

Privacy Policy

Effective date: 2026-10-01

This Privacy Policy describes how Glynce ("Glynce", "we", "us", or "our") collects, uses, and shares information when you use the Glynce mobile and watchOS applications and related services (the "App").

Glynce is a personal dashboard for adults with type 1 diabetes. It visualizes data from connected sources such as continuous glucose monitors and Apple Health for self-tracking and lifestyle purposes. **Glynce is not a medical device, not a medical app, and not a clinical tool**, and is not intended to diagnose, treat, cure, monitor, or prevent any disease. Always consult your healthcare provider for medical decisions. See the [Terms of Service](#) for the full disclaimer and your responsibilities.

If you have questions about this policy, contact us at support@glynce.app.

1. Who we are

The App is operated by **Glynce**, a company registered in the Netherlands under Chamber of Commerce (KvK) number **68577397**, with its registered address at Cruquiuskade 251, 1018 AM Amsterdam, Netherlands ("we", "us"). For privacy questions or to exercise your rights, contact support@glynce.app.

2. Information we collect

We collect the following categories of information.

2.1 Account information

The first time you open the App it creates an account identifier for you automatically. No email address, no name, and no password is involved, and you are not asked to create an account. The identifier is a random value that means nothing outside our systems, but it is still how we tell one user from another, so we treat it as personal data about you.

We use it to keep your settings with the right account, to work out whether you have a Glynce Plus subscription, and to apply the daily limit on the AI features to your account rather than to everyone at once.

The session that keeps the App attached to that identifier is stored in the iOS Keychain, which iOS keeps even when an app is deleted. If you reinstall Glynce on the same device you will normally come back to the same account identifier rather than get a new one.

Signing up is optional and happens later, in Settings. When you do, we attach an email address and a sign-in method to the identifier you already have. It stays the same account, so your settings, your subscription, and everything already stored under it stay where they are.

So the account information we hold is:

- An account identifier, created for every install
- The date your account was created (used to determine entitlement to legacy free access)
- If you sign up: your email address, and, if you used Apple Sign-In or Google Sign-In, the user identifier that provider issues

You can see your account identifier in the App under Settings → Account, where it is shown as your Account ID. Section 9 explains why that matters if you never sign up.

2.2 Continuous glucose monitor (CGM) data

If you connect a CGM, we receive glucose readings and related metadata (timestamps, trend arrows, sensor status) from the provider you authorize. Supported providers currently include:

- Dexcom
- Abbott (via LibreLinkUp)
- Medtronic (Guardian)
- Eversense
- Nightscout (self-hosted; URL and access token you provide)

The access tokens and login credentials needed to keep your CGM connection working are stored only on your device, in the iOS Keychain. We do not send your CGM credentials to our servers, and your glucose is processed on your device (see Section 2.9). You can disconnect a CGM at any time from within the App, which deletes the tokens from the Keychain.

2.3 Apple Health (HealthKit) data

With your permission, the App reads the following categories from Apple Health:

- Glucose readings
- Heart rate and heart rate variability
- Respiratory rate and blood oxygen
- Sleep
- Wrist temperature
- Steps, active energy, exercise minutes, stand hours, workouts
- Body weight

HealthKit data is read and processed on your device. We do not upload it to our servers, and it is not synced to your Glynce account, so it does not travel between your devices through us. If you reinstall the App or set up a new device, Glynce rebuilds your history by reading Apple Health again on that device.

Glynce also writes to Apple Health, if you allow it: the glucose readings you enter by hand, the readings we fetch from your CGM, and the meals and water you log. You control that in the same iOS settings as read access.

We do not sell HealthKit data, use it for advertising, share it with third parties for their own marketing, or disclose it to data brokers. You can revoke HealthKit access at any time in iOS Settings → Health → Data Access & Devices → Glynce.

2.4 Food, meal, and nutrition data

- Food entries you log: name, brand, serving size, calories, macronutrients (carbs, fat, protein), meal type, barcode
- Photos you take of meals, packaging, nutrition labels, or recipes for AI analysis

2.5 Activity, gamification, and in-app content

- Challenges, milestones, badges, and other gamification state
- Settings and preferences (e.g., chosen glucose unit, target range)

2.6 Service telemetry and analytics

- CGM-integration telemetry: an install-scoped UUID, the endpoint called, the outcome, HTTP status code, and error category. This is used to detect upstream API outages and provider changes. The same install-scoped UUID is also used for the usage limits and abuse prevention described in Section 2.11.
- Product analytics from PostHog: events that describe how you use features, screen views, and device/OS metadata. We do not record your screen: session replay is switched off in the App.
- App reliability diagnostics, sent through PostHog once a day: how old the glucose reading on your widgets was when they updated, how often the App refreshed in the background, how those refreshes went, whether Glynce may write glucose to Apple Health, and how many other apps wrote glucose there in the last day. These are counts, durations and yes/no answers only, and never include a glucose value, the time of a reading, or which apps they are.
- Crash and error logs.

You can turn product analytics off at any time with "**Share anonymous usage data**" in Settings under Account. It is **on by default**. When you turn it off, the App stops sending events and stops asking our analytics provider for anything, on that device. It also stops recording the reliability diagnostics above and deletes what it had already recorded on that device.

2.7 Feedback and support content

If you submit feedback or feature requests through the in-app feedback tool (Canny), the content you provide and any attached screenshots are stored to help us respond.

If you cancel a Glynce Plus subscription, we may ask why you cancelled. The question is shown at most a few times and answering is entirely optional. The reasons you tick are recorded without any free text in our analytics; anything you type in your own words is stored separately in our own EU database and is never sent to our analytics provider. It is deleted when you delete your account.

2.8 What we do not collect

We do not request or collect:

- Your precise location
- Contacts
- Browsing history outside the App
- Government identifiers

2.9 On-device glucose processing

Glynce processes your glucose on your device. Optional glucose notifications (for example, high, low, or rapid-change notices) are evaluated **on your device** while the App is running, using your CGM connection and the thresholds you set. We do **not** operate any server-side service that monitors your glucose, fetches your readings on your behalf, or sends you glucose alerts, and your CGM login is never stored on our servers.

2.10 Account profile and optional profile sync

When you start setting up the App we ask you to acknowledge that Glynce does not give medical advice. We record that acknowledgement, the date you gave it, the version of the notice you agreed to, and a yes or no flag that you meet our minimum age of 16, which is set by the date of birth you enter during setup. The date itself belongs to your profile rather than to this record. This **consent record** is kept on your device. If you have signed up with an email address, we also store it on our servers, so we can honor your consent choices

when you sign in on a new device. It contains no health data. While your account has no email address attached, our database refuses to store this record for you at all.

Separately, once you have signed up, you can turn on an optional **"Sync my profile across my devices"** setting, in Settings under Account. It is **off by default**. When you turn it on, we store a profile record on our servers so you can restore your setup after reinstalling the App or signing in on another device. This profile may include your name, date of birth, sex, height and weight, activity level, **diabetes type**, glucose target range, preferred glucose unit and measurement system, and your nutrition goals and settings. Some of these are health data (see Section 4 for the legal basis).

We upload this profile **only** while the setting is on. If you leave it off, no profile data is uploaded through this feature. An empty record is stored instead, and our database rejects any attempt to store profile data without your opt-in. It also rejects any record at all for an account with no email address attached, so no profile is ever uploaded for an account that never signed up. You can turn the setting off at any time to stop future syncing, and you can remove the stored consent record and profile by deleting your account (see Section 9). Your glucose readings and food logs are **not** part of this sync.

2.11 Abuse prevention and usage limits

Creating an account identifier costs nothing, so a limit counted per account would not stop anyone willing to create more of them. To keep the AI features available and their cost under control, our servers also count AI requests against two things that are harder to change:

- The install-scoped UUID described in Section 2.6. It is the same identifier, sent with your AI requests so that a daily limit can apply per installation of the App.
- Your IP address, as our servers see it when your device connects.

Each of those counters holds only the identifier or the IP address, a date, and a number of requests. They carry no account identifier and none of the content you submitted, and we keep them for up to 30 days.

We also keep a record that links your account identifier, your install-scoped UUID, and the IP address you connected from, so we can investigate abuse and block a specific account, device, or network. That record is deleted when you delete your account.

We rely on our legitimate interests for all of this, and Section 4 explains the balance we struck.

3. How we use information

We use the information described above to:

- Provide the App's core functions, including showing your glucose data, logging meals, and computing analytics
- Personalize features such as challenges, milestones, and the in-app companion ("Hero")
- Run AI-assisted features you choose to use (meal photo analysis, nutrition label OCR, recipe extraction)
- Maintain access to CGM provider APIs you have connected
- Detect outages, debug problems, and improve performance and reliability
- Apply usage limits to the AI features and prevent abuse of them
- Determine your subscription entitlement
- Respond to support requests and feedback
- Comply with legal obligations

We do not use your information for behavioral advertising, and we do not sell your personal information.

4. Legal bases (EEA / UK users)

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

- **Performance of a contract** — to provide the App and its features.
- **Legitimate interests** — to keep the App secure, debug problems, prevent abuse, and improve the product, balanced against your rights. This is also the basis for the abuse-prevention data in Section 2.11: your install-scoped UUID, your IP address, and the daily request counts we keep against them. Without them, anyone could run the AI features in a loop at our expense, and we would end up withdrawing those features from everyone. Against that we weighed how little this data says about you. It records how often a feature was used and where the request came from, not what you logged, and we do not use it to build a picture of you or to make decisions about you. You can object to this processing at any time by contacting us, although we may not be able to offer you the AI features if we cannot count their use.
- **Consent** — for HealthKit access, AI processing of meal photos, and the optional sync of your profile across your devices. Because the synced profile can include special-category health data (such as your diabetes type and body metrics), we rely on your **explicit consent** for it. You can withdraw consent at any time by turning the setting off. That stops future syncing and clears the profile we hold. Deleting your account is a separate action that removes the consent record too.
- **Compliance with legal obligations** — when we must keep records or respond to lawful requests.

5. Third-party services we use

We rely on the following service providers ("processors") to operate the App. Each receives only the information needed for its function.

Provider	Purpose
Supabase	Backend hosting, authentication, database, file storage, and AI-feature gateway
PostHog	Product analytics. Session replay is switched off
Apple (Sign in with Apple, HealthKit, Live Activities)	Authentication, on-device health data, system integrations
Google (Sign-In)	Authentication
Anthropic (Claude API)	AI analysis of food photos, nutrition labels, and recipes you submit
Dexcom, Abbott (LibreLinkUp), Medtronic (Guardian), Eversense, Nightscout	CGM providers you choose to connect
OpenFoodFacts, USDA FoodData Central, Edamam, Nutritionix	Food and nutrition database lookups
Canny	In-app feedback and feature requests
RevenueCat	Subscription and purchase management. Receives your account identifier as its App User ID
Resend	Sending account emails, such as sign-in links and confirmations
Cloudflare	Hosting and delivery of our website
Google Analytics	Website analytics only, and only if you accept it in our cookie banner. Not used in the App

Your account and the data we store for you sit in the European Union. Supabase hosts our database in an EU region, PostHog runs on its EU cloud, and Resend sends our email from the EU. Some other providers, including Anthropic, RevenueCat, Canny, Cloudflare, and Google Analytics, process data in the United States or in several countries. Where required, transfers from the EEA, UK, or Switzerland rely on the European Commission's Standard Contractual Clauses or an equivalent safeguard.

6. Sharing

We share information only:

- With the processors listed above, under contract, for the purposes described.
- With the CGM provider you authorize, so we can fetch your glucose data on your behalf.
- To comply with law, valid legal process, or to protect rights, safety, and property.
- In connection with a business transfer (merger, acquisition, asset sale), in which case you will be notified.

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

7. AI features

The App offers optional AI features (meal photo analysis, nutrition label OCR, recipe extraction) powered by Anthropic's Claude API, accessed through our backend. When you use one of these features, the relevant image or text is sent to Anthropic for processing. Anthropic does not train its models on this content. You can avoid using these features by not invoking them.

8. Data retention

- Account and health data are kept while your account is active.
- CGM telemetry events are retained for up to 12 months to support outage detection.
- The daily AI request counters kept against an install-scoped UUID or an IP address are kept for up to 30 days.
- The record linking your account identifier, install-scoped UUID, and IP address for abuse investigation is kept while the account exists, and is deleted when you delete your account.
- Analytics data is retained according to PostHog defaults (typically up to 12 months) unless you request earlier deletion.
- If you delete your account, we delete or anonymize your personal data within 30 days, except where we are required to retain it for legal, security, or fraud-prevention reasons.

9. Your rights and choices

Depending on where you live, you have some or all of the following rights:

- Access a copy of your personal data
- Correct inaccurate data
- Delete your data
- Restrict or object to certain processing
- Port your data to another service
- Withdraw consent
- Lodge a complaint with your local data protection authority

You can delete your account at any time from within the App (Settings → Delete account) or by emailing support@glynce.app. Account deletion removes your profile (including the consent record and any profile you chose to sync across devices), your saved foods, favorites, and recipes, and your gamification state from our servers. CGM credentials live only on your device. Disconnecting a CGM in the App removes them. Deleting the App does not, because iOS keeps Keychain items after an app is deleted, so disconnect your CGM in the App first if you want them gone. HealthKit data remains on your device and in Apple Health and is not affected.

If your account has no email address on it. Signing up is optional, so many Glynce accounts have no email address attached (see Section 2.1). That changes how you exercise the rights above, and we would rather say so plainly than describe a process that cannot work.

Deleting still works exactly as described. Settings → Delete account deletes the account and what is stored under it whether or not you ever signed up, and there is nothing for us to verify, because the request comes from the App that holds the account.

Everything else has to reach us by email, and there we run into a limit we cannot design away. The only thing you can give us is your account identifier, copied from Settings → Account. An identifier is not a password and it is not proof of anything, and we have no way to tell whether the person who sent it is the person whose device it came from. So we will not hand over data, correct it, or change anything about an account on the strength of an identifier alone, because that would let anyone who got hold of it do the same to you. For an account with no email address, deletion in the App is the route we can honor with confidence, and an emailed access or portability request is one we may have to refuse. If we refuse, we will tell you why.

Two things soften this. Most of what Glynce holds about you is on your device and not on our servers at all, including your glucose readings and your food logs, so there is less on our side to ask for than you might expect. And you can remove the limitation whenever you like by signing up in Settings, which attaches an email address to the account you already have and gives us a way to confirm that a request really came from you.

Apple HealthKit permissions can be reviewed or revoked in iOS Settings → Health → Data Access & Devices → Glynce.

10. Notice to California residents (CCPA / CPRA)

This section applies to California residents and supplements the rest of this Privacy Policy. It uses terms defined in the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("CCPA").

10.1 Categories of personal information we collect

In the last 12 months we have collected the following CCPA categories:

Category	Examples	Collected?
Identifiers	Account ID (created automatically on first launch, whether or not you sign up), email, sign-in provider ID, device identifiers, IP address, install-scoped UUID	Yes
Customer records (Cal. Civ. Code §1798.80(e))	Email tied to account, payment status, and — when you enable profile sync — your name, date of birth, sex, and activity level	Yes

Category	Examples	Collected?
Commercial information	Subscription and entitlement status	Yes
Internet/network activity	App events, screen views, feature usage, crash and error logs	Yes
Geolocation	Coarse country/region inferred from IP for routing and outage detection only	Yes (no precise location)
Sensory information	Photos you take of meals, packaging, nutrition labels, or recipes	Yes
Inferences	Engagement signals used to personalize challenges and milestones	Yes
Sensitive personal information	Account login credentials (sign-in provider tokens), health information including glucose readings, HealthKit metrics, and meal logs, and profile details you choose to sync (such as diabetes type, body metrics, and glucose targets)	Yes

We do not collect: precise geolocation, government IDs, biometric identifiers used for identification, racial or ethnic origin, religious beliefs, union membership, contents of mail/email/text messages, genetic data, or sexual-orientation information.

10.2 Sources

We collect this information from you directly, from your device, from CGM providers and Apple HealthKit when you authorize them, and from our service providers (analytics, error reporting).

10.3 Business purposes

We use personal information for the purposes described in Section 3, including providing the App, securing accounts, debugging, analytics, AI features you request, and complying with law.

10.4 Disclosures for a business purpose

In the last 12 months we have disclosed each category above to our service providers (listed in Section 5) under written contracts that restrict their use of the information to providing services to us.

10.5 Use of sensitive personal information

We use sensitive personal information (your health data, including glucose, HealthKit metrics, meal logs, the profile details you choose to sync, and your sign-in tokens) **only** to provide the App's core functions you request, to secure your account, to prevent fraud or abuse, and to comply with law. We do not use it to infer characteristics about you for any other purpose. Under CCPA, you have the right to limit the use of sensitive personal information to these permitted purposes — and that is already the only way we use it.

10.6 "Sale" and "sharing" of personal information

We do not sell your personal information, and we do not share it for cross-context behavioral advertising, as those terms are defined under the CCPA. We have not sold or shared personal information in the last 12 months, including information of consumers under 16.

10.7 Your California rights

Subject to verification, you have the right to:

- **Know** what personal information we collect, use, disclose, and (where applicable) share or sell.
- **Access** a copy of your personal information.
- **Delete** your personal information.
- **Correct** inaccurate personal information.
- **Opt out** of any sale or sharing of personal information (not applicable — we do neither).
- **Limit** the use and disclosure of sensitive personal information (not applicable — we already limit it to the purposes in Section 10.5).
- **Non-discrimination** for exercising any of these rights. We will not deny you service, charge you a different price, or provide a different quality of service because you exercised a CCPA right.

10.8 How to exercise your rights

Submit a request by email to **support@glynce.app** with the subject line "CCPA Request" and tell us which right you want to exercise. To protect you, we will verify your request by asking you to confirm it from the email address associated with your Glynce account and, where reasonable, to provide additional information that matches what we already hold.

If your Glynce account has no email address attached (see Section 2.1), we cannot verify a request that way. We can act on a deletion request you make in the App under Settings → Delete account, because that request comes from the App itself. For a request to know, access, correct, or port data held under such an account, an account identifier is the only thing you can offer us, and it is not proof that the account is yours. Where we cannot verify a request to the standard the CCPA requires, we have to deny it, and we will tell you why. Signing up in Settings attaches an email address to the same account and removes this limitation.

You may use an authorized agent to submit a request on your behalf. We will require the agent to provide signed written authorization from you and may still ask you to verify your identity directly.

We will respond within 45 days, with a possible 45-day extension if reasonably necessary.

10.9 Retention

We retain personal information for the periods described in Section 8.

10.10 "Shine the Light" (Cal. Civ. Code §1798.83)

We do not share personal information with third parties for their own direct marketing purposes.

11. Children

Glynce is intended for adults with type 1 diabetes. We do not knowingly collect personal information from children under 16 (or the equivalent minimum age in your jurisdiction). If you believe a child has provided us with personal information, contact **support@glynce.app** and we will delete it.

12. Security

We use industry-standard measures to protect your information, including encryption in transit (TLS), encryption at rest for backend storage, scoped access tokens, and row-level security in our database. No system is perfectly secure; if we become aware of a breach affecting your data, we will notify you and the relevant authorities as required by law.

13. International transfers

Our database is hosted by Supabase in an EU region, our analytics run on PostHog's EU cloud, and our account email is sent from the EU by Resend, so that data stays in the European Union. Other providers, including Anthropic, RevenueCat, Canny, Cloudflare, and Google Analytics, process data in the United States or in several countries. Where required, we rely on Standard Contractual Clauses or other approved transfer mechanisms.

14. Changes to this policy

We may update this Privacy Policy from time to time. When we make material changes, we will notify you in the App or by email and update the "Effective date" above. Continued use of the App after an update means you accept the revised policy.

15. Contact

Glynce KvK 68577397 Cruquiuskade 251, 1018 AM Amsterdam, Netherlands Email: **support@glynce.app**