

Rayse — Privacy Policy

Version: 2026-10-01 · Effective date: Oct 1, 2026

This Privacy Policy explains what personal data Rayse collects, why, how long we keep it and how you control it. It applies to the Rayse website at raysetrack.com, the Rayse web app at app.raysetrack.com and the Rayse apps for iOS and Android (together, the "Service").

Short version: we collect only what the trackers you use need, we store it in the EU (Germany), we encrypt your journal and book notes, we do not sell your data or show ads, the AI assistant works only if you switch it on, and you can export or permanently delete everything from your account settings.

1. Who we are

The controller of your personal data is:

- **Individual Entrepreneur Maksim Denisovich Chubarov, trading as "QuickSell"** (IP "QuickSell")
- IIN: 040808501427
- Registered address: 100A Akseleu Seidimbek St., Almaty, Republic of Kazakhstan
- Email: private@raysetrack.com

In this policy "Rayse", "we" and "us" mean this controller.

EU representative (GDPR Art. 27): [name and address of the EU representative — to be appointed]. You may contact our representative instead of us on any question about your data.

We have not appointed a data protection officer. For any privacy question, write to private@raysetrack.com.

2. Data we collect

We collect data you give us, data created when you use the trackers, and a minimum of technical data needed to run the Service securely.

Category	What it includes	Source
Account	Name, email address, password (stored only as an argon2id hash, never in plain text), language, theme, time zone	You
Sign in with Google or Apple	Provider name, your account ID at that provider, email address and whether the provider has verified it	Google or Apple, when you choose that sign-in
Consents	Which versions of the Terms of Service, this Privacy Policy and the AI consent you accepted, and when	Recorded when you accept
Finance	Months, income, expenses, savings, categories, budgets, display currency	You
Planning	Lists, tasks, dates and times, completion status	You
Routine	Habits and daily check-ins	You
Workouts	Exercises, sets, repetitions, weights	You
Goals	Goal names and texts, deadlines, sub-goals, progress, cover images you upload	You
Reading	Books, pages read, ratings, notes and quotes	You
Journal	Journal entries	You
Dashboard	Widget layout and settings, including an optional birth date (life-in-weeks widget) and a city (clock widget)	You

Category	What it includes	Source
Subscription	Subscription status, billing period, identifiers from our payment provider	Payment provider
Technical	IP address, active sessions (stored as hashed tokens with an expiry date), error logs that record the request type and route only	Your device, automatically

What we do not collect. We do not receive or store your full card details; payments are handled by our payment provider (section 5). We do not use advertising IDs, tracking pixels, or analytics or advertising cookies. Our logs do not contain your passwords, tokens, email address, journal text or the content of your requests.

Sensitive data. We do not ask for health or other special categories of data. If you choose to record such information (for example a medication habit or a journal entry about your health), we process it only to store it and show it back to you, based on your explicit consent given by entering it (GDPR Art. 9(2)(a)). You can withdraw that consent at any time by deleting the entry.

3. Why we use your data and on what legal basis

We use your data only for the purposes below. Each purpose relies on a legal basis under GDPR Art. 6(1).

Purpose	Data used	Legal basis
Create and run your account, provide the trackers and dashboard, sync between web and mobile apps	Account, tracker content, dashboard	Performance of our contract with you (Art. 6(1)(b))
Send service emails: email verification, password reset, email change	Name, email address	Performance of contract (Art. 6(1)(b))

Purpose	Data used	Legal basis
Process your subscription, issue invoices, meet tax and accounting duties	Subscription data	Performance of contract (Art. 6(1)(b)) and legal obligation (Art. 6(1)(c))
Run the AI assistant	See section 4	Your consent (Art. 6(1)(a))
Keep the Service secure: sign-in, rate limiting, preventing abuse, fixing errors	Technical data, sessions	Our legitimate interest in a secure, working Service (Art. 6(1)(f))
Keep a record of your consents	Consents	Legal obligation to demonstrate consent (Art. 6(1)(c), Art. 7(1))
Answer your requests and support messages	Your messages and contact details	Performance of contract or our legitimate interest in helping you (Art. 6(1)(b) or (f))
Establish or defend legal claims	Relevant records	Legitimate interest (Art. 6(1)(f))

We do not send marketing emails. If we start, we will ask for your consent first.

We do not make decisions about you based solely on automated processing that have legal or similarly significant effects. Statistics in the app (streaks, forecasts, progress) are calculations shown only to you.

4. AI assistant

The AI assistant is off by default and works only after you give separate consent in the app. Without that consent, none of your data is sent to an AI provider.

What it does. It writes summaries of your week, answers questions about your data, and can log entries from free text (for example, "read 30 pages and spent 15 EUR on coffee" adds a reading log and an expense).

What is sent. Your message and the parts of your tracker data needed to answer it, such as recent expenses, habits or reading progress.

Who processes it. Requests are processed by Anthropic, PBC (USA), which provides the Claude AI models, as our processor under a data processing agreement. Anthropic does not use data sent through its commercial API to train its models, and may keep inputs and

outputs for a limited period for safety and abuse monitoring, as set out in its terms.

Accuracy. AI answers can be wrong. Entries the assistant creates appear in your trackers, where you can check, edit or delete them.

Withdrawing consent. You can turn the assistant off at any time in settings. From that moment no new data is sent; it does not affect processing that happened before.

5. Who receives your data

We do not sell your personal data and do not share it for advertising. We share it only with the service providers below, each bound by a data processing agreement (GDPR Art. 28), and only as far as they need it.

Recipient	Purpose	Location	Safeguard
[Hosting provider]	Servers, database, backups, logs	EU (Germany)	DPA
[Storage provider]	Uploaded images	EU	DPA
[Email provider]	Service emails	EU	DPA
Anthropic, PBC	AI assistant, only with your consent	USA	DPA and Standard Contractual Clauses (Art. 46)
[Payment provider]	Subscription payments, invoices, sales tax	[location]	Acts as an independent controller (merchant of record) under its own privacy policy

Google and Apple. If you sign in with Google or Apple, that provider confirms your identity to us. They act as independent controllers under their own privacy policies; we do not send them your Rayse data. Apple and Google also distribute our mobile apps through the App Store and Google Play under their own terms.

Authorities. We may disclose data where the law requires it, for example to a court or a tax authority, and only to the extent required.

International transfers. Your data is stored in the EU (Germany). Rayse is operated from Kazakhstan, which has no EU adequacy decision; our team accesses data from Kazakhstan only as needed to run, maintain and support the Service, under the security measures in section 6. Transfers to Anthropic in the USA rely on Standard Contractual Clauses. You can ask us for a copy of the safeguards at private@raysetrack.com.

6. How long we keep data and how we protect it

We keep your data while your account exists and delete it as soon as you delete your account, with the exceptions below.

Data	Retention
Account, tracker content, uploaded images, consents	Until you delete them or your account. Account deletion is immediate and permanent, with no grace period
Accounts with an unverified email	Deleted automatically after 30 days
Sign-in sessions	Expire 30 days after last use; expired sessions are deleted daily
Email links	Verification and email change: 24 hours; password reset: 1 hour; deleted after use or expiry
Uploaded images not attached to a goal	Deleted within 24 hours
Encrypted backups	Deleted data disappears from backups within [30] days as they rotate
Server logs	[14] days
Billing and tax records	Kept by the payment provider for the period required by tax law

Security measures (GDPR Art. 32):

- All connections use TLS encryption.
- Passwords are hashed with argon2id.
- Journal entries and book notes are encrypted at rest with AES-256-GCM, bound to your account.

- Database backups are encrypted.
- Access tokens live 15 minutes; sessions use a secure, httpOnly cookie.
- Sign-in endpoints are rate-limited against password guessing.
- Every request is checked against your account, so no user can read another user's data.
- Logs contain no passwords, tokens, email addresses or personal content.

If a personal data breach is likely to put your rights at risk, we will notify the competent supervisory authority within 72 hours and inform you without undue delay where the law requires it.

7. Your rights

Under the GDPR you have the rights below. Most of them you can use yourself in the app; for the rest, write to private@raysetrack.com.

Right	How to use it
Access and data portability (Art. 15, 20)	Settings → Export data: a ZIP file with all your data in JSON and your uploaded files
Rectification (Art. 16)	Edit any of your data directly in the app
Erasure (Art. 17)	Settings → Delete account. After you confirm with your password or Google/Apple sign-in, all your data and files are deleted permanently
Withdraw consent (Art. 7(3))	Turn off the AI assistant in settings, or delete the entry concerned
Restriction (Art. 18) and objection (Art. 21)	Email private@raysetrack.com

We answer requests within one month. We may ask you to confirm your identity first.

You also have the right to lodge a complaint with a data protection supervisory authority, in particular in the EU country where you live, work or where the alleged infringement took place.

8. Cookies and app storage

The web app uses one strictly necessary cookie, `rayse_rt`. It keeps you signed in, cannot be read by scripts and expires after 30 days. Strictly necessary cookies do not require consent.

The mobile apps store your sign-in session in the device's secure storage.

We use no analytics, advertising or tracking cookies or SDKs. If this changes, we will update this policy and ask for your consent where required before using them.

9. Age limit

The Service is for people aged 16 and over. We do not knowingly collect data from anyone younger. If we learn that a user is under 16, we will delete the account.

10. Changes to this policy

The version date at the top shows the current version. If we make material changes, we will tell you by email or in the app before they take effect and, where required, ask you to accept the new version.

11. Contact

IP "QuickSell" (Maksim Denisovich Chubarov), 100A Akseleu Seidimbek St., Almaty, Republic of Kazakhstan. Email: private@raysetrack.com (general support: support@raysetrack.com).