

Satify Privacy Policy

Version 2026-10-22. Effective from publication on satify.study.

1. Operator and scope

Кыдырбай Дархан (Darkhan Kydyrbai), an individual in Almaty, Kazakhstan, operates Satify and determines how its account and learning data are used. Contact: support@satify.study. This policy covers satify.study. External providers also publish policies for their own services.

2. Data and purposes

Account data includes your email, name, authentication identifiers and credentials managed by Supabase Auth. Study data includes target score, exam date, weekly availability, plan, answers, timings, skill estimates, flashcard progress and test results. We use these to authenticate you, deliver lessons, save progress and personalise study.

We record accepted document version, language, acceptance time and your 13+ confirmation. The acceptance form separately asks for agreement to the Terms and consent to this processing. We do not collect a date of birth or parent's email. Self-registration starts at 13 and no parental verification occurs. This describes the product and is not a determination that every minor can legally consent in every jurisdiction. Contact us about an account belonging to a child under 13.

Payment data includes receipt/sale and subscription identifiers, purchaser email, amount, product, payment/refund state and verified provider response. It supports access, reconciliation, refunds and disputes. We do not collect full card numbers or security codes. Technical data may include IP address, browser information, authentication/security events and hosting request logs. These support service delivery and fault investigation. Support correspondence contains what you choose to send. Export/deletion records track completion or failure without storing the password used for reauthentication.

3. AI and other providers

Supabase provides authentication and the application database. Vercel hosts the application and executes server requests. Gumroad handles checkout, recurring payments, receipts and refunds, and independently processes payment information under its own terms.

Groq processes assistant messages and the relevant question, conversation or study context sent by the server. OpenRouter may process context for configured server functions such as plan explanations, skill prioritisation or error feedback and route it to the selected model provider. These are distinct integrations; not every AI feature uses both. Server-side functions may fall back to non-AI behaviour when not configured. AI-assisted preparation of educational content does not itself require sending account data. Avoid sensitive information in messages. We cannot promise zero retention or absence of provider model training without verified settings and contractual terms.

The embedded Desmos calculator connects to Desmos; its service receives ordinary connection data such as IP address and browser information. External links and payment pages operate under the respective provider's policy. We do not sell account data or run an advertising mailing list in the current product. Account confirmation, password recovery and payment receipts are service messages, not marketing consent.

4. Locations and disclosure

The configured Supabase project region is Singapore. Vercel, Gumroad, Groq, OpenRouter, underlying model providers and Desmos may process data outside Kazakhstan, including in other countries according to their infrastructure. We do not represent this infrastructure as Kazakhstan-local storage. The consent form discloses processing abroad. Consent does not by itself resolve all mandatory localisation, cross-border transfer or minors' consent requirements.

We disclose data to service providers for the functions above, to authorities where legally required, and as necessary to protect accounts or resolve a documented dispute. Access is limited to the task. We do not publish your study results to a Community feature. Contact us for information about a particular processing operation or provider.

5. Cookies and local storage

Supabase authentication cookies/session tokens keep you signed in. The browser also stores unfinished study/test sessions and interface preferences in local or session storage. These are functional storage, not an advertising profile. We have not added advertising trackers to this release. Third-party embedded services may use their own storage. Blocking necessary cookies can prevent login; clearing local storage can erase an unfinished session. On a shared device, sign out and clear browser data. Account deletion clears Satisfy saves on the browser completing deletion, not on other devices automatically.

6. Retention by category

Study data is kept until account deletion completes, when it is removed from the active application database. Account and acceptance records are also removed on completed deletion. The selected exam date does not by itself trigger deletion. Export files are generated on request; Satisfy does not keep an extra server copy. A downloaded copy stays under your control.

Unfinished browser sessions: approved target of 30 days after the last save. This covers unfinished lessons, diagnostics and practice tests. Retention-based automatic cleanup is disabled. Until that cleanup is implemented, verified and separately enabled, a save can remain longer than 30 days. It may be cleared earlier by successful completion, the feature replacing it, your clearing browser data, or account deletion in that browser. The approved target is not a claim that automatic expiry is already operating.

Successful export-operation logs: approved target of 14 days after completion. This concerns the operation record, not the exported study data or your downloaded file. Scheduled removal is disabled, so existing log entries may remain longer while cleanup awaits verification and separate authorisation. This target does not set a deadline for failed or pending operations or deletion records; their retention remains under review. Pending deletion requests remain until resolved.

Payment records: retention periods remain under review. Verified records support access, reconciliation, refunds and disputes. On completed account deletion, account links, email, subscription identifiers and the raw provider response are removed; minimal transaction evidence may remain. Unmatched payments remain available for investigation and reconciliation. This policy assigns no numerical retention period or automatic deletion schedule to payment records and makes no claim about a statutory minimum. Applicable obligations and any specific dispute must be assessed before a final period is published.

Backups, provider logs and support records: no new period is approved here. Their actual settings and applicable requirements still need verification. Removing data from the active database does not promise immediate erasure from every provider backup. Support records remain while a request or related obligation or dispute is being resolved. Turning on retention-based cleanup requires a separate decision; the approved targets above do not authorise it. The account deletion procedure requested by the account holder remains a separate operation.

7. Control, rights and security

You can correct study settings, download your data and request permanent deletion in Settings. Export and deletion require your current password. Cancel active recurring memberships through Gumroad first; if cancellation cannot be verified, deletion remains incomplete and you can retry or contact support. We retain enough operation state to make repeat requests safe. Withdrawal of consent, access/correction requests, questions about retention and complaints can also be sent to support@satify.study. We verify identity proportionately; do not send an identity document unless specifically needed and requested securely.

Where Kazakhstan law applies, withdrawal is handled by stopping processing or giving a reasoned refusal within fifteen working days; a legal duty may prevent immediate erasure of particular records. Other rights and deadlines may apply in your jurisdiction. You may contact the competent data protection authority or court. Necessary processing may be required to keep providing the account; withdrawal can therefore end the service.

We use authenticated server operations, restricted direct database permissions and encrypted network connections. No system is risk-free. Report suspected unauthorised access promptly. Significant policy changes receive a new version and an acceptance prompt. English, Russian and Kazakh versions describe the same processing; contact us about any inconsistency.