

PRIVACY POLICY

Zentree: Meditate and Sleep

Last updated: July 9, 2026

Controller / responsible party: Justin Kruse, doing business as Zentree, Westernstraße 11, 31655 Stadthagen, Germany. Email: app.zentree@gmail.com.

Scope: This Privacy Policy explains how personal information is processed when you download, access, or use the iOS app Zentree: Meditate and Sleep and related support communications.

Important transparency note: The app is designed to work without a traditional account, email login, password, advertising tracking, third-party analytics SDKs, social media plugins, or offer walls. Most app data is stored and processed locally on your device. Some limited technical, purchase, and subscription-related data is processed by Apple, RevenueCat, and Cloudflare as described below.

Table of Contents

1. Who We Are
2. Quick Summary
3. Information We Process
4. Information We Do Not Collect or Use
5. How We Use Information and Legal Bases
6. Apple Health / HealthKit
7. Apple Family Controls / Screen Time Features
8. Subscriptions, Apple, StoreKit, and RevenueCat
9. Cloudflare R2 and Content Delivery
10. Local Notifications and Device Permissions
11. Sharing With Service Providers
12. International Transfers
13. Retention
14. Security
15. Your Privacy Rights
16. United States Privacy Rights
17. Children and Minors
18. External Links
19. Changes to This Policy
20. Contact

1. Who We Are

The controller responsible for the processing described in this Privacy Policy is Justin Kruse, doing business as Zentree.

Postal address:

- Justin Kruse
- Westernstraße 11
- 31655 Stadthagen
- Germany

Email for privacy inquiries and data subject requests: app.zentree@gmail.com

We have not appointed a data protection officer because, based on the current nature and scale of the app, we do not believe we are legally required to appoint one. If this changes, this Privacy Policy will be updated.

2. Quick Summary

- No traditional account: You can use the app without creating an email/password account with us.
- Local-first design: onboarding selections, profile preferences, focus/rest settings, local notification settings, profile images, Apple Health sleep data, and app blocking selections are intended to stay on your device unless this policy says otherwise.
- Subscriptions: purchases and subscription status are handled through Apple and RevenueCat. We do not receive or store payment card numbers, bank account details, or security codes.
- Audio delivery: guided meditation and sleep audio files are delivered through Cloudflare R2 / Cloudflare infrastructure. Cloudflare may process technical request data such as IP address and request logs to deliver and secure content.
- No ads or tracking: we do not use advertising SDKs, targeted advertising, IDFA tracking, retargeting pixels, offer walls, or social media plugins.
- Health data: if you connect Apple Health, sleep-related HealthKit data is processed only on your device and is not sent to us, RevenueCat, Cloudflare, analytics providers, advertising providers, or AI providers.
- Family Controls / Screen Time: if you enable productivity or sleep features that block distracting apps or websites, the relevant selections and restrictions are handled through Apple frameworks and are intended to be processed locally on your device.

3. Information We Process

Depending on which features you use, the following categories of information may be processed:

Category	Examples	Where it is processed
Local app preferences and onboarding selections	Age range, mood/focus/rest preferences, sleep or productivity settings, tree/app state, profile preferences, selected routines, and similar app settings.	Stored and processed locally on the device. Not transmitted to us.
Profile image	If you choose to add a profile image from your device.	Stored locally on the device. Not transmitted to us.
Apple Health / HealthKit sleep data	Sleep-related data read from Apple Health if you grant HealthKit permission.	Processed locally on the device. Not transmitted to us or third-party analytics/advertising providers.
Family Controls / Screen Time selections	Apps, websites, categories, schedules, or restriction settings you choose for focus, sleep, or productivity features.	Processed through Apple Family Controls / Screen Time frameworks and stored/enforced locally on the device, unless Apple processes data as part of iOS/iCloud/Screen Time services under Apple rules.
Local notifications	Notification content, timing, and settings selected by you.	Stored locally and delivered by the device operating system. We do not operate a push-notification marketing system.
Subscription and purchase information	Apple App Store purchase status, product identifiers, transaction/receipt validation data, entitlement status, expiration/renewal status, and an	Processed by Apple and RevenueCat to provide paid features and restore purchases. We do not receive payment card

	app-specific RevenueCat user identifier.	details.
Technical content delivery data	IP address, device/browser request headers, user agent, requested audio/content URL, timestamps, response status, and security logs when audio/content is loaded.	Processed by Cloudflare to deliver audio/content, improve performance, and protect the service.
Support communications	Email address, message content, attachments, and any information you voluntarily provide when contacting us.	Processed by us to respond to your request and document support communications.
Apple developer diagnostics	Aggregated or user-consented crash, performance, or diagnostic information that Apple may make available to developers through App Store Connect.	Processed according to Apple's developer and privacy rules, and used only to improve reliability and security.

We do not intentionally collect more information than necessary for the features you choose to use. Local device data is not available to us and cannot be accessed, corrected, exported, or deleted by us remotely. You can delete local data by using in-app reset/delete options where available, revoking device permissions, or uninstalling the app.

4. Information We Do Not Collect or Use

Based on the current app design, we do not:

- require users to create an account with an email address and password;
- collect or store payment card numbers, bank details, or App Store billing credentials;
- use IDFA, advertising tracking, retargeting, advertising pixels, or offer walls;
- use Google Analytics, Facebook/Meta SDK, TikTok SDK, PostHog, Firebase Analytics, or similar analytics/tracking SDKs;
- sell personal information;
- share personal information for cross-context behavioral advertising;
- send Apple Health data, Family Controls selections, local profile images, or onboarding answers to us for analytics, advertising, or profiling;
- use user personal information to generate AI content or send user data to AI providers. Guided meditation or sleep audio may have been created by us using audio generation tools, but user personal information is not used for that content generation.

5. How We Use Information and Legal Bases

For users in the European Economic Area, the United Kingdom, and Switzerland, we rely on the legal bases below where applicable. The exact legal basis depends on the feature and the context.

Purpose	Data involved	Legal basis
Providing app functionality	Local preferences, app state, focus/rest/sleep settings, content access	Performance of a contract (Art. 6(1)(b) GDPR); legitimate interests in providing and improving basic app functionality (Art. 6(1)(f) GDPR).
HealthKit sleep feature	Sleep-related HealthKit data when you grant permission	Consent / explicit consent (Art. 6(1)(a) GDPR and, where applicable, Art. 9(2)(a) GDPR).
Family Controls / Screen Time features	Selected apps, websites, categories, schedules, and	Consent and user-initiated feature use (Art. 6(1)(a) and/or Art. 6(1)(b)

	restriction settings	GDPR).
Subscriptions and paid access	Purchase status, product IDs, receipts, entitlement status, RevenueCat app user ID	Performance of a contract (Art. 6(1)(b) GDPR); legal obligations for tax/accounting (Art. 6(1)(c) GDPR); legitimate interests in fraud prevention and service integrity (Art. 6(1)(f) GDPR).
Delivering audio/content and protecting infrastructure	Technical request data processed by Cloudflare	Performance of a contract (Art. 6(1)(b) GDPR); legitimate interests in secure and reliable content delivery (Art. 6(1)(f) GDPR).
Support and privacy requests	Email address, inquiry content, request verification data	Performance of a contract, legal obligations, and legitimate interests in responding to users and documenting requests (Art. 6(1)(b), 6(1)(c), and 6(1)(f) GDPR).

6. Apple Health / HealthKit

If you choose to connect Apple Health, the app may request permission to read sleep-related data from HealthKit in order to display sleep-related information inside the app and support sleep-related features.

- HealthKit permissions are optional and controlled by you through iOS.
- The app requests access only to the HealthKit data types needed for the selected feature.
- Sleep-related HealthKit data is processed locally on your device.
- We do not transmit HealthKit data to our servers, RevenueCat, Cloudflare, advertising networks, analytics providers, or AI providers.
- We do not use HealthKit data for advertising, tracking, profiling, or marketing.
- You can revoke HealthKit permissions at any time in the Health app or iOS Settings.

7. Apple Family Controls / Screen Time Features

The app may offer focus, productivity, or sleep features that use Apple Family Controls, Managed Settings, Device Activity, and related Screen Time APIs to help you temporarily block or limit distracting apps, websites, or categories selected by you.

- This feature is optional and requires Apple/iOS authorization.
- Selections and restrictions are chosen by you and are intended to be stored and enforced locally on your device using Apple frameworks.
- We do not receive a list of the apps or websites you choose to block.
- We do not sell, share, or use these selections for advertising, analytics, or profiling.
- You can change, disable, or revoke these restrictions through the app and/or iOS Settings, depending on the feature and Apple's available controls.
- Apple may process information as part of iOS, iCloud, Screen Time, Family Sharing, or other Apple services under Apple's own terms and privacy policy.

8. Subscriptions, Apple, StoreKit, and RevenueCat

The app may offer auto-renewable subscriptions or other in-app purchases through Apple App Store / StoreKit. Payments are processed by Apple. We use RevenueCat to manage subscriptions, entitlements, purchase restoration, and receipt validation.

For this purpose, Apple and/or RevenueCat may process information such as:

- purchase history and subscription status;
- product identifiers, prices, currency, transaction identifiers, receipt validation data, renewal/expiration status, and entitlement status;
- an app-specific RevenueCat user identifier, which may be anonymous if you do not create an account with us;
- technical information needed to prevent fraud, restore purchases, and provide paid access.

We do not collect or store your payment card number, bank account number, App Store password, or card security code. Refunds, billing, family sharing of subscriptions, and App Store payment issues are generally handled by Apple according to Apple's rules.

9. Cloudflare R2 and Content Delivery

We use Cloudflare, including Cloudflare R2 and related content delivery/security infrastructure, to host and deliver guided meditation audio files, sleep audio files, and/or other app content. The audio files are app content provided by us; they are not user-generated uploads.

When the app loads content through Cloudflare, Cloudflare may process technical information such as:

- IP address;
- date and time of the request;
- requested URL or object path;
- user agent, device/browser request data, and HTTP headers;
- response status, performance data, and security logs.

This processing is used for content delivery, performance, reliability, abuse prevention, and security. We do not use Cloudflare to build user profiles, serve ads, or track users across apps or websites.

10. Local Notifications and Device Permissions

The app may ask for optional permissions depending on the features you use, including notifications, Apple Health, photo or storage access for a profile image, and Apple Family Controls / Screen Time authorization.

- Local notifications: notification schedules and content are created on the device and delivered by iOS. We do not operate a marketing push-notification backend.
- Photo/storage access: used only if you choose a profile image or import content from your device. Profile images are intended to remain local.
- Apple Health: used only if you connect Apple Health for sleep-related functionality.
- Family Controls / Screen Time: used only if you enable productivity, sleep, or focus restrictions.

You can revoke device permissions at any time in iOS Settings. Some app features may stop working if the required permission is revoked.

11. Sharing With Service Providers

We disclose personal information only where necessary to provide the app, process subscriptions, deliver content, respond to support requests, comply with law, or protect the service. We do not sell personal information and do not share personal information for cross-context behavioral advertising.

Provider	Purpose	Data categories
Apple Inc. / Apple Distribution International	App Store distribution, StoreKit, in-app purchases, subscriptions, billing, refunds, family sharing, diagnostics, HealthKit permissions, Screen Time / Family Controls frameworks	Purchase/subscription data, App Store account/payment data handled by Apple, device permission processing, diagnostics as made available by Apple

RevenueCat, Inc.	Subscription management, entitlement status, purchase restoration, receipt validation	App-specific user identifier, product IDs, receipts, purchase/subscription status, entitlement data, technical data needed for the service
Cloudflare, Inc.	Cloudflare R2, content delivery, security, performance, abuse prevention	Technical request data such as IP address, request headers, timestamps, requested content, logs
Email provider	Receiving and responding to support and privacy requests	Email address, message content, attachments, inquiry metadata

We may also disclose information if required by law, to protect rights and safety, to respond to lawful requests, or in connection with a business transfer such as a merger, acquisition, or sale of assets. If that ever happens, we will take reasonable steps to ensure continued protection of personal information.

12. International Transfers

We are based in Germany. We do not currently operate user-account servers of our own. However, Apple, RevenueCat, Cloudflare, and other service providers may process information in the United States and other countries outside the European Economic Area, the United Kingdom, or Switzerland.

Where required, we rely on appropriate transfer safeguards such as adequacy decisions, the European Commission's Standard Contractual Clauses, the UK International Data Transfer Addendum or equivalent safeguards, Data Processing Agreements, and/or other lawful transfer mechanisms offered by the relevant service providers. Details may be provided upon request where applicable and where we are legally able to provide them.

13. Retention

Data type	Retention
Local app data	Until you delete it, reset app data, revoke the relevant permission, or uninstall the app.
HealthKit sleep data	Processed locally only; controlled by Apple Health and your device settings. We do not retain a server copy.
Family Controls / Screen Time selections	Stored/enforced locally according to the feature settings until you change or disable them, revoke permission, reset app data, or uninstall the app.
Subscription and purchase data	Kept by Apple and RevenueCat as needed to provide subscriptions, restore purchases, prevent fraud, comply with legal obligations, and according to their retention policies. We keep access only as long as needed for app operations and legal obligations.
Cloudflare technical logs	Retained according to Cloudflare's service configuration and retention rules, and only as needed for content delivery, performance, and security.
Support and privacy requests	Kept as long as needed to handle your request and document compliance, generally up to three years unless a longer legal retention period applies.
Tax/accounting/legal records	Kept for the period required by applicable law.

14. Security

We use reasonable technical and organizational measures intended to protect personal information. These measures include a local-first app design, limiting server-side data, using Apple's permission systems for sensitive device features, relying on established service providers, and avoiding advertising/tracking SDKs.

No system can be guaranteed to be completely secure. You are responsible for keeping your device, Apple ID, and device passcode secure. If you believe your information or device has been compromised, please contact us and take appropriate steps through Apple and your device settings.

15. Your Privacy Rights

Depending on your location, you may have rights to request access, correction, deletion, restriction, portability, objection, withdrawal of consent, and to lodge a complaint with a supervisory authority. These rights may be limited by law and may not apply to information we cannot access because it is stored only on your device.

For users in the EEA, UK, or Switzerland, you may contact us at the email address below. You may also complain to your local data protection authority. Because we are based in Lower Saxony, Germany, the relevant German supervisory authority is the Lower Saxony data protection authority (Landesbeauftragte für den Datenschutz Niedersachsen), without prejudice to your right to contact your own local authority.

To exercise your rights, contact us at: app.zentree@gmail.com

Because the app does not use traditional accounts, we may need limited information to verify your request. We will not use verification information for unrelated purposes. For local-only data, we may be unable to access or delete it remotely; in that case, we will explain how you can delete or reset the relevant data on your device.

16. United States Privacy Rights

This section applies to residents of U.S. states with applicable consumer privacy laws, to the extent those laws apply to us. The exact rights and thresholds vary by state.

16.1 Categories of personal information

Category	Examples	Collected/processed?	Disclosure
Identifiers	RevenueCat app user ID, technical identifiers, IP address in logs, support email if you contact us	Yes, limited	Service providers only; no sale/share
Commercial information	Subscription status, product IDs, purchase history, entitlement status	Yes, via Apple/RevenueCat	Apple and RevenueCat for subscription processing; no sale/share
Internet or network activity	Limited technical request data when content is delivered through Cloudflare; diagnostics through Apple if available	Yes, limited	Cloudflare/Apple as service providers; no advertising tracking
Geolocation	No precise location. Approximate location may be inferred from IP address by service providers for security, compliance, or content delivery.	Limited technical processing only	No sale/share
Protected classifications	Optional age range or similar onboarding	Local only	Not transmitted to us

	choices may be stored locally if you choose them.		
Health / sensitive information	Sleep-related Apple Health data if you grant permission.	Local only	Not transmitted to us; not used to infer characteristics for advertising
Audio/visual/sensory data	Optional profile image selected from your device.	Local only	Not transmitted to us
Inferences / profiling	We do not create consumer profiles for advertising, credit, employment, insurance, or legal/similarly significant decisions.	No	No sale/share

16.2 No sale, no targeted advertising, no profiling decisions

We do not sell personal information. We do not share personal information for cross-context behavioral advertising. We do not use personal information for targeted advertising or for profiling that produces legal or similarly significant effects.

16.3 U.S. consumer rights

Depending on your state, you may have the right to know/access, correct, delete, obtain a copy, opt out of sale/share/targeted advertising/profiling, limit certain sensitive data uses, and appeal a decision. Since we do not sell or share personal information for targeted advertising and do not conduct such profiling, opt-out rights for those practices are generally not applicable.

To submit a request or appeal, email us at app.zentree@gmail.com. We will respond in accordance with applicable law. Authorized agents may submit requests where permitted by law, but we may require proof of authorization and reasonable identity verification.

17. Children and Minors

The app is not directed to children under the age of 13. We do not knowingly collect personal information from children under 13. If you believe a child under 13 has provided personal information to us, please contact us and we will take appropriate steps to delete the information where required.

The app may include an onboarding option such as "Under 18." This selection is intended to be stored locally on the device and is not transmitted to us. If a minor uses the app, they should do so only with parental or guardian consent where required by applicable law.

18. External Links

The app may contain links to external websites or social media profiles, such as an Instagram account or support page. These are simple outbound links, not embedded social media plugins. If you open an external link, the external provider may process information under its own privacy policy. We are not responsible for the privacy practices of external websites or platforms.

19. Changes to This Policy

We may update this Privacy Policy from time to time. The updated version will be indicated by a new "Last updated" date. If we make material changes, we may provide additional notice in the app or through another appropriate channel where required.

20. Contact

If you have questions, comments, or requests about this Privacy Policy or our processing of personal information, contact us at:

- Email: app.zentree@gmail.com
- Postal address: Justin Kruse, Westernstraße 11, 31655 Stadthagen, Germany

Appendix: Service Provider Privacy Information

For convenience, the main provider privacy pages are:

- Apple Privacy Policy: <https://www.apple.com/legal/privacy/en-ww/>
- RevenueCat Privacy Policy: <https://www.revenuecat.com/privacy/>
- Cloudflare Privacy Policy: <https://www.cloudflare.com/privacypolicy/>
- Cloudflare Data Processing Addendum: <https://www.cloudflare.com/cloudflare-customer-dpa/>

This document is intended to describe the current privacy practices of the app. It should be reviewed and updated if new SDKs, analytics, advertising, AI processing, account functionality, cloud storage, push-notification backends, or additional data sharing are added.