

Dopa Defender Privacy Policy

Effective Date: September 12, 2026

Resanity LLC (“Resanity,” “we,” “us,” or “our”) operates the Dopa Defender iOS mobile application (the “App”). This Privacy Policy explains how we collect, use, disclose, retain, and protect information when you use the App.

Resanity LLC is located at:

418 Broadway, STE N
Albany, NY 12207
United States

For privacy questions or requests, contact us at help@dopadefender.com.

This Privacy Policy applies to the Dopa Defender iOS App. It does not apply to websites, services, applications, devices, or platforms operated by Apple, Google, or other third parties, including the Apple App Store, Apple Health, HealthKit, Core Location, iCloud, Google Sheets, or your wireless carrier. Those third parties’ handling of information is governed by their own terms and privacy policies.

1. Privacy Summary

Dopa Defender is a self-management tool designed to help people manage digital distractions. Most information used by Dopa Defender is stored locally on your device and is not transmitted to Resanity.

At launch:

- We do not create user accounts.
- We do not offer cross-device synchronization.
- We do not sell personal information.
- We do not use advertising SDKs, behavioral analytics, crash-reporting SDKs, attribution SDKs, tracking technologies, social logins, or third-party account integrations.
- We do not use personal information for targeted advertising.
- We do not collect, retain, or transmit a server-side history of your precise location, trips, routes, arrivals, departures, or places visited.
- We do not intentionally transmit Screen Time, DeviceActivity, FamilyControls, ManagedSettings, or HealthKit data to Resanity.
- We do not use HealthKit information for advertising, marketing, data mining, sale to data brokers, insurance, employment, credit, or other similarly consequential decisions.

- Apple processes App Store subscriptions. We do not receive or store your payment-card number or Apple Account password.
- Feedback that you voluntarily submit is the only information transmitted to Resanity through the App. Feedback includes the information you choose to submit and limited technical metadata automatically included with the submission, such as device model, iOS version, App version, and submission timestamp. Feedback is stored in a Google Sheet that we use as our feedback database.

2. Information We Collect

A. Information stored locally on your device

The App stores information locally on your device to provide its features. Depending on the features you choose to use, locally stored information may include:

- Your Dopa Defender preferences, onboarding choices, and feature settings.
- A name or label you choose for your Dopa Defender.
- Motivation-survey responses, custom warnings, and other text or preferences you choose to enter.
- Selected applications, categories, or websites for tracking, goals, warnings, schedules, manual blocks, and other App features.
- Daily app-usage goals and related local configuration.
- Scheduled-blocking rules, manual-block selections, block status, and related configuration.
- Location Rule configuration, such as a user-selected place name, coordinates, geographic radius, arrival/departure condition, and selected App action.
- Health Activity rule configuration, such as the activity type and threshold you choose.
- Local PIN Protection settings and PIN-reset waiting-period status.
- Locally generated information needed to operate or display App features.

This information is stored locally on your device. At launch, Dopa Defender does not provide a cross-device synchronization feature and does not send this information to Resanity simply because you use the App.

Deleting the App generally removes locally stored App data from that device and resets local App tools, subject to your device's operating system, backup settings, and other Apple-controlled behavior.

B. Apple Screen Time and device-activity information

If you authorize applicable Apple permissions and use Screen Time-related features, the App may use Apple frameworks and services such as FamilyControls, ManagedSettings, DeviceActivity, and related Screen Time functionality.

Depending on the permissions you grant and Apple's framework behavior, these features may allow the App to access, use, or display information related to applications, categories,

websites, usage activity, usage duration, device activity, and selected-app management features.

We use this information on your device to provide App features such as analytics, daily goals, warnings, scheduled blocking, and manual blocking. At launch, we do not intentionally transmit Screen Time or DeviceActivity information to Resanity.

Apple controls the relevant frameworks, permissions, and information available to applications. You can manage certain permissions through your Apple device settings.

C. HealthKit and Apple Health information

Health Activity features are optional. If you choose to enable them, the App may request access through Apple Health or HealthKit only to the data types needed for the specific activity rule you choose. Depending on the feature and your authorization, this may include:

- Step count.
- Walking or running distance.
- Flights climbed.
- Other activity measures that you specifically configure in the App, if available.

HealthKit authorization is controlled by Apple. You may grant, deny, or revoke access through Apple's Health and privacy controls.

We use HealthKit information on your device only to provide the Health Activity features you choose, such as showing progress toward an activity goal or determining whether an App-configured rule can be updated after you manually request a refresh.

At launch, we do not intentionally transmit HealthKit information to Resanity. We do not use HealthKit information for advertising, marketing, data mining, sale to data brokers, insurance, employment, credit, medical decisions, or other similarly consequential decisions.

D. Location information

Location Rules are optional. If you choose to use them, the App may request permission to use location information to operate a rule you configure around arriving at or leaving a saved place.

Location-related information used locally by the App may include a place name you choose, coordinates, geographic radius, and an arrival or departure condition. This information is used on your device to operate your Location Rules.

At launch, Resanity does not collect, retain, or transmit a server-side history of your precise location, trips, routes, arrivals, departures, or places visited. We do not use location information for advertising or targeted advertising.

Location features depend on Apple permissions, device settings, iOS behavior, connectivity, battery status, and environmental conditions. Location Rules are not real-time, continuous, precise, emergency, or safety location-monitoring services.

E. Feedback you choose to submit

The App may allow you to voluntarily submit feedback. Feedback is optional.

When you submit feedback, we collect:

- Feedback text, comments, suggestions, bug reports, or support requests that you choose to provide.
- Your name, email address, or other contact information if you include it.
- Screenshots, photos, diagnostic logs, or other attachments you choose to submit.
- Technical details that you include in the feedback or attachments.
- The device model associated with the feedback submission.
- The iOS version running on the device when feedback is submitted.
- The Dopa Defender App version associated with the feedback submission.
- The date and time at which the feedback is submitted.

The automatically included device model, iOS version, App version, and submission timestamp help us understand the context of a reported problem, reproduce technical issues, investigate compatibility issues, and improve the App.

Feedback, including this limited technical metadata, is the only information transmitted to Resanity through the App at launch. We store submitted feedback in a Google Sheet that we use as our feedback database. Feedback may be reviewed manually and irregularly.

Please do not submit passwords, authentication codes, payment-card information, government identification numbers, unnecessary health information, confidential information belonging to another person or organization, or any other sensitive information that is not reasonably necessary to describe your feedback.

F. Subscription and purchase information

Subscriptions are processed by Apple through the App Store. Apple may provide us with limited information necessary to determine whether an App Store subscription is active, expired, canceled, renewed, or eligible for certain offers.

We do not receive or store your full payment-card number, Apple Account password, or other payment credentials. Apple's processing of purchases, subscription transactions, payment information, and Apple Account information is governed by Apple's terms and privacy policy.

3. How We Use Information

We use information as follows:

- To provide, operate, maintain, and improve the App and its features.
- To save and apply your locally configured App selections, goals, schedules, blocks, warnings, PIN settings, and preferences.

- To provide on-device Screen Time-related functionality, including selected-app management, analytics, usage-goal features, blocking rules, and related user experiences.
- To provide Health Activity features that you expressly choose to use.
- To provide Location Rules that you expressly choose to use.
- To receive, store, review, and, where we choose, respond to feedback that you voluntarily submit.
- To use feedback-submission metadata, such as device model, iOS version, App version, and timestamp, to investigate reported issues, assess App compatibility, troubleshoot, and improve the App.
- To investigate, troubleshoot, prevent, and address bugs, errors, abuse, security issues, or violations of our Terms of Use.
- To comply with applicable law, legal process, lawful requests, and enforceable governmental requirements.
- To establish, exercise, or defend legal claims and protect the rights, safety, property, and security of Resanity, users, and others.

We do not use your personal information for targeted advertising. We do not sell personal information.

4. How We Share Information

We do not sell personal information. We do not share personal information for cross-context behavioral advertising or targeted advertising.

We may share information only in the following limited circumstances:

- **With Apple:** Apple processes information needed to provide Apple devices, iOS, the App Store, subscriptions, HealthKit, Screen Time-related frameworks, FamilyControls, ManagedSettings, DeviceActivity, Core Location, notifications, device backups, permissions, and other Apple services. Apple's handling of information is governed by its own policies and settings.
- **With Google:** Feedback you submit, including limited technical metadata automatically included with the submission, is stored in a Google Sheet. Google processes information stored in Google Sheets under Google's terms and privacy policies.
- **With service providers:** We may use service providers to host, store, secure, process, or support feedback that you voluntarily submit, but only as needed to provide services to us and subject to applicable agreements or obligations.
- **For legal and safety reasons:** We may disclose information if we reasonably believe disclosure is required by law, legal process, court order, subpoena, or governmental request; necessary to protect rights, safety, security, or property; or necessary to investigate fraud, abuse, or violations of our Terms of Use.
- **Business transfer:** If Resanity is involved in a merger, acquisition, financing, reorganization, bankruptcy, sale of assets, or similar transaction, information may be transferred as part of that transaction, subject to applicable law.

- **With your direction or consent:** We may share information when you direct us to do so or expressly consent.

At launch, we do not share HealthKit information with advertising networks, data brokers, or third parties for advertising, marketing, or data-mining purposes.

5. Data Storage, Retention, and Deletion

A. Local App data

Most Dopa Defender data is stored locally on your device. Dopa Defender does not provide cross-device synchronization at launch.

Deleting the App generally removes locally stored App data from that device and resets local App tools, including blocks, schedules, preferences, and PIN Protection-related state. Deleting the App does not necessarily cancel an App Store subscription. You must manage or cancel subscriptions through your Apple Account Settings.

Your device's operating system, backups, and other Apple-controlled services may retain data according to your device settings and Apple's practices. Resanity does not control those services.

B. Feedback retention

Feedback you submit, including associated device model, iOS version, App version, and submission timestamp, is stored in a Google Sheet used by Resanity as a feedback database. We retain feedback indefinitely by default unless we delete it, no longer need it, are required to delete it, or you make a valid deletion request.

We retain feedback to review submissions, respond where appropriate, improve the App, investigate and resolve technical issues, protect the App and users, establish or defend legal claims, comply with legal obligations, and maintain reasonable business records.

C. Feedback deletion requests

To request deletion of feedback that you submitted, contact us at help@dopadefender.com. Please include enough information for us to reasonably locate your submission, such as the email address you included, the approximate submission date, and a description of the feedback.

We may need to verify your request before acting on it. We may retain information where permitted or required by law, including for legal, security, fraud-prevention, recordkeeping, or dispute-resolution purposes.

6. Your Choices and Controls

You control many App features through the App and your Apple device settings.

A. Permissions

You can manage or revoke permissions for Dopa Defender through iOS settings, including permissions relating to:

- Screen Time-related features and FamilyControls.
- Apple Health and HealthKit.
- Location.
- Notifications.
- Photos or other attachment-related permissions, if requested.

Revoking a permission may limit or disable related App features.

B. HealthKit

You can manage Dopa Defender's HealthKit permissions through the Health app or iOS privacy settings. Apple controls the available permission controls and the data types you may authorize.

C. Location

You can manage location access in iOS Settings. If you disable location access, Location Rules may stop functioning or may not update as expected.

D. Subscriptions

You can manage or cancel an App Store subscription through Apple Account Settings, generally through Settings > [your name] > Subscriptions on your Apple device. Deleting the App does not necessarily cancel a subscription.

E. Feedback

You are not required to submit feedback. If you submit feedback, avoid including information that you do not want Resanity to receive. You may request deletion of submitted feedback as described in Section 5.C.

7. Data Security

We use reasonable administrative, technical, and organizational measures intended to protect feedback and other information that we control. However, no storage method, transmission method, or security measure is completely secure. We cannot guarantee absolute security.

Feedback, including device model, iOS version, App version, and timestamps, is stored in Google Sheets. Access to feedback should be limited to authorized persons acting for Resanity. You should not submit highly sensitive information through feedback.

You are responsible for protecting your device, device passcode, Apple Account, App settings, and access to information displayed through the App. If you allow someone else to use your

device, they may be able to view or change locally stored App information, subject to your device and App settings.

8. Children's Privacy

Dopa Defender is intended for users age 13 and older and is not directed to children under 13.

A parent or guardian may choose to install or use the App on a child's device as a local support tool. At launch, Dopa Defender does not provide remote parental monitoring, parent-child accounts, or Family Sharing administration.

If you believe a child under 13 has submitted personal information to us through feedback without appropriate authorization, contact us at help@dopadefender.com. We will take reasonable steps to investigate and address the issue as required by applicable law.

9. Third-Party Services

The App depends on Apple services and technologies, which may include iOS, the App Store, App Store subscriptions, Apple Health, HealthKit, Screen Time-related frameworks, FamilyControls, ManagedSettings, DeviceActivity, Core Location, notifications, and device backup services.

Feedback you submit, including automatically included limited technical metadata, is stored in Google Sheets, a Google service.

Apple, Google, and other third parties operate under their own terms and privacy policies. We encourage you to review their applicable terms, privacy policies, and device settings.

We are not responsible for the privacy, security, availability, or practices of third-party services.

10. No Advertising Tracking

We do not use your personal information to track you across third-party apps or websites for targeted advertising.

We do not use advertising SDKs, behavioral analytics, crash-reporting SDKs, attribution SDKs, tracking technologies, social logins, or third-party app-account integrations at launch.

We do not use or disclose HealthKit information for advertising, marketing, data mining, or sale to data brokers.

If our data practices materially change in the future, we will update this Privacy Policy and provide any required notice or obtain any required consent before using information in a materially different way.

11. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. When we do, we will post the updated policy and revise the Effective Date above. If we make material changes, we will provide additional notice when required by law, such as through the App, a linked webpage, or a request for acknowledgment.

Your continued use of the App after an updated Privacy Policy becomes effective is subject to the updated policy to the extent permitted by applicable law.

12. Contact Us

For privacy questions, feedback-deletion requests, or requests relating to this Privacy Policy, contact:

Resanity LLC
418 Broadway, STE N
Albany, NY 12207
United States
help@dopadefender.com