protection authority where you live or work. We would appreciate the chance to address your concern first.

11. Age limit

The Service is not intended for anyone under 16, and you must be at least 16 to create an account. If we learn that we have collected personal data from someone under 16, we will delete it. If you believe this has happened, contact us at info@repetio.ai.

12. Changes to this policy

We may update this Privacy Policy when the Service or the law changes. The effective date at the top shows when it was last changed. If we make material changes, we will notify you by email or in the app before they take effect.

13. Contact

Hearttec Software AS, Norway

Email: info@repetio.ai

Website: <https://www.repetio.ai>