Quitli

Privacy Policy

Effective date: November 13, 2026

Applies to: the iOS app "Quitli" (the "App") for users worldwide.

This policy explains what personal data we process when you use Quitli, why, who receives it, and what rights you have. Quitli is a self-help app for men who want to stop watching pornography. Because of that, some of the data you enter in the App relates to your sexual behaviour and wellbeing. We treat this data as sensitive (see Section 5).

US residents: please also read Section 13 (US State Privacy Rights) and our separate Consumer Health Data Privacy Policy at https://quitli.de/en/health-data.

1) Who is responsible (controller)

Jaron Marec Braun, MRC E-Commerce
Brandvorwerkstr. 69, 04275 Leipzig, Germany
Email: mrc.ecommerce1@gmail.com
Phone: +49 176 23560172

We are the "controller" under the EU General Data Protection Regulation (GDPR). Because we are based in Germany, the GDPR applies to all our processing, wherever you live. Where the law of your country or US state gives you additional rights, you have those rights too.

2) Summary

- You need an account to use the App (Google Sign-In, Sign in with Apple, or email and password).
- We store your account, your onboarding answers, your progress (streaks, check-ins, statistics, triggers, plan) and any community posts on our backend provider Supabase.
- Some onboarding results (your dependency score, your target date and whether you skipped the paywall) are sent to Superwall, which shows our subscription screens.
- Messages you type into the AI chat are sent to OpenAI to generate replies.
- The panic button uses your camera only as a live self-view on your device. Nothing is recorded or uploaded.
- Advertising attribution (Meta SDK, AppsFlyer) only runs if you allow tracking in Apple's App

Tracking Transparency (ATT) prompt.
- We do not sell your personal data.
- You can delete your account directly in the App.

3) What data we process

3.1 Account data

- Email and password login: email address, password (stored only in hashed form by our authentication provider Supabase), user ID.
- Google Sign-In: a Google user ID and, depending on your Google settings, your name and email address.
- Sign in with Apple: an Apple user identifier and, depending on your choice, your email address (or an Apple relay address) and name.
- The display name (pseudonym) you choose for the community, if any.

3.2 Onboarding quiz

During onboarding we ask you questions about your habits and goals. From your answers the App calculates:

- a dependency score,
- your goals, and
- a target date.

We store your answers and these results in your account so the App can create your personal plan. The dependency score, the target date and the information whether you skipped the paywall are also sent to Superwall (see Section 4).

3.3 App usage data you create

- Streaks, check-ins and statistics
- Trigger tracking entries and the warnings the App shows you
- Your personal plan and progress
- AI chat messages and replies, insofar as they are saved in your account (see Section 3.5)

3.4 Community

Posts and comments you publish, the time of posting, your display name, and reports you submit about other users' content. Community posts are visible to other users of the App. Please do not

post information that identifies you.

3.5 AI chat

The text you type into the AI chat is sent to OpenAI to generate a reply. Only text is sent – no images, videos or files. The AI chat is not a therapist and not medical care (see our Terms of Use at https://quitli.de/en/terms).

3.6 Panic button and camera

If you allow camera access, the panic button shows a live view of yourself on your screen. The camera image is processed only on your device. It is not recorded, stored or uploaded. You can revoke camera access at any time in your iPhone settings.

3.7 Subscription data

When you buy a subscription, Apple processes the payment. We never receive your card or bank details. We receive the information needed to unlock and manage your subscription (product, status, renewal, cancellation, refund, transaction identifiers).

3.8 Technical data

When the App communicates with our servers, technical data is processed automatically: IP address, date and time of the request, device type, operating system version, app version, and error or status codes. This is needed to run the App securely.

3.9 Advertising identifiers (only with your permission)

If you allow tracking in the ATT prompt: your advertising identifier (IDFA), IDFV, IP address, install source and certain in-app events (for example install, registration, purchase). We do not intentionally send your quiz answers, your dependency score or your progress data to advertising partners. Advertising SDKs only run with your ATT permission.

3.10 Contact

If you email us: your email address, the content of your message and our reply.

3.11 Push notifications

If you allow notifications in your iPhone settings, a device token is used to deliver them through Apple's Push Notification service. You can turn notifications off at any time in your iPhone settings.

4) Who receives your data (processors and recipients)

- Supabase, Inc. – backend, database, authentication and hosting of account and app data – all data in Sections 3.1 to 3.5 that is stored in your account, technical data – USA (company seat)
- Superwall (Nest 22, Inc.) – showing subscription screens (paywalls), managing and analysing subscriptions – pseudonymous user ID, dependency score, target date, whether you skipped the paywall, paywall views, subscription status, device information – USA
- Apple (Apple Distribution International Ltd., Ireland / Apple Inc., USA) – Sign in with Apple, In-App Purchase payments, App Store – login identifier, purchase data – Ireland / USA
- Google (Google Ireland Ltd. / Google LLC) – Google Sign-In – login identifier, name, email, IP address – Ireland / USA
- OpenAI – generating AI chat replies – text you type into the AI chat – USA
- AppsFlyer (AppsFlyer Ltd., Israel; EU representative AppsFlyer Germany GmbH, Berlin) – install attribution and campaign measurement, only with ATT permission – see Section 3.9 – Israel / other countries
- Meta (Meta Platforms Ireland Ltd. / Meta Platforms, Inc.) – ad attribution and campaign measurement via the Meta SDK, only with ATT permission – see Section 3.9 – Ireland / USA

Supabase, Superwall and OpenAI act on our behalf as processors. Where required, we have concluded data processing agreements with our processors. Apple, Google, Meta and AppsFlyer also process data for their own purposes under their own privacy policies.

We may disclose data to authorities if we are legally required to do so, or to protect our legal rights.

We do not sell your personal data and we do not share it for money.

5) Sensitive data and health-related data

Your onboarding answers, dependency score, streaks, check-ins, triggers, AI chat messages and community posts can reveal information about your sexual behaviour and mental wellbeing. Under the GDPR this is a special category of data (Art. 9 GDPR). Under some US state laws it is "consumer health data" or "sensitive data".

- We process this data only to provide the App's functions to you.
- Processing of these data is based on your explicit consent (Art. 9(2)(a) GDPR), which you give by voluntarily providing the information in the App, for example by answering the onboarding quiz or writing in the AI chat.

- We do not use this data for advertising and we do not intentionally send it to Meta, AppsFlyer or other advertising partners.
- You can withdraw your consent at any time by deleting the data or your account in the App, or by emailing us. Withdrawal does not affect processing that happened before.

6) Legal bases (GDPR)

- Account, login, providing the App, subscriptions – contract (Art. 6(1)(b) GDPR)
- Onboarding answers, score, progress data, AI chat, community content about your habits – explicit consent (Art. 6(1)(a) and Art. 9(2)(a) GDPR)
- Sending score, target date and paywall status to Superwall – contract (Art. 6(1)(b)) and legitimate interest in showing a suitable offer (Art. 6(1)(f)); because the score is health-related, also your explicit consent (Art. 9(2)(a))
- Ad attribution (Meta SDK, AppsFlyer) – consent (Art. 6(1)(a) GDPR, § 25(1) TDDDG) via ATT
- Camera for the panic button – consent (Art. 6(1)(a)) via iOS permission
- Push notifications – consent (Art. 6(1)(a)) via iOS permission
- Technical logs, security, abuse prevention, community moderation – legitimate interest (Art. 6(1)(f))
- Tax and accounting records – legal obligation (Art. 6(1)(c))
- Answering your emails – legitimate interest (Art. 6(1)(f))

7) App Tracking Transparency (ATT) and tracking

On iOS, the App asks for your permission to track you across apps and websites owned by other companies. Only if you tap "Allow" do the Meta SDK and AppsFlyer use your advertising identifier for attribution. If you tap "Ask App Not to Track", no tracking for advertising purposes takes place. You can change your choice at any time in iPhone Settings > Privacy & Security > Tracking.

The App does not show third-party advertising.

8) International data transfers

We are based in Germany. Several of our providers are located in the USA or other countries outside the EU/EEA (see Section 4). Transfers are based on adequacy decisions of the European Commission, the EU-US Data Privacy Framework (where the recipient is certified) or the European Commission's Standard Contractual Clauses (Art. 46(2)(c) GDPR).

If you use the App outside the EU, your data is transferred to the EU and to the countries listed above.

9) How long we keep your data

- Account and app data: as long as your account exists and as long as necessary to provide the App. When you delete your account, we delete this data, unless we are legally required to keep it.
- Data at our processors (for example Superwall, OpenAI): as long as necessary for the purpose described in Section 4, in line with the providers' retention rules.
- Purchase and accounting records: up to 10 years where German tax and commercial law requires it.
- Technical logs: as long as necessary for security and stable operation of the App.
- Emails: until your request is resolved, unless retention is legally required.
- Attribution data (Meta, AppsFlyer): according to the providers' retention periods.

10) Deleting your account

You can delete your account directly in the App.

What happens:

- Your account, onboarding answers, score, progress data and other personal data stored by us are deleted (except data we must keep by law, see Section 9).
- Community posts and comments: your posts are deleted or anonymised so they are no longer linked to you.
- Deleting your account does not cancel your subscription. Subscriptions are managed by Apple. Please cancel in iPhone Settings > (your name) > Subscriptions before deleting your account.

You can also email us at mrc.ecommerce1@gmail.com to request deletion.

11) Children

Quitli is not intended for children. Users must be at least 16 years old. This applies in all countries, including the United States.

We do not knowingly collect data from children below this age. If we learn that we have, we will delete the data. Parents who believe their child uses the App can contact us.

12) Your rights (GDPR and similar laws)

You have the right to:

- access your data (Art. 15 GDPR),
- correct inaccurate data (Art. 16),

- delete your data (Art. 17),
- restrict processing (Art. 18),
- data portability (Art. 20),
- withdraw consent at any time with effect for the future (Art. 7(3)),
- object to processing based on legitimate interest (Art. 21), see below,
- lodge a complaint with a supervisory authority, in particular in your country of residence. Our lead authority is the Saxon Data Protection and Transparency Commissioner (Sächsische Datenschutz- und Transparenzbeauftragte), Germany.

Right to object: Where we process your data based on our legitimate interests, you may object at any time for reasons arising from your particular situation. We will then stop, unless we have compelling legitimate grounds or need the data for legal claims.

To exercise your rights, email mrc.ecommerce1@gmail.com. We may need to verify your identity. We reply within one month (GDPR) or within the deadline set by your local law.

13) US State Privacy Rights

13.1 California Online Privacy Protection Act (CalOPPA)

- Categories of personally identifiable information we collect: see Section 3.
- Third parties we share it with: see Section 4.
- How you can review and request changes: email us or delete your account in the App (Section 10).
- How we notify you of changes: see Section 15.
- Do Not Track: The App does not respond to browser "Do Not Track" signals. On iOS, tracking for advertising only happens if you allow it in the ATT prompt (Section 7).
- Other parties' tracking: The Meta SDK and AppsFlyer may collect information about your activity over time and across apps only if you allow tracking via ATT.
- Effective date: see the top of this policy.

13.2 Your rights under US state privacy laws

Depending on the state you live in (for example California, Colorado, Connecticut, Virginia, Utah, Texas, Oregon, Montana, and other states with comprehensive privacy laws), you may have the right to:

- know and access the personal data we hold about you,
- correct inaccurate personal data,
- delete your personal data,

- obtain a copy of your data in a portable format,
- opt out of targeted advertising, the "sale" of personal data and profiling with legal or similarly significant effects,
- limit the use of sensitive personal data, or have it processed only with your consent,
- not be discriminated against for exercising your rights.

Some of these laws only apply to businesses above certain size thresholds. We nevertheless offer these rights to all US users.

Sale and targeted advertising: We do not sell personal data. Sharing your advertising identifier with Meta and AppsFlyer for ad attribution may count as "targeted advertising" or "sharing" under some state laws. It only happens if you allow tracking via ATT. To opt out, choose "Ask App Not to Track" or turn off tracking in iPhone Settings > Privacy & Security > Tracking. You can also email us to opt out.

Sensitive data and consumer health data: We process sensitive data (see Section 5) only with your consent and only to provide the App. Washington and Nevada residents: see our Consumer Health Data Privacy Policy at https://quitli.de/en/health-data.

How to submit a request: email mrc.ecommerce1@gmail.com with the subject "US Privacy Request" and your state. You may use an authorised agent; we may ask for proof of authorisation and verify your identity. We respond within 45 days (extendable once by 45 days where the law allows).

Appeals: If we decline your request, you can appeal by replying to our decision email with the subject "Appeal". We will respond within the period required by your state law (generally 45 to 60 days). If you are not satisfied with our appeal decision, you may contact your state Attorney General.

13.3 California "Shine the Light"

We do not disclose personal information to third parties for their own direct marketing purposes.

14) Security

Data is transmitted encrypted (TLS). Access to our backend is restricted. No method of transmission or storage is completely secure, but we use reasonable measures to protect your data.

15) Changes to this policy

We may update this policy when the App or the law changes. The current version is always available at https://quitli.de/en/privacy. For material changes we will inform you in the App before they take effect and, where required, ask for your consent again.

16) Contact

Jaron Marec Braun, MRC E-Commerce
Brandvorwerkstr. 69, 04275 Leipzig, Germany
Email: mrc.ecommerce1@gmail.com
Phone: +49 176 23560172

Support: https://quitli.de/support