

TOPUNDRED INC.

Jellywalk Privacy Policy

Effective July 21, 2026 · Last updated July 21, 2026 · Version 1.0

Jellywalk turns walking activity into in-app progress and rewards. Doing that requires unusually sensitive information, including health and fitness data and, when you start a tracked walk, precise location data. This Privacy Policy explains what Jellywalk processes, why it is needed, when it is shared, how long it is kept, and the choices available to you.

Jellywalk is operated by Topundred Inc. ("Topundred," "Jellywalk," "we," "us," or "our").

Topundred is the controller responsible for the personal information covered by this Policy.

Key points. Health, motion, photo-library, notification, and location access are controlled through your device. Precise and background location is used during an active walking session, including while the app is in the background or the screen is off. We do not sell personal information. We do not use Health Connect, HealthKit, precise location, or route data for advertising, insurance, credit, or employment decisions. You can delete your account in Jellywalk settings and can contact us about a narrower data request.

1. Scope

This Policy applies to the Jellywalk mobile application, Jellywalk APIs and servers, customer support, and related services that link to it (collectively, the "Service"). It covers information about Jellywalk users and people who contact us.

This Policy does not govern an independent third-party service, even if Jellywalk links to or works with it. Examples include Apple, Google, HealthKit, Health Connect, Auth0, mobile operating systems, app stores, map-tile providers, and websites opened from Jellywalk. Those parties process information under their own terms and privacy notices.

2. Information we process

The information we process depends on the features you use and the permissions you grant.

2.1 Account, authentication, and profile information

We process:

- email address;
- username or nickname;
- password credentials for email registration, which are handled through our authentication provider rather than stored by Jellywalk in readable form;
- authentication provider, provider subject identifier, access and refresh tokens, login status, and account creation/update timestamps;
- profile image, if you choose one;
- notification consent and topic preferences; and
- account identifiers and the number and last-login time of registered devices.

If you use Google or Apple sign-in, the selected provider and our authentication provider may give us an account identifier, email address, display name, profile image, and authentication tokens according to your provider settings. We do not receive your Google or Apple password.

2.2 Health, fitness, motion, and step information

With your permission, Jellywalk may read the following from Apple HealthKit or Google Health Connect:

- step count;
- distance; and
- active energy burned.

Jellywalk also uses the device pedometer and motion/activity-recognition interfaces to count steps during a walk and determine whether the device reports a walking or stopped state. We process daily step totals, per-session steps, accepted and discarded steps, and timestamps associated with those measurements.

Health-store data is requested for visible fitness, walking-progress, gameplay, and reward features. Jellywalk does not seek clinical records, diagnoses, medications, heart rate, contacts, or unrelated health categories through its current health permissions.

2.3 Precise location and route information

When you start a location-enabled walking session and grant the required permission, Jellywalk processes precise device location. A session may continue collecting location while Jellywalk is in the background or while the screen is off. Depending on the device and session, this can include:

- latitude and longitude;
- start and end coordinates;
- a sequence of coordinates forming the walking route or polyline;
- capture timestamps and location accuracy;
- distance traveled, speed, and changes between successive points;
- foreground/background session status; and
- permission and location-service status.

Jellywalk uses high-accuracy location at intervals during an active walk. It does not use this permission to track another person, provide emergency rescue, or continuously monitor you when no tracked session is active. Operating-system behavior may nevertheless show a background-location indicator or persistent notification while a session is running.

2.4 Walking-session and integrity information

For each walking session, we may process:

- session identifier, status, start/end time, active time, elapsed time, and game day;
- steps, distance, route, average speed, score, energy and in-app health consumed, and equipped virtual shoe;
- sequence numbers, capture times, GPS accuracy, connection state, and session synchronization records;
- movement-validation results, including accepted or rejected distance, time, or steps;
- signals indicating impossible speed, unusual cadence, stale or duplicated messages, location spoofing, sequence gaps, inaccurate GPS, automation, or other suspicious activity; and
- eligibility status, hold/exclusion reason, failure reason, reward outcome, and records used to investigate an appeal.

These integrity signals protect users and the reward system. A rule-based system may automatically clamp, reject, hold, or exclude activity that does not meet published or internal validation rules. You may ask us to review a result as described in Section 11.

2.5 Gameplay, rewards, and transaction information

We process account mode and in-app state such as:

- points, jellybeans, energy, in-app health, and scores;
- virtual shoes, shoe grades and attributes, equipped/representative status, and item inventory;
- daily missions, checkpoints, progress, claim dates, and rewards;
- virtual-item purchases, usage, and balance-change histories;
- reward-ledger, allocation, and distribution records; and
- leaderboard dates, rankings, scores, expected or distributed rewards, and related history.

The leaderboard feature makes a participating user's username, profile image, ranking, score, and reward information visible to other Jellywalk users. Do not use a username or profile image that reveals information you do not want associated with leaderboard participation.

2.6 Device, notification, and local-storage information

We process device and app information needed to operate the Service, including:

- Firebase Cloud Messaging token and token refresh events;
- device/account association and last-login time;
- operating system, app version, package identifier, locale, and device or browser user agent;
- on Android builds that include Google Analytics for Firebase, an app-instance identifier, app opens and sessions, basic interaction and diagnostic events, device/app characteristics, approximate location derived from IP address, and an Android advertising identifier if the operating system and SDK make it available;
- when you open a route map, the requested map-tile coordinates or viewport area, source IP address, user agent, and request time received by the CARTO map-tile delivery service; and
- push-notification permission, subscription, delivery, read, and message-log information; and
- locally stored access/refresh tokens, push token, permission acknowledgments, notification records, notice preferences, daily-step cache, pending step sync, and daily-mission cache.

Authentication and preference information is stored using the device's secure-storage facilities where supported. Removing the app may clear local data but does not by itself delete records already synchronized to our servers.

The current Android analytics integration is used for basic product measurement and reliability, not to personalize advertising. We do not intentionally send account credentials, Health Connect or HealthKit records, precise coordinates, route polylines, usernames, or profile images as

analytics event parameters. A map-tile request identifies the part of the map needed for display but does not intentionally include your Jellywalk account identifier or complete route polyline.

2.7 Technical, network, security, and support information

When your device communicates with the Service, we and our infrastructure providers may process:

- source IP address, user agent, referring source, request identifier, request time, endpoint, method, headers, query parameters, response status, response size, and latency;
- WebSocket connection and session events;
- sanitized request or error details, crash-like server errors, stack traces, and fraud/security alerts; and
- support messages, email address, attachments, and any information you include in a request.

We redact known credentials and authentication headers from application logs. Please do not include sensitive information in a support message unless it is necessary for us to help you.

2.8 Information we do not intentionally collect

The current Service does not intentionally request your contacts, microphone, SMS messages, government identifiers, payment-card details, or medical diagnosis records. Jellywalk does not currently display third-party ads or include an ad-serving SDK. The Android analytics integration described above can process a platform advertising identifier when available, but we do not use it or sensitive Jellywalk information for ad personalization or cross-context behavioral advertising. If the Service later begins processing materially different categories, we will update this Policy and obtain consent where required.

3. How we receive information

We receive information:

- **from you**, such as registration details, a username, profile image, permission choices, support requests, and account-deletion instructions;
- **from your device and its sensors**, such as pedometer, motion, location, network, app, and notification information;
- **from health platforms you authorize**, such as Apple HealthKit and Google Health Connect;
- **from authentication providers**, such as Auth0, Google, or Apple when you register, sign in, refresh a session, or delete an authentication account;

- **from Service activity**, such as missions, virtual-item use, rewards, leaderboards, and walking-session validation; and
- **from service providers**, such as push-delivery status, authentication results, infrastructure logs, and fraud/security signals.

4. Why we process information

We process personal information for the purposes below.

1. **Provide the Service.** Create and authenticate accounts; maintain sessions; show profile and app state; count and synchronize steps; track an active walk; calculate route, time, distance, speed, and progress; maintain workout history; operate missions, checkpoints, leaderboards, inventories, and virtual rewards.
2. **Validate activity and allocate rewards.** Detect duplicate, impossible, automated, spoofed, or otherwise ineligible activity; protect the daily reward pool; investigate disputes; correct technical or balance errors.
3. **Communicate.** Send essential service, security, account, and transaction messages; provide optional push or marketing communications when you consent; respond to support and privacy requests.
4. **Protect the Service and users.** Secure accounts and infrastructure; prevent abuse, fraud, unauthorized access, and violations of our Terms; diagnose incidents; keep audit and access records.
5. **Maintain and improve Jellywalk.** Troubleshoot performance, measure reliability, understand aggregate feature use, test changes, and improve accessibility and user experience. Basic Android app analytics may support these purposes. Health information, precise coordinates, and route polylines are not used for general analytics or advertising and are used only where necessary for the user-facing fitness, gameplay, integrity, support, or security purpose described here.
6. **Comply with law and enforce rights.** Meet legal, tax, accounting, consumer, privacy, location-information, and law-enforcement obligations; establish, exercise, or defend legal claims; enforce our agreements.
7. **Handle organizational changes.** Conduct due diligence and complete a merger, financing, reorganization, sale, or transfer, subject to applicable notice, consent, and confidentiality requirements.

5. Legal grounds

The legal ground depends on the information, purpose, and law that applies:

- **Your consent** supports access to health/fitness information, motion sensors, precise and background location, photos, optional notifications or marketing, certain overseas transfers, and other processing for which consent is legally required. You can withdraw consent, but withdrawal does not invalidate earlier lawful processing.
- **Performance of our agreement with you** supports account administration and the walking, history, gameplay, virtual-item, reward, and support functions you request.
- **Our legitimate interests, where recognized by law**, support proportionate security, anti-fraud, debugging, service improvement, and protection of users and reward integrity, after considering the effect on your rights.
- **Compliance with a legal obligation** supports required records, regulatory responses, lawful requests, and protection of legal rights.

Where Korean law requires a separate consent instead of another ground, we rely on the required consent. If you decline information that is necessary for a requested feature, that feature may not work. Optional profile photos and optional marketing are not required to maintain an account.

6. Health and fitness data commitments

Information obtained from Health Connect or HealthKit is treated as personal and sensitive information. In addition to the rest of this Policy:

- we request only the health categories needed for visible walking, fitness, progress, and reward features;
- we do not sell health or fitness information;
- we do not transfer, sell, or use Health Connect or HealthKit information for behavioral advertising, data brokerage, creditworthiness, lending, insurance eligibility, or employment decisions;
- we do not send Health Connect or HealthKit information to Google Analytics for Firebase or another general-purpose analytics or advertising service;
- we do not use it to provide a regulated medical-device function or make a diagnosis;
- human access is limited to what is needed for support you request, security/abuse investigation, legal compliance, or appropriately controlled internal operations;
- we do not disclose it to another independent party without your explicit direction or consent unless law permits or requires the disclosure; and

- you can revoke Jellywalk's health permissions in Health Connect, Apple Health, or device settings. Revocation stops future access but does not automatically erase information already synchronized to Jellywalk; use the deletion options in Section 11 for that.

Jellywalk is a fitness and game service, not a healthcare provider. Health-store and sensor measurements may be delayed, incomplete, duplicated, estimated, or inaccurate.

7. Automated activity validation

Jellywalk uses rule-based processing to validate movement and protect rewards. The rules can consider step changes, elapsed time, cadence, distance, speed, GPS accuracy, coordinate sequence, capture times, session state, and duplicate or stale events. The result may affect accepted steps or distance, score, leaderboard position, eligibility, and virtual rewards.

These systems are designed to detect technical errors and manipulation, but they can be wrong. If an automated result has a significant effect on your account or reward, email info@topundred.com with your username, session date/time, and a short explanation. We may ask for information needed to verify the request. Where applicable law grants a right to object to or obtain human review of an automated decision, we will honor that right.

8. When information is disclosed

We do not sell personal information. We disclose information only as described below.

8.1 Other Jellywalk users

Participating users can see leaderboard and public-profile information such as username, profile image, rank, score, and reward. We may also make aggregate or de-identified statistics available, provided they cannot reasonably identify you.

8.2 Processors and contractors

Vendors process information for us under instructions and contractual or legal safeguards. Current service functions use or are designed to use the following providers or provider categories:

Provider or category	Function	Information involved
Auth0 / Okta	Registration, email/password authentication, social login, token issuance, account deletion	Email, authentication identifier/provider, credentials, tokens, login and account metadata
Google Firebase, Google Cloud, and Google Analytics for Firebase	Push messaging, notification delivery, profile-image and service-asset storage; basic Android app measurement and reliability analytics	Push token, notification data, profile image, account/object identifier, storage and delivery metadata; on Android, app-instance identifier, automatically collected app/session events, device/app characteristics, approximate location derived from IP address, and advertising identifier when available
Apple and Google identity services	Optional social sign-in selected by the user	Provider identifier, email/name or image made available by the provider, authentication token
CARTO map-tile delivery service	Display a base map behind a workout route	Source IP address, user agent, request time, and requested tile coordinates or approximate map viewport; no Jellywalk account identifier or complete route polyline is intentionally included in the tile request
Hosting, database, cache, network, and backup providers	API delivery, MySQL records, temporary live-session state, security, resilience, backup	Service data necessary to host the requested feature, which can include account, activity, route, reward, device, and log data
Logging, observability, email, and incident-	Reliability monitoring, error alerting, support, and operational security	Request and error logs, user/account identifiers where present, support content, incident metadata

Provider or category	Function	Information involved
response providers		

Processors may not use Jellywalk information for their own unrelated purposes. We limit the data and access provided to what is reasonably necessary for the service they perform.

8.3 Legal, safety, and rights-related disclosures

We may disclose information when we reasonably believe it is necessary to comply with law or valid legal process; respond to a competent authority; protect a person from serious harm; investigate fraud, security, or a Terms violation; or establish, exercise, or defend legal claims. Jellywalk is not an emergency location service and does not promise that it can provide a live location to rescuers.

8.4 Corporate transactions

Information may be reviewed or transferred as part of a proposed or completed merger, acquisition, investment, financing, reorganization, insolvency, or sale of assets. The recipient must respect this Policy or provide legally required notice and choices before materially changing the processing.

9. Overseas processing and transfer

Topundred is based in the Republic of Korea. Some providers operate infrastructure outside Korea, so personal information may be remotely accessed, stored, or otherwise processed overseas.

Current core cross-border arrangements include:

Recipient and destination	Purpose and method	Categories and timing	Retention
Auth0 / Okta; Australian service region and related support locations	Encrypted network transfer for account authentication and token management	Account, provider identifier, credentials and token data when registering, signing in, refreshing, or deleting an account	For the account term and the provider's secure deletion/backup cycle, subject to legal requirements
Google Firebase / Google Cloud / Google Analytics; the configured project region and other locations from which Google provides the relevant service or support, including the United States where applicable	Encrypted network transfer for push delivery, cloud storage, and basic Android app measurement	Push token and delivery data when notifications are enabled; profile images and associated identifiers when uploaded; Android app-instance identifier, automatically collected app/session events, device/app characteristics, approximate location derived from IP address, and advertising identifier when available	Until the token is replaced/deleted, the image is replaced/deleted, or the applicable provider cycle ends; user-level Android analytics event data for no longer than 14 months, subject to shorter configured settings, while aggregate reports may remain without direct account identifiers
Apple or Google; provider-operated regions, including the United States where applicable	User-initiated social authentication	Provider identifier, authentication token, and account attributes made available during sign-in	According to the linked account, our account term, and provider policy
CARTO and its map-tile delivery	Encrypted network	Source IP address, user agent, request	Under CARTO's applicable security-

Recipient and destination	Purpose and method	Categories and timing	Retention
infrastructure; locations used by its global content-delivery network	requests for the base-map tiles needed to display a workout route	time, and requested tile coordinates or approximate map viewport when a route map is opened	log and service-retention cycle
Cross-border infrastructure, logging, or support vendors used in production	Secure hosting, reliability, support, fraud prevention, and incident response	The minimum Service records or logs needed for the function, transferred when the relevant operation occurs	Under the retention schedule below and the vendor contract

We use contractual, technical, and organizational safeguards and rely on consent or another transfer ground recognized by applicable law. Countries may have different data-protection rules from your country. You may contact us for the current production processor and destination register. Where a transfer is optional and applicable law gives you a right to refuse it, we will explain the consequence; refusing a transfer essential to authentication or hosting may mean we cannot provide the relevant Service.

10. Retention and destruction

We keep personal information only for the period needed for its disclosed purpose, a legal requirement, a dispute, security, or fraud prevention. The typical criteria are below.

Information	Typical retention criterion
Account and profile	While the account is active; after account deletion, removed from active use and deleted or anonymized through applicable database, provider, and backup cycles unless a lawful exception applies
Authentication records and tokens	Until logout, expiration, replacement, or account deletion, plus limited security records retained by the authentication provider
Daily steps, completed walks, routes, and workout history	While needed to show your history, calculate/verify rewards, and handle disputes; ordinarily until the record or account is deleted or you make a valid deletion request
Live walking-session state	For the active/recoverable session and a short closing period; converted into a completed/failed record or cleared when the session is finished, abandoned, or closed as stale
Gameplay, virtual-item, balance, reward, and leaderboard records	While the account is active and afterward only as needed to correct balances, prevent abuse, resolve disputes, or meet legal/accounting requirements
Push tokens and notification preferences	Until replaced, disabled, disassociated, or the account is deleted; delivery and notification logs for the operational/security period
Profile images	Until replaced or deleted, subject to cache and backup expiration
Android app analytics	User-level event data for no longer than 14 months, subject to a shorter configured Google Analytics setting; aggregate reports may remain longer without direct Jellywalk account identifiers
CARTO map-tile requests	Controlled by CARTO's applicable security-log and service-retention cycle; Jellywalk does not receive a

Information	Typical retention criterion
	separate copy of CARTO request logs through the current map display
Server, access, error, security, and fraud logs	For the shortest operational period reasonably needed, generally no longer than 12 months unless an incident, investigation, legal hold, or law requires longer
Support and privacy requests	For the request and follow-up period, generally up to 3 years after resolution when needed to document the response or protect legal rights
Location collection/use/provision verification records required by Korean law	For the period required by law or the location terms, kept separately from location content where appropriate

Deletion may occur by secure erasure, overwriting, cryptographic deletion, or irreversible anonymization. Data in backups, caches, fraud-prevention records, or provider systems may remain until the normal protected deletion cycle completes. While retained for an exception, information is isolated from ordinary product use where practicable.

11. Your choices and rights

11.1 Device permissions

You can manage permissions through iOS, Android, Apple Health, or Health Connect settings:

- **Health, motion, and activity recognition:** disabling access stops or reduces step and activity features.
- **Precise/background location:** disabling access prevents route tracking and may prevent a reward-eligible walking session. Ending the session stops Jellywalk's active route tracking.
- **Photo library:** disabling access prevents selection of a new profile image but does not remove an existing uploaded image.
- **Notifications:** disabling access stops push notifications. Essential notices may still appear in the app or be sent by email where necessary.

Changing a permission prevents future device access; it does not itself delete synchronized server data.

11.2 Marketing and push preferences

Marketing consent is optional and can be withdrawn through available settings or by contacting us. Service, security, legal, and account messages are not marketing and may still be sent when necessary.

11.3 Analytics and device identifiers

The current Android build does not expose a separate in-app analytics switch. You may use available Android privacy controls to reset or limit the advertising identifier. Removing and reinstalling the app or clearing app data can cause a new analytics app-instance identifier to be created, but it does not delete server records associated with your Jellywalk account. You may contact us to request deletion of identifiable analytics information; we will use available provider tools and honor the request where the information can reasonably be linked and applicable law requires deletion.

11.4 Profile correction

You can update your username and profile image in the app. An email or linked-login change may require support and authentication-provider verification.

11.5 Workout and account deletion

- To delete your **account**, open Jellywalk **Settings** and select **Delete Account**. This action is intended to disable the Jellywalk and Auth0 account and remove the account from active Service use. It is irreversible and causes loss of access to workout history, virtual balances, items, shoes, rewards, and profile information, subject to the limited retention exceptions above.
- To request deletion of a **specific workout, route, or all workout records without deleting the account**, email info@topundred.com. If self-service workout deletion is available in your app version, you may use that option instead.
- Uninstalling Jellywalk does not delete the server account or synchronized records.

11.6 Privacy rights

Subject to applicable law, you or an authorized representative may ask us to:

- confirm whether we process your information and provide access or a copy;

- correct inaccurate or incomplete information;
- delete information;
- suspend or restrict processing or transmission;
- withdraw consent;
- provide portable information where the right applies;
- object to certain processing; or
- explain and obtain review of a qualifying automated decision.

Send a request to info@topundred.com. Describe the right and account involved. We may verify identity, authority, and account ownership before acting. We will respond within the period required by applicable law. A request may be limited where law allows, for example to protect another person's rights, preserve security/fraud evidence, comply with law, or establish legal claims. We will explain a denial when required.

12. Security

We use administrative, technical, and physical safeguards appropriate to the nature of the information. Measures include role-based access, authentication, encrypted production transport, secure device storage for session tokens, credential/header redaction in logs, signed access to stored media, network and database controls, monitoring, incident procedures, vendor controls, and staff confidentiality obligations.

No storage or transmission method is completely secure. You are responsible for protecting your device, email account, password, and social-login account and for notifying us promptly if you suspect unauthorized access.

13. Children

Jellywalk is not directed to children under 14, and they may not create or use an account. We do not knowingly collect personal, health, or location information from a child under 14 without legally valid guardian consent. If you believe a child under 14 has used Jellywalk, contact us so that we can investigate and delete the information as required.

If local law sets a higher age for independent consent, a user below that age must have permission from a parent or legal guardian. Jellywalk does not offer guardian tracking or a child-location safety service.

14. International users

Depending on where you live, local law may provide additional rights or restrictions. We apply this Policy together with mandatory local rules. Nothing in this Policy limits a right that cannot lawfully be waived.

For users in the European Economic Area, United Kingdom, or Switzerland, Topundred is the controller; the legal grounds in Section 5 apply; you may complain to your local data-protection authority; and international transfers will use a recognized transfer mechanism where required.

For residents of U.S. states with comprehensive privacy laws, the categories processed are described in Section 2, the purposes in Section 4, and recipients in Section 8. We do not sell personal information or share it for cross-context behavioral advertising. We do not discriminate against a user for exercising a privacy right. State-specific rights apply only where the relevant law covers Topundred and the processing.

15. Changes to this Policy

We may update this Policy as Jellywalk, its providers, or law changes. We will post the updated version and change the “Last updated” date. Where required, we will provide advance notice in the app, by email, or through another prominent method. We aim to provide at least 7 days’ notice of material changes and at least 30 days’ notice of changes materially adverse to users, unless an urgent security, legal, or technical reason requires faster action. We will request renewed consent where law requires it.

16. Privacy and location-information contact

Controller and operator: Topundred Inc.

Business registration number: 230-86-03029

Responsible department: Privacy and Location Information Team

Email: info@topundred.com

Address: 501-A110, 5F, 61, Daehak-ro 12-gil, Jongno-gu, Seoul, 03086, Republic of Korea

Please use the subject line **“Jellywalk Privacy Request”** and do not send a password, authentication token, or unnecessary health/location details by email.

Korean users may also seek assistance from the following public bodies:

- Personal Information Infringement Report Center (Korea Internet & Security Agency): **118**, privacy.kisa.or.kr
- Personal Information Dispute Mediation Committee: **1833-6972**, www.kopico.go.kr

[Skip to main content](#)

- Personal Information Protection Commission / Privacy Portal: www.privacy.go.kr

These bodies are independent of Topundred. Contacting us first is welcome but is not a condition of using an available regulatory remedy.

Questions about this document? Email info@topundred.com.