HYPERITY INC. · ALLRUNNER

Security Overview

Version 1.0 · November 22, 2026
support@hyperitycorp.com
hyperitycorp.com/en/trust

AllRunner is a walking and running challenge platform (mobile app and admin console) operated by Hyperity Inc., a Samsung Electronics C-Lab spin-off founded in 2017 in Seongnam, Republic of Korea. This document summarizes how participant data is stored and protected. Every statement has been checked against our production configuration and source code as of the date above.

Seoul, Korea	**Google Cloud**	**7-day PITR**	**No certifications yet**
Database, files and servers (asia-northeast3)	Firebase / Google Cloud platform	Point-in-time recovery + daily backup	SOC 2 / ISO 27001 / ISMS-P not held

1. Architecture and data location

- The app and admin console are built on Firebase and Google Cloud. There are no self-managed servers.
- Production database: Cloud Firestore (Native mode), location `asia-northeast3` (Seoul).
- Files (e.g. photos): Cloud Storage bucket in `asia-northeast3`.
- Server logic: all 134 production Cloud Functions run in `asia-northeast3`.
- AI features (photo verification, post and nickname checks, AI answers in customer support) send the relevant content to Google's Gemini models, which may process it outside Korea. Content is deleted after processing and is not used for model training, as stated in our privacy policy.

2. Encryption

- **In transit:** all traffic between the app, admin console and Google Cloud APIs uses HTTPS (TLS). Our web domains return HSTS headers and redirect HTTP to HTTPS.
- **At rest:** Google Cloud default encryption at rest (AES-256). We do not use customer-managed keys or field-level encryption.
- **Pseudonymization:** phone numbers used for friend search are compared as HMAC-SHA256 values with a secret salt; SMS verification codes are stored as hashes.
- **Secrets:** API keys and passwords are stored in Google Secret Manager and excluded from source control.

3. Identity and access control

- All data access requires Firebase Authentication. Participants sign in with phone, email, Google or Apple.
- Firestore and Storage security rules restrict sensitive data (health, location, legal names, points, friend chats, survey responses, support inquiries; about 80 collections) to the data subject and authorized administrators.
- Server-only data cannot be read or written by clients.
- Role-based access: platform roles (super admin, support, admin) and organization roles (owner, admin, manager, editor, viewer). Only a super admin can change platform roles.
- Firebase App Check is required on callable server functions and on Firebase Authentication.
- Cloud console access is limited to the CEO and designated developers.

4. Logging and audit

- Customer support actions (customer lookups, support sessions) are recorded with actor, action and time.
- Point balance corrections are written to an audit log in the same transaction as the change.
- Server logs are kept in Google Cloud Logging under its default retention.

5. Backup and recovery

- Firestore point-in-time recovery (PITR) is enabled with a 7-day window.
- A scheduled Firestore backup runs daily.
- Firestore and Cloud Storage use regional configurations that replicate data across multiple zones in the Seoul region.

6. Data retention and deletion

- Participants can delete their account in the app. A server process then deletes running records, GPS route files, location usage logs, friends and chats, join requests, legal name records, health data and the authentication account.
- Participation and winner records of completed challenges and community posts may remain as operating records; they are deleted on request.
- Location usage logs are deleted automatically after 12 months.
- Customers (companies and institutions) may request deletion of their participants' data at the end of the contract by email.

7. Sub-processors

Company	Purpose	Data
Google LLC — Firebase / Google Cloud	Authentication, database and file storage (Seoul), server functions (Seoul), push notifications, crash reporting, hosting	Service data
Google LLC — Vertex AI / Gemini	Photo verification, post and nickname checks, AI support answers	Photos, posts, nicknames, inquiry text
Google LLC — Gmail	Service emails	Email address, message content
Cloudflare, Inc.	Network route for access from public-sector networks; image delivery	Connection traffic, published images
Solapi	SMS and KakaoTalk notifications (verification codes, prize notices)	Phone number, message content
Kakao Corp. — Kakao Local API	Coordinate-to-address conversion	Coordinates only, no identifiers
SK Telecom — TMAP	Walking route guidance	Coordinates only, no identifiers

On-device integrations (Apple HealthKit, Google Health Connect) read only the data types the user permits and are not sub-processors.

8. Privacy principles

- Data minimization: location is collected only while a run is being recorded; health data is limited to the types the user permits (steps, distance, workout time; heart rate and routes are optional).
- No sharing with third parties without consent, except where required by law or to deliver prizes.
- Organizers see their own participants' records in the admin console to run challenges and deliver rewards. Sponsor reports contain totals only.
- We act under Korea's Personal Information Protection Act.

9. Incident response

- Report suspected security issues or breaches to support@hyperitycorp.com. Investigation starts on receipt.
- Confirmed personal data breaches are notified to affected individuals and, where required, reported to the Personal Information Protection Commission or KISA under the Personal Information Protection Act. Contracted customers are informed directly.

10. Certifications and documents

- Hyperity does not currently hold SOC 2, ISO/IEC 27001 or ISMS-P certification, and has not commissioned an external penetration test.
- Available on request: security questionnaire responses (SIG Lite / CAIQ-based) and a data processing agreement (DPA) template.

Hyperity Inc. · 804-C49, 8F, 124 Unjung-ro, Bundang-gu, Seongnam-si, Gyeonggi-do 13461, Republic of Korea

Privacy contact: support@hyperitycorp.com